

In only a couple of decades, computer networks have evolved from being a complex technology accessible to only the most tech-savvy of users to being part of most people's everyday lives. Computer networks can be found in almost every business, school, and home. The use of networks is available to anyone with a computer and a network connection, but installation and upkeep of all but the smallest of networks still require a considerable degree of know-how. This chapter starts you on the path toward acquiring the skills to manage a large corporate network or simply configure a home network with a wireless router.

This chapter begins by discussing the computer and its role in a network to give you a foundation for the topics in this book. Next, you examine the components of a network and the fundamentals of communication between computers. Many new terms are introduced and defined, and the varied types of networks and network servers you might encounter are described. Finally, some specialized network types are introduced.

---

## An Overview of Computer Concepts

At the heart of a computer network is the computer. Networks were created to facilitate communication between computing devices, which ultimately facilitates communication between people. So to better understand computer networks, how they work, and how to support them, you must have a solid understanding of computer operations. In fact, most of the devices you encounter when working with a network involve a computer. The most obvious are network servers and workstations that run operating systems, such as Windows, Linux, UNIX, and Mac OS X. Not as obvious are devices such as routers and switches, which move network data from computer to computer and network to network. These complex devices are also computers, although they're specialized computers for performing specific tasks. The next sections discuss the basic functions of a computer and its associated components, along with computer hardware, the boot procedure, and the basic functions of an operating system.

### Basic Functions of a Computer

A computer's functions and features can be broken down into the three basic tasks all computers perform: input, processing, and output. Information is input to a computer from a device such as a keyboard or from a storage device such as a hard drive; the central processing unit (CPU) processes the information, and then output is usually created. The following example illustrates the process:

- *Input*—A user running a word-processing program types the letter A on the keyboard, which results in sending a code representing the letter A to the computer.
- *Processing*—The computer's CPU determines what letter was typed by looking up the keyboard code in a table.
- *Output*—The CPU sends instructions to the graphics cards to display the letter A, which is then sent to the computer monitor.

Some components of today's computers are designed to perform only one of these three functions; others are designed to perform two or all three functions. For example, a standard keyboard and mouse perform input functions, and storage devices, such as hard drives, perform



both input (when files are read from the drive) and output (when files are written to the drive). Network cards can perform all three functions. A network card is an output device when data is sent from the computer to the network and an input device when data comes from the network to the computer. In addition, many network cards have rudimentary processors that perform actions on incoming and outgoing data to help supplement the computer's main CPU.

**Input Components** Before a computer can do any processing, it requires input, commonly from user-controlled devices, such as keyboards and mice, but includes devices such as microphones, Web cameras, and scanners. External interfaces, such as serial, FireWire, and USB ports, can also be used to get input from peripheral devices.

Input is also generated by storage devices, such as hard disks and CDs/DVDs that store computer programs and data files containing computer instructions and data. For example, a spreadsheet program, such as Microsoft Excel, might contain instructions for the CPU to calculate formulas for adding the values of two columns of data and a spreadsheet file called MyBudget.xls containing the numbers and formulas the spreadsheet program should use. Both the program (Microsoft Excel) and the data file (MyBudget.xls) are used as input to the CPU, which then processes the program instructions and data.

Of course, a spreadsheet program is normally started only when a user double-clicks the spreadsheet program icon or the icon representing the spreadsheet data file. These actions are instigated by user input. Sometimes, however, your computer seems to start performing actions without user input. For example, you might have noticed that your hard drive sometimes shows activity without any obvious action from you to initiate it. However, inputs to a computer can include timers that cause programs to run periodically and data arriving from network cards, for example, that cause a program or process to run. So although it sometimes seems as though your computer has a mind of its own, computers don't actually do anything without first getting input to jolt them into action.

**Processing Components** A computer's main processing component is the CPU, which executes instructions from computer programs, such as word-processing programs and Web browsers. It also runs the instructions composing the operating system (OS), which provides a user interface and the environment in which applications run. Aside from the CPU, modern computers usually include ancillary processors associated with input/output (I/O) devices, such as graphics cards. These processors are often referred to as onboard processors. The processor on a graphics card, called a graphics processing unit (GPU), takes a high-level graphics instruction, such as "draw a circle," and performs the calculations needed to draw the circle on the display device. With an onboard GPU, the main CPU doesn't have to handle many of the complex calculations current graphical applications require, thereby improving overall system performance. Other devices, such as network interface cards and disk controller cards, might also include onboard processors.

CPUs now are often composed of two or more processors, called **cores**, in one package. A **multicore CPU** is like a person with two brains. With only one brain, you could add four numbers together, but you would probably do it in three sequential summing operations: Add the first number to the second number, take the first sum and add it to the third number, and add that sum to the fourth number to arrive at the final sum. If you had two brains, you'd still need three summing operations, but two could be done simultaneously:

The first brain adds the first two numbers while the second brain is adding the third and fourth numbers; then the second brain gives its results to the first brain, and the first brain sums the results of the first two summing operations. So multicore CPUs enable computers to carry out multiple instructions simultaneously, which results in better overall performance when running demanding applications.

**Output Components** Output components include monitors and printers, but they also include storage devices, network cards, and speakers, to name a few. The external interfaces mentioned previously as input components can be used as output components, too. For example, a disk drive connected to a USB port allows reading files from the disk (input) and writing files to the disk (output).

## Storage Components

Storage components are a major part of a computer's configuration. Generally speaking, the more storage a computer has, the better the performance is. As you saw in the previous section, most storage components are both input and output devices, allowing data to be saved (output) and then accessed again later (input). When most people think of storage, they think of disk drives, CD/DVD drives, and USB flash drives. However, there are two main categories of storage: short-term storage and long-term storage.

**RAM: Short-Term Storage** Short-term storage is the random access memory (RAM) on a computer. RAM is short-term storage because when power to the computer is turned off, RAM's contents are gone, just as though you erased a whiteboard. When power is restored, RAM has no data stored until the CPU begins to write data to it.

The amount of RAM, or memory, in a computer is crucial to the computer's capability to operate efficiently. RAM is also referred to as "working storage." Everything the CPU is currently processing must be available in RAM, including program instructions and the data the current application requires. So to run a spreadsheet program, there must be enough RAM to load both the spreadsheet program and the data in the spreadsheet. If there's not enough available memory, the spreadsheet program won't run, or the computer will use the disk drive to supplement RAM temporarily.

Neither option is desirable. The reason temporary use of the disk drive isn't optimal is because RAM is thousands of times faster than the fastest disk drives. The time required to access data in RAM is measured in nanoseconds (billions of a second), but access to data on a disk drive is measured in milliseconds (thousandths of a second). So if the disk drive must be used to supplement RAM while running an application, that application, and indeed the entire computer, slows down precipitously.

On current computers, the amount of RAM installed is usually 1 GB or more. More is generally better, but the amount of RAM that a system can use effectively depends on the OS installed. The 32-bit version of an OS can usually access a maximum of 4 GB of RAM, whereas the 64-bit version can access many thousands of gigabytes. The amount of RAM you actually need depends on how you use your computer. If you usually have only one or two typical business applications open at once, 1 GB or even less is probably enough.

However, if you run complex graphics applications or games or have several applications open simultaneously, you'll likely benefit from having more RAM.



**Long-Term Storage** Long-term storage maintains its data even when there's no power. Examples include hard disks, CDs/DVDs, and USB flash drives as well as other types of removable media. Long-term storage is used to store document and multimedia files as well as the files that make up applications and the OS. The amount of storage a computer needs depends on the type and quantity of files to be stored. In general, office documents, such as word-processing files, spreadsheets, and presentations, require comparatively little space. Multimedia files—pictures, music files, and videos—require much more space. Long-term storage is plentiful and extremely inexpensive. Hard drive specifications are in units of tens or hundreds of gigabytes, with terabyte (1000 GB) drives quite commonplace now. More details about hard disks are discussed later in “Personal Computer Hardware.”

**Data Is Stored in Bits** Whether storage is long term or short term, data on a computer is stored and processed as binary digits (“bits,” for short). A bit holds a 1 or 0 value, which make representing bits with electrical pulses easy. For example, a pulse of 5 volts of electricity can represent a 1 bit, and a pulse of 0 volts (or absence of a pulse) can represent a 0 bit. Bits can also be stored as pulses of light, as with fiber-optic cable: A 1 bit is represented by the presence of light and a 0 bit as the absence of light.

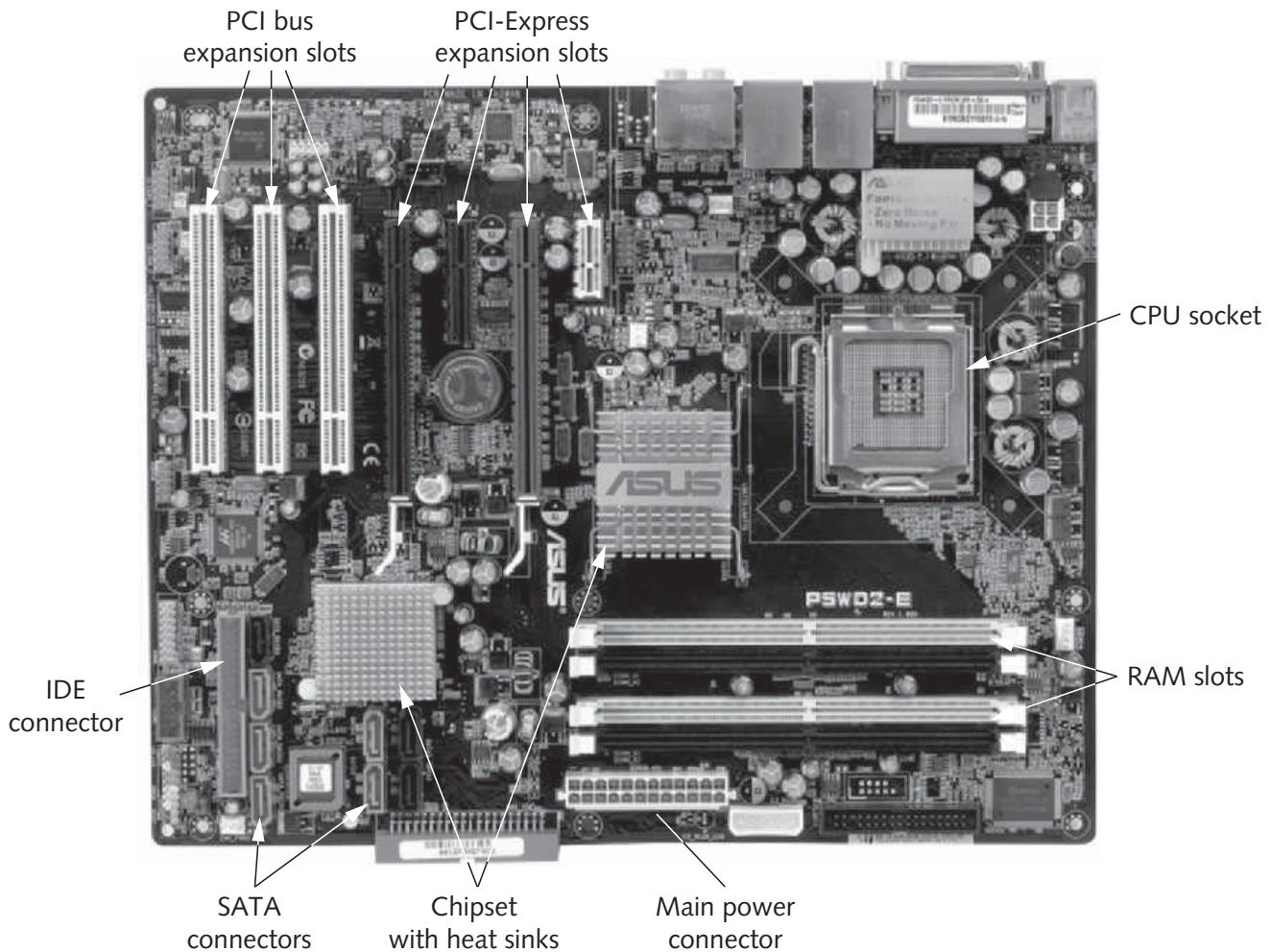
Data in a computer, such as the letters in a word-processing document or the music you hear when you play an MP3 music file, is represented by collections of 8 bits, called a byte. You can look at each byte as a printable character in a document. A single byte from an MP3 file plays about 1/17 thousandth of a second of music. To put it another way, one second of MP3 music takes more than 17,000 bytes.

## Personal Computer Hardware

Most people are familiar with personal computer (PC) hardware. Other types of computers, such as minicomputers and mainframes, are usually locked away in a heavily air-conditioned room and privy only to the eyes of IT staff. Besides, the basic hardware used to build a PC or a mainframe differs only in the details. This section describes four major PC components housed in a computer case:

- Motherboard
- Hard drive
- RAM
- BIOS/CMOS

**The Motherboard and Its Components** The motherboard is the nerve center of a computer, much like the spinal cord is the nerve center of the human body. It's a network of wires and controlling circuits that connects all computer components, including the CPU, RAM, disk drives, and I/O devices, such as network interface cards. Some key components of a motherboard are labeled in Figure 1-1 and explained in Table 1-1.



**Figure 1-1** A PC motherboard

Courtesy of Course Technology/Cengage Learning

**Table 1-1** Key components of a motherboard

Component	Description
CPU socket	The CPU is installed in this socket.
PCI bus expansion slots	Used to add functionality to a PC by adding expansion cards that have a Peripheral Component Interconnect (PCI) connector.
PCI-Express expansion slots	PCI-Express supersedes PCI and supports faster data transfer speeds. The larger slots are suitable for high-performance expansion cards, such as graphics cards and disk controllers. The smaller slots are best suited to sound cards and network interface cards.
RAM slots	Slots for installing RAM on the motherboard.
Chipset with heat sinks	The chipset consists of two chips referred to as the Northbridge and the Southbridge. These chips control data transfers between memory, expansion slots, I/O devices, and the CPU. The heat sink sits on top of the chipset to prevent it from overheating.
SATA connectors	Used for connecting hard drives and CD/DVD drives that use the Serial AT Attachment (SATA) specification.

(continues)

**Table 1-1 Key components of a motherboard (continued)**

Component	Description
IDE connector	Used for connecting Integrated Drive Electronics (IDE) hard drives and CD/DVD-ROM drives. Most systems now use SATA for hard drives and IDE for CD/DVD drives.
Main power connector	This connector is where the motherboard receives power from the system power supply.

All data that goes into or comes out of a computer goes through the motherboard because all storage and I/O devices are connected to the motherboard, as is the CPU, which processes data going in and coming out of a computer.

**Computer Bus Fundamentals** Table 1-1 mentions PCI bus expansion slots as a component of a motherboard. So what is a bus? A **bus** is a collection of wires carrying data from one place to another on the computer. There are many bus designs and formats, each designed for a particular purpose. Although bus types come and go, it's safe to say that replacements for an older bus design will almost certainly be faster than their predecessor.

In a computer, there are buses between the CPU and RAM, between the CPU and disk drives, and between the CPU and expansion slots, among others. For the purposes of this book, you're most interested in the bus connecting expansion slots to the motherboard because you usually connect a network interface card (NIC) into one of these slots. NIC installation and expansion slot bus types are discussed in Chapters 2 and 7. What you need to know now is that not all motherboards come with all types of expansion slots, and the faster and busier your computer is, the faster its bus type needs to be.

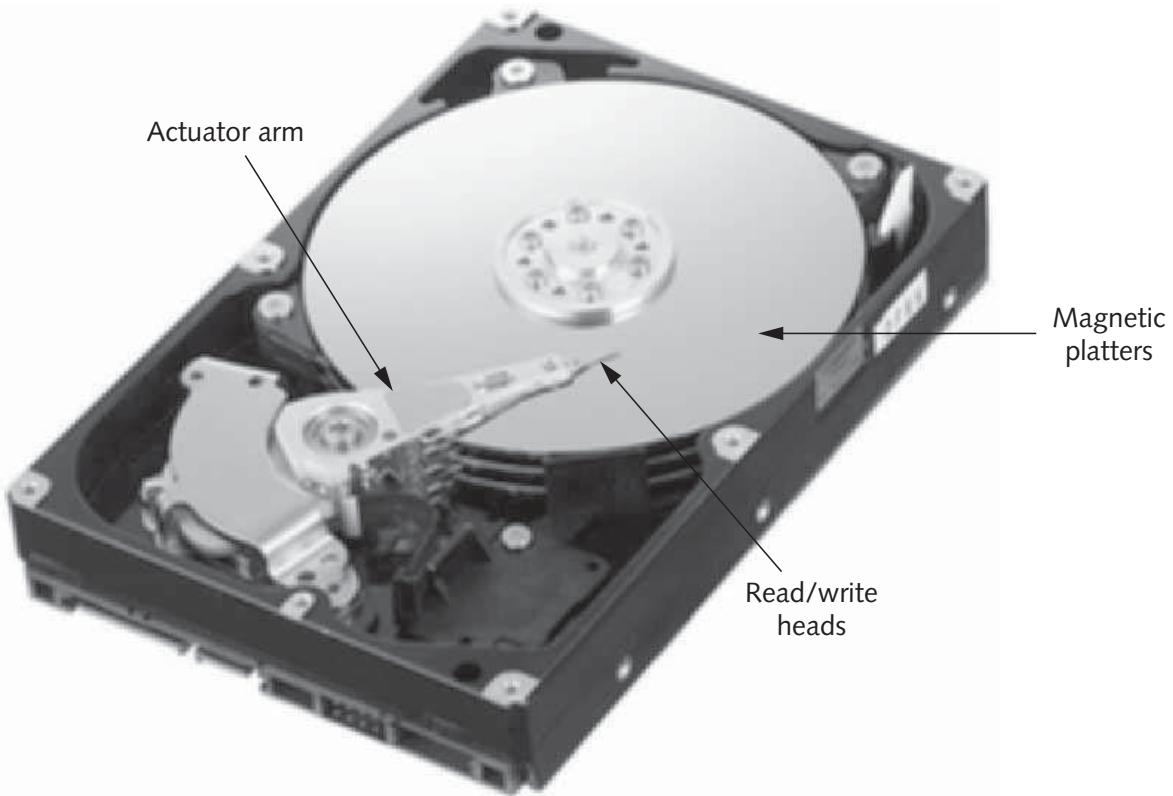
**Hard Drive Fundamentals** The hard drive is the primary long-term storage component on your computer. Hard drives consist of magnetic disks, called platters, that store data in the form of magnetic pulses. These magnetic pulses are maintained even when power is turned off. Each pulse represents a single bit of data.

The platters spin at extremely fast speeds, with some of the fastest disks having rotational speeds of 15,000 revolutions per minute (rpm). A read/write head is attached to an actuator arm that moves across the spinning platters in response to commands from the computer to read or write a file (see Figure 1-2). Generally, the faster the rotational speed, the better the hard drive performance is. When a file is requested to be written or read, its location is determined, and then the read/write heads are moved over the corresponding spot on the platter. After the platter spins to the file's starting location, the read/write heads are activated to read or write the data. The average amount of time platters take to spin into position is called the rotational delay or latency. The amount of time required to move read/write heads to the correct place is referred to as the seek time, and the time it takes to read or write data is called the transfer time. The average amount of time between the request to read or write data and the time the action is completed is referred to as the access time.



The terms used to measure hard drive performance aren't universal among manufacturers, but the terms used in the preceding paragraph represent most specifications.

**NOTE**



**Figure 1-2** Inside a hard drive

Courtesy of © 2010 Western Digital Technologies, Inc.

Hard disks store the documents you use with your computer as well as the applications that open these documents. In addition, the hard disk stores the OS your computer loads when it boots. As mentioned, the hard disk acts as an input device when files are read. When the computer boots, the OS files are read from the disk, and instructions in these files are processed by the CPU. However, the files don't go directly from the hard disk to the CPU; first, they're transferred to short-term storage (RAM).

**RAM Fundamentals** RAM, the main short-term storage component on your computer, consists of capacitors to store data and transistors to control access to data. Capacitors require power to maintain the bits they store. Because RAM requires continuous power to store data, it's referred to as "volatile memory."

RAM has no moving parts, so as mentioned, accessing data in RAM is much faster than accessing data on a hard drive—there's no seek time or rotational delay. Because RAM is so much faster than a hard drive, any information the CPU processes should be in RAM. If data the CPU requires is located on the hard drive, it's loaded into RAM first, which takes considerable time. Therefore, the more RAM your system has, the more likely it is that all the data running programs need can be stored in RAM, making the system perform much faster.

**BIOS/CMOS Fundamentals** A key component of every computer is its basic input/output system (BIOS), which is a set of instructions located in a chip on the motherboard. A main function of the BIOS is to tell the CPU to perform certain tasks when power is first applied to the computer, including initializing motherboard hardware, performing a power-on self test (POST), and beginning the boot procedure.



Because of the complexity of motherboards, configuring some of their hardware components and tuning performance parameters are often necessary. When a computer begins to boot, the BIOS program offers the user an opportunity to run the Setup utility to perform this configuration. The configuration data the user enters is stored in complementary metal oxide semiconductor (CMOS) memory. It holds information such as on which devices the CPU should look for an OS to boot, the status of hardware devices, and even a system password, if needed. CMOS is a type of low-power memory that requires only a small battery to maintain its data. It's also referred to as nonvolatile memory because it doesn't require power from the computer's main power supply.

## Computer Boot Procedure

The following six steps are necessary to take a computer from a powered-off state to running a current OS, such as Windows or Linux:

1. Power is applied to the motherboard.
2. The CPU starts.
3. The CPU carries out the BIOS startup routines, including the POST.
4. Boot devices, as specified in the BIOS configuration, are searched for an OS.
5. The OS is loaded into RAM.
6. OS services are started.

These steps apply to almost every type of computer, including very small computing devices, such as cell phones and iPods. Probably the biggest difference between computers is what occurs in the last step. OS services are programs that are part of the OS rather than applications a user starts. The particular services an OS starts can vary greatly, depending on which OS is loaded and how it's configured. The number and type of services started on a system are what, at least in part, account for the time it takes a system to boot completely. Examples of common OS services include the user interface, the file system, and, of course, networking services.



The projects in this book involving a Windows client OS use Windows 7 Enterprise Edition. Other editions of Windows 7 can be used, except Windows 7 Home Edition. Windows Vista can also be used, with some small changes to step-by-step instructions. Windows XP can be used in most cases but might require additional changes.



## Hands-On Project 1-1: Examining a Computer's Boot Procedure

**Time Required:** 10 minutes

**Objective:** Examine the computer boot procedure and BIOS setup utility.

**Required Tools/Equipment:** Your classroom computer and access to the BIOS Setup utility

**Description:** In this project, you examine the computer boot procedure from beginning to end, using a Windows computer. You also examine the BIOS Setup utility and view the configuration that specifies which devices the BIOS should search for an OS. Because the BIOS is different for different computers, your instructor might have to assist with the specific keystrokes you enter to run the BIOS Setup utility and view the boot order menu. This project uses a

virtual machine and the BIOS Setup utility in VMware Workstation 6.x. If you aren't using virtual machines for the projects in this book, the BIOS on most computers is similar.



Your computer must be turned off before you begin this project. Read the first step carefully before turning on the computer, as you need to act quickly to enter the BIOS Setup utility.

1. Turn on your computer. Watch the screen carefully for a message telling you what key to press to activate the BIOS Setup utility. On many systems, this key is F1, F2, or Delete. If you don't press the key in time, the OS boots normally. If this happens, shut down the computer and try again.
2. When you have entered the BIOS Setup utility, your screen should look similar to Figure 1-3. Before continuing, write down the steps of the boot procedure that have taken place to this point:

---

---

---

**PhoenixBIOS Setup Utility**

Main   Advanced   Security   Boot   Exit

<b>System Time:</b>	[11:08:57]	<b>Item Specific Help</b>
<b>System Date:</b>	[04/17/2010]	
<b>Legacy Diskette A:</b>	[1.44/1.25 MB 3½"]	<Tab>, <Shift-Tab>, or <Enter> selects field.
<b>Legacy Diskette B:</b>	[Disabled]	
▶ Primary Master	[None]	
▶ Primary Slave	[None]	
▶ Secondary Master	[VMware Virtual IDE]	
▶ Secondary Slave	[None]	
▶ Keyboard Features		
<b>System Memory:</b>	640 KB	
<b>Extended Memory:</b>	1047552 KB	
<b>Boot-time Diagnostic Screen:</b>	[Disabled]	

**F1 Help   F11 Select Item   -/+ Change Values   F9 Setup Defaults**

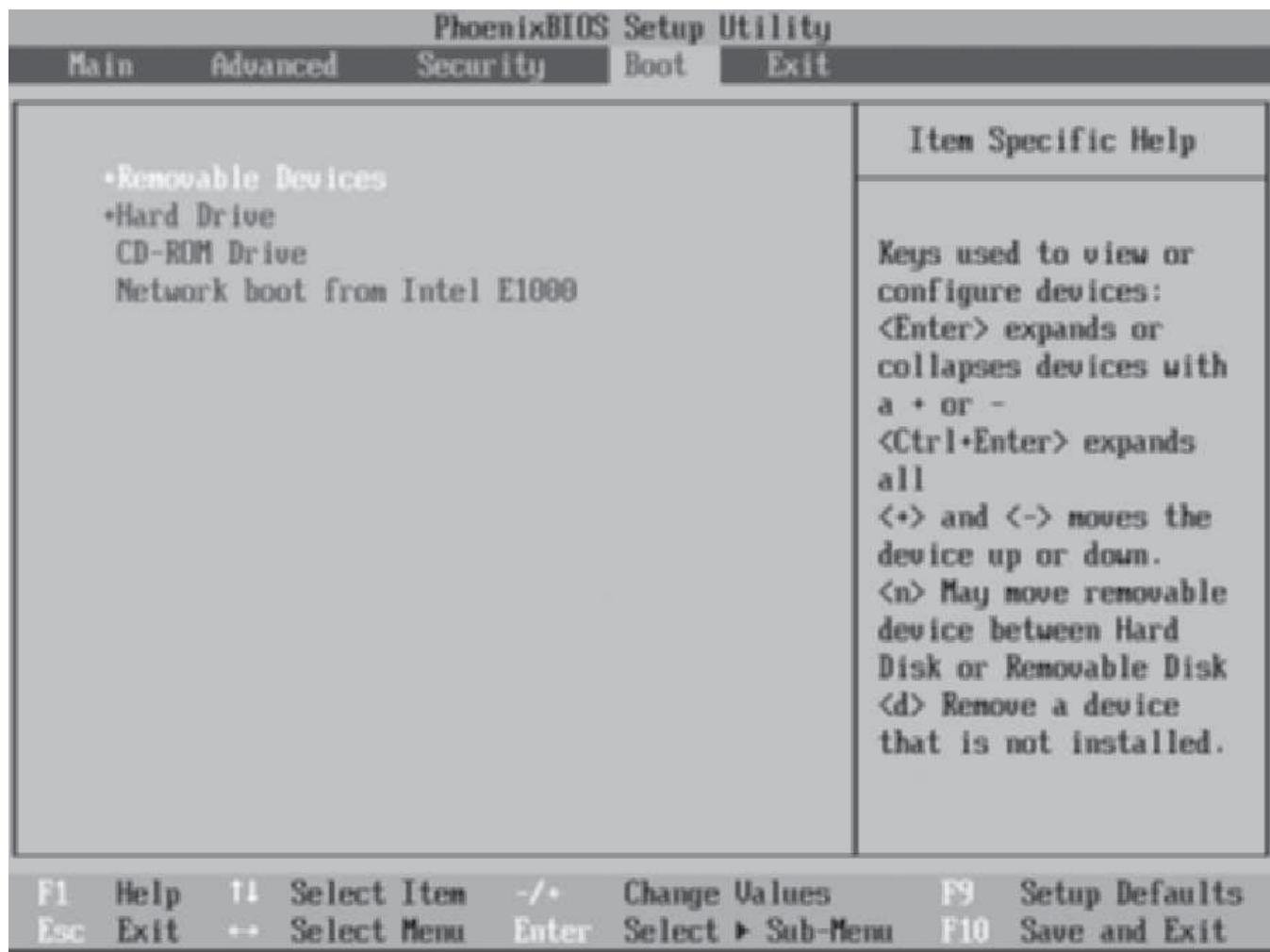
**Esc Exit   -- Select Menu   Enter Select ▶ Sub-Menu   F10 Save and Exit**

**Figure 1-3** The BIOS Setup utility

Courtesy of Course Technology/Cengage Learning



3. Navigate the BIOS Setup utility until you find the boot order menu (see Figure 1-4). From this menu, you can change the order in which the BIOS looks for boot devices, or you can exclude a device from the boot order. The BIOS boots from the first device in which it finds an OS. You might need to change the boot order if, for example, you have an OS installed on the hard drive but want to boot from an installation CD/DVD to install a new OS. In this case, you move the CD/DVD device to the first entry in the boot order.



**Figure 1-4** The BIOS boot order menu

Courtesy of Course Technology/Cengage Learning

4. For now, you can leave the boot order as it is. To quit the Setup utility, press the correct key (usually specified at the bottom of the screen). In Figure 1-4, you press Esc to exit without saving changes or F10 to save the changes before exiting. In either case, when you exit, the computer restarts. Press the key for exiting without saving changes.
5. Write the final steps of the boot procedure that occurred as Windows started:

---

---

---

6. Shut down the computer for the next project.

## How the Operating System and Hardware Work Together

A computer's OS provides a number of critical services, including a user interface, memory management, a file system, multitasking, and the interface to hardware devices. Without an OS, each application would have to provide these services, and if a user wanted to run multiple applications at once (multitasking), the applications would have to run cooperatively. In short, without an OS, computing would still be in the proverbial Stone Age. The following sections describe these services briefly, and Chapter 8 discusses OS components in more detail.

**User Interface** The user interface enables people to interact with computers. With graphical user interfaces (GUIs), users can point and click their way around the computer to run applications, access network services, manage hard drives and files, and configure the working environment to their liking. In short, users provide input, and the OS, along with the CPU, processes that input, whether it's mouse clicks or keystrokes, and generates output. Without a user interface, computers could process only information that has been programmed into memory or storage. If something went wrong, there would be no way to indicate the problem to a person, making a computer without a user interface of little value except when it has a narrowly defined task, such as running a piece of machinery.

**Memory Management** Computers are now equipped with memory measured in hundreds of megabytes or gigabytes, whereas in the early 1990s, the typical amount of memory was about 1 megabyte. Each application requires a certain amount of memory in which to run. When the OS loads an application, memory must be allocated for the application to run in, and when the application exits, the memory it was using must be marked as available. The OS handles these memory management tasks. Without a central memory manager, an application could use any memory in the system, and it might be memory already being used by a running application or the OS itself. If this happens, the system can crash or perform erratically. Today's OSs usually detect an application's attempt to access another process's memory and force the offending application to terminate.

**File System** The file system is used to organize space on storage devices, such as disk drives and flash drives, for the purpose of storing and locating files. Contemporary file systems typically have the following objectives:

- Provide a convenient interface for users and applications to open and save files.
- Provide an efficient method to organize space on a drive.
- Provide a hierarchical filing method to store files.
- Provide an indexing system for fast retrieval of files.
- Provide secure access to files by authorized users.

When a user double-clicks a file to open it, the user interface calls the file system with a request to open the file. The file type determines exactly how the file is opened. If the file is an application, the application is loaded into memory and run by the CPU. If the file is a document, the application associated with the document type is loaded into memory and opened by the application. For example, if you double-click the Budget.xls file, the Excel

application is loaded into memory and then opens the Budget.xls document file. If a user creates a new file or changes an existing file and wants to save it, the application calls the file system to store the new or changed file on the disk. Most users of an OS interact with the file system by using Windows Explorer or a similar file manager program on another OS, but as a future computer or network professional, you need to have a deeper understanding of how a file system works so that you can make informed choices when you need to install a file system or troubleshoot file system-related problems. You can find more discussion on this topic in Chapter 8.



**Multitasking** Quite simply, **multitasking** is an operating system's capability to run more than one application or process at a time. Multitasking is what allows you to listen to a music file while browsing the Web, for example. Computer hardware can't do that by itself. The OS is designed to look for applications that have some kind of work to do (such as load a new Web page or continue playing the current music file) and then schedule CPU time so that the work gets done. For example, if you're browsing the Web and reading the current page loaded in your Web browser, the computer isn't really doing any work.

However, if you click a link on the Web page, you're telling the Web browser you want to load a new page. The OS responds by telling the CPU to start executing the part of the Web browser application responsible for loading a new Web page. You might wonder how can you play a music file at the same time the CPU is loading a new Web page. There are two possible answers: The computer contains more than one CPU or a multicore CPU and can literally do two things at once (in this case, load a Web page and play a music file), or the OS instructs the CPU to switch between the two tasks rapidly, giving the illusion that they're happening simultaneously. Because CPUs can execute hundreds of millions of instructions per second, this illusion isn't difficult to carry off.

**Interface to Hardware Devices** When an application needs to communicate with computer hardware, as when writing information to the display device or sending data to the network, it calls on the OS, which then calls on a device driver. A **device driver** is software that provides the interface between the OS and computer hardware. The reason the application can't simply read or write data directly to hardware is that other applications might also need to communicate with the same device at the same time. If this were allowed to happen, it would be akin to two or more people on different extensions of the same land line trying to dial a different number. Nobody's phone call would go through, or one person might call an unintended destination. The OS queues up each request and sends it to the device driver when it's not busy. This procedure ensures that every application's request is taken care of in a nice orderly fashion.

Every device performing an input or output function requires a device driver. When an input device has data ready for processing, or when an output device is ready to accept data, the device must signal the OS. Most devices use a signal called an interrupt to let the OS know it has data ready to be read or is ready for more data to be written. Computers spend a considerable amount of time servicing interrupts on a busy computer. For example, when the mouse is moved or a key on the keyboard is pressed, an interrupt is generated so that the OS knows the mouse pointer must be redrawn onscreen or a character must be written to

the screen. On a networked computer, an interrupt is generated by the NIC when a packet arrives.

Every time an interrupt occurs, the OS must stop what it's doing to service the interrupt. It takes many instructions for an OS to stop what it's doing, service the interrupt, and then resume what it was doing before the interrupt occurred. Because computers can execute millions of instructions per second, users don't usually notice the interruption. If enough interrupts occur simultaneously and for a prolonged period, however, a system can become noticeably sluggish or even seem to freeze. Malfunctioning hardware and network errors that generate excessive packets are two of the many possible causes of this problem. Remember this idea about excessive interrupts caused by the NIC; it's an important point later when you learn about network protocols in Chapter 5.

Networking is, of course, the focus of this book, but your grasp of the fundamentals of computer components and operations will facilitate your understanding of networking components and operations.

---

## The Fundamentals of Network Communication

A computer **network** consists of two or more computers connected by some kind of transmission medium, such as a cable or air waves. After they're connected, correctly configured computers can communicate with one another. The primary motivation for networking was the need for people to share resources, such as printers and hard drives, and information such as word-processing files and to communicate by using applications such as e-mail. These motivations remain, especially for businesses, but another motivating factor for networking for both businesses and homes is to get "online"—to access the Internet. The Internet, with its wealth of information, disinformation, fun, and games, has had a tremendous impact on how and why networks are used today. Indeed, many of the networking technologies used now that you learn about in this book were developed as a result of the Internet explosion.

You might know how to use a network already; in particular, you probably know how to use programs that access the Internet, such as Web browsers and e-mail programs. To understand *how* networks work, however, you need to learn about the underlying technologies and processes that are put into action when you open a Web browser or an e-mail program. A good place to start is with the components that make a stand-alone computer a networked computer.

### Network Components

Imagine a computer with no networking components—no networking hardware, no networking software. It's hard to imagine in this age of seemingly everything and everybody being connected. However, not too long ago, when you bought a computer, its main purpose was to run applications such as word-processing and spreadsheet programs, not Web browsers and e-mail. In fact, the computer had neither the necessary hardware nor software to run these programs. These computers were called **stand-alone computers**. If you wanted to network such a computer, you had to add the necessary components:

# **Hardware Reference Guide**

## **HP Compaq 8000 Elite Small Form Factor Business PC**

© Copyright 2009 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Microsoft, Windows, and Windows Vista are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

This document contains proprietary information that is protected by copyright. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company.

**Hardware Reference Guide**

HP Compaq 8000 Elite Small Form Factor Business PC

First Edition (November 2009)

Document Part Number: 588912-001

## About This Book

This guide provides basic information for upgrading this computer model.

 **WARNING!** Text set off in this manner indicates that failure to follow directions could result in bodily harm or loss of life.

 **CAUTION:** Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

 **NOTE:** Text set off in this manner provides important supplemental information.

---



---

# Table of contents

## 1 Product Features

Standard Configuration Features .....	1
Front Panel Components .....	2
Media Card Reader Components .....	3
Rear Panel Components .....	4
Keyboard .....	5
Using the Windows Logo Key .....	5
Serial Number Location .....	7

## 2 Hardware Upgrades

Serviceability Features .....	8
Warnings and Cautions .....	8
Unlocking the Smart Cover Lock .....	9
Smart Cover FailSafe Key .....	9
Using the Smart Cover FailSafe Key to Remove the Smart Cover Lock .....	9
Removing the Computer Access Panel .....	11
Replacing the Computer Access Panel .....	12
Removing the Front Bezel .....	13
Replacing Bezel Blanks .....	14
Replacing the Front Bezel .....	15
Using the Small Form Factor Computer in a Tower Orientation .....	16
Installing Additional Memory .....	17
DIMMs .....	17
DDR3-SDRAM DIMMs .....	17
Populating DIMM Sockets .....	18
Installing DIMMs .....	19
Removing or Installing an Expansion Card .....	22
Drive Positions .....	28
Installing and Removing Drives .....	29
System Board Drive Connections .....	30
Removing an External 5.25-inch Drive .....	31
Installing an Optical Drive into the 5.25-inch Drive Bay .....	33
Removing an External 3.5-inch Drive .....	36
Installing a Drive into the 3.5-inch External Drive Bay .....	38

Removing and Replacing the Primary 3.5-inch Internal SATA Hard Drive .....	39
Removing and Replacing a Removable 3.5-inch SATA Hard Drive .....	42
<b>Appendix A Specifications</b>	
<b>Appendix B Battery Replacement</b>	
<b>Appendix C External Security Devices</b>	
Installing a Security Lock .....	52
HP/Kensington MicroSaver Security Cable Lock .....	52
Padlock .....	53
HP Business PC Security Lock .....	53
Front Bezel Security .....	55
<b>Appendix D Electrostatic Discharge</b>	
Preventing Electrostatic Damage .....	57
Grounding Methods .....	57
<b>Appendix E Computer Operating Guidelines, Routine Care and Shipping Preparation</b>	
Computer Operating Guidelines and Routine Care .....	58
Optical Drive Precautions .....	59
Operation .....	59
Cleaning .....	59
Safety .....	59
Shipping Preparation .....	59
<b>Index .....</b>	<b>60</b>

---

# 1 Product Features

## Standard Configuration Features

The HP Compaq Small Form Factor features may vary depending on the model. For a complete listing of the hardware and software installed in the computer, run the diagnostic utility (included on some computer models only).

 **NOTE:** The Small Form Factor computer can also be used in a tower orientation. For more information, see [Using the Small Form Factor Computer in a Tower Orientation on page 16](#) in this guide.

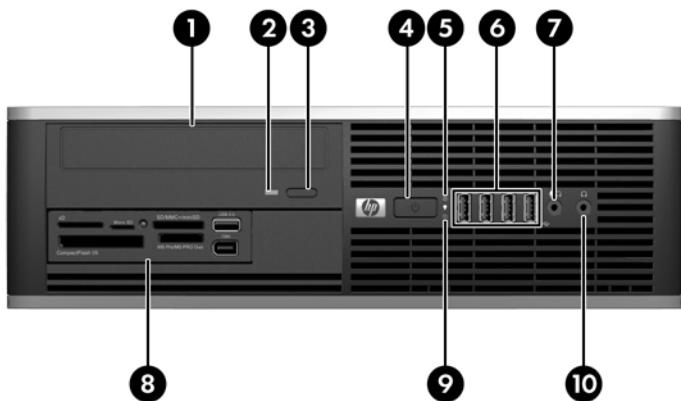
**Figure 1-1** Small Form Factor Configuration



# Front Panel Components

Drive configuration may vary by model. Some models have a bezel blank covering one or more drive bays.

**Figure 1-2** Front Panel Components



**Table 1-1** Front Panel Components

1	5.25-inch Optical Drive	6	USB (Universal Serial Bus) Ports
2	Optical Drive Activity Light	7	Microphone/Headphone Connector
3	Optical Drive Eject Button	8	3.5-inch Media Card Reader (optional)
4	Dual-State Power Button	9	Hard Drive Activity Light
5	Power On Light	10	Headphone Connector

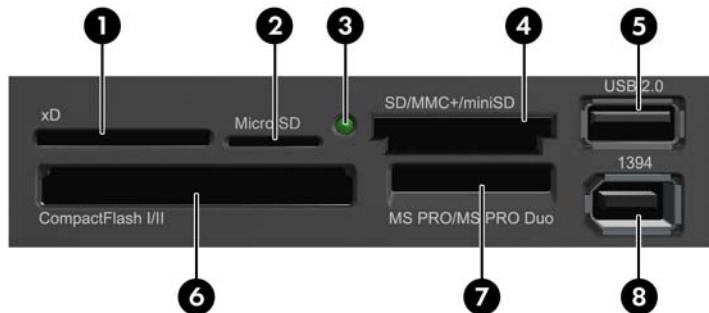
**NOTE:** When a device is plugged into the Microphone/Headphone Connector, a dialog box will pop up asking if you want to use the connector for a microphone line Line-In device or a headphone. You can reconfigure the connector at any time by double-clicking the Realtek HD Audio Manager icon in the Windows taskbar.

**NOTE:** The Power On Light is normally green when the power is on. If it is flashing red, there is a problem with the computer and it is displaying a diagnostic code.

# Media Card Reader Components

The media card reader is an optional device available on some models only. Refer to the following illustration and table to identify the media card reader components.

**Figure 1-3** Media Card Reader Components



**Table 1-2** Media Card Reader Components

No.	Slot	Media			
1	<b>xD</b>	• xD-Picture Card (xD)			
2	<b>MicroSD</b>	• MicroSD (T-Flash)	• MicroSDHC		
3	<b>Media Card Reader Activity Light</b>				
4	<b>SD/MMC+/miniSD</b>	• Secure Digital (SD) • Secure Digital High Capacity (SDHC) • MiniSD	• MiniSDHC • MultiMediaCard (MMC) • Reduced Size MultiMediaCard (RS MMC)	• MultiMediaCard 4.0 (MMC Plus) • Reduced Size MultiMediaCard 4.0 (MMC Mobile) • MMC Micro (adapter required)	
5	<b>USB</b>	• USB (Universal Serial Bus) Port			
6	<b>CompactFlash I/II</b>	• CompactFlash Card Type 1	• CompactFlash Card Type 2	• MicroDrive	
7	<b>MS PRO/MS PRO DUO</b>	• Memory Stick (MS) • MagicGate Memory Stick (MG) • MagicGate Memory Duo	• Memory Stick Select • Memory Stick Duo (MS Duo) • Memory Stick PRO (MS PRO)	• Memory Stick PRO Duo (MS PRO Duo) • Memory Stick PRO-HG Duo • Memory Stick Micro (M2) (adapter required)	
8	<b>1394</b>	• 1394 Port (available on select models only)			

# Rear Panel Components

Figure 1-4 Rear Panel Components

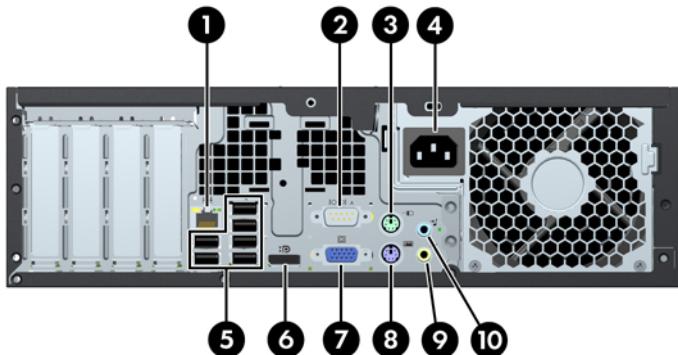


Table 1-3 Rear Panel Components

1	RJ-45 Network Connector	6	DisplayPort Monitor Connector
2	IOIOIA Serial Connector	7	VGA Monitor Connector
3	PS/2 Mouse Connector (green)	8	PS/2 Keyboard Connector (purple)
4	Power Cord Connector	9	Line-Out Connector for powered audio devices (green)
5	Universal Serial Bus (USB)	10	Line-In Audio Connector (blue)

**NOTE:** Arrangement and number of connectors may vary by model.

An optional second serial port and an optional parallel port are available from HP.

When a device is plugged into the blue Line-In Audio Connector, a dialog box will pop up asking if you want to use the connector for a line-in device or a microphone. You can reconfigure the connector at any time by double-clicking the Realtek HD Audio Manager icon in the Windows taskbar.

The monitor connectors on the system board are inactive when a graphics card is installed in the computer.

If a graphics card is installed into the PCI or PCI Express x1 slot, the connectors on the graphics card and the system board may be used at the same time. Some settings may need to be changed in Computer Setup to use both connectors.

# Keyboard

**Figure 1-5** Keyboard Components



**Table 1-4** Keyboard Components

1	Function Keys	Perform special functions depending on the software application being used.
2	Editing Keys	Includes the following: Insert, Home, Page Up, Delete, End, and Page Down.
3	Status Lights	Indicate the status of the computer and keyboard settings (Num Lock, Caps Lock, and Scroll Lock).
4	Numeric Keys	Work like a calculator keypad.
5	Arrow Keys	Used to navigate through a document or Web site. These keys allow you to move left, right, up, and down, using the keyboard instead of the mouse.
6	Ctrl Keys	Used in combination with another key; their effect depends on the application software you are using.
7	Application Key <sup>1</sup>	Used (like the right mouse button) to open pop-up menus in a Microsoft Office application. May perform other functions in other software applications.
8	Windows Logo Keys <sup>1</sup>	Used to open the Start menu in Microsoft Windows. Used in combination with other keys to perform other functions.
9	Alt Keys	Used in combination with another key; their effect depends on the application software you are using.

<sup>1</sup> Keys available in select geographic regions.

## Using the Windows Logo Key

Use the Windows Logo key in combination with other keys to perform certain functions available in the Windows operating system. Refer to [Keyboard on page 5](#) to identify the Windows Logo key.

**Table 1-5** Windows Logo Key Functions

The following Windows Logo Key functions are available in Microsoft Windows XP, Microsoft Windows Vista, and Microsoft Windows 7.

**Table 1-5 Windows Logo Key Functions (continued)**

Windows Logo Key	Displays or hides the Start menu
Windows Logo Key + d	Displays the Desktop
Windows Logo Key + m	Minimizes all open applications
Shift + Windows Logo Key + m	Undoes Minimize All
Windows Logo Key + e	Launches My Computer
Windows Logo Key + f	Launches Find Document
Windows Logo Key + Ctrl + f	Launches Find Computer
Windows Logo Key + F1	Launches Windows Help
Windows Logo Key + l	Locks the computer if you are connected to a network domain, or allows you to switch users if you are not connected to a network domain
Windows Logo Key + r	Launches the Run dialog box
Windows Logo Key + u	Launches the Utility Manager
Windows Logo Key + Tab	Windows XP - Cycles through the Taskbar buttons  Windows Vista and Windows 7 - Cycles through programs on the Taskbar using the Windows Flip 3-D

In addition to the Windows Logo Key functions described above, the following functions are also available in Microsoft Windows Vista and Windows 7.

Ctrl + Windows Logo Key + Tab	Use the arrow keys to cycle through programs on the Taskbar by using Windows Flip 3-D
Windows Logo Key + Spacebar	Brings all gadgets to the front and select Windows Sidebar
Windows Logo Key + g	Cycles through Sidebar gadgets
Windows Logo Key + t	Cycles through programs on the taskbar
Windows Logo Key + u	Launches Ease of Access Center
Windows Logo Key + any number key	Launches the Quick Launch shortcut that is in the position that corresponds to the number (for example, Windows Logo Key + 1 launches the first shortcut in the Quick Launch menu)

In addition to the Windows Logo Key functions described above, the following functions are also available in Microsoft Windows 7.

Windows Logo Key + Ctrl + b	Switches to the program that displayed a message in the notification area
Windows Logo Key + p	Choose a presentation display mode
Windows Logo Key + up arrow	Maximizes the window
Windows Logo Key + left arrow	Snaps the window to the left side of the screen
Windows Logo Key + right arrow	Snaps the window to the right side of the screen
Windows Logo Key + down arrow	Minimizes the window
Windows Logo Key + Shift + up arrow	Stretches the window to the top and bottom of the screen
Windows Logo Key + Shift + left arrow or right arrow	Moves a window from one monitor to another

**Table 1-5 Windows Logo Key Functions (continued)**

Windows Logo Key + + (on numpad)	Zooms in
Windows Logo Key + - (on numpad)	Zooms out

## Serial Number Location

Each computer has a unique serial number and product ID number in the location shown below. Keep these numbers available for use when contacting customer service for assistance.

**Figure 1-6** Serial Number and Product ID Location



---

## 2 Hardware Upgrades

### Serviceability Features

The computer includes features that make it easy to upgrade and service. No tools are needed for most of the installation procedures described in this chapter.

### Warnings and Cautions

Before performing upgrades be sure to carefully read all of the applicable instructions, cautions, and warnings in this guide.

**⚠ WARNING!** To reduce the risk of personal injury from electrical shock, hot surfaces, or fire:

Disconnect the power cord from the wall outlet and allow the internal system components to cool before touching.

Do not plug telecommunications or telephone connectors into the network interface controller (NIC) receptacles.

Do not disable the power cord grounding plug. The grounding plug is an important safety feature.

Plug the power cord in a grounded (earthed) outlet that is easily accessible at all times.

To reduce the risk of serious injury, read the *Safety & Comfort Guide*. It describes proper workstation, setup, posture, and health and work habits for computer users, and provides important electrical and mechanical safety information. This guide is located on the Web at <http://www.hp.com/ergo>.

**WARNING!** Energized and moving parts inside.

Disconnect power to the equipment before removing the enclosure.

Replace and secure the enclosure before re-energizing the equipment.

**⚠ CAUTION:** Static electricity can damage the electrical components of the computer or optional equipment. Before beginning these procedures, ensure that you are discharged of static electricity by briefly touching a grounded metal object. See Appendix D, [Electrostatic Discharge on page 57](#) for more information.

When the computer is plugged into an AC power source, voltage is always applied to the system board. You must disconnect the power cord from the power source before opening the computer to prevent damage to internal components.

---

# Unlocking the Smart Cover Lock



**NOTE:** The Smart Cover Lock is an optional feature included on some models only.

The Smart Cover Lock is a software-controllable cover lock, controlled by the setup password. This lock prevents unauthorized access to the internal components. The computer ships with the Smart Cover Lock in the unlocked position. For more information about locking the Smart Cover Lock, refer to the *Desktop Management Guide*.

## Smart Cover FailSafe Key

If you enable the Smart Cover Lock and cannot enter your password to disable the lock, you will need a Smart Cover FailSafe Key to open the computer cover. You will need the key to access the internal computer components in any of the following circumstances:

- Power outage
- Startup failure
- PC component (for example, processor or power supply) failure
- Forgotten password



**NOTE:** The Smart Cover FailSafe Key is a specialized tool available from HP. Be prepared; order this key before you need it.

To obtain a FailSafe Key:

- Contact an authorized HP reseller or service provider. Order PN 166527-001 for the wrench-style key or PN 166527-002 for the screwdriver bit key.
- Refer to the HP Web site (<http://www.hp.com>) for ordering information.
- Call the appropriate number listed in the warranty or in the *Support Telephone Numbers* guide.

## Using the Smart Cover FailSafe Key to Remove the Smart Cover Lock

To open the access panel with the Smart Cover Lock engaged:

1. Remove/disengage any security devices that prohibit opening the computer.
2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
3. Turn off the computer properly through the operating system, then turn off any external devices.
4. Disconnect the power cord from the power outlet and disconnect any external devices.

△ **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.
5. If the computer is on a stand, remove the computer from the stand.

6. Use the Smart Cover FailSafe Key to remove the tamper-proof screw that secures the Smart Cover Lock to the chassis.

**Figure 2-1** Removing the Smart Cover Lock Screw



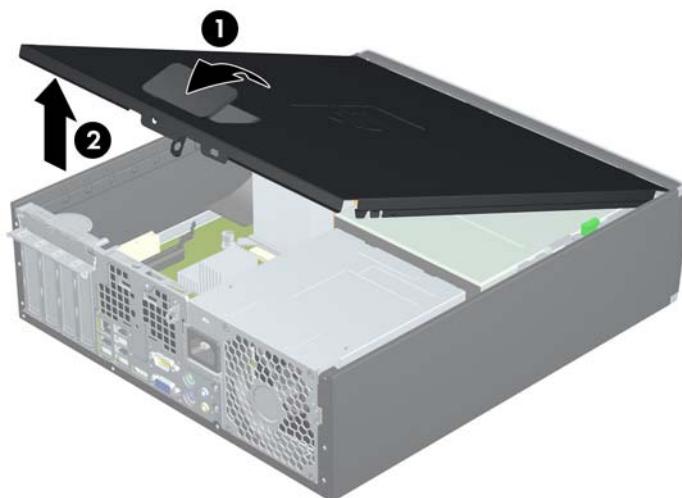
You can now remove the access panel. See [Removing the Computer Access Panel on page 11](#).

To reattach the Smart Cover Lock, secure the lock in place with the tamper-proof screw.

## Removing the Computer Access Panel

1. Remove/disengage any security devices that prohibit opening the computer.
  2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
  3. Turn off the computer properly through the operating system, then turn off any external devices.
  4. Disconnect the power cord from the power outlet and disconnect any external devices.
- △ **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.
5. If the computer is on a stand, remove the computer from the stand.
  6. Lift up on the access panel handle (1) then lift the access panel off the computer (2).

**Figure 2-2** Removing the Access Panel



## Replacing the Computer Access Panel

Slide the lip on the front end of the access panel under the lip on the front of the chassis (1) then press the back end of the access panel onto the unit so that it locks into place (2).

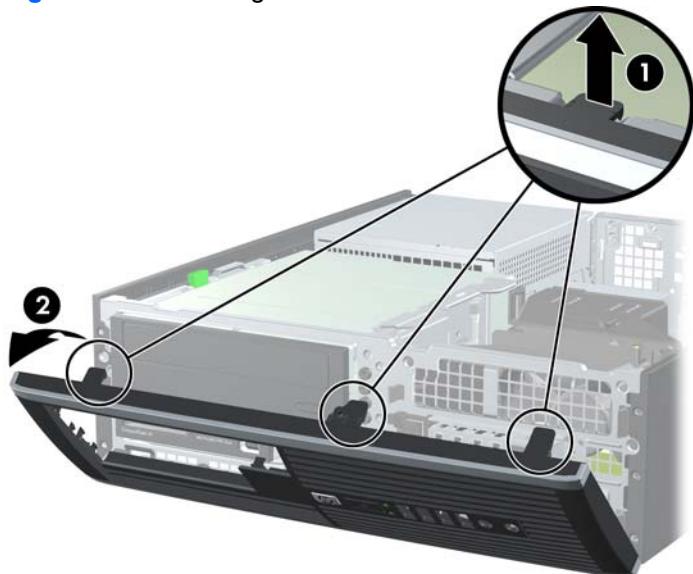
**Figure 2-3** Replacing the Access Panel



## Removing the Front Bezel

1. Remove/disengage any security devices that prohibit opening the computer.
  2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
  3. Turn off the computer properly through the operating system, then turn off any external devices.
  4. Disconnect the power cord from the power outlet and disconnect any external devices.
- △ **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.
5. Remove the access panel.
  6. Lift up the three tabs on the side of the bezel (1), then rotate the bezel off the chassis (2).

**Figure 2-4** Removing the Front Bezel

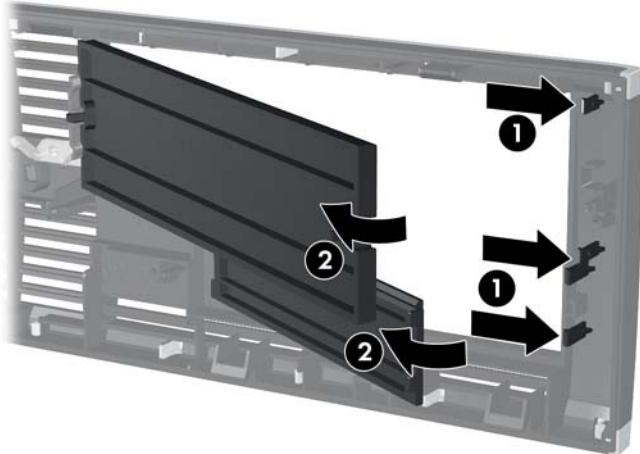


## Removing Bezel Blanks

On some models, there are bezel blanks covering the 3.5-inch and 5.25-inch external drive bays that need to be removed before installing a drive. To remove a bezel blank:

1. Remove the access panel and front bezel.
2. To remove a bezel blank, push the two retaining tabs that hold the bezel blank in place towards the outer right edge of the bezel (1) and slide the bezel blank back and to the right to remove it (2).

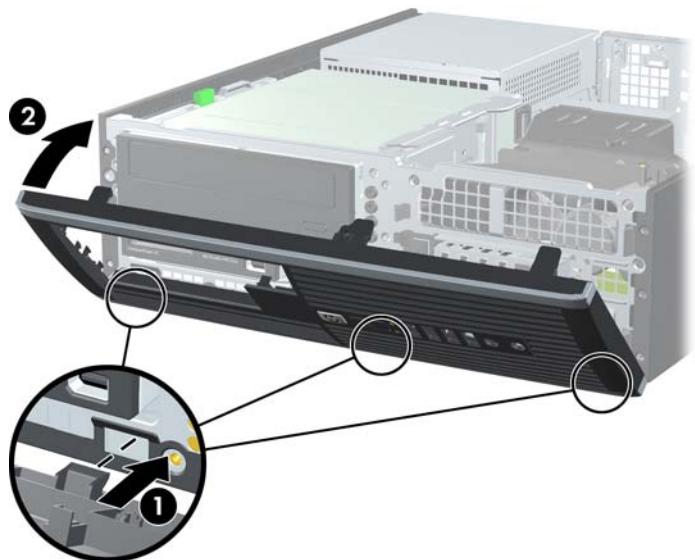
**Figure 2-5** Removing a Bezel Blank



## Replacing the Front Bezel

Insert the three hooks on the bottom side of the bezel into the rectangular holes on the chassis (1) then rotate the top side of the bezel onto the chassis (2) and snap it into place.

**Figure 2-6** Replacing the Front Bezel



## Using the Small Form Factor Computer in a Tower Orientation

The Small Form Factor computer can be used in a tower orientation with an optional tower stand that can be purchased from HP.

1. Remove/disengage any security devices that prohibit opening the computer.
2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
3. Turn off the computer properly through the operating system, then turn off any external devices.
4. Disconnect the power cord from the power outlet and disconnect any external devices.

△ **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.

5. Orient the computer so that its right side is facing down and place the computer in the optional stand.

**Figure 2-7** Changing from Desktop to Tower Orientation



☒ **NOTE:** To stabilize the computer in a tower orientation, HP recommends the use of the optional tower stand.

6. Reconnect the power cord and any external devices, then turn on the computer.

☒ **NOTE:** Ensure at least 10.2 centimeters (4 inches) of space on all sides of the computer remains clear and free of obstructions.

# Installing Additional Memory

The computer comes with double data rate 3 synchronous dynamic random access memory (DDR3-SDRAM) dual inline memory modules (DIMMs).

## DIMMs

The memory sockets on the system board can be populated with up to four industry-standard DIMMs. These memory sockets are populated with at least one preinstalled DIMM. To achieve the maximum memory support, you can populate the system board with up to 16-GB of memory configured in a high-performing dual channel mode.

## DDR3-SDRAM DIMMs

For proper system operation, the DDR3-SDRAM DIMMs must be:

- industry-standard 240-pin
- unbuffered non-ECC PC3-8500 DDR3-1066 MHz-compliant or PC3-10600 DDR3-1333 MHz-compliant
- 1.5 volt DDR3-SDRAM DIMMs

The DDR3-SDRAM DIMMs must also:

- support CAS latency 7 DDR3 1066 MHz (7-7-7 timing) and CAS latency 9 DDR3 1333 MHz (9-9-9 timing)
- contain the mandatory JEDEC SPD information

In addition, the computer supports:

- 512-Mbit, 1-Gbit, and 2-Gbit non-ECC memory technologies
- single-sided and double-sided DIMMs
- DIMMs constructed with x8 and x16 DDR devices; DIMMs constructed with x4 SDRAM are not supported

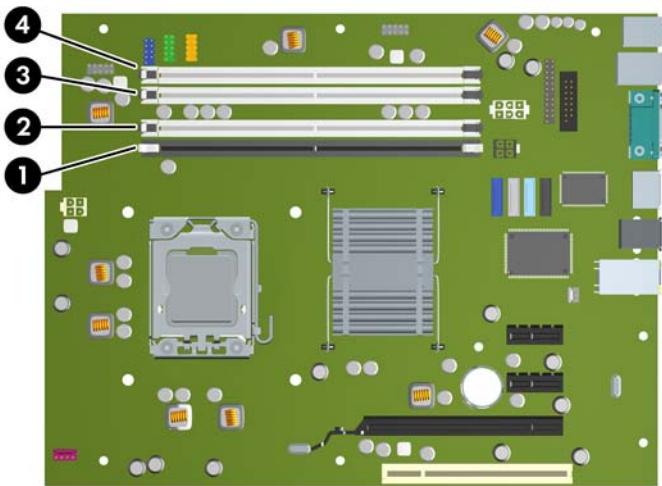


**NOTE:** The system will not operate properly if you install unsupported DIMMs.

## Populating DIMM Sockets

There are four DIMM sockets on the system board, with two sockets per channel. The sockets are labeled DIMM1, DIMM2, DIMM3, and DIMM4. Sockets DIMM1 and DIMM2 operate in memory channel A. Sockets DIMM3 and DIMM4 operate in memory channel B.

**Figure 2-8** DIMM Socket Locations



**Table 2-1** DIMM Socket Locations

Item	Description	Socket Color
1	DIMM1 socket, Channel A (populate first)	Black
2	DIMM2 socket, Channel A (populate third)	White
3	DIMM3 socket, Channel B (populate second)	White
4	DIMM4 socket, Channel B (populate fourth)	White

**NOTE:** A DIMM must occupy the black DIMM1 socket. Otherwise, the system will display a POST error message indicating that a memory module must be installed in the wrong socket.

The system will automatically operate in single channel mode, dual channel mode, or flex mode, depending on how the DIMMs are installed.

- The system will operate in single channel mode if the DIMM sockets are populated in one channel only.
- The system will operate in a higher-performing dual channel mode if the total memory capacity of the DIMMs in Channel A is equal to the total memory capacity of the DIMMs in Channel B. The technology and device width can vary between the channels. For example, if Channel A is populated with two 1-GB DIMMs and Channel B is populated with one 2-GB DIMM, the system will operate in dual channel mode.
- The system will operate in flex mode if the total memory capacity of the DIMMs in Channel A is not equal to the total memory capacity of the DIMMs in Channel B. In flex mode, the channel populated with the least amount of memory describes the total amount of memory assigned to dual channel

and the remainder is assigned to single channel. For optimal speed, the channels should be balanced so that the largest amount of memory is spread between the two channels. If one channel will have more memory than the other, the larger amount should be assigned to Channel A. For example, if you are populating the sockets with one 2-GB DIMM, and three 1-GB DIMMs, Channel A should be populated with the 2-GB DIMM and one 1-GB DIMM, and Channel B should be populated with the other two 1-GB DIMMs. With this configuration, 4-GB will run as dual channel and 1-GB will run as single channel.

- In any mode, the maximum operational speed is determined by the slowest DIMM in the system.

## Installing DIMMs

**△ CAUTION:** You must disconnect the power cord and wait approximately 30 seconds for the power to drain before adding or removing memory modules. Regardless of the power-on state, voltage is always supplied to the memory modules as long as the computer is plugged into an active AC outlet. Adding or removing memory modules while voltage is present may cause irreparable damage to the memory modules or system board. If you see an LED light on the system board, voltage is still present.

The memory module sockets have gold-plated metal contacts. When upgrading the memory, it is important to use memory modules with gold-plated metal contacts to prevent corrosion and/or oxidation resulting from having incompatible metals in contact with each other.

Static electricity can damage the electronic components of the computer or optional cards. Before beginning these procedures, ensure that you are discharged of static electricity by briefly touching a grounded metal object. For more information, refer to Appendix D, [Electrostatic Discharge on page 57](#).

When handling a memory module, be careful not to touch any of the contacts. Doing so may damage the module.

1. Remove/disengage any security devices that prohibit opening the computer.
2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
3. Turn off the computer properly through the operating system, then turn off any external devices.
4. Disconnect the power cord from the power outlet and disconnect any external devices.

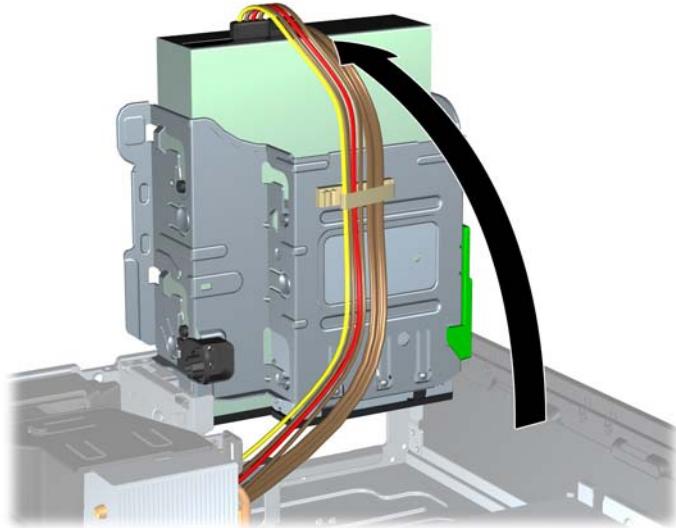
**△ CAUTION:** You must disconnect the power cord and wait approximately 30 seconds for the power to drain before adding or removing memory modules. Regardless of the power-on state, voltage is always supplied to the memory modules as long as the computer is plugged into an active AC outlet. Adding or removing memory modules while voltage is present may cause irreparable damage to the memory modules or system board. If you see an LED light on the system board, voltage is still present.

5. If the computer is on a stand, remove the computer from the stand.
6. Remove the access panel.

**⚠ WARNING!** To reduce risk of personal injury from hot surfaces, allow the internal system components to cool before touching.

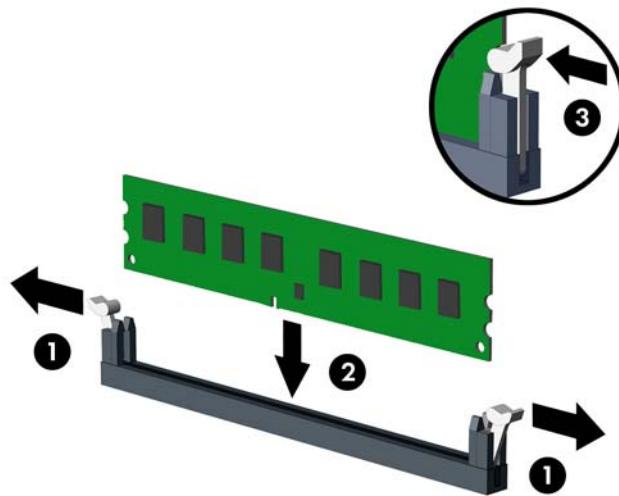
7. Rotate up the external drive bay housing to access the memory module sockets on the system board.

**Figure 2-9** Rotating the Drive Cage Up



8. Open both latches of the memory module socket (1), and insert the memory module into the socket (2).

**Figure 2-10** Installing a DIMM



 **NOTE:** A memory module can be installed in only one way. Match the notch on the module with the tab on the memory socket.

A DIMM must occupy the black DIMM1 socket.

Populate the DIMM sockets in the following order: DIMM1, DIMM3, DIMM2, then DIMM4.

For maximum performance, populate the sockets so that the memory capacity is spread as equally as possible between Channel A and Channel B. Refer to [Populating DIMM Sockets on page 18](#) for more information.

9. Push the module down into the socket, ensuring that the module is fully inserted and properly seated. Make sure the latches are in the closed position (3).
10. Repeat steps 8 and 9 to install any additional modules.
11. Replace the access panel.
12. If the computer was on a stand, replace the stand.
13. Reconnect the power cord and turn on the computer.
14. Lock any security devices that were disengaged when the access panel was removed.

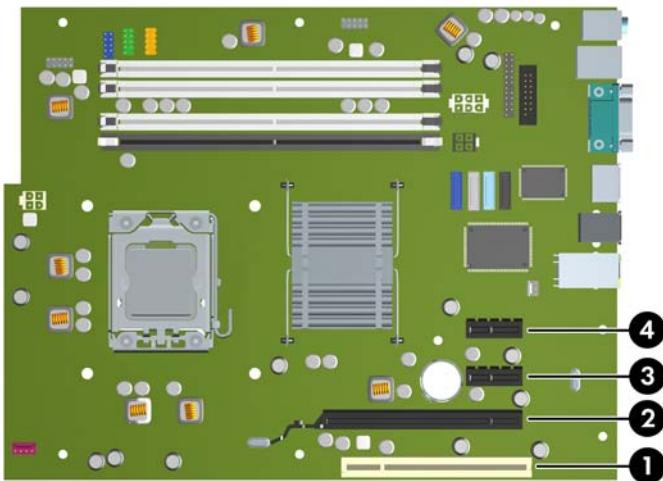
The computer should automatically recognize the additional memory the next time you turn on the computer.

# Removing or Installing an Expansion Card

The computer has one PCI expansion slot, two PCI Express x1 expansion slots, and one PCI Express x16 expansion slot.

 **NOTE:** The PCI and PCI Express slots support only low profile cards.

**Figure 2-11** Expansion Slot Locations



**Table 2-2** Expansion Slot Locations

Item	Description
1	PCI expansion slot
2	PCI Express x16 expansion slot
3	PCI Express x1 expansion slot
4	PCI Express x1 expansion slot

 **NOTE:** You can install a PCI Express x1, x4, x8, or x16 expansion card in the PCI Express x16 slot.

To install an expansion card:

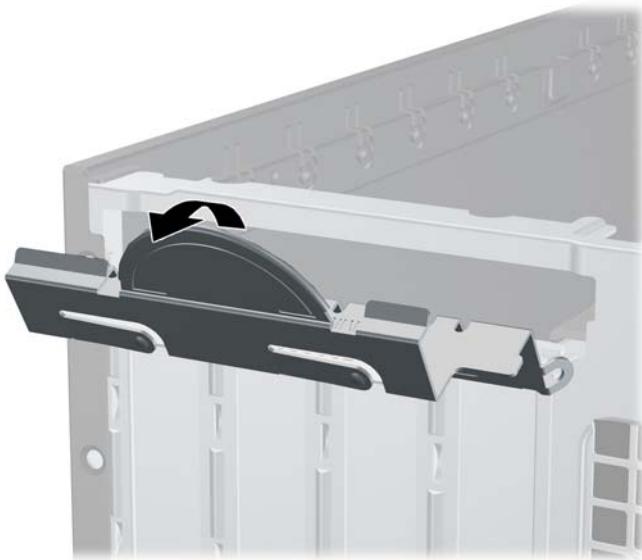
1. Remove/disengage any security devices that prohibit opening the computer.
2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
3. Turn off the computer properly through the operating system, then turn off any external devices.
4. Disconnect the power cord from the power outlet and disconnect any external devices.

 **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.

5. If the computer is on a stand, remove the computer from the stand.

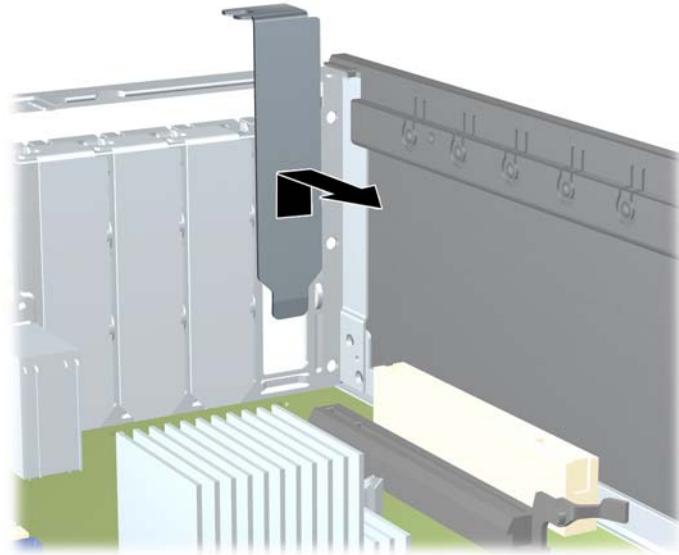
6. Remove the access panel.
7. Locate the correct vacant expansion socket on the system board and the corresponding expansion slot on the back of the computer chassis.
8. Release the slot cover retention latch that secures the PCI slot covers by lifting the green tab on the latch and rotating the latch to the open position.

**Figure 2-12** Opening the Expansion Slot Retainer



9. Before installing an expansion card, remove the expansion slot cover or the existing expansion card.
  - a. If you are installing an expansion card in a vacant socket, remove the appropriate expansion slot cover on the back of the chassis. Pull the slot cover straight up then away from the inside of the chassis.

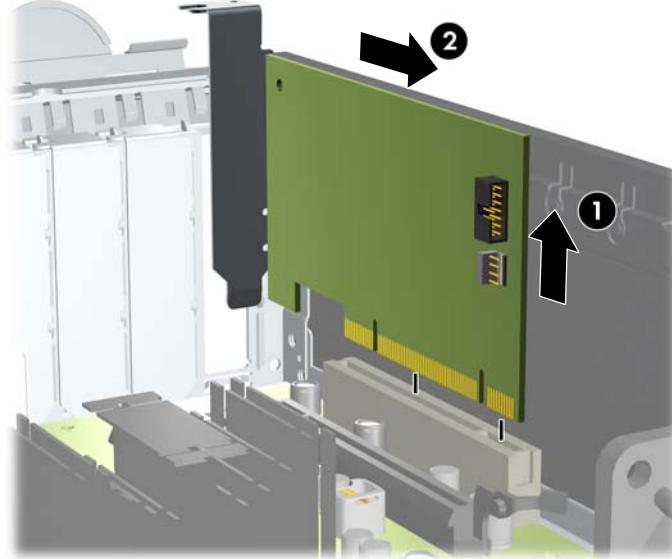
**Figure 2-13** Removing an Expansion Slot Cover



- b. If you are removing a standard PCI card or PCI Express x1 card, hold the card at each end, and carefully rock it back and forth until the connectors pull free from the socket. Pull the expansion card straight up from the socket (1) then away from the inside of the chassis to release it from the chassis frame (2). Be sure not to scrape the card against the other components.

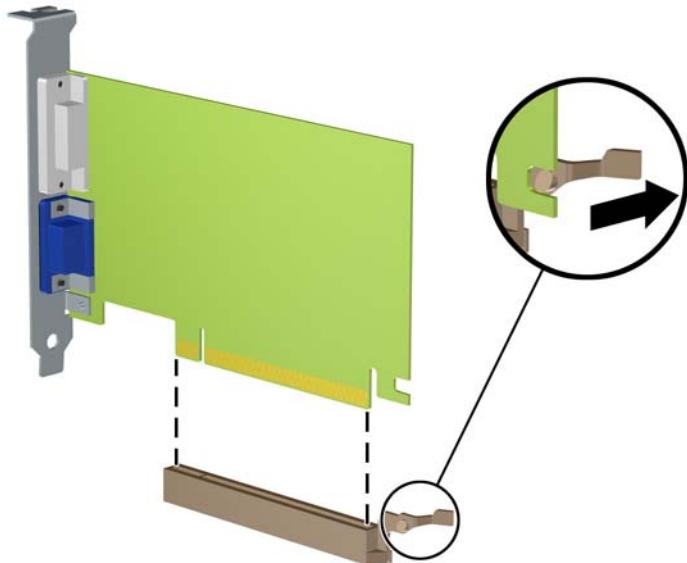
 **NOTE:** Before removing an installed expansion card, disconnect any cables that may be attached to the expansion card.

**Figure 2-14** Removing a Standard PCI Expansion Card



- c. If you are removing a PCI Express x16 card, pull the retention arm on the back of the expansion socket away from the card and carefully rock the card back and forth until the connectors pull free from the socket. Pull the expansion card straight up from the socket then away from the inside of the chassis to release it from the chassis frame. Be sure not to scrape the card against the other components.

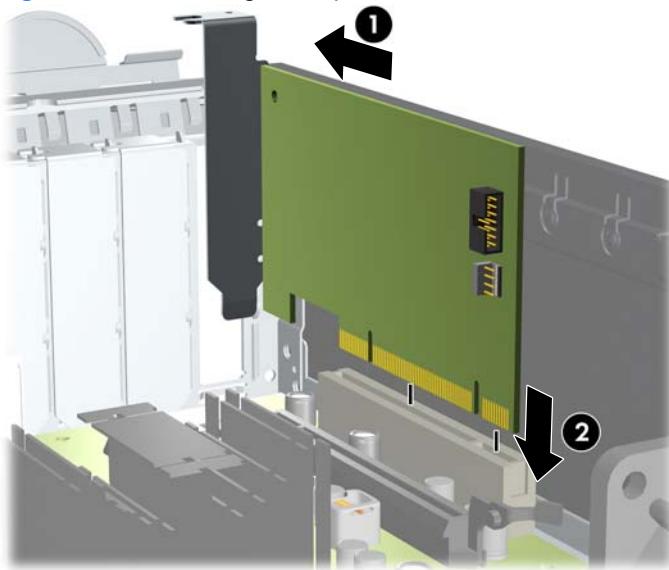
**Figure 2-15** Removing a PCI Express x16 Expansion Card



10. Store the removed card in anti-static packaging.
  11. If you are not installing a new expansion card, install an expansion slot cover to close the open slot.
- 
- △ **CAUTION:** After removing an expansion card, you must replace it with a new card or expansion slot cover for proper cooling of internal components during operation.

- 12.** To install a new expansion card, hold the card just above the expansion socket on the system board then move the card toward the rear of the chassis (1) so that the bracket on the card is aligned with the open slot on the rear of the chassis. Press the card straight down into the expansion socket on the system board (2).

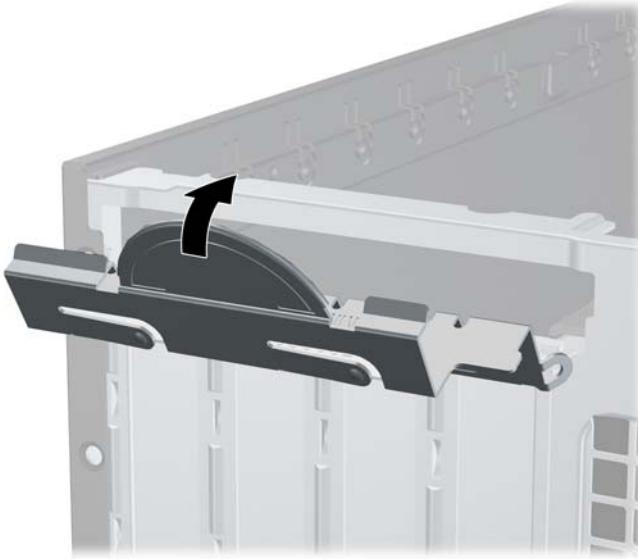
**Figure 2-16** Installing an Expansion Card



 **NOTE:** When installing an expansion card, press firmly on the card so that the whole connector seats properly in the expansion card slot.

- 13.** Rotate the slot cover retention latch back in place to secure the expansion card.

**Figure 2-17** Closing the Expansion Slot Retainer

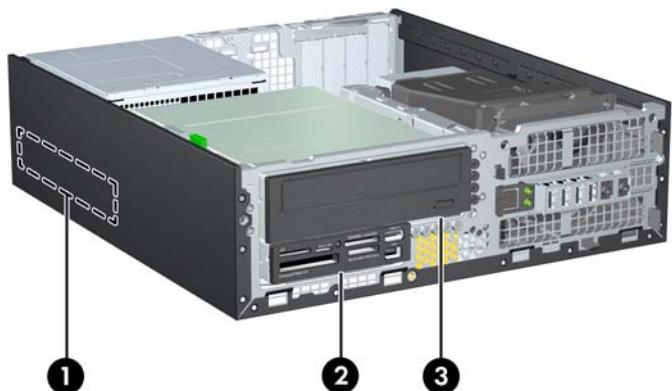


- 14.** Connect external cables to the installed card, if needed. Connect internal cables to the system board, if needed.
- 15.** Replace the access panel.

16. If the computer was on a stand, replace the stand.
17. Reconnect the power cord and turn on the computer.
18. Lock any security devices that were disengaged when the access panel was removed.
19. Reconfigure the computer, if necessary.

## Drive Positions

**Figure 2-18** Drive Positions



**Table 2-3** Drive Positions

1	3.5-inch internal hard drive bay
2	3.5-inch external drive bay for optional drives (media card reader shown)
3	5.25-inch external drive bay for optional drives (optical drive shown)

**NOTE:** The drive configuration on your computer may be different than the drive configuration shown above.

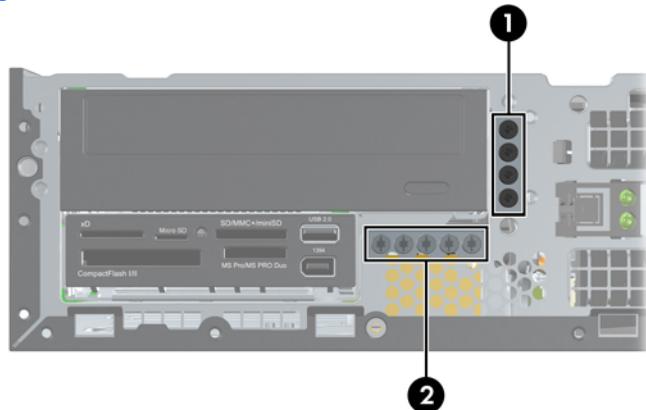
To verify the type, size, and capacity of the storage devices installed in the computer, run Computer Setup.

# Installing and Removing Drives

When installing additional drives, follow these guidelines:

- The primary Serial ATA (SATA) hard drive must be connected to the dark blue primary SATA connector on the system board labeled SATA0.
- Connect a SATA optical drive to the white SATA connector on the system board labeled SATA1.
- Connect devices in order of SATA0, SATA1, then SATA2
- Connect an optional eSATA adapter cable to the black ESATA connector on the system board.
- Connect a media card reader USB cable to the USB connector on the system board labeled MEDIA. If the media card reader has a 1394 port, connect the 1394 cable to the 1394 PCI card.
- The system does not support Parallel ATA (PATA) optical drives or PATA hard drives.
- You must install guide screws to ensure the drive will line up correctly in the drive cage and lock in place. HP has provided extra guide screws for the external drive bays (five 6-32 standard screws and four M3 metric screws), installed in the front of the chassis, under the front bezel. The 6-32 standard screws are required for a secondary hard drive. All other drives (except the primary hard drive) use M3 metric screws. The HP-supplied metric screws are black and the HP-supplied standard screws are silver. If you are replacing the primary hard drive, you must remove the four silver and blue 6-32 isolation mounting guide screws from the old hard drive and install them in the new hard drive.

**Figure 2-19** Extra Guide Screw Locations



No.	Guide Screw	Device
1	Black M3 Metric Screws	All Drives (except hard drives)
2	Silver 6-32 Standard Screws	Secondary Hard Drive

There are a total of five extra silver 6-32 standard screws. Four are used as guide screws for a secondary hard drive. The fifth is used for bezel security (see [Front Bezel Security on page 55](#) for more information).

△ **CAUTION:** To prevent loss of work and damage to the computer or drive:

If you are inserting or removing a drive, shut down the operating system properly, turn off the computer, and unplug the power cord. Do not remove a drive while the computer is on or in standby mode.

Before handling a drive, ensure that you are discharged of static electricity. While handling a drive, avoid touching the connector. For more information about preventing electrostatic damage, refer to Appendix D, [Electrostatic Discharge on page 57](#).

Handle a drive carefully; do not drop it.

Do not use excessive force when inserting a drive.

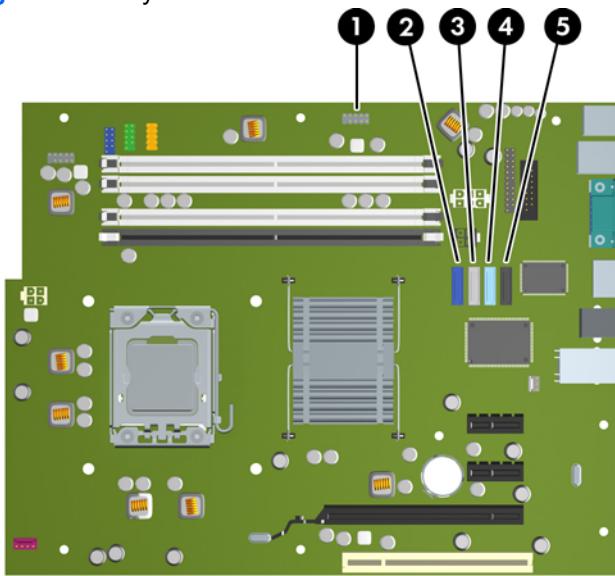
Avoid exposing a hard drive to liquids, temperature extremes, or products that have magnetic fields such as monitors or speakers.

If a drive must be mailed, place the drive in a bubble-pack mailer or other protective packaging and label the package “Fragile: Handle With Care.”

## System Board Drive Connections

Refer to the following illustration and table to identify the system board drive connectors.

**Figure 2-20** System Board Drive Connections



**Table 2-4** System Board Drive Connections

No.	System Board Connector	System Board Label	Color
1	Media Card Reader	MEDIA	black
2	SATA0	SATA0	dark blue
3	SATA1	SATA1	white
4	SATA2	SATA2	light blue
5	eSATA	ESATA	black

## Removing an External 5.25-inch Drive

△ **CAUTION:** All removable media should be taken out of a drive before removing the drive from the computer.

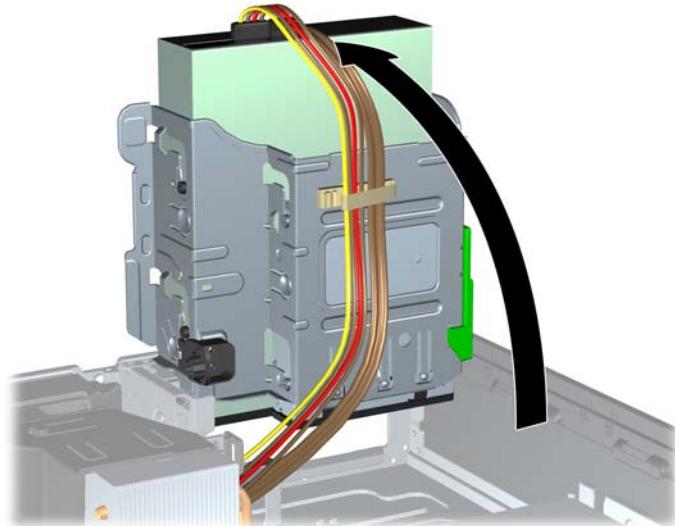
To remove a 5.25-inch external drive:

1. Remove/disengage any security devices that prohibit opening the computer.
2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
3. Turn off the computer properly through the operating system, then turn off any external devices.
4. Disconnect the power cord from the power outlet and disconnect any external devices.

△ **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.

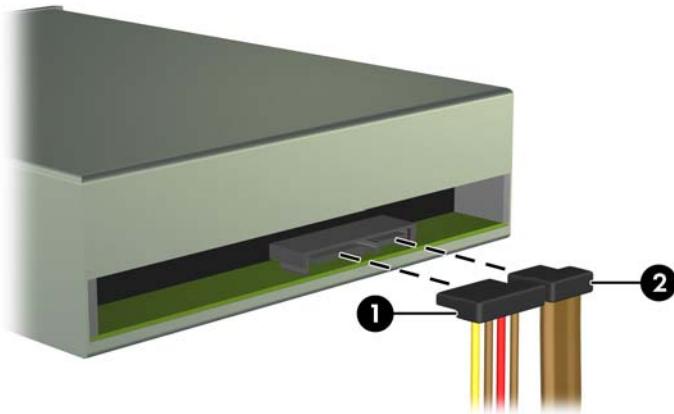
5. If the computer is on a stand, remove the computer from the stand.
6. Remove the access panel.
7. Rotate the drive cage to its upright position.

**Figure 2-21** Rotating the Drive Cage Up



8. If removing an optical drive, disconnect the power cable (1) and data cable (2) from the rear of the optical drive.

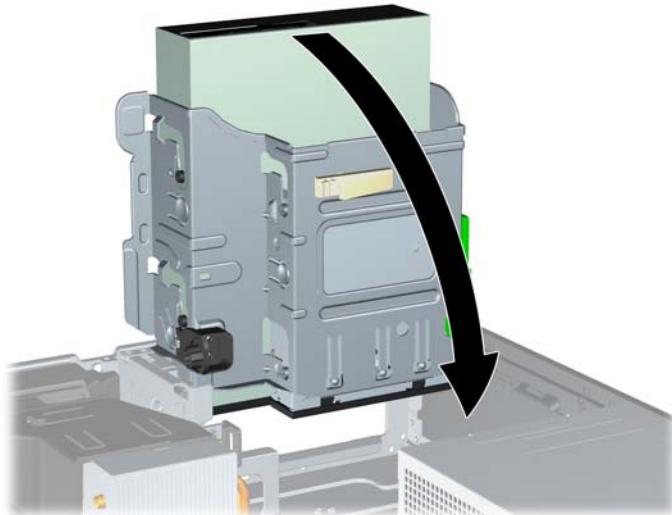
**Figure 2-22** Disconnecting the Power and Data Cables



9. Rotate the drive cage back down to its normal position.

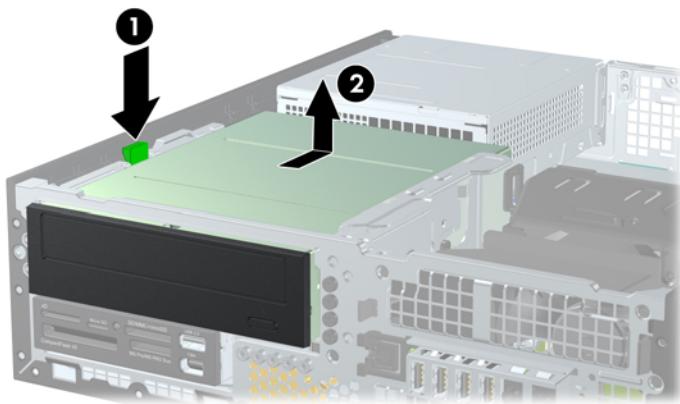
△ **CAUTION:** Be careful not to pinch any cables or wires when rotating the drive cage down.

**Figure 2-23** Rotating the Drive Cage Down



10. Press down on the green drive retainer button located on the left side of the drive to disengage the drive from the drive cage (1). While pressing the drive retainer button, slide the drive back until it stops, then lift it up and out of the drive cage (2).

**Figure 2-24** Removing the 5.25-inch Drive



 **NOTE:** To replace the drive, reverse the removal procedure. When replacing a drive, transfer the four guide screws from the old drive to the new one.

## Installing an Optical Drive into the 5.25-inch Drive Bay

To install an optional 5.25-inch optical drive:

1. Remove/disengage any security devices that prohibit opening the computer.
  2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
  3. Turn off the computer properly through the operating system, then turn off any external devices.
  4. Disconnect the power cord from the power outlet and disconnect any external devices.
-  **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.
5. If the computer is on a stand, remove the computer from the stand.
  6. Remove the access panel.
  7. If you are installing a drive in a bay covered by a bezel blank, remove the front bezel then remove the bezel blank. See [Removing Bezel Blanks on page 14](#) for more information.

8. Install four M3 metric guide screws in the lower holes on each side of the drive. HP has provided four extra M3 metric guide screws on the front of the chassis, under the front bezel. The M3 metric guide screws are black. Refer to [Installing and Removing Drives on page 29](#) for an illustration of the extra M3 metric guide screws location.

△ **CAUTION:** Use only 5-mm long screws as guide screws. Longer screws can damage the internal components of the drive.

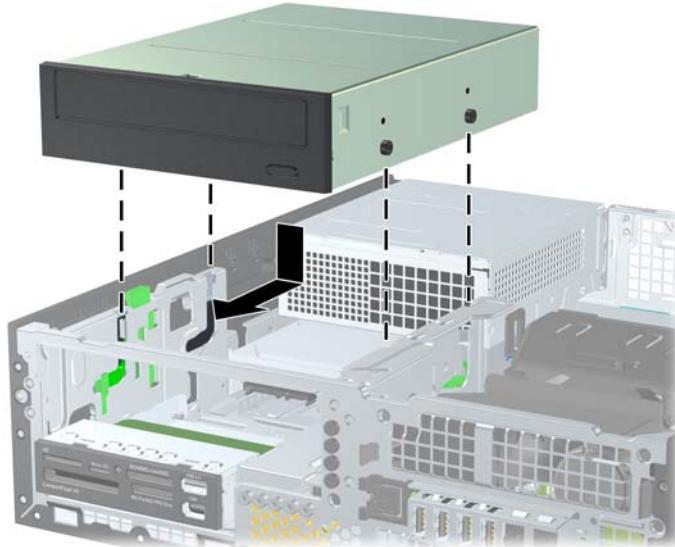
☒ **NOTE:** When replacing the drive, transfer the four M3 metric guide screws from the old drive to the new one.

**Figure 2-25** Installing Guide Screws in the Optical Drive



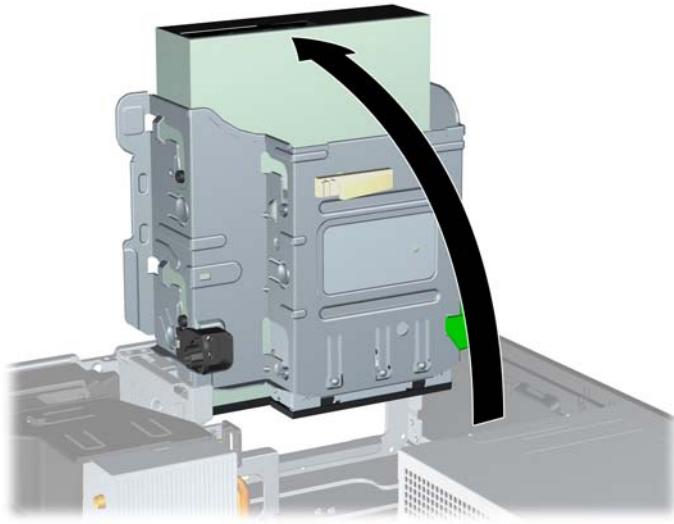
9. Position the guide screws on the drive into the J-slots in the drive bay. Then slide the drive toward the front of the computer until it locks into place.

**Figure 2-26** Installing the Optical Drive



10. Rotate the drive cage to its upright position.

**Figure 2-27** Rotating the Drive Cage Up



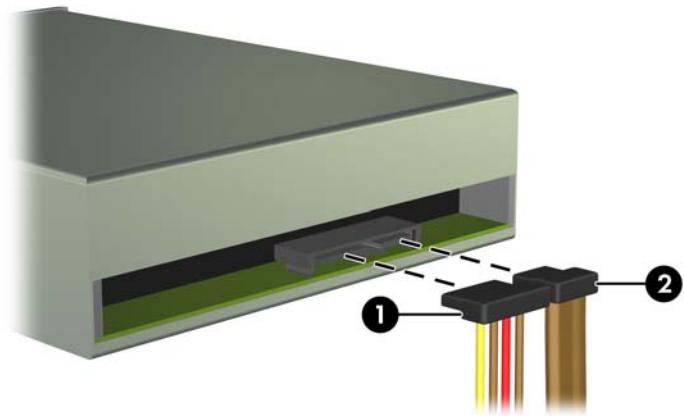
11. Connect the SATA data cable to the white system board connector labeled SATA1.

12. Route the data cable through the cable guides.

△ **CAUTION:** There are two cable guides that keep the data cable from being pinched by the drive cage when raising or lowering it. One is located on the bottom side of the drive cage. The other is located on the chassis frame under the drive cage. Ensure that the data cable is routed through these guides before connecting it to the optical drive.

13. Connect the power cable (1) and data cable (2) to the rear of the optical drive.

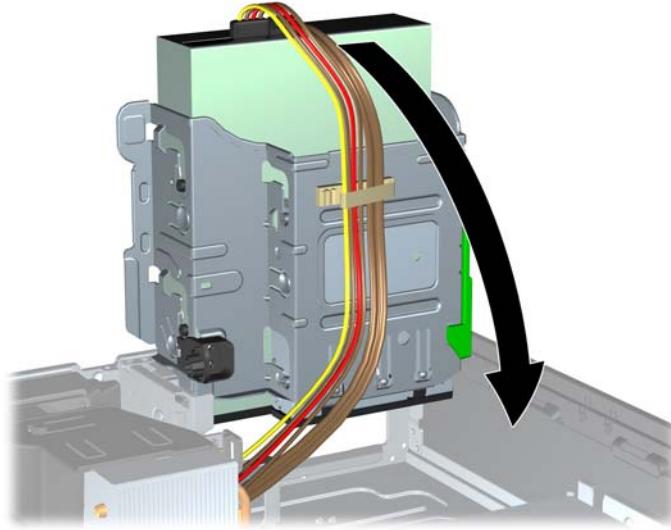
**Figure 2-28** Connecting the Power and Data Cables



14. Rotate the drive cage back down to its normal position.

△ **CAUTION:** Be careful not to pinch any cables or wires when rotating the drive cage down.

**Figure 2-29** Rotating the Drive Cage Down



15. Replace the access panel.
16. If the computer was on a stand, replace the stand.
17. Reconnect the power cord and turn on the computer.
18. Lock any security devices that were disengaged when the access panel was removed.

The system automatically recognizes the drive and reconfigures the computer.

## Removing an External 3.5-inch Drive

△ **CAUTION:** All removable media should be taken out of a drive before removing the drive from the computer.

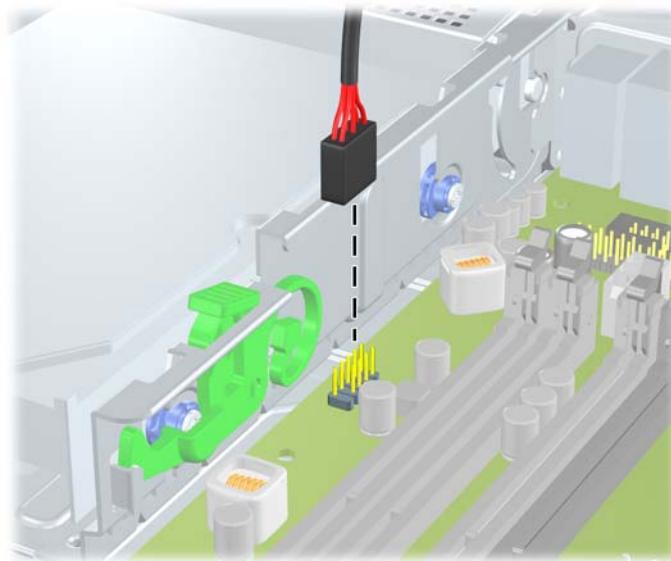
The 3.5-inch drive is located underneath the 5.25-inch drive. You must remove the external 5.25-inch drive before removing the external 3.5-inch drive.

1. Follow the procedure in [Removing an External 5.25-inch Drive on page 31](#) to remove the 5.25-inch drive and access the 3.5-inch drive.
- △ **CAUTION:** Ensure that the computer is turned off and that the power cord is disconnected from the electrical outlet before proceeding.

2. Disconnect the drive cables from the rear of the drive, or, if you are removing a media card reader, disconnect the USB and 1394 cables from the system board as indicated in the following illustrations.

 **NOTE:** On some models, the media card reader does not include a 1394 port or cable.

**Figure 2-30** Disconnecting the Media Card Reader USB Cable

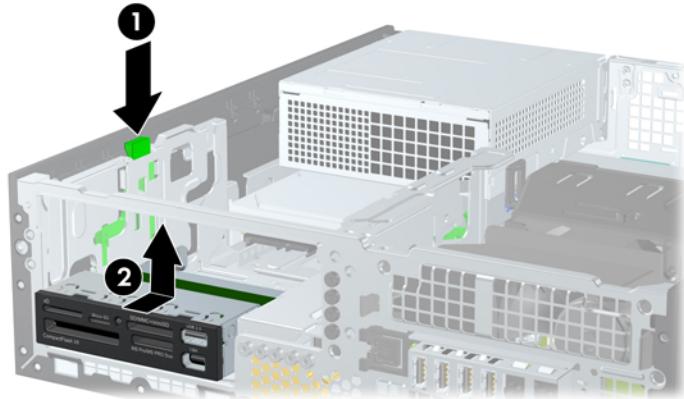


**Figure 2-31** Disconnecting the Media Card Reader 1394 Cable



3. Press down on the green drive retainer button located on the left side of the drive to disengage the drive from the drive cage (1). While pressing the drive retainer button, slide the drive back until it stops, then lift it up and out of the drive cage (2).

**Figure 2-32** Removing a 3.5-inch Drive (Media Card Reader Shown)



 **NOTE:** To replace the 3.5-inch drive, reverse the removal procedure.

When replacing a 3.5-inch drive, transfer the four guide screws from the old drive to the new one.

## Installing a Drive into the 3.5-inch External Drive Bay

The 3.5-inch bay is located underneath the 5.25-inch drive. To install a drive into the 3.5-inch bay:

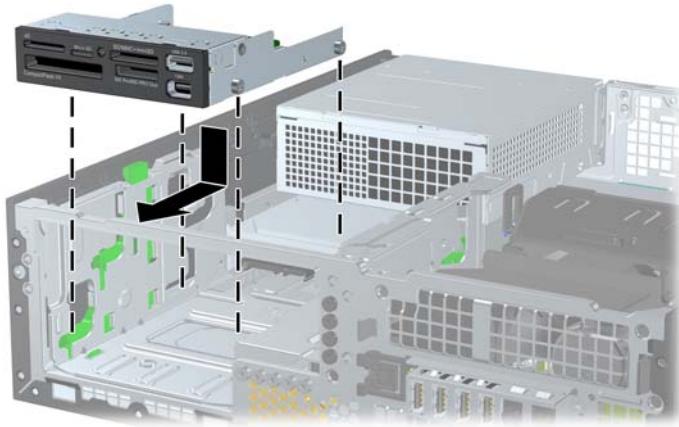
 **NOTE:** Install guide screws to ensure the drive will line up correctly in the drive cage and lock in place. HP has provided extra guide screws for the external drive bays (four 6-32 standard screws and four M3 metric screws), installed in the front of the chassis, under the front bezel. A secondary hard drive uses 6-32 standard screws. All other drives (except the primary hard drive) use M3 metric screws. The HP-supplied M3 metric screws are black and the HP-supplied 6-32 standard screws are silver. Refer to [Installing and Removing Drives on page 29](#) for illustrations of the guide screw locations.

1. Follow the procedure in [Removing an External 5.25-inch Drive on page 31](#) to remove the 5.25-inch drive and access the 3.5-inch drive bay.

 **CAUTION:** Ensure that the computer is turned off and that the power cord is disconnected from the electrical outlet before proceeding.
2. If you are installing a drive in a bay covered by a bezel blank, remove the front bezel then remove the bezel blank. See [Removing Bezel Blanks on page 14](#) for more information.

3. Position the guide screws on the drive into the J-slots in the drive bay. Then slide the drive toward the front of the computer until it locks into place.

**Figure 2-33** Installing a Drive into the 3.5-inch Drive Bay (Media Card Reader Shown)



4. Connect the appropriate drive cables:
  - a. If installing a second hard drive, connect the power and data cables to the rear of the drive and connect the other end of the data cable to the next available (unpopulated) SATA connector on the system board by following the numbered sequence of the connectors.
  - b. If installing a media card reader, connect the USB cable from the media card reader to the USB connector on the system board labeled MEDIA. If the media card reader includes a 1394 port, connect the 1394 cable to the 1394 PCI card.
5. Replace the 5.25-inch drive.
6. Replace the front bezel and access panel.
7. If the computer was on a stand, replace the stand.
8. Reconnect the power cord and turn on the computer.
9. Lock any security devices that were disengaged when the access panel was removed.

**NOTE:** Refer to [System Board Drive Connections on page 30](#) for an illustration of the system board drive connectors.

## Removing and Replacing the Primary 3.5-inch Internal SATA Hard Drive

**NOTE:** The system does not support Parallel ATA (PATA) hard drives.

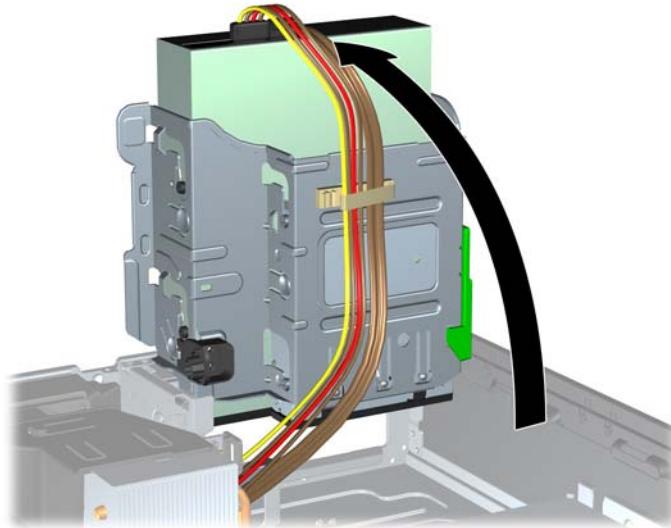
Before you remove the old hard drive, be sure to back up the data from the old hard drive so that you can transfer the data to the new hard drive.

The preinstalled 3.5-inch hard drive is located under the power supply. To remove and replace the hard drive:

1. Remove/disengage any security devices that prohibit opening the computer.
2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
3. Turn off the computer properly through the operating system, then turn off any external devices.

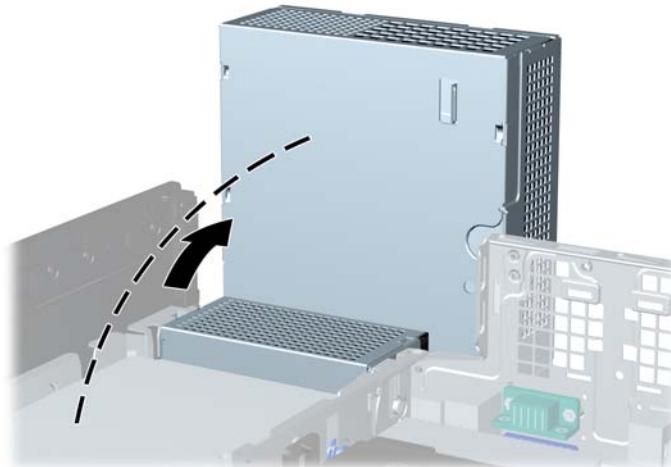
4. Disconnect the power cord from the power outlet and disconnect any external devices.
- △ **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.
5. If the computer is on a stand, remove the computer from the stand.
6. Remove the access panel.
7. Rotate the drive cage for external drives to its upright position.

**Figure 2-34** Rotating the Drive Cage Up



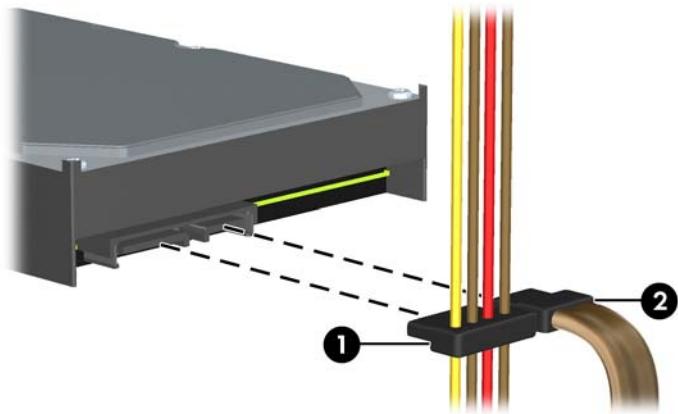
8. Rotate the power supply to its upright position. The hard drive is located beneath the power supply.

**Figure 2-35** Raising the Power Supply



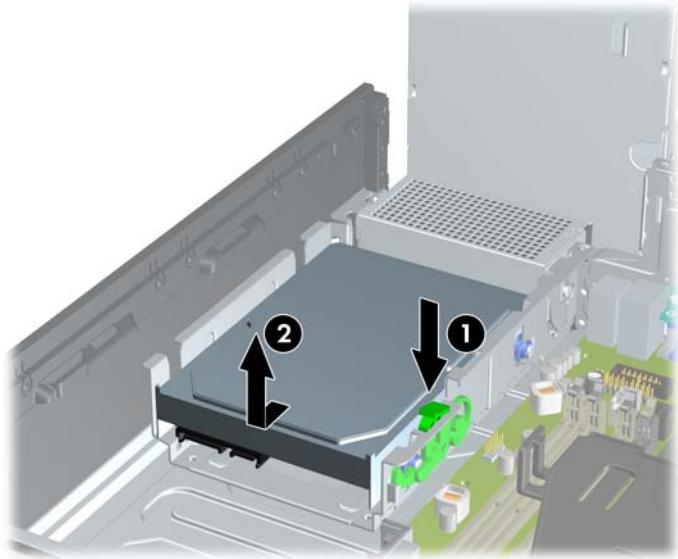
9. Disconnect the power cable (1) and data cable (2) from the back of the hard drive.

**Figure 2-36** Disconnecting the Hard Drive Power Cable and Data Cable



10. Press down on the green release latch next to the hard drive (1). While holding the latch down, slide the drive forward until it stops, then lift the drive up and out of the bay (2).

**Figure 2-37** Removing the Hard Drive



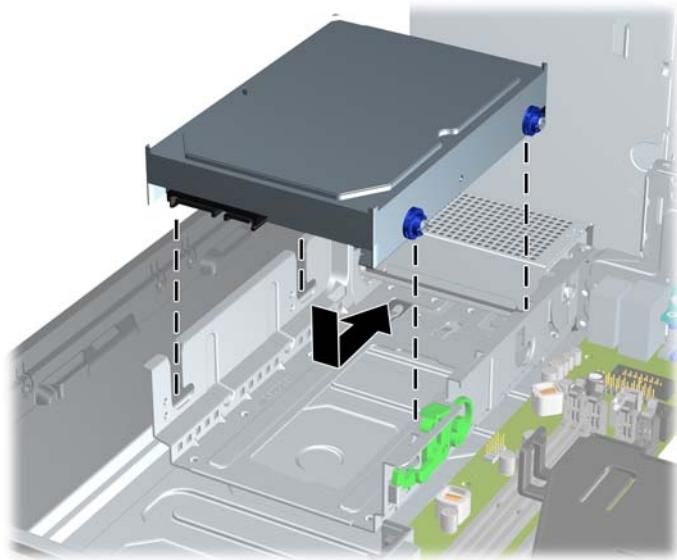
11. To install a hard drive, you must transfer the silver and blue isolation mounting guide screws from the old hard drive to the new hard drive.

**Figure 2-38** Installing Hard Drive Guide Screws



12. Align the guide screws with the slots on the chassis drive cage, press the hard drive down into the bay, then slide it back until it stops and locks in place.

**Figure 2-39** Installing the Hard Drive



13. Connect the power and data cables to the back of the hard drive.

**NOTE:** When replacing the primary hard drive, be sure to route the SATA and power cables through the cable guide on the bottom of the chassis frame behind the hard drive.

If the system has only one SATA hard drive, the data cable must be connected to the dark blue connector labeled SATA0 on the system board to avoid any hard drive performance problems.

14. Rotate the drive cage for external drives and the power supply down to their normal positions.
15. Replace the access panel.
16. If the computer was on a stand, replace the stand.
17. Reconnect the power cord and turn on the computer.
18. Lock any security devices that were disengaged when the access panel was removed.

## Removing and Replacing a Removable 3.5-inch SATA Hard Drive

Some models are equipped with a Removable SATA Hard Drive Enclosure in the 5.25-inch external drive bay. The hard drive is housed in a carrier that can be quickly and easily removed from the drive bay. To remove and replace a drive in the carrier:

**NOTE:** Before you remove the old hard drive, be sure to back up the data from the old hard drive so that you can transfer the data to the new hard drive.

1. Unlock the hard drive carrier with the key provided and slide the carrier out of the enclosure.

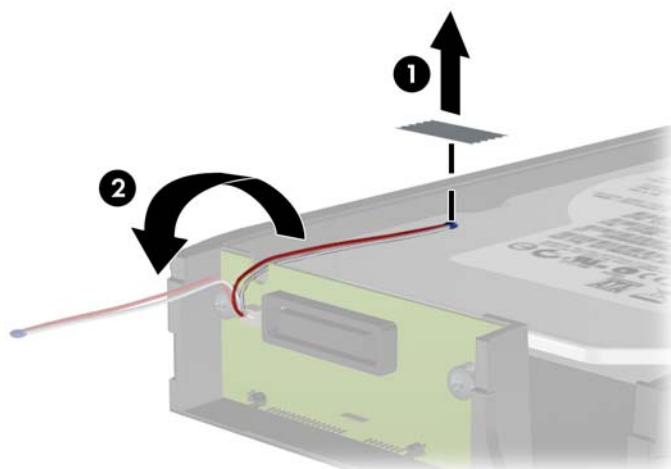
2. Remove the screw from the rear of the carrier (1) and slide the top cover off the carrier (2).

**Figure 2-40** Removing the Carrier Cover



3. Remove the adhesive strip that secures the thermal sensor to the top of the hard drive (1) and move the thermal sensor away from the carrier (2).

**Figure 2-41** Removing the Thermal Sensor



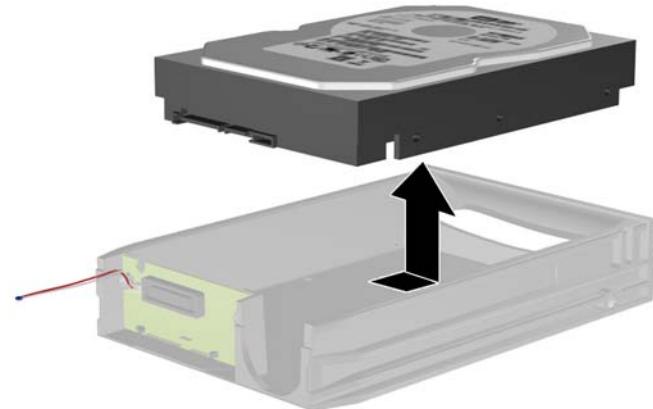
4. Remove the four screws from the bottom of the hard drive carrier.

**Figure 2-42** Removing the Security Screws



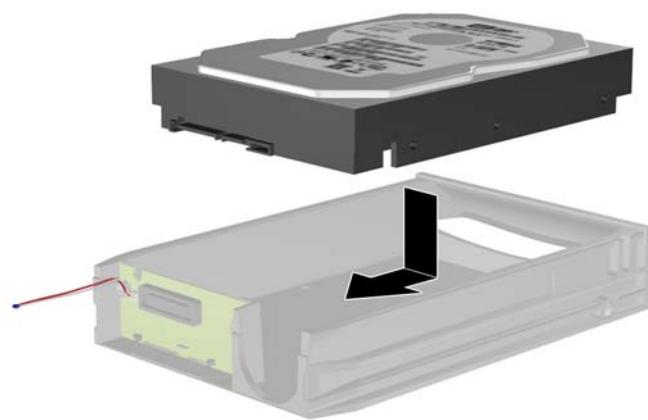
5. Slide the hard drive back to disconnect it from the carrier then lift it up and out of the carrier.

**Figure 2-43** Removing the Hard Drive



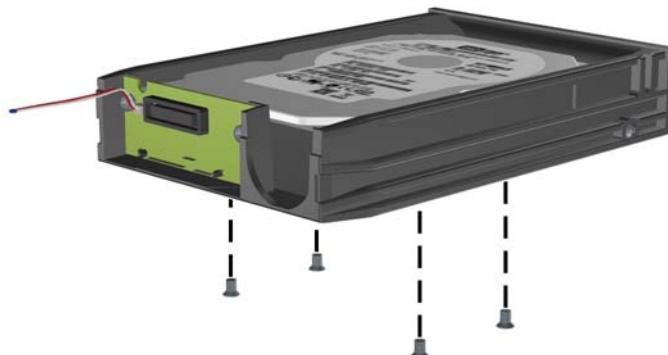
6. Place the new hard drive in the carrier then slide the hard drive back so that it seats in the SATA connector on the carrier's circuit board. Be sure the connector on the hard drive is pressed all the way into the connector on the carrier's circuit board.

**Figure 2-44** Replacing the Hard Drive



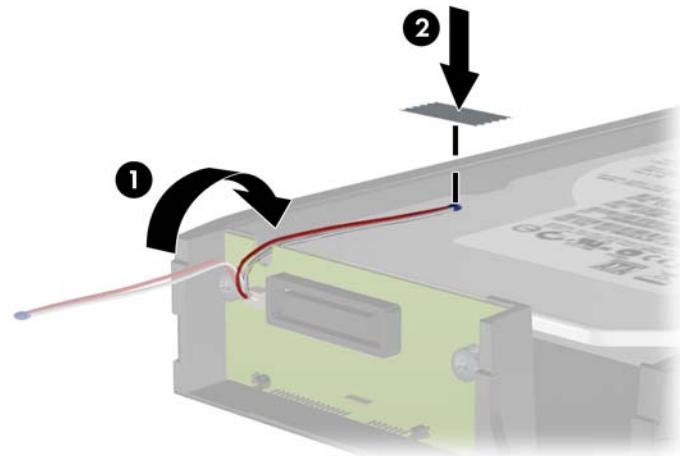
7. Replace the four screws in the bottom of the carrier to hold the drive securely in place.

**Figure 2-45** Replacing the Security Screws



8. Place the thermal sensor on top of the hard drive in a position that does not cover the label (1) and attach the thermal sensor to the top of the hard drive with the adhesive strip (2).

**Figure 2-46** Replacing the Thermal Sensor



9. Slide the cover on the carrier (1) and replace the screw on the rear of the carrier to secure the cover in place (2).

**Figure 2-47** Replacing the Carrier Cover



10. Slide the hard drive carrier into the enclosure on the computer and lock it with the key provided.

**NOTE:** The carrier must be locked for power to be supplied to the hard drive.

# A Specifications

**Table A-1 Specifications**

Desktop Dimensions (in the desktop position)		
Height	3.95 in	10.0 cm
Width	13.3 in	33.8 cm
Depth	14.9 in	37.8 cm
Approximate Weight	16.72 lb	7.6 kg
Weight Supported (maximum distributed load in desktop position)	77 lb	35 kg
Temperature Range		
Operating	50° to 95°F	10° to 35°C
Nonoperating	-22° to 140°F	-30° to 60°C
<b>NOTE:</b> Operating temperature is derated 1.0° C per 300 m (1000 ft) to 3000 m (10,000 ft) above sea level; no direct sustained sunlight. Maximum rate of change is 10° C/Hr. The upper limit may be limited by the type and number of options installed.		
Relative Humidity (noncondensing)		
Operating	10-90%	10-90%
Nonoperating (38.7°C max wet bulb)	5-95%	5-95%
Maximum Altitude (unpressurized)		
Operating	10,000 ft	3048 m
Nonoperating	30,000 ft	9144 m
Heat Dissipation		
Max STD PS	1063 BTU/hr	268 kg-cal/hr
Typical STD PS idle	198 BTU/hr	50 kg-cal/hr
Max EPA 87/89/85% @ 20/50/100% load PS	941 BTU/hr	237 kg-cal/hr
Typical EPA 87/89/85% @ 20/50/100% load PS idle	150 BTU/hr	38 kg-cal/hr
Power Supply		
Operating Voltage Range (STD PS)	90-264 VAC	90-264 VAC
Operating Voltage Range (EPA 87/89/85% @ 20/50/100% load PS)	90-264 VAC	90-264 VAC
Rated Voltage Range (STD PS)	100-240 VAC	100-240 VAC
Rated Voltage Range (EPA 87/89/85% @ 20/50/100% load PS)	100-240 VAC	100-240 VAC

**Table A-1 Specifications (continued)**

Rated Line Frequency	50-60 Hz	50-60 Hz
<b>Power Output</b>	240W	240W
<b>Rated Input Current (maximum)<sup>1</sup></b>		
STD PS	4A @ 100 VAC	2A @ 230 VAC
EPA 87/89/85% @ 20/50/100% load PS	4A @ 100 VAC	2A @ 230 VAC

<sup>1</sup> This system utilizes an active power factor corrected power supply. This allows the system to pass the CE mark requirements for use in the countries of the European Union. The active power factor corrected power supply also has the added benefit of not requiring an input voltage range select switch.

---

## B Battery Replacement

The battery that comes with the computer provides power to the real-time clock. When replacing the battery, use a battery equivalent to the battery originally installed in the computer. The computer comes with a 3-volt lithium coin cell battery.

**⚠ WARNING!** The computer contains an internal lithium manganese dioxide battery. There is a risk of fire and burns if the battery is not handled properly. To reduce the risk of personal injury:

Do not attempt to recharge the battery.

Do not expose to temperatures higher than 60°C (140°F).

Do not disassemble, crush, puncture, short external contacts, or dispose of in fire or water.

Replace the battery only with the HP spare designated for this product.

**⚠ CAUTION:** Before replacing the battery, it is important to back up the computer CMOS settings. When the battery is removed or replaced, the CMOS settings will be cleared.

Static electricity can damage the electronic components of the computer or optional equipment. Before beginning these procedures, ensure that you are discharged of static electricity by briefly touching a grounded metal object.

**💡 NOTE:** The lifetime of the lithium battery can be extended by plugging the computer into a live AC wall socket. The lithium battery is only used when the computer is NOT connected to AC power.

HP encourages customers to recycle used electronic hardware, HP original print cartridges, and rechargeable batteries. For more information about recycling programs, go to <http://www.hp.com/recycle>.

1. Remove/disengage any security devices that prohibit opening the computer.
2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
3. Turn off the computer properly through the operating system, then turn off any external devices.
4. Disconnect the power cord from the power outlet and disconnect any external devices.

**⚠ CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.

5. If the computer is on a stand, remove the computer from the stand.
6. Remove the access panel.
7. Locate the battery and battery holder on the system board.

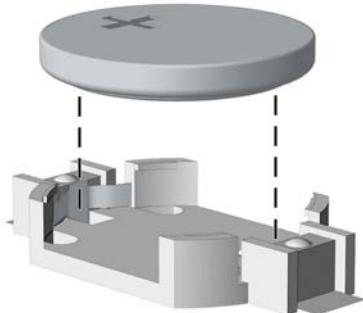
 **NOTE:** On some computer models, it may be necessary to remove an internal component to gain access to the battery.

8. Depending on the type of battery holder on the system board, complete the following instructions to replace the battery.

#### Type 1

- a. Lift the battery out of its holder.

**Figure B-1** Removing a Coin Cell Battery (Type 1)

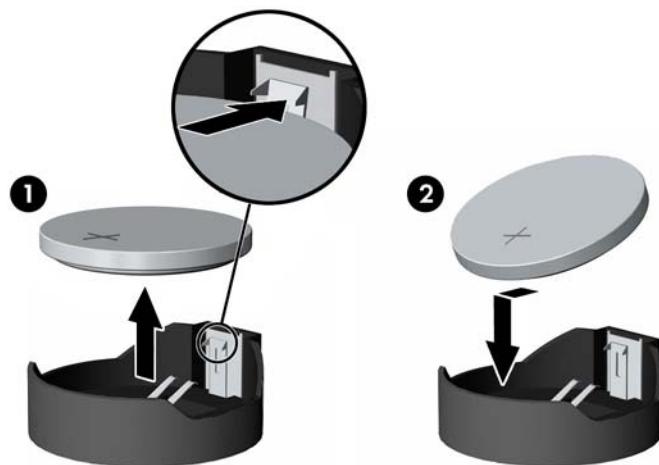


- b. Slide the replacement battery into position, positive side up. The battery holder automatically secures the battery in the proper position.

#### Type 2

- a. To release the battery from its holder, squeeze the metal clamp that extends above one edge of the battery. When the battery pops up, lift it out (1).
- b. To insert the new battery, slide one edge of the replacement battery under the holder's lip with the positive side up. Push the other edge down until the clamp snaps over the other edge of the battery (2).

**Figure B-2** Removing and Replacing a Coin Cell Battery (Type 2)

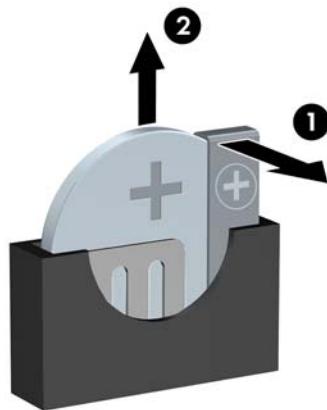


#### Type 3

- a. Pull back on the clip (1) that is holding the battery in place, and remove the battery (2).

- b. Insert the new battery and position the clip back into place.

**Figure B-3** Removing a Coin Cell Battery (Type 3)



 **NOTE:** After the battery has been replaced, use the following steps to complete this procedure.

9. Replace the access panel.
10. If the computer was on a stand, replace the stand.
11. Plug in the computer and turn on power to the computer.
12. Reset the date and time, your passwords, and any special system setups using Computer Setup.
13. Lock any security devices that were disengaged when the access panel was removed.

# C External Security Devices

 **NOTE:** For information on data security features, refer to the *Desktop Management Guide* and the *HP ProtectTools Security Manager Guide* (some models) at <http://www.hp.com>.

## Installing a Security Lock

The security locks displayed below and on the following pages can be used to secure the computer.

### HP/Kensington MicroSaver Security Cable Lock

**Figure C-1** Installing a Cable Lock



## Padlock

**Figure C-2** Installing a Padlock



## HP Business PC Security Lock

1. Fasten the security cable by looping it around a stationary object.

**Figure C-3** Securing the Cable to a Fixed Object



2. Thread the keyboard and mouse cables through the lock.

**Figure C-4** Threading the Keyboard and Mouse Cables



3. Screw the lock to the chassis using the screw provided.

**Figure C-5** Attaching the Lock to the Chassis



4. Insert the plug end of the security cable into the lock (1) and push the button in (2) to engage the lock. Use the key provided to disengage the lock.

**Figure C-6** Engaging the Lock



## Front Bezel Security

The front bezel can be locked in place by installing a security screw provided by HP. To install the security screw:

1. Remove/disengage any security devices that prohibit opening the computer.
2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
3. Turn off the computer properly through the operating system, then turn off any external devices.
4. Disconnect the power cord from the power outlet and disconnect any external devices.

△ **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.

5. If the computer is on a stand, remove the computer from the stand.
6. Remove the access panel and front bezel.

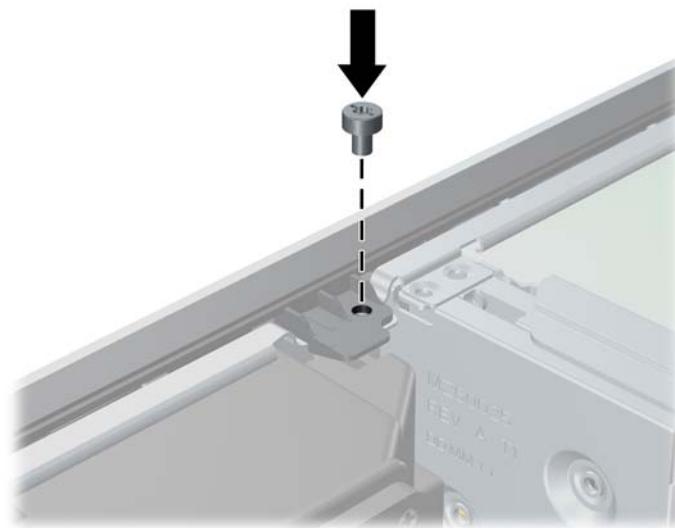
7. Remove one of the five silver 6-32 standard screws located on the front of the chassis behind the bezel.

**Figure C-7** Retrieving the Front Bezel Security Screw



8. Replace the front bezel.
9. Install the security screw next to the middle front bezel release tab to secure the front bezel in place.

**Figure C-8** Installing the Front Bezel Security Screw



10. Replace the access panel.
11. If the computer was on a stand, replace the stand.
12. Reconnect the power cord and turn on the computer.
13. Lock any security devices that were disengaged when the access panel was removed.

---

# D Electrostatic Discharge

A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

## Preventing Electrostatic Damage

To prevent electrostatic damage, observe the following precautions:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly.

## Grounding Methods

There are several methods for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm +/- 10 percent resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heelstraps, toestraps, or bootstraps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, contact an HP authorized dealer, reseller, or service provider.

---

 **NOTE:** For more information on static electricity, contact an HP authorized dealer, reseller, or service provider.

---

---

# E Computer Operating Guidelines, Routine Care and Shipping Preparation

## Computer Operating Guidelines and Routine Care

Follow these guidelines to properly set up and care for the computer and monitor:

- Keep the computer away from excessive moisture, direct sunlight, and extremes of heat and cold.
- Operate the computer on a sturdy, level surface. Leave a 10.2-cm (4-inch) clearance on all vented sides of the computer and above the monitor to permit the required airflow.
- Never restrict the airflow into the computer by blocking any vents or air intakes. Do not place the keyboard, with the keyboard feet down, directly against the front of the desktop unit as this also restricts airflow.
- Never operate the computer with the access panel or any of the expansion card slot covers removed.
- Do not stack computers on top of each other or place computers so near each other that they are subject to each other's re-circulated or preheated air.
- If the computer is to be operated within a separate enclosure, intake and exhaust ventilation must be provided on the enclosure, and the same operating guidelines listed above will still apply.
- Keep liquids away from the computer and keyboard.
- Never cover the ventilation slots on the monitor with any type of material.
- Install or enable power management functions of the operating system or other software, including sleep states.
- Turn off the computer before you do either of the following:
  - Wipe the exterior of the computer with a soft, damp cloth as needed. Using cleaning products may discolor or damage the finish.
  - Occasionally clean the air vents on all vented sides of the computer. Lint, dust, and other foreign matter can block the vents and limit the airflow.

# Optical Drive Precautions

Be sure to observe the following guidelines while operating or cleaning the optical drive.

## Operation

- Do not move the drive during operation. This may cause it to malfunction during reading.
- Avoid exposing the drive to sudden changes in temperature, as condensation may form inside the unit. If the temperature suddenly changes while the drive is on, wait at least one hour before you turn off the power. If you operate the unit immediately, it may malfunction while reading.
- Avoid placing the drive in a location that is subject to high humidity, extreme temperatures, mechanical vibration, or direct sunlight.

## Cleaning

- Clean the panel and controls with a soft, dry cloth or a soft cloth lightly moistened with a mild detergent solution. Never spray cleaning fluids directly on the unit.
- Avoid using any type of solvent, such as alcohol or benzene, which may damage the finish.

## Safety

If any object or liquid falls into the drive, immediately unplug the computer and have it checked by an authorized HP service provider.

## Shipping Preparation

Follow these suggestions when preparing to ship the computer:

1. Back up the hard drive files on PD discs, tape cartridges, CDs, or USB flash drives. Be sure that the backup media is not exposed to electrical or magnetic impulses while stored or in transit.

---

 **NOTE:** The hard drive locks automatically when the system power is turned off.

---

2. Remove and store all removable media.
3. Turn off the computer and external devices.
4. Disconnect the power cord from the electrical outlet, then from the computer.
5. Disconnect the system components and external devices from their power sources, then from the computer.

---

 **NOTE:** Ensure that all boards are seated properly and secured in the board slots before shipping the computer.

---

6. Pack the system components and external devices in their original packing boxes or similar packaging with sufficient packing material to protect them.

# Index

- A**  
access panel  
    locking and unlocking 9, 52  
audio connectors 2, 4
- B**  
battery replacement 49
- C**  
computer  
    specifications 47  
computer access panel  
    removing 11  
    replacing 12  
computer operating guidelines 58  
connecting drive cables 29
- D**  
DIMMs. See memory  
drives  
    connecting cables 29  
    installing 29  
    locations 28
- E**  
electrostatic discharge, preventing  
    damage 57  
expansion card  
    installing 22  
    removing 22  
    slot locations 22  
expansion slot cover  
    removing 24  
    replacing 26
- F**  
FailSafe Key 9  
front bezel  
    removing 13  
    removing blanks 14
- G**  
guide screws 29
- H**  
hard drive  
    installing 39  
    installing secondary 38  
    removing 39  
headphone connector 2
- I**  
installation guidelines 8  
installing  
    battery 49  
    drive cables 29  
    expansion card 22  
    guide screws 29  
    hard drive 39  
    media card reader 38  
    memory 17  
    optical drive 33  
    removable hard drive 42  
    security locks 52
- K**  
keyboard  
    components 5  
    connector 4
- L**  
line-in connector 4  
line-out connector 4  
locks  
    cable lock 52  
    front bezel 55
- M**  
HP Business PC Security Lock 53  
padlock 53  
Smart Cover Lock 9
- N**  
media card reader  
    features 3  
    installing 38  
    removing 36  
memory  
    installing 17  
    populating sockets 18  
    specifications 17  
microphone connector 2  
monitor connector  
    DisplayPort 4  
    VGA 4  
mouse connector 4
- O**  
optical drive  
    cleaning 59  
    installing 33  
    precautions 59  
    removing 31
- P**  
PCI card 22, 25  
PCI Express card 22, 26  
power supply 47  
product ID location 7
- R**  
rear panel components 4  
removable hard drive  
    replacing 42

removing  
battery 49  
bezel blanks 14  
computer access panel 11  
expansion card 22  
expansion slot cover 24  
front bezel 13  
hard drive 39  
media card reader 36  
optical drive 31  
PCI card 25  
PCI Express card 26  
Smart Cover Lock 9

## S

security  
cable lock 52  
front bezel 55  
HP Business PC Security  
Lock 53  
padlock 53  
Smart Cover Lock 9  
serial connector 4  
serial number location 7  
shipping preparation 59  
Smart Cover Lock 9  
specifications  
computer 47  
memory 17  
system board drive  
connections 30

## T

tower orientation 16

## U

unlocking access panel 9, 52  
USB ports  
front panel 2  
rear panel 4

## V

ventilation guidelines 58

## W

Windows Logo key 5

# **Nmap Security Scanner: The Definitive Guide**

**Fyodor**

**Edited by**

**Nmap Security Scanner: The Definitive Guide**

by Fyodor

Edited by

First Edition

Published (TBA)

# Table of Contents

Preface.....	i
1. Foreword.....	i
2. What's Inside.....	i
3. Style Conventions.....	i
4. Examples .....	i
5. Comments and Questions.....	i
6. Acknowledgments .....	ii
<b>1. Getting Started with Nmap .....</b>	<b>1</b>
1.1. Introduction .....	1
1.2. Nmap overview and demonstration.....	1
1.2.1. Avatar Online .....	1
1.2.2. Saving the Human Race.....	6
1.2.3. MadHat in Wonderland.....	9
1.3. Legal issues .....	11
1.3.1. Is unauthorized port scanning a crime? .....	11
1.3.2. Can port scanning crash the target computer/networks? .....	16
1.3.3. Misc: Copyright, license, (lack of) warranty, export control information .....	16
<b>2. Obtaining, Installing, and Removing Nmap.....</b>	<b>20</b>
2.1. Introduction .....	20
2.1.1. Testing whether Nmap is already installed.....	20
2.1.2. Verifying the integrity of Nmap downloads .....	20
2.1.3. Command-line and graphical interfaces .....	21
2.2. UNIX Compilation and installation from source code.....	22
2.2.1. Configure directives .....	23
2.2.2. If you encounter compilation problems .....	24
2.3. Linux Distributions.....	25
2.3.1. RPM-based distributions (Red Hat, Mandrake, Suse, Fedora).....	25
2.3.2. Debian Linux .....	26
2.3.3. Gentoo Linux .....	26
2.3.4. Other Linux distributions.....	26
2.4. Windows .....	27
2.4.1. Command line .zip binaries .....	27
2.4.2. Nmapwin.....	29
2.4.3. Compile from source code.....	29
2.5. Sun Solaris.....	30
2.6. Apple Mac OS X .....	31
2.7. FreeBSD / OpenBSD / NetBSD .....	31
2.7.1. OpenBSD binary packages and source ports instructions .....	31
2.7.2. FreeBSD binary package and source ports instructions .....	32
2.7.3. NetBSD binary package instructions.....	32
2.8. Amiga, HP-UX, IRIX, and Other Platforms .....	33
2.9. [RECIPE] Installing Nmap on a PDA .....	33
2.9.1. Installing Nmap on the Zaurus .....	34
2.9.2. Using Nmap and NmapFE on the Zaurus.....	35
2.10. Removing Nmap.....	37

<b>3. Host Enumeration ("Ping Scanning") .....</b>	<b>39</b>
3.1. Introduction .....	39
3.2. Specifying Target Hosts and Networks .....	39
3.3. Host Enumeration Controls .....	39
3.3.1. List Scan (-sL) .....	39
3.3.2. Ping Scan (-sP) .....	40
3.3.3. Disable Ping (-p0).....	41
3.4. Host Enumeration Techniques.....	42
3.4.1. TCP SYN Ping (-PS[portlist]).....	43
3.4.2. TCP ACK Ping (-PA[portlist]).....	44
3.4.3. UDP Ping (-PU[portlist]) .....	45
3.4.4. ICMP Ping Types (-PE, -PP, and -PM).....	45
3.4.5. Default Combination (-PB) .....	45
3.4.6. ARP Scan (-P?).....	46
3.5. Putting it All Together: Host Enumeration Strategies.....	46
3.5.1. Related Options .....	46
3.5.2. Choosing and Combining Ping Options .....	48
3.6. Finding an Organization's IP addresses to Scan .....	51
3.7. Host Enumeration Code Algorithms .....	51
<b>4. Port Scanning Overview .....</b>	<b>53</b>
4.1. Introduction to Port Scanning .....	53
4.1.1. What exactly is a port? .....	53
4.1.2. What is port scanning?.....	56
4.1.3. Why scan ports?.....	57
4.2. A Quick Port Scanning Tutorial .....	58
4.3. Command-line flags .....	60
4.3.1. Selecting scan techniques .....	60
4.3.2. Selecting ports to scan .....	62
4.3.3. Timing-related options.....	62
4.3.4. Output format and verbosity options .....	63
4.3.5. Firewall and IDS evasion options .....	64
4.3.6. Specifying targets .....	65
4.3.7. Miscellaneous options .....	65
4.4. IPv6 Scanning [-6] .....	66
4.5. [RECIPE] Scanning a large network for a certain open TCP port.....	66
4.5.1. Problem.....	67
4.5.2. Solution.....	67
4.5.3. Discussion.....	67
4.5.4. See Also .....	72
<b>5. Port Scanning Techniques and Algorithms .....</b>	<b>73</b>
5.1. Introduction .....	73
5.2. TCP SYN (Stealth) Scan .....	74
5.3. TCP Connect() Scan.....	77
5.4. UDP Scan .....	79
5.4.1. Disambiguating open from filtered UDP ports.....	80
5.4.2. Speeding up UDP scans.....	82
5.5. TCP Null, FIN, and Xmas Scans.....	83

5.6. Custom scan types with --scanflags .....	86
5.6.1. Custom SYN/FIN scan .....	86
5.6.2. PSH scan .....	87
5.7. TCP ACK Scan.....	88
5.8. TCP Window Scan .....	89
5.9. TCP Maimon Scan .....	91
5.10. TCP Idle Scan.....	92
5.10.1. Finding a working idle scan zombie host .....	94
5.10.2. Executing an Idle scan .....	94
5.10.3. Idle scan implementation algorithms.....	95
5.11. IP Protocol Scan .....	99
5.12. TCP FTP Bounce Scan.....	101
5.13. Scan Code and Algorithms.....	102
5.13.1. Network condition monitoring .....	102
5.13.2. Host and port parallelization.....	103
5.13.3. Round trip time estimation .....	103
5.13.4. Congestion control.....	104
5.13.5. Port scan pings.....	104
5.13.6. Inferred neighbor times.....	104
5.13.7. Adaptive retransmission .....	105
5.13.8. Scan delay .....	105
<b>6. Optimizing Nmap Performance.....</b>	<b>106</b>
<b>7. Service and Application Version Detection.....</b>	<b>107</b>
7.1. Introduction .....	107
7.2. Usage/Examples .....	108
7.3. Technique Described .....	110
7.4. Technique Demonstrated.....	111
7.5. Post-processors.....	114
7.5.1. RPC Grinding .....	114
7.5.2. SSL Post-processor notes .....	115
7.6. nmap-service-probes File Format .....	116
7.6.1. The probe directive .....	116
7.6.2. The match directive .....	117
7.6.3. The softmatch directive.....	118
7.6.4. The ports and sslports directives.....	118
7.6.5. The totalwaitms directive .....	119
7.6.6. Putting it all together .....	119
7.7. Community Contributions.....	119
7.8. [RECIPE] Find all servers running an insecure or nonstandard version of an application.....	121
7.9. [RECIPE] Hack version detection to suit custom needs, such as open proxy detection.....	121
<b>8. OS Fingerprinting.....</b>	<b>122</b>
<b>9. Detecting and Subverting Firewalls and Intrusion Detection Systems.....</b>	<b>123</b>
9.1. Introduction .....	123
9.2. Why would whitehats ever do this?.....	123
9.3. Determining Firewall Rules .....	124
9.3.1. Standard SYN scan.....	124
9.3.2. ACK scan.....	125

9.3.3. IPID tricks.....	127
9.3.4. UDP version scanning .....	129
9.4. Bypassing Firewall Rules.....	130
9.4.1. Exotic scan flags .....	130
9.4.2. Source port manipulation.....	131
9.4.3. IPv6 attacks.....	132
9.4.4. IPID Idle Scanning .....	133
9.4.5. Multiple ping probes.....	133
9.4.6. Fragmentation.....	134
9.4.7. Proxies .....	134
9.4.8. Source routing.....	135
9.4.9. FTP Bounce Scan .....	135
9.4.10. Take an alternative path .....	135
9.5. Subverting Intrusion Detection Systems .....	136
9.5.1. Intrusion detection system detection .....	136
9.5.2. Avoiding intrusion detection systems.....	138
9.5.3. Misleading intrusion detection systems.....	142
9.5.4. Exploiting intrusion detection systems.....	144
9.5.5. Ignoring intrusion detection systems .....	145
9.6. Detecting packet forgery by firewall and intrusion detection systems.....	145
9.6.1. Look for TTL consistency .....	146
9.6.2. Look for IPID and sequence number consistency .....	147
9.6.3. The Bogus Checksum trick.....	147
9.6.4. Close Analysis of packet headers and contents .....	148
9.6.5. Unusual network uniformity .....	148
<b>10. Defenses against Nmap .....</b>	<b>149</b>
10.1. Introduction .....	149
10.2. Proactive Scanning .....	149
10.3. Blocking and Slowing Nmap with Firewalls.....	149
10.4. Detecting Nmap Scans .....	150
10.5. Clever Trickery .....	151
10.5.1. Hiding Services on Obscure Ports .....	152
10.5.2. Port knocking.....	153
10.5.3. Honeypots and Honeynets .....	154
10.5.4. OS Spoofing.....	155
10.5.5. Tar pits .....	156
10.5.6. Reactive port scan detection .....	156
10.5.7. Escalating arms race .....	157
<b>11. Nmap Output Formats .....</b>	<b>158</b>
11.1. Introduction .....	158
11.2. Command-line flags .....	159
11.2.1. Controlling output type.....	159
11.2.2. Controlling verbosity of output .....	160
11.2.3. Enabling debugging output.....	163
11.2.4. Enabling packet tracing .....	164
11.2.5. Resuming canceled scans .....	165
11.3. Interactive output.....	165

11.4. Normal output (-oN) .....	165
11.5. \$crIpT kIddI3 0uTPut (-oS) .....	166
11.6. XML output (-oX).....	167
11.6.1. Using XML Output.....	169
11.7. Manipulating XML output with Perl.....	170
11.8. Output to a database .....	172
11.9. Creating HTML reports.....	173
11.10. Grepable output (-oG).....	173
11.10.1. Grepable output fields.....	174
11.10.2. Parsing grepable output on the command line.....	178
<b>12. Understanding and Customizing Nmap Data Files .....</b>	<b>179</b>
12.1. Introduction .....	179
12.2. nmap-services .....	179
12.3. nmap-service-probes.....	180
12.4. nmap-rpc.....	181
12.5. nmap-os-fingerprints.....	182
12.6. nmap-mac-prefixes .....	183
12.7. nmap-protocols.....	183
12.8. Using Customized Data Files.....	184
<b>13. Nmap Cookbook .....</b>	<b>186</b>
<b>14. The History and Future of Nmap .....</b>	<b>187</b>
<b>15. Nmap Reference Guide.....</b>	<b>188</b>
<b>A. Nmap XML Output DTD .....</b>	<b>189</b>
A.1. .....	189
<b>B. Appendix A: Complementary Tools .....</b>	<b>195</b>

# List of Tables

2-1. The Sharp Zaurus is an excellent platform for highly mobile security applications.....	33
3-1. Valuable TCP probe ports, in descending order of accessibility.....	48
5-1. ICMP destination unreachable (type 3) code values .....	74
5-2. How Nmap interprets responses to a SYN probe .....	76
5-3. How Nmap interprets responses to a UDP probe .....	79
5-4. How Nmap interprets responses to a Null, FIN, or Xmas scan probe.....	83
5-5. How Nmap interprets responses to an ACK scan probe.....	88
5-6. How Nmap interprets responses to a Window scan ACK probe .....	89
5-7. How Nmap interprets responses to a Maimon scan probe .....	91
5-8. How Nmap interprets responses to an IP protocol probe .....	100

# List of Figures

1-1. Trinity begins her assault.....	7
1-2. Trinity Scans the Matrix .....	8
1-3. Terminal-view of the hack .....	8
1-4. Strong opinions on port scanning legality and morality.....	11
2-1. NmapFE presents a simple graphical interface to Nmap .....	21
2-2. Executing Nmap from a Windows command shell .....	28
2-3. NmapWin provides a slick Windows interface to Nmap.....	29
2-4. The Sharp Zaurus SL-C760 PDA .....	36
2-5. The SL-C760 executing Nmap in a terminal window .....	36
4-1. IPv4 Header Layout.....	53
4-2. TCP Header Layout.....	53
4-3. UDP Header Layout .....	54
5-1. ICMPv4 Destination Unreachable Header Layout.....	73
5-2. SYN scan of open port 22.....	75
5-3. SYN scan of closed port 113 .....	75
5-4. SYN scan of filtered port 139 .....	76
5-5. Connect scan of open port 22 ( <b>nmap -sT -p22 scanme.nmap.org</b> ) .....	78
5-6. Idle Scan Technique (Simplified) .....	92
9-1. BlackIce discovers an unusual intruder .....	137
9-2. An attacker masked by dozens of decoys .....	142
11-1. Reading XML in a web browser.....	169

# List of Examples

1-1. Nmap list scan against Avatar Online IP addresses.....	2
1-2. Nmap results against an AO firewall .....	4
1-3. Another interesting AO machine .....	5
1-4. Nmap-diff typical output .....	10
1-5. Nmap-report execution .....	11
2-1. Checking for Nmap and determining its version number.....	20

2-2. Verifying the Nmap download checksum.....	21
2-3. Installing Nmap from binary RPMs .....	25
2-4. Building and installing Nmap from source RPMs.....	26
3-1. Enumerating hosts surrounding WWW.Stanford.Edu with list scan.....	40
3-2. Attempts to ping popular Internet hosts .....	42
3-3. Retry Host Enumeration using port 80 SYN probes .....	43
3-4. Attempted ACK ping against Microsoft.....	44
3-5. Generating 50,000 IP Addresses, then ping scanning with default options .....	50
3-6. Repeating ping scan with extra probes .....	51
4-1. Viewing and increasing the ephemeral port range on Linux .....	55
4-2. Simple scan: nmap scanme.nmap.org.....	58
4-3. More complex: nmap -p0- -v -A -T4 scanme.nmap.org.....	59
4-4. A simple IPv6 scan.....	66
4-5. Discovering Playboy's IP space.....	67
4-6. Pinging Playboy's Web Server for a Latency Estimate .....	68
4-7. Digging through Playboy's DNS records .....	68
4-8. Pinging the MX servers .....	69
4-9. TCP Pinging the MX servers.....	70
4-10. Launching the scan .....	71
4-11. Egrep for open ports .....	71
5-1. A SYN Scan showing three port states.....	74
5-2. Using --packet_trace to understand a SYN scan.....	77
5-3. Connect scan example .....	78
5-4. UDP scan example.....	79
5-5. UDP scan example.....	80
5-6. Improving Felix's UDP scan results with version detection .....	80
5-7. Improving Scanme's UDP scan results with version detection .....	81
5-8. Attempting to disambiguate UDP ports with TTL discrepancies.....	81
5-9. Example FIN and Xmas scans.....	84
5-10. SYN scan of docsrv.caldera.com .....	85
5-11. FIN scan of docsrv.caldera.com .....	85
5-12. A SYN/FIN scan of Google.....	87
5-13. A custom PSH scan .....	87
5-14. A Typical ACK Scan .....	88
5-15. An ACK scan of Docsrv .....	89
5-16. Window scan of docsrv.caldera.com .....	90
5-17. A failed Maimon scan.....	91
5-18. An Idle scan against the RIAA .....	95
5-19. IPID scan packet trace .....	96
5-20. IP protocol scan of a router and a typical Linux 2.4 box.....	100
5-21. Attempting an FTP bounce scan.....	101
5-22. Successful FTP bounce scan.....	102
7-1. Simple usage of version detection .....	107
7-2. Version detection against WWW.Microsoft.Com .....	108
7-3. Complex version detection .....	109
7-4. Detailed trace of version detection .....	111
7-5. Enumerating RPC services with rpcinfo .....	114
7-6. Nmap direct RPC scan.....	115

7-7. Version scanning through SSL .....	116
9-1. Detection of closed and filtered TCP ports.....	124
9-2. ACK scan against Scanme.....	125
9-3. Contrasting SYN and ACK scans against Para .....	126
9-4. UDP scan against firewalled host .....	129
9-5. UDP version scan against firewalled host.....	130
9-6. FIN scan against stateless firewall .....	130
9-7. Bypassing Windows IPsec filter using source port 88.....	131
9-8. Comparing IPv4 and IPv6 scans.....	132
9-9. Exploiting a printer with the FTP bounce scan .....	135
9-10. Host names can be deceiving.....	137
9-11. Noting TTL gaps with traceroute .....	138
9-12. Slow scan to bypass the default Snort 2.2.0 Flow-portscan fixed time scan detection method .....	139
9-13. Default Snort rules referencing Nmap.....	141
9-14. Detection of closed and filtered TCP ports.....	146
9-15. Testing IPID sequence number consistency .....	147
10-1. An all-tcp-port version scan .....	152
10-2. Deceiving Nmap with IP Personality .....	155
11-1. Scanrand output against a local network .....	158
11-2. Grepding for verbosity conditionals .....	161
11-3. A comparison of interactive output with and without verbosity enabled.....	162
11-4. Some representative debugging lines .....	163
11-5. Using --packet_trace to detail a ping scan of Scanme .....	164
11-6. A typical example of normal output .....	166
11-7. A typical example of \$crIpt KiDDi3 0utPut.....	166
11-8. An example of Nmap XML output.....	167
11-9. Nmap XML port elements.....	168
11-10. Nmap::Parser sample code .....	171
11-11. Nmap::Scanner sample code .....	172
11-12. A typical example of grepable output.....	173
11-13. Grepable output for IP protocol scan.....	176
11-14. Ping scan grepable output.....	177
11-15. List scan grepable output.....	177
11-16. Parsing grepable output on the command line.....	178
12-1. Excerpt from nmap-services .....	179
12-2. Excerpt from nmap-service-probes .....	181
12-3. Excerpt from nmap-rpc .....	181
12-4. Excerpt from nmap-os-fingerprints.....	182
12-5. Excerpt from nmap-mac-prefixes .....	183
12-6. Excerpt from nmap-protocols.....	184

# Preface

## 1. Foreword

Blah blah blah ... see preface example from dblite distribution when I am ready to write this section

## 2. What's Inside

The book is organized into the following chapters:

## 3. Style Conventions

Items appearing in the book are sometimes given a special appearance to set them apart from the regular text. Here's how they look:

## 4. Examples

The examples from this book are freely downloadable from the book's web site at  
<http://www.oreilly.com/catalog/learnxml>.

## 5. Comments and Questions

We have tested and verified the information in this book to the best of our ability, but you may find that features have changed (or even that we have made mistakes!). Please let us know about any errors you find, as well as your suggestions for future editions, by writing to:

O'Reilly & Associates, Inc.  
101 Morris Street  
Sebastopol, CA 95472  
(800) 998-9938 (in the United States or Canada)  
(707) 829-0515 (international or local)  
(707) 829-0104 (fax)

We have a web page for this book, where we list errata, examples, or any additional information. You can access this page at:

<http://www.oreilly.com/catalog/learnxml>

To comment or ask technical questions about this book, send email to:

[bookquestions@oreilly.com](mailto:bookquestions@oreilly.com)

You can sign up for one or more of our mailing lists at:

<http://elists.oreilly.com>

For more information about our books, conferences, software, Resource Centers, and the O'Reilly Network, see our web site at:

<http://www.oreilly.com>

## **6. Acknowledgments**

Thanks to everyone who contributed.....

# Chapter 1. Getting Started with Nmap

## 1.1. Introduction

On September 1, 1997, I released a security scanner named Nmap in the fifty-first issue of Phrack magazine. My goal was to consolidate the fragmented field of special-purpose port scanners into one powerful and flexible free tool, providing a consistent interface and efficient implementation of all practicable port scanning techniques. Nmap then consisted of 3 files (barely 2,000 lines of code) and supported only the Linux operating system. It was written for my own purposes, and released in the hope that others would find it useful.

From these humble beginnings, and through the power of Open Source development, Nmap grew into the world's most popular network security scanner<sup>1</sup>. Over the years, Nmap has continued to add advanced functionality such as remote OS detection via TCP/IP fingerprinting, version/service detection, IPID Idle scanning, and fast multi-probe ping scanning. All major Windows and UNIX platforms are now supported. Nmap has been recognized as "security tool of the year" by publications including *Linux Journal*, *Info World*, *LinuxQuestions.Org*, and the *Codetalker Digest*. It was even featured in several movies, including the 2003 hit *The Matrix Reloaded*.

Nmap was designed for security auditors to explore a network and discover potential vulnerabilities. Many systems and network administrators have also found it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

This chapter uses fictional stories to provide a broad overview of Nmap and how it is typically used. An important legal section helps users avoid (or at least be aware of) controversial usage that could leave them expelled from their ISP or even facing civil or criminal charges. It also discusses the risks of crashing remote machines as well as miscellaneous issues such as the Nmap license (GNU GPL), copyright, and export control restrictions. Readers can then move to chapter two (download/installation) with an understanding of why to use Nmap and how to do so safely.

## 1.2. Nmap overview and demonstration

Sometimes the best way to understand something is to see it in action. This section includes examples of Nmap being used in (mostly) fictional yet typical circumstances. Nmap newbies should not expect to understand everything at once. This is simply a broad overview of features that are described in depth in later chapters. The "recipes" included throughout this book (index in Chapter 11) demonstrate many other common Nmap tasks for both security auditors and network administrators.

### 1.2.1. Avatar Online

Felix dutifully arrives at work on December 15th, although he does not expect many structured tasks. The small San Francisco penetration-testing firm he works for has been very quiet lately, due to impending holidays. Felix is able to spend business hours pursuing his latest hobby of building powerful Wi-Fi antennas for wireless assessments and war driving exploration. Nevertheless, Felix is hoping for more business. Hacking has been his hobby and fascination since a childhood spent learning everything he could about networking, security, UNIX, and phone systems. Occasionally his curiosity took him too far, and Felix was almost swept up in the 1990 Operation Sundevil prosecutions. Fortunately Felix emerged from adolescence without a criminal record, while retaining his expert knowledge of security weaknesses. As a professional, he is now able to perform the same types of network intrusions as before, but with the added benefit of contractual immunity from prosecution and even a paycheck! Rather than having to keep his creative exploits secret, he is able to brag about them to client management when presenting his

reports. So Felix was not disappointed when his boss interrupted his antenna soldering to announce that the sales department finally closed a pen-testing deal with the Avatar Online gaming company.

Avatar Online (AO) is a small company working to create the next generation of massive multi-player online role-playing games (MMORPGs). Their product, inspired by the Metaverse envisioned in Neil Stevenson's *Snow Crash*, is fascinating but still highly confidential. After witnessing the high-profile leak (<http://www.smh.com.au/articles/2003/10/03/1064988378345.html>) of Valve Software's upcoming game source code, AO quickly hired the security consultants. Felix's task is to initiate an external (from outside the firewall) vulnerability assessment while his partners work on physical security, source code auditing, social engineering, and so forth. Felix is permitted to exploit any vulnerabilities found.

The first step in a vulnerability assessment is network discovery. This reconnaissance stage determines what IP address ranges the target is using, what hosts are available and what services those hosts are offering, general network topology details, and what firewall/filtering policies are in effect.

Determining the IP ranges to scan would normally be an elaborate process involving ARIN (or other geographical registry) lookups, DNS queries and zone transfer attempts, various web sleuthing techniques, and more. But in this case, Avatar Online explicitly specified what networks they want tested: the corporate network on 6.209.42.0/24 and their production/DMZ systems residing on 6.207.0.0/22. Felix checks the ARIN IP allocation records anyway and confirms that these IP ranges belong to AO<sup>2</sup>. Felix subconsciously decodes the CIDR notation and recognizes this as 1,280 IP addresses. No problem.

Being the careful type, Felix first starts out with what is known as an Nmap list scan (-sL option). This Nmap feature simply enumerates every IP address in the given target netblock(s) and does a reverse-DNS lookup (unless -n was specified) on each. One reason to do this first is stealth. The names of the hosts can hint at potential vulnerabilities and allow for a better understanding of the target network, all without raising alarm bells<sup>3</sup>. Felix is doing this for another reason - to double-check that the IP ranges are correct. The systems administrator who provided the IPs might have made a mistake, and scanning the wrong company would be a disaster. The contract signed with Avatar Online may act as a get-out-of-jail-free card for penetrating their networks, but will not help if Felix accidentally roots another company's server! The command he uses and an excerpt of the results are shown in Example 1-1.

### **Example 1-1. Nmap list scan against Avatar Online IP addresses**

```
felix> nmap -sL 6.209.24.0/24 6.207.0.0/22

Starting nmap 3.49 ( http://www.insecure.org/nmap/ )
Host 6.209.24.0 not scanned
Host fw.corp.avataronline.com (6.209.24.1) not scanned
Host dev2.corp.avataronline.com (6.209.24.2) not scanned
Host 6.209.24.3 not scanned
Host 6.209.24.4 not scanned
Host 6.209.24.5 not scanned
...
Host dhcp-21.corp.avataronline.com (6.209.24.21) not scanned
Host dhcp-22.corp.avataronline.com (6.209.24.22) not scanned
Host dhcp-23.corp.avataronline.com (6.209.24.23) not scanned
Host dhcp-24.corp.avataronline.com (6.209.24.24) not scanned
Host dhcp-25.corp.avataronline.com (6.209.24.25) not scanned
Host dhcp-26.corp.avataronline.com (6.209.24.26) not scanned
...
Host 6.207.0.0 not scanned
Host gw.avataronline.com (6.207.0.1) not scanned
```

```

Host ns1.avataaronline.com (6.207.0.2) not scanned
Host ns2.avataaronline.com (6.207.0.3) not scanned
Host ftp.avataaronline.com (6.207.0.4) not scanned
Host 6.207.0.5 not scanned
Host 6.207.0.6 not scanned
Host www.avataaronline.com (6.207.0.7) not scanned
Host 6.207.0.8 not scanned
...
Host cluster-c120.avataaronline.com (6.207.2.120) not scanned
Host cluster-c121.avataaronline.com (6.207.2.121) not scanned
Host cluster-c122.avataaronline.com (6.207.2.122) not scanned
Host cluster-c123.avataaronline.com (6.207.2.123) not scanned
Host cluster-c124.avataaronline.com (6.207.2.124) not scanned
...
Host 6.207.3.253 not scanned
Host 6.207.3.254 not scanned
Host 6.207.3.255 not scanned
Nmap run completed -- 1280 IP addresses (0 hosts up) scanned in 330.694 seconds
felix>

```

Reading over the results, Felix finds that all of the machines with reverse-DNS entries resolve to Avatar Online. No other businesses seem to share the IP space. Moreover, these results give Felix a rough idea of how many machines are in use and a good idea of what many are used for. He is now ready to get a bit more intrusive and try a port scan. He uses Nmap features that try to determine the application and version number of each service listening on the network. He also requests that Nmap try to guess the remote operating system via a series of low-level TCP/IP probes known as OS fingerprinting. This sort of scan is not at all stealthy, but that does not concern Felix. He is interested in whether the admins of AO even notice these blatant scans. After a bit of consideration, Felix settles on the following command:

```
nmap -ss -p- -PS22,80,113,33334 -PA80,113,21000 -PU19000 -PE -A -T4 -oA
avatartcpscan-121503 6.209.24.0/24 6.207.0.0/22
```

These options are described in later chapters, but here is a quick summary of them.

**-sS**

Enables the efficient TCP port scanning technique known as SYN scan. Felix would have added a U at the end if he also wanted to do a UDP scan, but he is saving that for later. SYN scan is the default scan type, but stating it explicitly does not hurt.

**-p-**

Requests that Nmap scan *every* port from 1-65535. The default is to scan only ports one through 1024, plus about 600 others explicitly mentioned in the nmap-services database. This option format is simply a short cut for -p1-65535. He could have specified -p0-65535 if he wanted to scan the rather illegitimate port zero as well. The -p option has a very flexible syntax, even allowing the specification of a differing set of UDP and TCP ports.

**-PS22,80,113,33334 -PA80,113,21000 -PU19000 -PE**

These are all "ping" types used in combination to determine whether a host is really available and avoid wasting a lot of time scanning IP addresses that are not in use. This particular incantation sends a TCP SYN packet to ports 22, 80, 113, and 33334; a TCP ACK packet to ports 80, 113, and 21000; a UDP packet to port 19000; and

a normal ICMP echo request packet. If Nmap receives a response from the target host itself to any of these probes, it considers the host to be up and available for scanning. This is more extensive than the Nmap default, which simply sends an echo request and an ACK packet to port 80. In a pen-testing situation, you often want to scan every host even if they do not seem to be up. After all, they could just be heavily filtered in such a way that the probes you selected are ignored but some other obscure port may be available. To scan every IP whether it shows an available host or not, specify the `-P0` option instead of all of the above. Felix starts such a scan in the background, though it may take a day to complete.

#### `-A`

This shortcut option turns on *advanced* and *aggressive* features such as OS and service detection. At the time of this writing it is equivalent to `-sV -O` (version/service and remote operating system detection), though more features may be added to `-A` later.

#### `-T4`

Adjusts timing to the "aggressive" level (#4 of 5). This is the same as specifying `-T aggressive`, but does not require the same level of spelling competence. In general, the `-T4` option is recommended if the connection between you and the target networks are faster than modem dialups.

#### `-oA avatartcpscan-121503`

Outputs results in every format (normal, XML, grepable) to files named `avatartcpscan-121503.extension` where `extension` are `.nmap`, `.xml`, and `.gnmap` respectively. All of the output formats include the start date and time, but Felix likes to note the date explicitly in the filename. Normal output and errors are still sent to `stdout`<sup>4</sup> as well.

#### 6.209.24.0/24 6.207.0.0/22

These are the Avatar Online netblocks discussed above. They are given in CIDR notation, but Nmap allows them to be specified in many other formats. For example, `6.209.24.0/24` could instead be specified as `6.209.24.0-255`.

Since such a comprehensive scan against more than a thousand IP addresses could take a while, Felix simply starts it executing and resumes work on his Yagi antenna. A couple hours later he notices that it has finished and takes a peek at the results. Example 1-2 shows one of the machines discovered.

#### **Example 1-2. Nmap results against an AO firewall**

```
Interesting ports on fw.corp.avataronline.com (6.209.24.1):
(The 65530 ports scanned but not shown below are in state: filtered)
PORT      STATE    SERVICE        VERSION
22/tcp     open     ssh           OpenSSH 3.7.1p2 (protocol 1.99)
53/tcp     open     domain        ISC Bind 9.2.1
110/tcp    open     pop3          Courier pop3d
113/tcp    closed   auth
143/tcp    open     imap          Courier Imap 1.6.X - 1.7.X
3128/tcp   open     http-proxy    Squid webproxy 2.2.STABLE5
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 3.134 days (since Mon Dec 12 11:49:58 2003)
```

To the trained eye, this conveys substantial information about AO's security posture. Felix first notes the reverse DNS name - this machine is apparently meant to be a firewall for their corporate network. The next line is important, but all too often ignored. It states that the vast majority of the ports on this machine are in the `filtered` state. This means that Nmap is unable to reach the port because it is blocked by firewall rules. The fact that all ports except for a few chosen ones are in this state is a sign of security competence. Deny-by-default is a security mantra for good reasons - it means that even if someone accidentally left SunRPC (port 111) open on this machine, the firewall rules would prevent us (attackers) from communicating with it.

Felix then looks at every port line in turn. The first port is Secure Shell (OpenSSH). Version 3.7.1p2 is very recent (as of December 15, 2003). The administrators probably upgraded it because of the potentially exploitable buffer management bugs affecting earlier versions. This is another hint that the administrator knows what they are doing. A truly paranoid sysadmin would only allow ssh connections from certain trusted IP addresses, but one can argue for open access in case the administrator needs emergency access while far from home. Security often involves trade-offs, and this one may be justifiable. Felix makes a note to try his brute force password cracker and especially his private timing-based ssh user enumeration tool against the server.

Felix is not so charitable about port 53. It is running ISC bind, which has a long history of remotely exploitable security holes. Visit the Bind security page (<http://www.isc.org/products/BIND/bind-security.html>) for further details. Bind 9.2.1 even has a potentially exploitable buffer overflow, although the default build is not vulnerable. Felix checks and finds that this server is not vulnerable to the libbind issue, but that is besides the point. This server almost certainly should not be running an externally-accessible nameserver. A firewall should only run the bare essentials to minimize the risk of a disastrous compromise. Besides, this server is not authoritative for any domains - the real nameservers are on the production network. An administrator probably only meant for clients within the firewall to contact this nameserver, but he did not bother locking it down to only the internal interface. Felix will later try to gather important information from this unnecessary server using zone transfer requests and intrusive queries. He may attempt cache poisoning as well. By spoofing the IP of `windowsupdate.microsoft.com` or another important download server, Felix may be able to trick unsuspecting internal client users into running a trojan-horse program that provides him with full network access behind the firewall.

The next two open ports are 110 (pop3) and 143 (imap). Note that 113 (auth) in between them is `closed` instead of `open`. Pop3 and Imap are mail retrieval services which, like Named, have no legitimate place on this server. They are also a security risk in that they generally transfer the mail and (even worse) authentication credentials unencrypted. Users should probably VPN in and check their mail from an internal server. These ports could also be wrapped in SSL encryption. Nmap would have then listed the services as "ssl/pop3" and "ssl/imap". Felix will try his user enumeration and password guessing attacks on these services, which will probably be much more effective than against ssh.

The final open port is a Squid proxy. This is another service that may have been intended for internal client use and should not be accessible from the outside (and particularly not on the firewall). Felix's initially positive opinion of the AO security administrators drops further. Felix will test whether he can abuse this proxy to connect to other sites on the Internet. Spammers and malicious hackers often use proxies in this way to hide their tracks. Even more critical, Felix will try to proxy his way into the *internal* network. This common attack is how Adrian Lamo (<http://www.freelamo.org/>) broke into the New York Times internal network in 2002. Lamo was caught after he called reporters to brag about his exploits against the NY Times and other companies in detail (<http://www.securityfocus.com/news/340>).

The following lines disclose that this is a Linux box, which is valuable information when attempting exploitation. The low 3-day uptime was detected during OS fingerprinting by sending several probes for the TCP timestamp option value and extrapolating the line back to zero.

Felix then examines the Nmap output for another machine, as shown in Example 1-3

**Example 1-3. Another interesting AO machine**

```
Interesting ports on dhcp-23.corp.avataronline.com (6.209.24.23):
(The 65526 ports scanned but not shown below are in state: closed)
PORT      STATE     SERVICE      VERSION
135/tcp    filtered msrpc
136/tcp    filtered profile
137/tcp    filtered netbios-ns
138/tcp    filtered netbios-dgm
139/tcp    filtered netbios-ssn
445/tcp    open      microsoft-ds Microsoft Windows XP microsoft-ds
1002/tcp   open      windows-icfw?
1025/tcp   open      msrpc          Microsoft Windows msrpc
16552/tcp  open      unknown
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Professional RC1+ through final release
```

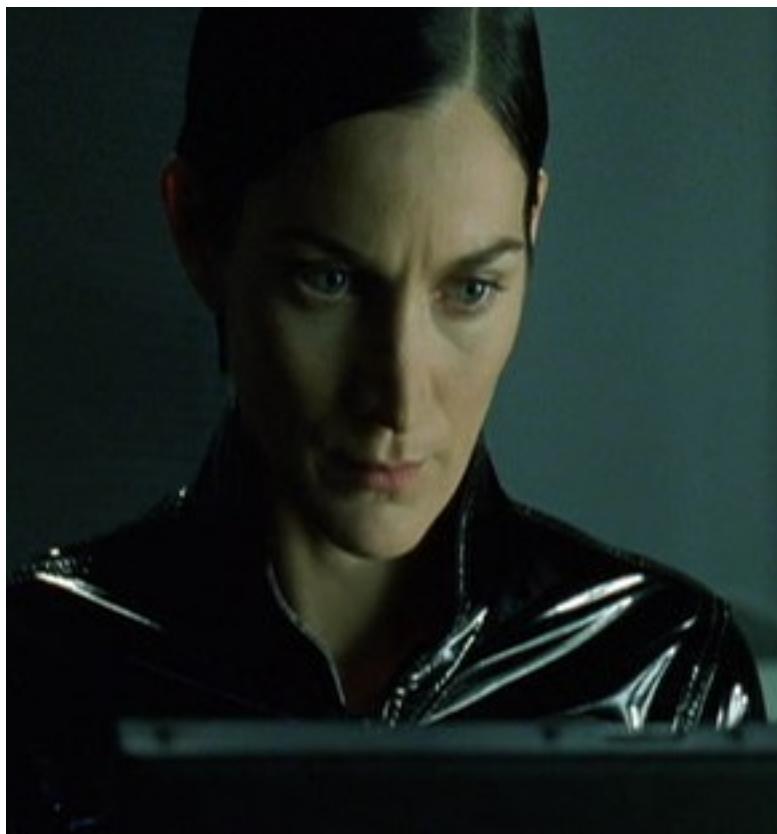
Felix smiles when he spies this Windows XP box on the Network. Thanks to a recent spate of MS RPC vulnerabilities, those machines are often trivial to compromise. The second line shows that the default state is closed, meaning the firewall does not have the same deny-by-default policy for this machine as for itself. Instead they tried to specifically block the Windows ports they consider dangerous on 135-139. This filter is woefully inadequate, as MS exports MS RPC functionality on many other ports in Windows XP. TCP ports 445 and 1025 are two examples on this scan. While Nmap failed to recognize 16552, Felix has seen this pattern enough to know that it is probably the MS Messenger Service. If AO had been using deny-by-default filtering, port 16552 would not be accessible in the first place. Looking through the results page, Felix sees several other Windows machines on this DHCP network. Felix cannot wait to try his favorite DCOM RPC exploit against them. It was written by HD Moore and is available at <http://www.metasploit.com/tools/dcom.c>. If that fails, there are a couple newer MS RPC vulnerabilities he will try.

Felix continues poring over the results for vulnerabilities he can leverage to compromise the network. On the production network, he sees that gw.avataronline.com is a Cisco router that also acts as a rudimentary firewall for the systems. They fall into the trap of only blocking "privileged ports" (those under 1024), which leaves a bunch of vulnerable SunRPC and other services accessible on that network. The machines with names like clust-\* each have dozens of ports open that Nmap does not recognize. There are probably custom daemons running the AO game engine. www.avataronline.com is a Linux box with an open Apache server on the http and https ports. Unfortunately, it is linked with an exploitable version of the OpenSSL library. Oops! Before the sun sets, Felix has gained privileged access to hosts on both the corporate and production networks.

*As Felix has demonstrated, Nmap is frequently used by security auditors and network administrators to help locate vulnerabilities on client/corporate networks. Subsequent chapters describe the techniques used by Felix, as well as many other Nmap features, in much greater detail.*

## 1.2.2. Saving the Human Race

**Figure 1-1. Trinity begins her assault**



Trinity is in quite a pickle! Having discovered that the world we take for granted is really a virtual "Matrix" run by machine overlords, Trinity decides to fight back and free the human race from this mental slavery. Making matters worse, her underground colony of freed humans (Zion) is under attack by 250,000 powerful alien sentinels. Her only hope involves deactivating the emergency power system for 27 city blocks in less than 5 minutes. The previous team died trying. In life's bleakest moments when all hope seems to be lost, what should you turn to? Nmap, of course! But not quite yet.

She first must defeat the perimeter security, which on many networks involves firewalls and intrusion detection systems (IDS). She is well aware of advanced techniques for circumventing these devices (covered later in this book). Unfortunately, the emergency power system admins knew better than to connect such a critical system to the Internet, even indirectly. No amount of source routing or IPID spoofed scanning will help Trinity overcome this "air gap" security. Thinking fast, she devises a clever plan that involves jumping her motorcycle off the rooftop of a nearby building, landing on the power station guard post, and then beating up all of the security guards. This advanced technique is not covered in any physical security manual, but proved highly effective. This demonstrates how clever hackers research and devise their own attacks, rather than always utilizing the script-kiddie approach of canned exploits.

Trinity fights her way to the computer room and sits down at a terminal. She quickly determines that the network is using the RFC1918-blessed 10.0.0.0/8 private network. A ping to the network address generates responses from dozens of machines. An Nmap "ping scan" would have provided a more comprehensive list of available machines,

but using the broadcast technique saved precious seconds. Then she whips out Nmap<sup>5</sup>. The terminal has version 2.54BETA25 installed. This version is ancient (2001) and less efficient than newer releases, but Trinity had no time to install a better version from the future. This job will not take long anyway. She runs the command **nmap -v -ss -o 10.2.1.3**. This executes a TCP SYN scan and OS detection against 10.2.1.3 and provides verbose output. The host appears to be a security disaster - AIX 3.2 with well over a dozen ports open. Unfortunately, this is not the machine she needs to compromise. So she runs the same command against 10.2.2.2. This time the target OS is unrecognized (she should have upgraded Nmap!) and only has port 22 open. This is the Secure Shell encrypted administration service. As any sexy PVC-clad hacker goddess knows, many SSH servers around that time (2001) had an exploitable vulnerability in the CRC32 compensation attack detector. Trinity whips out an all-assembly-code exploit written by her or her fallen comrade, and utilizes the exploit to change the root password of the target box to "Z10N0101". Trinity uses much more secure passwords under normal circumstances. She logs in as root and issues a command to disable the emergency backup power system for 27 city blocks, finishing just in time! Here are some shots of the action - squint just right and you should be able to read the text.

**Figure 1-2. Trinity Scans the Matrix**



**Figure 1-3. Terminal-view of the hack**

In addition, a terminal-view video showing the whole hack is available on the Internet. At least it will be until the MPAA finds out and sends sentinels or lawyers after the webmasters.

### 1.2.3. MadHat in Wonderland

This story differs from the previous ones in that it is actually true. Written by frequent Nmap user and contributor MadHat, it describes how he enhanced and customized Nmap for daily use in a large enterprise. In true open source spirit, he has released these valuable scripts on his Web site (<http://www.unspecific.com/.go/nmap/>). IP addresses have been changed to protect the corporate identity. The remainder of this section is in his own words.

After spending the past couple of decades learning computers and working my way up from tech support through sysadmin and into my dream job of Information Security Officer for a major Internet company, I found myself with a problem. I was handed the sole responsibility of security monitoring for our entire IP space. This was almost 50,000 hosts worldwide when I started several years ago, and it has doubled since then.

Scanning all of these machines for potential vulnerabilities as part of monthly or quarterly assessments would be tough enough, but management wanted it done daily. Attackers will not wait a week or month to exploit a newly exposed vulnerability, so I cannot wait that long either.

Looking around for tools, I quickly chose Nmap as my port scanner. It is widely considered to be the best scanner, and I had already been using it for years to troubleshoot networks and test security. Next I needed software to aggregate Nmap output and print differences between runs. I considered several existing tools, such as James Levine's NDiff (<http://www.vinecorp.com/ndiff/>), and HD Moore's Nlog (<http://www.secureaustin.com/nlog>). While these are great tools, they did not monitor changes in the way I desired. I had to know whenever a router or firewall access control list was misconfigured or a host was publicly sharing inappropriate content. I also worried about the scalability of these other solutions, so I decided to tackle the problem myself.

The first issue to come up was speed. Our networks are located worldwide, yet I was provided with only a single U.S.-based host to do the scanning. In many cases, firewalls between the sites slowed the scanning down significantly. Scanning all 100,000 hosts took over 30 hours, which is unacceptable for a daily scan. So I wrote a

script called nmap-wrapper which runs dozens of Nmap processes in parallel, reducing the scan time to fifteen hours, even including OS detection.

The next problem was dealing with so much data. A SQL database seemed like the best approach for scalability and data-mining reasons, but I had to abandon that idea due to time pressures. A future version may add this support. Instead, I used a flat file to store the results of each class C address range for each day. The most powerful and extensible way to parse and store this information was the Nmap XML format, but I chose the "grepable" (-oG option) format because it is so easy to parse from simple script. Per-host timestamps are also stored for reporting purposes. These have proven quite helpful when administrators try to blame machine or service crashes on the scanner. They cannot credibly claim a service crash at 7:12AM when I have proof that the scan ran at 9:45AM.

The describe process produces copious data, with no convenient access method. The standard UNIX **diff** tool is not smart enough to report only the changes I care about, so I wrote a Perl script named nmap-diff to provide daily change reports. A typical output report is shown in Example 1-4.

#### Example 1-4. Nmap-diff typical output

```
> nmap-diff.pl -c3
  5 IPs showed changes

  10.12.4.8 (ftp-box.foocompany.biz)
    21/tcp    open   ftp
    80/tcp    open   http
    443/tcp   open   https
    1027/tcp  open   IIS
    + 1029/tcp open   ms-lsa
    38292/tcp open   landesk-cba
  OS: Microsoft Windows Millennium Edition (Me)
      Windows 2000 Professional or Advanced Server
      or Windows XP

  10.16.234.3 (media.foocompany.biz)
    80/tcp    open   http
    + 554/tcp  open   rtsp
    + 7070/tcp open   realserver

  192.168.10.186 (testbox.foocompany.biz)
    + 8082/tcp open   blackice-alerts
  OS: Linux Kernel 2.4.0 - 2.5.20

  172.24.12.58 (mtafoocompany.biz)
    + 25/tcp    open   smtp
  OS: FreeBSD 4.3 - 4.4PRERELEASE

  172.23.76.22 (media2.foocorp.biz)
    80/tcp    open   http
    1027/tcp  open   IIS
    + 1040/tcp open   netsaint
    1755/tcp  open   wms
    3372/tcp  open   msdtc
    6666/tcp  open   irc-serv
    7007/tcp  open   afs3-bos
  OS: Microsoft Windows Millennium Edition (Me)
```

Windows 2000 Professional or Advanced Server  
or Windows XP

Management and staff were impressed when I demonstrated this new system at an internal company security symposium. But instead of allowing me to rest on my laurels, they began asking for new features. They wanted counts of mail and web servers, growth estimates, and more. This data was all available from the scans, but was difficult to access. So I created yet another Perl script, nmap-report, which made querying the data much easier. It takes specifications such as open ports or operating systems and finds all the systems that matched on a given day.

One problem with this approach to security monitoring is that employees do not always place services on their IANA-registered official ports. For example, they might put a web server on port 22 (ssh) or vice versa. Just as I was debating how to address this problem, Nmap came out with an advanced service and version detection system (see Chapter 7). Nmap-report now has a rescan feature that uses version scanning to report the true services rather than guessing based on port number. I hope to further integrate version detection in future versions. Example 1-5 shows nmap-report listing FTP servers.

#### **Example 1-5. Nmap-report execution**

```
> nmap-report -p21 -rV
[...]
172.21.199.76 (ftp1.foocorp.biz)
  21/tcp  open  ssl|ftp Serv-U ftpd 4.0

192.168.12.56 (ftp2.foocorp.biz)
  21/tcp  open  ftp      NcFTPD

192.168.13.130 (dropbox.foocorp.biz)
  21/tcp  open  ftp      WU-FTPD 6.00LS
```

While being far from perfect, these scripts have proven themselves quite valuable at monitoring large networks for security-impacting changes. Since Nmap itself is open source, it only seemed fair to release my scripts to the public as well. I have made them freely available at <http://www.unspecific.com/.go/nmap>.

## **1.3. Legal issues**

### **1.3.1. Is unauthorized port scanning a crime?**

The legal ramifications of scanning networks with Nmap are complex and so controversial that third-party organizations have printed T-shirts and bumper stickers promulgating opinions on the matter<sup>6</sup>.

**Figure 1-4. Strong opinions on port scanning legality and morality**



While I agree with the sentiment that port scanning *should not* be illegal, it is rarely wise to take legal advice from a T-shirt. Indeed, taking it from a software engineer and author is only slightly better. Speak to a competent lawyer within your jurisdiction for a better understanding of how the law applies to your particular situation. With that important disclaimer out of the way, here is some general information that may prove helpful.

The best way to avoid controversy when using Nmap is to always secure written authorization from the target network representatives before initiating any scanning. There is still a chance that your ISP will give you trouble if they notice it (or if the target admins accidentally send them an abuse report), but this is usually not terribly difficult to resolve. When you are performing a penetration test, this authorization should be in the Statement of Work. When testing your own company, make certain that this activity clearly falls within your job description. Security consultants should be familiar with the excellent Open Source Security Testing Methodology Manual (OSSTMM) (<http://www.osstmm.org/>), which provides current best practices for these situations.

While civil and (especially) criminal court cases are the nightmare scenario for Nmap users, these happen very rarely. After all, no US federal laws explicitly make port scanning illegal. A much more frequent occurrence is that the target network will notice a scan and then send a complaint to the network service provider where the scan initiated (your ISP). Most network admins do not seem to care or notice the many scans bouncing off their networks daily. But a few complain. The scanner's ISP may track down the user corresponding to the reported IP address and time, then chide the user or even kick them off the service. Port scanning without authorization is sometimes against the provider's acceptable use policy (AUP). For example, the AUP for the huge cable-modem ISP Comcast presently says<sup>7</sup>:

<sup>7</sup>"Network probing or port scanning tools are only permitted when used in conjunction with a residential home network, or if

explicitly authorized by the destination host and/or network. Unauthorized port scanning, for any reason, is strictly prohibited."

Even if an ISP does not explicitly ban unauthorized port scanning, they might claim that some "anti-hacking" provision applies. Of course this does *not* make port scanning illegal. Many perfectly legal and (in the United States) constitutionally protected activities are banned by ISPs. For example, the AUP quoted from above also prohibits users from transmitting, storing, or posting "any information or material which a reasonable person could deem to be objectionable, offensive, indecent, pornographic, ... embarrassing, distressing, vulgar, hateful, racially or ethnically offensive, or otherwise inappropriate, regardless of whether this material or its dissemination is unlawful." In other words, some ISPs ban any behavior that could possibly offend or annoy someone. Indiscriminate scanning of other people's networks/computers does have the potential to do so. If you decide to perform such controversial scanning anyway, never do it from work, school, or any other service provider that has substantial control over your well-being. Use a dialup or commercial broadband provider instead. Losing your DSL connection and having to change providers is a slight nuisance, but it is immeasurably preferable to being expelled or fired.

While legal cases involving port scanning (without follow-up hacking attacks) are rare, they do happen. One of the most notable cases involved a man named Scott Moulton who had an ongoing consulting contract to maintain the Cherokee County, Georgia emergency 911 system. In December 1999, he was tasked with setting up a router connecting the Canton, Georgia Police Department with the E911 Center. Concerned that this might jeopardize the E911 Center security, Moulton initiated some preliminary port scanning of the networks involved. In the process he scanned a Cherokee County web server that was owned and maintained by a competing consulting firm named VC3. They noticed the scan and emailed Moulton, who replied that he worked for the 911 Center and was testing security. VC3 then reported the activity to the police. Moulton lost his E911 maintenance contract and was arrested for allegedly violating the Computer Fraud and Abuse Act of America Section 1030(a)(5)(B)<sup>8</sup>. This act applies against anyone who "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage" (and meets other requirements). The damage claimed by VC3 involved time spent investigating the port scan and related activity. VC3 also filed a civil suit against Moulton claiming violation of the same act as well as the Georgia Computer Systems Protection Act, after Moulton sued VC3 for defamation.

The civil case against Moulton was dismissed before trial, implying a complete lack of merit. The ruling made many Nmap users smile:

"Court holds that plaintiff's act of conducting an unauthorized port scan and throughput test of defendant's servers does not constitute a violation of either the Georgia Computer Systems Protection Act or the Computer Fraud and Abuse Act." -- Civ. Act. No. 1:00-CV-434-TWT (N.D. Ga. November 6, 2000)

This was an exciting victory in the civil case, but Scott still had the criminal charges hanging over his head. Fortunately he kept his spirits high, sending the following note to the nmap-hackers mailing list<sup>9</sup>:

"I am proud that I could be of some benefit to the computer society in defending and protecting the rights of specialists in the computer field, however it is EXTREMELY costly to support such an effort, of which I am not happy about. But I will continue to fight and prove that there is nothing illegal about port scanning especially when I was just doing my job."

Eventually, the criminal court came to the same conclusion and all charges were dropped. While Moulton was vindicated in the end, he suffered six-figure legal bills and endured stressful years battling through the court system. While his case does set a good example (if not legal precedent), different courts or situations could still lead to worse outcomes. Remember that many states have their own computer abuse laws, some of which can arguably make even pinging a remote machine without authorization illegal<sup>10</sup>.

Laws in other nations obviously differ as well. For example, A 17-year-old youth was convicted in Finland (<http://www.osborneclarke.com/publications/text/ITM0903f.htm>) of attempted computer intrusion for simply port scanning a bank. He was fined to cover the target's investigation expenses. The Moulton court might also have ruled differently if the VC3 machine had actually crashed and they were able to justify the \$5,000 damage figure required by the act.

At the other extreme, an Israeli judge acquitted (<http://www.haaretz.com/hasen/spages/399602.html>) Avi Mizrahi in early 2004 for vulnerability scanning the Mossad secret service. Judge Abraham Tennenbaum even praised Avi as follows:

"In a way, Internet surfers who check the vulnerabilities of Web sites are acting in the public good. If their intentions are not malicious and they do not cause any damage, they should even be praised."

ISP accounts will continue to be terminated regardless of the legal status of port scanning if too many complaints are generated. The best way to avoid ISP abuse reports or civil/criminal charges is to avoid annoying the target network admins in the first place. Here are some practical suggestions:

- Probably at least 90% of network scanning is non-controversial. You are rarely badgered for scanning your own machine or the networks you administer. The controversy comes when scanning other networks. There are many reasons (good and bad) for doing this sort of network exploration. Perhaps you are scanning the other systems in your dorm or department to look for publicly shared files (FTP, SMB, WWW, etc.). Or maybe you are just trying to find the IP of a certain printer. You scanned your favorite web site to see if they are offering any other services, or because you were curious what OS they run. Perhaps you are just trying to test connectivity, or maybe you wanted to do a quick security sanity check before handing off your credit card details to that e-commerce company. You might be conducting Internet research. Or are you performing initial reconnaissance in preparation for a break-in attempt? The remote administrators rarely know your true intentions, and do sometimes get suspicious. The best approach is to get permission first. I have seen a few people with non-administrative roles land in hot water after deciding to "prove" network insecurity by launching an intrusive scan of the entire company or campus. Admins tend to be more cooperative when asked in advance than when woken up at 3AM by an IDS alarm claiming they are under massive attack. So whenever possible, obtain written authorization before scanning a network. Adrian Lamo would probably not be in jail at the time of this writing if he had asked the New York Times to test their security rather than telling reporters about the flaws afterward. Unfortunately they would likely have said no. Be prepared for this answer.
- Target your scan as tightly as possible. Any machine connected to the Internet is scanned regularly enough that most admins ignore such Internet "white noise". But scanning enough networks or executing very noisy/intrusive scans increases the probability of generating complaints. So if you are only looking for web servers, specify -p80 rather than scanning all 65,535 TCP ports on each machine. If you are only trying to find available hosts, do an Nmap ping scan rather than full port scan. Do not scan a CIDR /16 (65K hosts) when a /24 netblock suffices. The random scan mode now takes an argument specifying the number of hosts, rather than running forever. So consider -iR 1000 rather than -iR 10000 if the former is sufficient. Use the default timing (or even "-T Polite") rather than "-T Insane". Avoid noisy and relatively intrusive scans such as version detection (-sV). Similarly, a SYN scan (-sS) is quieter than a connect() scan (-sT) while providing the same information and often being faster.
- As noted previously, do not do anything controversial from your work or school connections. Even though your intentions may be good, you have too much to lose if someone in power (e.g. boss, dean) decides you are a malicious cracker. Do you really want to explain your actions to someone who may not even understand the terms "port scanner" or "packet"? Spend \$10-\$50 bucks a month for a dialup, shell, or residential broadband account. Not only are the repercussions less severe if you offend someone from such an account, but target network admins

are less likely to even bother complaining to mass-market providers. Also read the relevant AUP and choose a provider accordingly. If your provider (like Comcast discussed above) bans any unauthorized port scanning and posting of "offensive" material, do not be surprised if you are kicked off for this activity. In general, the more you pay to a service provider the more accommodating they are. A T1 provider is highly unlikely to yank your connection without notice because someone reported being port scanned. A dialup or residential DSL/cable provider very well might. This can happen even when the scan was forged by someone else.

- Nmap offers many options for stealthy scans, including source-IP spoofing, decoy scanning, and the more recent Idle Scan technique. These are discussed in the IDS evasion chapter. But remember that there is always a trade-off. You are harder to find if you launch scans from an open WAP far from your house, with 17 decoys, while doing subsequent probes through a chain of 9 open proxies. But if anyone does track you down, they will be mighty suspicious of your intentions.
- Always have a legitimate reason for performing scans. An offended admin might write to you first (or your ISP might forward his complaint to you) expecting some sort of justification for the activity. In the Moulton case discussed above, VC3 first emailed Moulton to ask what was going on. If they had been satisfied with his answer, matters might have stopped there rather than escalating into civil and criminal litigation. Groups scanning large portions of the Internet for research purposes often use a reverse-DNS name that describes their project and runs a web server with detailed information and opt-out forms.

Also remember that ancillary and subsequent actions are often used as evidence of intent. A port scan by itself does not always signify an attack. A port scan followed closely by an IIS exploit, however, broadcasts the intention loud and clear. This is important because decisions to prosecute (or fire, expel, complain, etc.) are often based on the whole event and not just one component (such as a port scan). One dramatic case involved a Canadian man named Walter Nowakowski, who was apparently the first person to be charged in Canada with theft of communications<sup>11</sup> for accessing the Internet through an someone's unsecured Wi-Fi network. Thousands of Canadian "war drivers" do this every day, so why was he singled out? Because of ancillary actions and intent. He was allegedly caught driving the wrong way on a one-way street, naked from the waist down, with laptop in hand, while downloading child pornography through the aforementioned unsecured wireless access point<sup>12</sup>. The police apparently considered his activity egregious enough that they brainstormed for relevant charges and tacked on theft of communications to the many child pornography-related charges. Similarly, charges involving port scanning are usually reserved for the most egregious cases. Even when paranoid administrators notify the police that they have been port scanned, prosecution (or any further action) is exceedingly rare. The fact that a 911 emergency service was involved is likely what motivated prosecutors in the Moulton case. Your author has scanned hundreds of thousands of Internet hosts and has only been contacted by police and investigative agencies when they file bug reports and feature requests.

To summarize this whole section, the question of whether port scanning is legal does not have a simple answer. I cannot unequivocally say "port scanning is never a crime", as much as I would like to. Laws differ dramatically between jurisdictions, and cases hinge on their particular details. Even when facts are nearly identical, different judges and prosecutors do not always interpret them the same way. I can only urge caution and reiterate the suggestions above.

For testing purposes, you have permission to scan the host `scanme.nmap.org`. You may have noticed that it was used in several examples already. Note that this permission only includes scanning via Nmap and not testing exploits or denial of service attacks. To conserve bandwidth, please do not initiate more than a dozen scans against that host per day. If this free scanning target service is abused, it will be taken down and Nmap will report `Failed to resolve given hostname/IP: scanme.nmap.org`. These permissions also apply to the hosts `scanme2.nmap.org`, `scanme3.nmap.org`, and so on, though those hosts do not currently exist.

This section provides an overview of legal issues related to port scanning, but cannot hope to cover everything. A valuable forum for discussing legal issues related to security is the `seclegal` mailing list. Details are available at

<http://seclegal.jscript.dk>

### 1.3.2. Can port scanning crash the target computer/networks?

Nmap does not have any features designed to crash target networks. It usually tries to tread lightly. For example, Nmap detects dropped packets and slows down when they occur in order to avoid overloading the network. Nmap also does not send any corrupt packets. The headers and such are always appropriate although the destination host is not necessarily expecting the packets. For these reasons, no application, host, or network component *should* ever crash based on an Nmap scan. If they do, that is a bug in the system which should be repaired by the vendor.

Reports of systems being crashed by Nmap are rare, but they do happen. Many of these systems were probably unstable in the first place and Nmap either pushed them over the top or they crashed at the same time as an Nmap scan by pure coincidence. In other cases, poorly written applications, TCP/IP stacks, and even operating systems have been demonstrated to crash reproducibly given a certain Nmap command. These are usually older legacy devices, as newer equipment is rarely released with these problems. Smart companies use Nmap and many other common network tools to test devices prior to shipment. Even those who don't often find out about the problem in early beta tests when a box is first deployed on the Internet. It rarely takes long for a given IP to be scanned as part of Internet white noise. Keeping systems and devices up-to-date with the latest vendor patches and firmware should reduce the susceptibility of your machines to these problems, while also improving the security and usability of your network.

In many cases, finding that a machine crashes from a certain scan is valuable information. After all, attackers can do anything Nmap can do by using Nmap itself or their own custom scripts. They should not be allowed to crash your devices, and a patch should be demanded of vendors if devices do suffer. In other Nmap usage scenarios, you may want to do very light scanning in order to reduce the risk of these problems. Here are a few suggestions:

- Use SYN scan (-sS) instead of Connect() scan (-sT). User-mode applications such as web servers can rarely even detect the former because it is all handled in kernel space (some older Linux kernels are an exception) and thus the services have no excuse to crash.
- Version scanning (-sV) risks crashing poorly written applications. Similarly, some lame operating systems have been reported to crash when OS fingerprinted (-O). Omit these options for particularly sensitive environments or where you do not care about the results.
- Using -T2 or slower (-T1, -T0) timing modes can reduce the chances that a port scan will harm a system, though they slow your scan dramatically. Older Linux boxes had an identd that would block services temporarily if they were accessed too frequently. This could happen in a port scan, as well as during legitimate high-load situations. Slower timing might help here.
- Limit the number of ports and machines scanned to the fewest that are required. Every machine scanned has a minuscule chance of crashing, and so cutting the number of machines down improves your odds. Reducing the number of ports scanned reduces the risks to end hosts as well as network devices. Many NAT/Firewall devices keep a state entry for every port probe. Most of them expire old entries when the table fills out, but occasional (pathetic) implementations crash instead. Reducing the ports/hosts scanned reduces the number of state entries and thus might help those sorry devices stay up.

### 1.3.3. Misc: Copyright, license, (lack of) warranty, export control information

These important legal notices come from the Nmap manual page.

The Nmap Security Scanner is (C) 1996-2004 Insecure.Com LLC. Nmap is also a registered trademark of Insecure.Com LLC. This program is free software; you may redistribute and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; Version 2. This guarantees your right to use, modify, and redistribute this software under certain conditions. If you wish to embed Nmap technology into proprietary software, we may be willing to sell alternative licenses (contact sales@insecure.com). Many security scanner vendors already license Nmap technology such as our remote OS fingerprinting database and code, service/version detection system, and port scanning code.

Note that the GPL places important restrictions on "derived works", yet it does not provide a detailed definition of that term. To avoid misunderstandings, we consider an application to constitute a "derivative work" for the purpose of this license if it does any of the following:

- Integrates source code from Nmap
- Reads or includes Nmap copyrighted data files, such as nmap-os-fingerprints or nmap-service-probes.
- Executes Nmap and parses the results (as opposed to typical shell or execution-menu apps, which simply display raw Nmap output and so are not derivative works.)
- Integrates/includes/aggregates Nmap into a proprietary executable installer, such as those produced by InstallShield.
- Links to a library or executes a program that does any of the above

The term "Nmap" should be taken to also include any portions or derived works of Nmap. This list is not exclusive, but is just meant to clarify our interpretation of derived works with some common examples. These restrictions only apply when you actually redistribute Nmap. For example, nothing stops you from writing and selling a proprietary front-end to Nmap. Just distribute it by itself, and point people to <http://www.insecure.org/nmap/> to download Nmap.

We don't consider these to be added restrictions on top of the GPL, but just a clarification of how we interpret "derived works" as it applies to our GPL-licensed Nmap product. This is similar to the way Linus Torvalds has announced his interpretation of how "derived works" applies to Linux kernel modules. Our interpretation refers only to Nmap - we don't speak for any other GPL products.

If you have any questions about the GPL licensing restrictions on using Nmap in non-GPL works, we would be happy to help. As mentioned above, we also offer alternative license to integrate Nmap into proprietary applications and appliances. These contracts have been sold to many security vendors, and generally include a perpetual license as well as providing for priority support and updates as well as helping to fund the continued development of Nmap technology. Please email sales@insecure.com for further information.

As a special exception to the GPL terms, Insecure.Com LLC grants permission to link the code of this program with any version of the OpenSSL library which is distributed under a license identical to that listed in the included Copying.OpenSSL file, and distribute linked combinations including the two. You must obey the GNU GPL in all respects for all of the code used other than OpenSSL. If you modify this file, you may extend this exception to your version of the file, but you are not obligated to do so.

If you received these files with a written license agreement or contract stating terms other than the terms above, then that alternative license agreement takes precedence over these comments.

Source is provided to this software because we believe users have a right to know exactly what a program is going to do before they run it. This also allows you to audit the software for security holes (none have been found so far).

Source code also allows you to port Nmap to new platforms, fix bugs, and add new features. You are highly encouraged to send your changes to fyodor@insecure.org for possible incorporation into the main distribution. By sending these changes to Fyodor or one the Insecure.Org development mailing lists, it is assumed that you are

offering Fyodor and Insecure.Com LLC the unlimited, non-exclusive right to reuse, modify, and relicense the code. Nmap will always be available Open Source, but this is important because the inability to relicense code has caused devastating problems for other Free Software projects (such as KDE and NASM). We also occasionally relicense the code to third parties as discussed above. If you wish to specify special license conditions of your contributions, just say so when you send them.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details (it is included as an appendix, and is also available from <http://www.gnu.org/copyleft/gpl.html>).

It should also be noted that Nmap has been known to crash certain poorly written applications, TCP/IP stacks, and even operating systems (see previous section). Nmap should never be run against mission critical systems unless you are prepared to suffer downtime. We acknowledge here that Nmap may crash your systems or networks and we disclaim all liability for any damage or problems Nmap could cause.

Because of the slight risk of crashes and because a few black hats like to use Nmap for reconnaissance prior to attacking systems, there are administrators who become upset and may complain when their system is scanned. Thus, it is often advisable to request permission before doing even a light scan of a network.

Nmap should never be run with privileges (e.g. suid root) for security reasons.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). The Libpcap portable packet capture library is distributed along with nmap. Libpcap was originally copyrighted by Van Jacobson, Craig Leres and Steven McCanne, all of the Lawrence Berkeley National Laboratory, University of California, Berkeley, CA. It is now maintained at <http://www.tcpdump.org>.

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. See <http://www.pcre.org/>.

Nmap can optionally link to the OpenSSL cryptography toolkit, which is available from [http://www.openssl.org/](http://www.openssl.org).

**US Export Control:** Insecure.Com LLC believes that Nmap falls under US ECCN (export control classification number) 5D992. This category is called "'Information Security" "software" not controlled by 5D002'. The only restriction of this classification is AT (anti-terrorism), which applies to almost all goods and denies export to a handful of rogue nations such as Iran and North Korea. Thus exporting Nmap does not require any special license, permit, or other governmental authorization.

## Notes

1. Based on having the highest download frequency, number of Google hits, and Freshmeat.Net software "popularity" ranking.
2. These IP addresses are actually registered to the United States Army Yuma Proving Ground, which is used to test a wide variety of artillery, missiles, tanks, and other deadly weapons. The moral is to be very careful about who you scan, lest you accidentally hit a highly sensitive network. The scan results in this story are not actually from this IP range.
3. It is possible that the target nameserver will log a suspicious bunch of reverse-DNS queries from Felix's nameserver, but most organizations don't even keep such logs, much less analyze them.
4. stdio is the "C" notation for representing the standard output mechanism for a system, such as to the UNIX xterm or Windows command window in which Nmap was initiated.

5. A sexy leather-clad attacker from the previous team actually started the session. It is unclear at what point she died and left the remaining tasks to Trinity.
6. These are from <http://www.americansushi.com/>. I have no affiliation with them except that they were cool enough to send me samples.
7. <http://www.comcast.net/terms/use.jsp>
8. <http://www4.law.cornell.edu/uscode/18/1030.html>
9. <http://seclists.org/lists/nmap-hackers/2001/Apr-Jun/0011.html>
10. An excellent paper on this topic by lawyer Ethan is available at <http://grove.ufl.edu/~techlaw/vol6/Preston.html>  
He has also written an excellent paper relating to the legal risks of publishing security information and exploits at <http://www.mcndl.com/computer-security.html>.
11. Canadian Criminal Code Section S.342.1 - [http://www.digitaldefence.ca/Canada\\_CriminalCode\\_S342.1.htm](http://www.digitaldefence.ca/Canada_CriminalCode_S342.1.htm)
12. <http://www.canoe.ca/NewsStand/LondonFreePress/News/2003/11/22/264890.html>

# Chapter 2. Obtaining, Installing, and Removing Nmap

## 2.1. Introduction

This chapter describes how to install Nmap on many platforms, from Windows to OpenBSD, including both source code compilation and binary installation methods. Graphical and command-line versions of Nmap are described and contrasted. A recipe describes how to install and use Nmap on the Sharp Zaurus PDA. Finally, Nmap removal instructions are provided in case you change your mind.

### 2.1.1. Testing whether Nmap is already installed

The first step toward obtaining Nmap is to check whether you already have it. Many free operating system distributions (including most Linux and BSD systems) come with Nmap, although it may not be installed by default. On UNIX systems, open a terminal window and try executing the command `nmap --version`. If Nmap exists and is in your \$PATH, you should see output similar to Example 2-1.

#### Example 2-1. Checking for Nmap and determining its version number

```
felix~>nmap --version

nmap version 3.50 ( http://www.insecure.org/nmap )
felix~>
```

If Nmap does *not* exist on the system (or if your PATH is incorrectly set), an error message such as `nmap: Command not found` displays. As the example above shows, Nmap responds to the command by printing its version number (here 3.50).

Even if your system already has a copy of Nmap, you should consider upgrading to the latest version available from [http://www.insecure.org/nmap/nmap\\_download.html](http://www.insecure.org/nmap/nmap_download.html). Newer versions often run faster, fix important bugs, and feature updated operating system and service version detection databases. A list of changes since the version already on your system can be found at [http://www.insecure.org/nmap/nmap\\_changelog.html](http://www.insecure.org/nmap/nmap_changelog.html). Nmap output examples in this book usually include a version number near the top, and they may not work with older versions.

### 2.1.2. Verifying the integrity of Nmap downloads

It often pays to be paranoid about the integrity of files downloaded from the Internet. While nobody has ever compromised Insecure.Org or (as far as I know) distributed a trojaned version of Nmap, one should always be cautious. Popular packages such as Sendmail<sup>1</sup>, OpenSSH<sup>2</sup>, tcpdump, libpcap, BitchX, Fragrouter, and many others have been infected with malicious trojans. Popular software distributions sites at the Free Software Foundation, Debian, and SourceForge have also been successfully compromised. To help people verify the authenticity of Nmap releases, I always send a PGP-signed announcement to the nmap-hackers list. That announcement includes MD5 cryptographic checksums of the source code and binaries. Visit <http://seclists.org/> for subscription information and archives. The message should be signed by my key, which is available from the public keyservers or from [http://www.insecure.org/fyodor\\_gpgkey.txt](http://www.insecure.org/fyodor_gpgkey.txt). The KeyID is 0x53587D95 and the fingerprint is

972F:93AB:9CB0:0980:D951:406B:B9BC:E17E. The checksum can be verified with the md5sum or md5 utilities available on most UNIX boxes. Example 2-2 demonstrates this.

#### **Example 2-2. Verifying the Nmap download checksum**

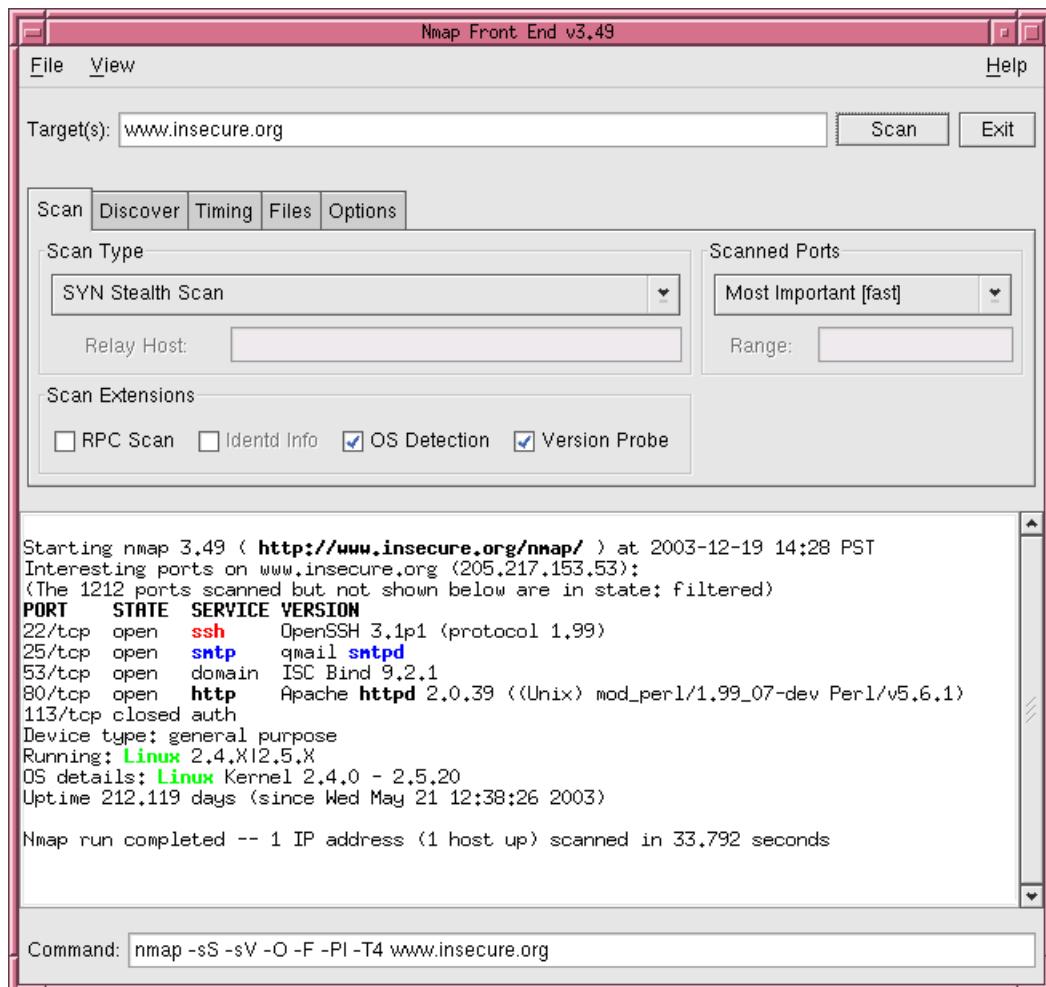
```
felix~> gpg --verify Nmap-3.50-announce-email.txt
gpg: Warning: using insecure memory!
gpg: Signature made Wed 21 Jan 2004 02:54:38 PM PST using RSA key ID 53587D95
gpg: Good signature from "Fyodor <fyodor@insecure.org>"
gpg:                               aka "Fyodor <fyodor@dhp.com>""
felix~> md5sum nmap-3.50.tgz
9823bcd72f87051707e6e1c2b10d5d62  nmap-3.50.tgz
felix~>
```

While releases from Insecure.Org are signed as described above, certain Nmap add-ons, interfaces, and platform-specific binaries are developed and distributed by other parties. They may have different mechanisms for establishing the authenticity of their downloads.

### **2.1.3. Command-line and graphical interfaces**

Nmap has traditionally been a command-line application run from a UNIX shell or (more recently) Windows command prompt. This allows experts to quickly execute a command that does exactly what they want without having to maneuver through a bunch of configuration panels and scattered option fields. This also makes Nmap easier to script and enables easy sharing of useful commands among the user community.

One downside of the command-line approach is that it can be intimidating for new and infrequent users. Nmap offers more than a hundred command-line options, although many are obscure features or debugging controls that most users can ignore. Many graphical frontends have been created for those users who prefer a GUI interface. The most common GUI for UNIX is NmapFE, which is distributed as part of the Nmap project. It offers a number of option panes (**Scan**, **Discover**, **Timing**, **Files**, and **Options**), which are all used to build an appropriate Nmap command. The Nmap command-line is shown at the bottom of the window as it is constructed. This feature helps people learn the syntax in case they wish to migrate to the command-line version. There is not presently a field for entering arbitrary Nmap options, but one trick is to stick them in the big **Target(s)** field. Once the command is constructed to your liking, press the **Scan** button to launch Nmap. Raw Nmap output (with added color for service emphasis) is shown in a large white window, as seen in Figure 2-1.

**Figure 2-1.** NmapFE presents a simple graphical interface to Nmap

Unfortunately, NmapFE does not yet work well on the Windows platform. The good news is that Jens Vogt has created a popular Windows Nmap GUI named Nmapwin. It is organized a little differently than NmapFE, but retains the same paradigm of constructing a command-line from multiple tabbed option panes and then displaying the raw output in a big scrollable box. Instructions for installing Nmapwin are provided in Section 2.4.2.

This book focuses almost exclusively on command-line invocations of Nmap. Once you understand how the command-line options work and can interpret the output, using any of the available Nmap GUIs is trivial. The options are all the same whether you choose them from radio buttons and menus or type them at a command-line.

## 2.2. UNIX Compilation and installation from source code

While binary packages discussed in later sections are available for most platforms, compilation and installation from source code is the traditional and most powerful way to install Nmap. This insures that the latest version is available and allows Nmap to adapt to the library availability and directory structure of your system. For example, Nmap uses the OpenSSL cryptography libraries for version detection (Chapter 7) when available, but most binary packages do

not include this functionality. On the other hand, binary packages are generally quicker and easier to install, and allow for consistent management (installation, removal, upgrading, etc.) of all packaaged software on the system.

Source installation is usually a painless process - the build system is designed to auto-detect as much as possible. Here are the steps required for a default install:

1. Download the latest version of Nmap in .tar.bz2 (bzip2 compression) or .tgz (gzip compression) format from [http://www.insecure.org/nmap/nmap\\_download.html](http://www.insecure.org/nmap/nmap_download.html).

2. Decompress the downloaded tarball with a command such as:

```
bzip2 -cd nmap-VERSION.tar.bz2 | tar xvf -
```

If you downloaded the .tgz version, replace bzip2 with gzip in the command above.

3. Change into the newly created directory: **cd nmap-VERSION**

4. Configure the build system: **./configure**

5. Build Nmap (and GUI nmapfe if requirements met): **make**

6. Become a privileged user for systemwide install: **su root**

7. Install Nmap, support files, docs, etc.: **make install**

As you can see above, a simple source compilation and install consists of little more than **./configure;make;make install**. However, there are a number of options available to configure that affect the way Nmap is built.

### 2.2.1. Configure directives

Most of the UNIX build options are controlled by the **configure** script, as used in step number four above. There are dozens of command-line parameters and environmental variables which affect the way Nmap is built. Run **./configure --help** for a huge list with brief descriptions. Here are the ones that are specific to Nmap or particularly important:

**--prefix=directoryname**

This option, which is standard to the configure scripts of most software, determines where Nmap and its components are installed. By default, the prefix is `/usr/local`, meaning that nmap is installed in `/usr/local/bin`, the man page (`nmap.1`) is installed in `/usr/local/man/man1`, and the data files (`nmap-os-fingerprints`, `nmap-services`, `nmap-service-probes`, etc.) are installed under `/usr/local/share/nmap`. If you only wish to change the path of certain components, use the options `--bindir`, `--datadir`, and/or `--mandir`. An example usage of `--prefix` would be to install Nmap in my account as an unprivileged user. I would run **./configure --prefix=/home/fyodor**. Nmap creates subdirs like `/home/fyodor/man/man1` in the install stage if they do not already exist.

**--without-nmapfe**

This option prevents the NmapFE graphical X-Window frontend from being built. Normally the build system checks your system for requirements such as the GTK graphical widget library and then build NmapFE if they are all available.

--with-openssl=*directoryname*

The version detection subsystem of Nmap is able to probe SSL-encrypted services using the free OpenSSL libraries. Normally the Nmap build system looks for these libraries on your system and include this capability if they are found. If they are in a location your compiler does not search for by default, but you still want them to be used, specify --with-openssl=*directoryname*. Nmap then looks in *directoryname*/libs for the OpenSSL libraries themselves and *directoryname*/include for the necessary header files.

--with-libpcap=*directoryname*

Nmap uses the Libpcap library (<http://www.tcpdump.org>) for capturing raw IP packets. Nmap normally looks for an existing copy of Libpcap on your system and use that if the version number and platform is appropriate. Otherwise Nmap includes its own recent copy of Libpcap, which has been modified for improved Linux functionality. The specific changes are described in *libpcap-possiblymodified/CHANGES* in the Nmap source directory. Because of these Linux-related changes, Nmap always uses its own Libpcap by default on that platform. If you wish to force Nmap to link with your own Libpcap, pass the option --with-libpcap=*directoryname* to configure. Nmap then expects the Libpcap library to be in *directoryname*/lib/libpcap.a and the include files to be in *directoryname*/include.

--with-libpcre=*directoryname*

LibPCRE is a Perl-compatible regular expression library available from <http://www.pcre.org>. Nmap normally looks for a copy on your system, and then fall back to its own copy if that fails. If your PCRE library is not in your compiler's standard search path, Nmap probably will not find it. In that case you can tell Nmap where it can be found by specifying the option --with-libpcre=*directoryname* to configure. Nmap then expects the library files to be in *directoryname*/lib and the include files to be in *directoryname*/include. In some cases, you may wish to use the PCRE libraries included with Nmap in preference to those already on your system. In that case, specify --with-libpcre=included.

--with-localdirs

This simple option tells Nmap to look in /usr/local/lib and /usr/local/include for important library and header files. This should never be necessary, except that some people put such libraries in /usr/local without configuring their compiler to find them. If you are one of those people, use this option.

## 2.2.2. If you encounter compilation problems

In an ideal world, software would always compile perfectly (and quickly) on every system you maintain. Unfortunately, society has not yet reached that state of nirvana. Despite all the efforts to make Nmap portable, compilation issues occasionally arise. Here are some suggestions in case the source distribution compilation fails.

Upgrade to the latest Nmap

Check [http://www.insecure.org/nmap/nmap\\_download.html](http://www.insecure.org/nmap/nmap_download.html) to make sure you are using the latest version of Nmap. The problem may have already been fixed.

Read the error message carefully

Scroll up in the output screen and examine the error messages given when commands fail. It is often best to find the first error message, as that often causes a cascade of further errors. Read the error message carefully, as it could indicate a system problem such as low disk space or a broken compiler. Users with programming skills may be able to resolve a wider range of problems themselves. If you make code changes to fix the problem,

please send a patch (created with **diff -uw oldfile newfile**) and any details about your problem and platform to me at <fyodor@insecure.org>. Integrating the change into the base Nmap distribution allows many other users to benefit, and prevents you from having to make the changes with each new Nmap version.

#### Ask Google and other Internet resources

Try searching for the exact error message on Google or other search engines. You might also want to browse recent activity on the Nmap development (nmap-dev) list -- archives are available at <http://seclists.org>.

#### Ask nmap-dev

If none of your research has led to a solution for your problem, try sending a report to the Nmap development (nmap-dev) list. If you subscribe first, your message gets through faster because it does not go through moderation. Subscribe by sending a blank email to <nmap-dev-subscribe@insecure.org> and post to the list by mailing <nmap-dev@insecure.org>. Be sure to describe your problem in full, including the Nmap version number, platform you are running on, and any relevant output snippets showing the error.

#### Consider binary packages

Binary packages of Nmap are available on most platforms and are usually easy to install. The downsides are that they may not be as up-to-date and you lose some of the flexibility of self-compilation. Previous sections of this chapter describe how to find binary packages on many platforms, and even more are available via Internet searching.

## 2.3. Linux Distributions

Linux is far and away the most popular platform for running Nmap. In a 2003 survey of roughly 2000 Nmap users, 86% said that Linux was at least one of the platforms on which they run Nmap.

Linux users can choose between a source code install or using binary packages provided by their distribution. The binary packages are generally quicker and easier to install, and are often slightly customized to use the distribution's standard directory paths and such. These packages also allow for consistent management in terms of upgrading, removing, or surveying software on the system. A downside is that packages created by the distributions are necessarily behind the Insecure.Org source releases. Most Linux distributions (particularly Debian and Gentoo) keep their Nmap package relatively current, though a few are way out of date. Choosing the source install allows for more flexibility in determining how Nmap is built and optimized for your system. To build Nmap from source, see Section 2.2. Here are simple package instructions for the most common distributions.

### 2.3.1. RPM-based distributions (Red Hat, Mandrake, Suse, Fedora)

I build RPM packages for every release of Nmap and post them to the Nmap download page at [http://www.insecure.org/nmap/nmap\\_download.html](http://www.insecure.org/nmap/nmap_download.html). I build two packages: The `nmap` package contains just the command-line executable and data files, while the `nmap-frontend` package contains the optional X-Window graphical frontend named `nmapfe`. The `nmap-frontend` package is optional and only necessary for those who want a GUI interface to Nmap. It does require that the `nmap` package be installed first.

Installing via rpm is quite easy - it even downloads the package for you when given the proper URLs. The following example downloads and installs Nmap 3.48, including the frontend. Of course you should use the latest version at the download site above instead. Any existing RPM-installed versions are upgraded. Example 2-3 demonstrates this installation process.

**Example 2-3. Installing Nmap from binary RPMs**

```
# rpm -vhU http://download.insecure.org/nmap/dist/nmap-3.48-1.i386.rpm
Retrieving http://download.insecure.org/nmap/dist/nmap-3.48-1.i386.rpm
Preparing... #####
1:nmap #####
# rpm -vhU http://download.insecure.org/nmap/dist/nmap-frontend-3.48-1.i386.rpm
Retrieving http://download.insecure.org/nmap/dist/nmap-frontend-3.48-1.i386.rpm
Preparing... #####
1:nmap-frontend #####
core/home/fyodor#
```

As the filenames above imply, these binary RPMs were created for normal PCs (X86 architecture). So they do not work for the relatively few Linux users on other platforms such as SPARC, Alpha, or PowerPC. They also may refuse to install if your library versions are sufficiently different from what the RPMs were initially built on. One option in these cases would be to find binary RPMs prepared by your Linux vendor for your specific distribution. The original install CDs or DVD are a good place to start. Unfortunately, those may not be current or available. Another option is to install Nmap from source code as described previously, though you lose the binary package maintenance consistency benefits. A third option is to build and install your own binary RPMs from the source RPMs distributed from the download page above. Example 2-4 demonstrates this technique with Nmap 3.48.

**Example 2-4. Building and installing Nmap from source RPMs**

```
> rpm --rebuild http://download.insecure.org/nmap/dist/nmap-3.48-1.src.rpm
[ hundreds of lines cut ]
Wrote: /home/fyodor/rpmdir/RPMS/i386/nmap-3.48-1.i386.rpm
Wrote: /home/fyodor/rpmdir/RPMS/i386/nmap-frontend-3.48-1.i386.rpm
[ cut ]
> su
Password:
# rpm -vhU /home/fyodor/rpmdir/RPMS/i386/nmap-*3.48-1.i386.rpm
Preparing... #####
1:nmap #####
2:nmap-frontend #####
#
```

Removing RPM packages is as easy as **rpm -e nmap nmap-frontend**.

**2.3.2. Debian Linux**

LaMont Jones does a fabulous job maintaining the Nmap .deb packages, including keeping them reasonably up-to-date. The proper upgrade/install command is **apt-get install nmap**. Information on the latest Debian "stable" Nmap package is available at <http://packages.debian.org/stable/net/nmap.html> and the development ("unstable") package info is available from <http://packages.debian.org/unstable/net/nmap.html>.

**2.3.3. Gentoo Linux**

\* I believe Gentoo uses "emerge nmap" or some such. Can anyone send me details?

### 2.3.4. Other Linux distributions

There are far too many Linux distributions available to list here, but even many of the obscure ones include Nmap in their package tree. Even if they do not, you can simply compile from source code as described in Section 2.2.

*\* If I am missing any important distributions, please send me details on installing their Nmap binary package*

## 2.4. Windows

Although Windows support is a relatively recent Nmap phenomenon, it has quickly grown into the second most popular Nmap platform. Because of this popularity and the fact that many Windows users do not have a compiler, binary executables are distributed for each major Nmap release. While it is improving rapidly, the Windows port is still not as efficient or stable as on UNIX. Here are some known limitations (at the time of this writing):

- You cannot generally scan your own machine from itself (using a loopback IP such as 127.0.0.1 or any of its registered IP addresses)
- Most scanning over RAS connections (such as PPP dialups) are only supported under Windows 2000/XP.
- Version detection cannot use SSL scan-through (discussed in Chapter 6)
- Scans from Windows often take longer than on UNIX

I would like to thank Ryan Permeh of eEye, Andy Lutomirski, and Jens Vogt for their hard work on the Nmap Windows port. For many years, Nmap was a UNIX-only tool, and it would likely still be that way if not for their efforts.

Windows users have three choices for installing Nmap, all of which are available from the download page at [http://www.insecure.org/nmap/nmap\\_download.html](http://www.insecure.org/nmap/nmap_download.html).

### 2.4.1. Command line .zip binaries

Every major "stable" Nmap release comes with Windows command-line binaries and associated files in a Zip archive. No graphical interface is included, so you need to run `nmap.exe` from a DOS/command window. Or you can download and install a superior command shell such as those included with the free Cygwin system available from <http://www.cygwin.com>. Here are the step-by-step instructions for installing and executing the Nmap .Zip binaries.

#### 2.4.1.1. Installing the Nmap .Zip binaries

1. Read the Nmap Win32 support page (<http://www.insecure.org/nmap/data/README-WIN32>) for the latest updates
2. Download the .Zip binaries from [http://www.insecure.org/nmap/nmap\\_download.html](http://www.insecure.org/nmap/nmap_download.html).
3. Uncompress the zip-file into the directory you want Nmap to reside in. An example would be "C:\Program Files\". A directory called `nmap-VERSION` should be created, which includes the Nmap executable and data files. If you do not have a Zip decompression program, there is one (called `unzip`) in Cygwin above, or you can download the open source and free 7-zip utility from <http://www.7-zip.org>. Commercial alternatives are Winzip and PKZIP from <http://www.winzip.com> and <http://www.pkware.com> respectively.

4. For improved performance, apply the Nmap registry changes by clicking on nmap\_performance.reg in the new Nmap directory. This increases the number of ephemeral ports reserved for user applications (such as Nmap) and decreases the amount of time before a closed connection can be reused.
5. Nmap requires the free WinPcap packet capture library. Obtain and install the latest version from <http://winpcap.polito.it>. They distribute an executable installer which makes this easy. At the time of this writing, the latest version is 3.01 and is known to work. Downloading the newest version available is recommended.

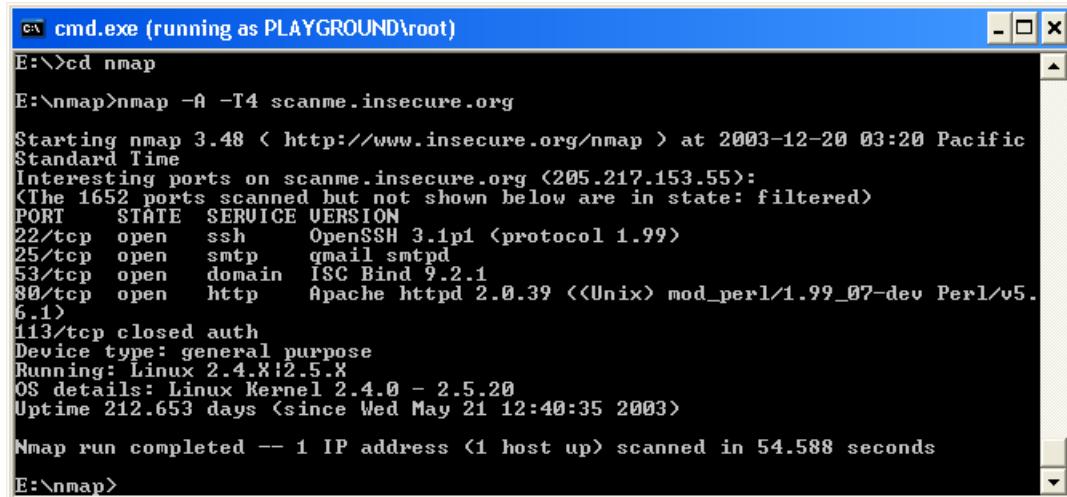
#### 2.4.1.2. Executing Nmap as installed above

1. Make sure the user you are logged in as has administrative privileges in the box (should be in the administrators group).
2. Open a command/DOS Window. Though it can be found in the program menu tree, the simplest approach is to choose Start -> Run and type cmd<enter>. Opening a Cygwin window (if you installed it) by clicking on the Cygwin icon on the desktop works too, although the necessary commands differ slightly from those shown below.
3. Change to the directory you installed Nmap into. Assuming the example directory name used in the install section above, type the following commands.

```
c:  
cd "\program files\nmap-VERSION" (replace VERSION with the Nmap version number)
```

4. Execute nmap.exe. Figure 2-2 is a screen shot showing a simple example

**Figure 2-2. Executing Nmap from a Windows command shell**



```
cmd.exe (running as PLAYGROUND\root)
E:\>cd nmap
E:\nmap>nmap -A -T4 scanme.insecure.org
Starting nmap 3.48 < http://www.insecure.org/nmap > at 2003-12-20 03:20 Pacific
Standard Time
Interesting ports on scanme.insecure.org (205.217.153.55):
(The 1652 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 3.1p1 <protocol 1.99>
25/tcp    open  smtp   gmail smtpd
53/tcp    open  domain ISC Bind 9.2.1
80/tcp    open  http   Apache httpd 2.0.39 <<Unix> mod_perl/1.99_07-dev Perl/v5.
6.1>
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.4.8!2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 212.653 days <since Wed May 21 12:40:35 2003>
Nmap run completed -- 1 IP address (1 host up) scanned in 54.588 seconds
E:\nmap>
```

If you execute Nmap frequently, you can the Nmap directory (c:\program files\nmap-VERSION in this case) to your command execution path. The exact place to set this varies by Windows platform. On my Windows XP box, I do the following:

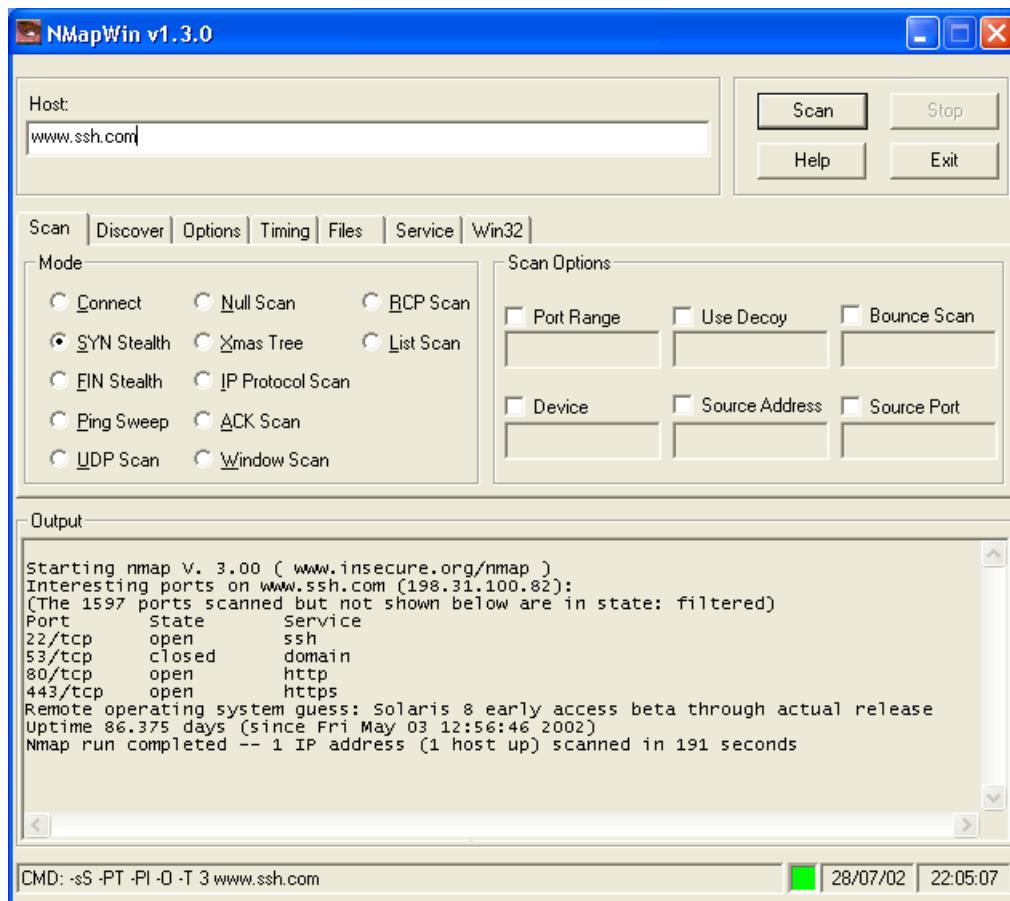
1. From the desktop, right click on My Computer and then click properties.

2. In the System Properties window, click the Advanced tab.
3. Click the Environment Variables button.
4. Choose Path from the System variables section, then hit edit.
5. Add a semi-colon and then your Nmap directory (such as c:\program files\nmap-VERSION) to the end of the value.
6. Open a new DOS window and you should be able to execute a command such as **nmap scanme.nmap.org** from any directory.

## 2.4.2. Nmapwin

\* I am going to save this until later in case the Nmapwin landscape changes. When I do cover it, I should note instructions for upgrading the Nmap version that comes in the Nmapwin installer.

**Figure 2-3. NmapWin provides a slick Windows interface to Nmap**



### 2.4.3. Compile from source code

Most Windows users prefer to use the Nmap binary distribution, but compilation from source code is an option. Compilation presently requires certain versions of the commercial Microsoft Visual C++ compiler (part of MS Visual Studio). The following steps are required.

#### Compiling Nmap on Windows from Source.

1. Read the Nmap Win32 support page at <http://www.insecure.org/nmap/data/README-WIN32> for the latest updates. The Windows compilation instructions do change occasionally.
2. Make sure you have installed Microsoft Visual Studio .Net 2003 or later. Apparently the "solution files" with build instructions do not even work in the 2002 version of the software. This is typical Microsoft behavior and it exemplifies why most Windows users use the binary package while many UNIX users prefer source compilation.
3. Download the latest Nmap source distribution from [http://www.insecure.org/nmap/nmap\\_download.html](http://www.insecure.org/nmap/nmap_download.html). It has the name nmap-*version*.tgz or nmap-*version*.tar.bz2 . Those are the same tar file compressed using gzip or bzip2, respectively.
4. Uncompress the source code file you just downloaded. Recent releases of the free Cygwin distribution (<http://www.cygwin.com/>) can handle both the .tgz and .tar.bz2 . Use the command **tar xvzf nmap-*version*.tgz** or **tar xvjf nmap-*version*.tar.bz2**, respectively. Alternatively, the common Winzip application can decompress the .tgz version.
5. Open Visual Studio and the Nmap solution file ( nmap-VERSION/mswin32/nmap.sln )
6. From the Build Menu, select Configuration Manager and set Active Solution Configuration to Release.
7. Choose Build Solution from the Build Menu. Nmap should begin compiling, and end with the line "-- Done --" saying that all projects built successfully and there were 0 failures.
8. The executable and data files can be found in nmap-VERSION/mswin32/Release/ . You can copy them to a preferred directory as long as they are all kept together.
9. Nmap requires the free WinPcap packet capture library. Obtain and install the latest version from <http://winpcap.polito.it>. They distribute an executable installer which makes this easy.
10. Instructions for executing your compiled Nmap are the same as given above for the .zip binaries.

Many people have asked whether Nmap can be compiled with the gcc/g++ included with Cygwin or other compilers. At this time, only Visual Studio is supported because that is what the original Windows porters used. If someone develops a clean patch which allows for compilation by free compilers, it is likely to be integrated into the project build system. Because of this unfortunate requirement for commercial tools to build Nmap on Windows, new binaries are frequently made available on the download page.

## 2.5. Sun Solaris

Solaris has long been well-supported by Nmap. Sun even donated a complete SPARCstation to the project, which is still being used to test new Nmap builds. For this reason, many Solaris users compile and install from source code as described in Section 2.2.

Users who prefer native Solaris packages will be pleased to learn that Steven Christensen does an excellent job of maintaining Nmap packages over at <http://www.sunfreeware.com>. Instructions are on his site, and are generally very simple: download the appropriate Nmap package for your version of Solaris, decompress it, and then run **pkgadd -d packagename**. As is generally the case with contributed binary packages, these Solaris packages are simple and quick to install. The advantages of compiling from source are that a newer version may be available and you have more flexibility in the build process. Certain optional features such as OpenSSL version detection are often not available in prebuilt packages.

## 2.6. Apple Mac OS X

Thanks to several people graciously donating shell accounts on their OS X boxes, Nmap usually compiles on that platform without problems. Doing this does require the Apple Developer Tools system. If you are not careful, Apple tries to charge for them. Brian Hatch sent me the following steps for obtaining the Developer Tools for free (as of September 2003).

1. Browse to <http://connect.apple.com> and join the ADC (Apple Developer Connection)
2. Fill out several forms to create a new account
3. Eventually you reach a page for buying support and/or CD media. Ignore this page and return to <http://connect.apple.com>.
4. Log in with your new account credentials.
5. Hit the Download link on the left and then choose Developer Tools.
6. Download the most recent Dev Tools and install.
7. Download the most recent Dev Tools Updates and install.

\* Verify that these steps have not changed shortly before release

These exact steps may change, but it is hoped that this general approach will continue to work.

Once you have the developer tools installed, you can follow the compilation instructions found in Section 2.2. Note that on some older versions of Mac OS X, you may have to replace the command **./configure** with **./configure CPP=/usr/bin/cpp**.

Users who prefer binary packages may want to have a look at the Fink project (<http://fink.sourceforge.net>). Their stated goal is “to bring the full world of Unix Open Source software to Darwin and Mac OS X,” and so they offer Nmap and hundreds of other useful packages. As with all contributed binary packages, the disadvantage is that they may not be up-to-date with the latest Nmap releases and you have less flexibility in the build process. But it is certainly worth a look if you want to install many popular UNIX tools at once.

## 2.7. FreeBSD / OpenBSD / NetBSD

The BSD flavors are well supported by Nmap, so you can simply compile it from source as described in Section 2.2. This provides the normal advantages of always having the latest version and a flexible build process. If you prefer binary packages, these \*BSD variants each maintain their own Nmap packages. Many BSD systems also have a “ports” tree which standardizes the compilation of popular applications. Instructions for installing Nmap on the most popular \*BSD variants follow.

### 2.7.1. OpenBSD binary packages and source ports instructions

According to the OpenBSD FAQ (<http://www.openbsd.org/faq/>), users “are HIGHLY advised to use packages over building an application from ports. The OpenBSD ports team considers packages to be the goal of their porting work, not the ports themselves.”. That same FAQ contains detailed instructions for each method. Here is a summary.

#### Installation using binary packages

1. Choose a mirror from <http://www.openbsd.org/ftp.html>. FTP in and grab the Nmap package from `/pub/OpenBSD/version/packages/platform/nmap-version.tgz`. Or obtain it from the OpenBSD distribution CD-ROM.
2. As root, execute: `pkg_add -v nmap-version.tgz`

#### Installation using the source ports tree

1. If you do not already have a copy of the ports tree, obtain it via CVS using instructions at <http://www.openbsd.org/faq/faq8.html#CVS>.
2. As root, execute the following command (replace `/usr/ports` with your local ports directory if it differs):

```
cd /usr/ports/net/nmap && make install clean
```

### 2.7.2. FreeBSD binary package and source ports instructions

The FreeBSD has a whole chapter ([http://www.freebsd.org/doc/en\\_US.ISO8859-1/books/handbook/ports.html](http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/ports.html)) in their Handbook describing the package and port installation processes. A brief summary of the process follows.

#### 2.7.2.1. Installation of the binary packages

The easiest way to install the binary Nmap package is to run `pkg_add -r nmap`. You can then run the same command with an `nmapfe` option if you want the X-Window front-end. If you wish to obtain the package manually instead, retrieve it from <http://www.freebsd.org/cgi/ports.cgi?query=nmap> or the CDROM and run `pkg_add packagename.tgz`.

#### Installation using the source ports tree

1. The ports tree is often installed with the system itself (usually in `/usr/ports`). If you do not already have it, specific installation instructions are provided in the FreeBSD Handbook chapter referenced above.
2. As root, execute the following command (replace `/usr/ports` with your local ports directory if it differs):

```
cd /usr/ports/security/nmap && make install clean
```

### 2.7.3. NetBSD binary package instructions

NetBSD has packaged Nmap for an enormous number of platforms, from the normal i386 to Playstation 2, PowerPC, Vax, SPARC, MIPS, Amiga, ARM, and several platforms that I have never even heard of! Unfortunately they are not very up-to-date. A list of NetBSD Nmap packages is available from

<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/net/nmap/README.html> and a description of using their package system to install applications is available at <http://www.netbsd.org/Documentation/pkgsrc/using.html#id2956484>.

## **2.8. Amiga, HP-UX, IRIX, and Other Platforms**

One of the wonders of Open Source development is that resources are often biased towards what people find exciting rather than having an exclusive focus on profits as most corporations do. It is along those lines that the Amiga port came about. Diego Casorran performed most of the work and sent in a clean patch which was integrated into the main Nmap distribution. In general, AmigaOS users should be able to simply follow the source compilation instructions in Section 2.2. You may encounter a few hurdles on some systems, but I presume that must be part of the fun for Amiga fanatics.

Nmap supports many proprietary UNIX flavors such as HP-UX and SGI IRIX. The Nmap project mostly depends on the user community to maintain adequate support for these systems. If you have trouble, try sending a report with full details to the nmap-dev mailing list (<[nmap-dev@insecure.org](mailto:nmap-dev@insecure.org)>). If you develop a patch which improves support on your platform, please email it to me at <[fyodor@insecure.org](mailto:fyodor@insecure.org)>.

## **2.9. [RECIPE] Installing Nmap on a PDA**

Previous sections have described the installation of Nmap on notebook and desktop computers running a wide variety of operating systems. However, some users want greater portability and stealth than even the smallest notebook computers provide. They wish to do their security auditing from a personal digital assistant (PDA) small enough to fit in their pocket or to hide near an ethernet jack in a corporate office or datacenter. Walking around while using a notebook can raise eyebrows. With a PDA, passers by may assume you are just checking your calendar or shopping list while you locate insecure wireless access points or scan their internal network for vulnerabilities. Thanks in a large part to enthusiastic user communities, Nmap supports numerous PDAs. Two of the best supported are the Sharp Zaurus and Compaq IPAQ. Nmap has not been ported to PalmOS systems.

**Table 2-1. The Sharp Zaurus is an excellent platform for highly mobile security applications**

---



This recipe focuses on the Sharp Zaurus because it is the most popular PDA for running Nmap. Users of the Compaq IPAQ may wish to investigate the Familiar Linux distribution for similar functionality. Many other PDAs have active developer communities that are easily found with Google or through sites such as <http://www.handhelds.org>. The Zaurus is popular with mobile security auditors for many reasons.

### Advantages of the Sharp Zaurus for hackers

- Keyboard (sliding or folding) allows easy use of Linux console commands
- Lightweight, compact form factor is convenient and inconspicuous
- Reasonably fast (200Mhz+) ARM processor and adequate RAM (32MB+) provide plenty of power for running Nmap and other security tools
- A wide variety of CF networking cards are supported without bulky adapters. Secure Digital cards are also supported for extra flash storage.
- Ships with Linux pre-installed, making it compatible with a wide variety of popular free security tools (and other software).
- The OpenZaurus project provides convenient support for Nmap, NmapFE, and many other security tools

Many thanks go to Kevin Milne, Adrian Crenshaw (AKA IronGeek), and David Malcher (KillingJoke), avid Zaurus users who provided much of the content and screenshots for this recipe.

#### 2.9.1. Installing Nmap on the Zaurus

Before beginning, make sure you have sufficient hardware.

##### System Requirements

- A Sharp Zaurus (any model)
- 64MB or larger Compact Flash (CF) card for the OpenZaurus ROMS

- A CF networking card such as a basic ethernet card and/or wireless 802.11X. Wireless cards with the Prism2 chipset are recommended. Kevin uses a Xircom 10MB ethernet card and a Netgear MA701 wireless card. Adrian uses an Ambicom WL1100C-CF Wi-Fi card and an TRENDnet/TRENDware TE-CF100 ethernet card.

The most common way to install Nmap is using the OpenZaurus project (<http://www.openzaurus.org>). They provide an alternative ROM image (Linux kernel and filesystem) with a greater emphasis on development and open source tools than the ROM Sharp provides. OpenZaurus is based on the popular Debian Linux distribution. Many other Zaurus Linux distributions are available to suit different needs and preferences. The OpenZaurus project may be subsumed by the more general OpenEmbedded distribution.

Rather than describe the installation process here, readers are advised to follow the directions in the OpenZaurus Install Guide available from [http://www.openzaurus.org/oz\\_website/content/installguide](http://www.openzaurus.org/oz_website/content/installguide). Follow those directions carefully to avoid damaging your Zaurus.

Once OpenZaurus is installed, thousands of open source applications are available for easy installation as IPK files (the file extensions should be .ipk). These are available for download from the OpenZaurus site, or a number of 3rd party sites such as <http://www.killefiz.de/zaurus/>. While finding IPK files on the Internet is quite convenient, they are not always up-to-date. At the time of this writing, the latest IPK of Nmap available via the sites OpenZaurus.Org and Killefiz.de is almost 2 years old. A bit of Internet searching turned up IronGeek's excellent resource site at <http://www.irongeek.com/all.php>. He includes instructions for installing the very latest Nmap version. As with many emerging technologies, browsing and searching specialized web sites is highly recommended as a supplement to book information. Even an efficient dead-tree publisher like O'Reilly cannot hope to disseminate news as quickly as (some) Web sites can.

After downloading IPK files to the Zaurus, they can be installed with the ipkg program. An example execution would be **ipkg install nmap\_3.27-1\_armv4l-strongarm.ipk**. Type **ipkg** with no arguments for help.

A convenient alternative to manually downloading and installing IPK files is the Zaurus Package Manager. It makes installing a large number of packages simple and quick.

### **Installing Nmap using the Zaurus Package Manager**

1. Click on the **Settings** tab and choose **Packages**.
2. The first time you start the Package Manager, activate the feeds through the **Options -> Configure** screen and configure the stable, testing, and/or unstable feeds. Nmap is currently part of the testing feed.
3. Since the available packages are frequently updated, perform a feed update by choosing **Actions** and then **Update Lists**.
4. A huge list of available software is provided. You may have to switch to the **testing** feed to obtain Nmap and NmapFE. NmapFE is the official UNIX GUI frontend that is distributed with Nmap. What OpenZaurus.Org calls NmapFE is actually Qopenmapfe (<http://home.midsouth.rr.com/zaurus/>), a simplified clone written by Dennis Webb. Scroll down the list of software packages and check Nmap, NmapFE, and anything else that catches your fancy. Many excellent security tools are available.
5. After selecting all of the appropriate software, click the GO (green arrow) icon on the top right hand of the screen. The installation manager screen shows the progress of software download and installation.

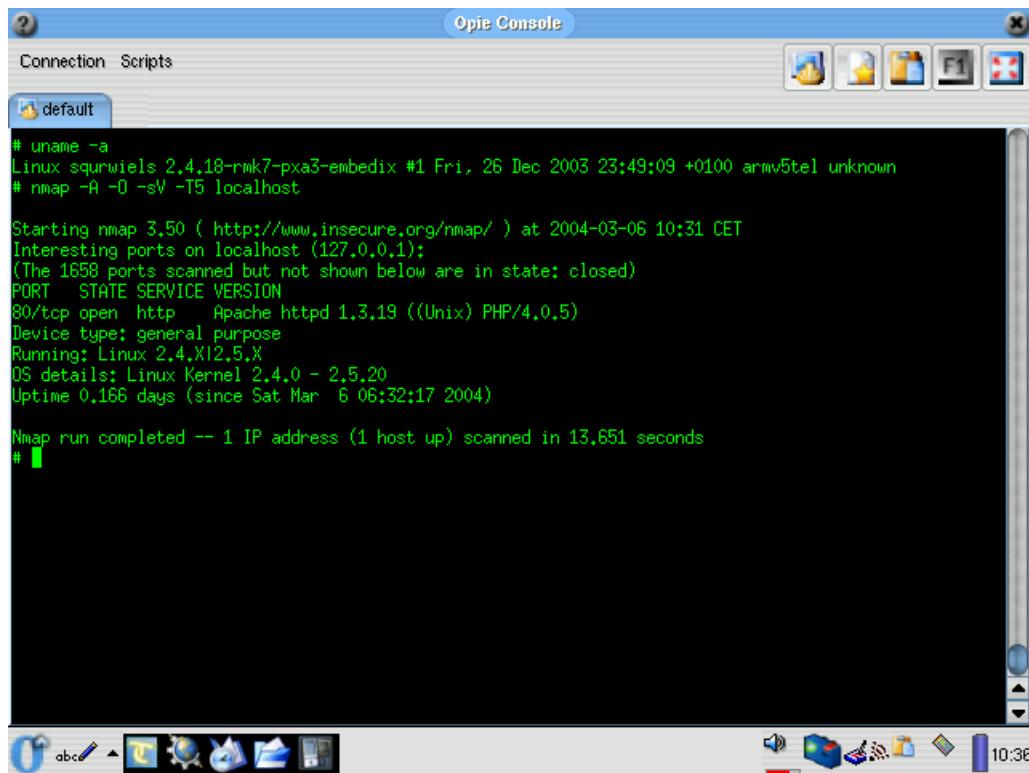
### **2.9.2. Using Nmap and NmapFE on the Zaurus**

Once NmapFE and Nmap have been properly installed, a new NmapFE icon should appear in the Applications menu. If it does not appear, try restarting Opie. Simply click the icon to use it. If you prefer the command-line version of Nmap, start the console and execute the appropriate command. The screenshots at the top of this recipe demonstrate

both methods. Except for a simplified option set in qopenmapfe, usage of Nmap is the same as described in the rest of this book. The following figures show another type of Zaurus (the SL-C760) and how to run Nmap on it.

**Figure 2-4. The Sharp Zaurus SL-C760 PDA**



**Figure 2-5.** The SL-C760 executing Nmap in a terminal window

## 2.10. Removing Nmap

If your purpose for removing Nmap is simply to upgrade to the latest version, you can usually use the "upgrade" option provided by most binary package managers. Similarly, installing the latest source code (as described in Section 2.2) generally overwrites any previous from-source installations. Removing Nmap is a good idea if you are changing install methods (such as from source to RPM or vice versa) or if you are not using Nmap anymore and you care about a few megabytes of disk space.

How to remove Nmap depends on how you installed it initially (see previous sections). Ease of removal (and other maintenance) is a major advantage of most binary packages. For example, when Nmap is installed using the RPM system common on Linux distributions, it can be removed by running the command **rpm -e nmap nmap-frontend** as root. Analogous options are offered by most other package managers -- consult their documentation for further information.

If you installed Nmap from source code, removal is slightly more difficult. If you still have the build directory available (where you initially ran **make install**), you can remove Nmap by running **make uninstall**. If you no longer have that build directory, type **nmap -v** to obtain the Nmap version number. Then download that source tarball for that version of Nmap from <http://download.insecure.org/nmap/dist/>. Uncompress the tarball and change into the newly created directory (**nmap-VERSION**). Run **./configure**, including any install-path options that you specified the first time (such as **--prefix** or **--datadir**). Then run **make uninstall**. Alternatively, you can simply delete all the Nmap-related files. If you used a default source install of Nmap versions 3.00 or higher, the following command

removes it.

```
# cd /usr/local  
# rm -f bin/nmap bin/nmapfe bin/xnmap  
# rm -f man/man1/nmap.1 man/man1/nmapfe.1 man/man1/xnmap.1  
# rm -rf share/nmap share/gnome/apps/Utilities/nmapfe.desktop
```

You may have to adjust the above commands slightly if you specified `--prefix` or other install-path option when first installing Nmap. The files relating to nmapfe/xnmap do not exist if you did not install the NmapFE frontend initially.

## Notes

1. <http://www.cert.org/advisories/CA-2002-28.html>
2. <http://www.cert.org/advisories/CA-2002-24.html>

# Chapter 3. Host Enumeration ("Ping Scanning")

## 3.1. Introduction

One of the very first steps in any network reconnaissance mission is to reduce a (sometimes huge) set of IP ranges into a list of active or interesting hosts. Scanning every port of every single IP address is slow and usually unnecessary. Of course what makes a host interesting depends greatly on the scan purposes. Network administrators may only be interested in hosts running a certain service, while security auditors may care about every single device with an IP address. An administrator may be comfortable using just an ICMP ping to locate hosts on his internal network, while an external penetration tester may use a diverse set of dozens of probes in an attempt to evade firewall restrictions.

Because host enumeration needs are so diverse, Nmap offers a wide variety of options for customizing the techniques used. Despite the name ping scan, this goes well beyond the simple ICMP echo request packets associated with the ubiquitous ping tool. Users can skip the ping step entirely with a list scan (-sL) or by disabling ping (-P0), or engage the network with arbitrary combinations of multi-port TCP SYN/ACK, UDP, and ICMP probes. The goal of these probes is to solicit responses which demonstrate that an IP address is actually active (is being used by a host or network device). On many networks, only a small percentage of IP addresses are active at any given time. This is particularly common with RFC1918-blessed private address space such as 10.0.0.0/8. That network has 16 million IPs, but I have seen it used by companies with less than a thousand machines. Host enumeration can find those machines in a sparsely allocated sea of IP addresses.

This chapter first discusses how Nmap ping scanning works overall, with high-level control options. Then specific techniques are covered, including how they work and when each is most appropriate. Nmap offers many ping techniques because it often takes carefully crafted combination to get through a series of firewalls and router filters leading to a target network. Effective overall ping scanning strategies are discussed, followed by a low-level look at the algorithms used.

## 3.2. Specifying Target Hosts and Networks

## 3.3. Host Enumeration Controls

By default, Nmap will include a ping scanning stage prior to more intrusive probes such as port scans, OS detection, or version detection. Nmap usually only performs intrusive scans on machines that are shown to be available in the ping scan stage. This saves substantial time and bandwidth over trying to scan every single IP address. However, this approach is not ideal for all circumstances. There are times when you *do* want to scan every IP (-P0), and other times when you want to do host enumeration and nothing more (-sP). There are even times when you want to print out the target hosts and exit prior to even sending ping probes (-sL). Nmap offers several high-level options to control this behavior.

### 3.3.1. List Scan (-sL)

The list scan is a degenerate form of host enumeration that simply lists each host of the network(s) specified, without sending any packets to the target hosts. By default, Nmap still does reverse-DNS resolution on the hosts to learn their names. Nmap also reports the total number of IP addresses at the end. The list scan is a good sanity check to ensure

that you have proper IP addresses for your targets. If the hosts sport domain names you do not recognize, it is worth investigating further to prevent scanning the wrong company's network.

There are many reasons target IP ranges can be incorrect. Even network administrators can mistype their own netblocks, and pen-testers have even more to worry about. In some cases, security consultants are given the wrong addresses. In others, they try to find proper IP ranges through resources such as whois databases and routing tables. The databases can be out of date, or the company could be loaning IP space to other organizations. Whether to scan corporate parents, siblings, service providers, and subsidiaries is an important issue that should be worked out with the customer in advance. A preliminary list scan helps confirm exactly what targets are being scanned.

Another reason for an advance list scan is stealth. In some cases, you do not want to begin with a full-scale assault on the target network that is likely to trigger IDS alerts and bring unwanted attention. A list scan is unobtrusive and provides information that may be useful in choosing which individual machines to target. It is possible, though highly unlikely, that the target will notice all of the reverse-DNS requests.

A list scan is specified with the `-sL` command-line option. Since the idea is to simply print a list of target hosts, options for higher level functionality such as port scanning, OS detection, or ping scanning cannot be combined with this. If you wish to disable ping scanning while still performing such higher level functionality, read up on the `-p0` option described in the next section. Example 3-1 shows list scan being used to enumerate the CIDR<sup>1</sup> /28 network range (16 IP addresses) surrounding the main Stanford webserver.

### **Example 3-1. Enumerating hosts surrounding WWW.Stanford.Edu with list scan**

```
felix~> nmap -sL www.stanford.edu/28

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Host www9.Stanford.EDU (171.67.16.80) not scanned
Host www10.Stanford.EDU (171.67.16.81) not scanned
Host scriptorium.Stanford.EDU (171.67.16.82) not scanned
Host coursework-a.Stanford.EDU (171.67.16.83) not scanned
Host coursework-e.Stanford.EDU (171.67.16.84) not scanned
Host www3.Stanford.EDU (171.67.16.85) not scanned
Host leland-dev.Stanford.EDU (171.67.16.86) not scanned
Host coursework-preprod.Stanford.EDU (171.67.16.87) not scanned
Host stanfordwho-dev.Stanford.EDU (171.67.16.88) not scanned
Host workgroup-dev.Stanford.EDU (171.67.16.89) not scanned
Host courseworkbeta.Stanford.EDU (171.67.16.90) not scanned
Host www4.Stanford.EDU (171.67.16.91) not scanned
Host coursework-i.Stanford.EDU (171.67.16.92) not scanned
Host leland2.Stanford.EDU (171.67.16.93) not scanned
Host coursework-j.Stanford.EDU (171.67.16.94) not scanned
Host 171.67.16.95 not scanned
Nmap run completed -- 16 IP addresses (0 hosts up) scanned in 0.384 seconds
```

### **3.3.2. Ping Scan (-sP)**

This option tells Nmap to *only* perform a ping scan, then print out the available hosts that responded to the scan. No further testing (such as port scanning or OS detection) is performed. This is one step more intrusive than the list scan, and can often be used for the same purposes. It allows light reconnaissance of a target network without attracting much attention. Knowing how many hosts are up is more valuable to attackers than the list of every single IP and host name provided by list scan.

Systems administrators often find this option valuable as well. It can easily be used to count available machines on a network or monitor server availability. This is often called a ping sweep, and is more reliable than pinging the broadcast address because many hosts do not reply to broadcast queries.

The following example shows a quick ping sweep against the CIDR /24 (256 IPs) surrounding one of my favorite Linux web sites, LWN.Net.

```
# nmap -sP -T4 www.lwn.net/24

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Host 66.216.68.0 seems to be a subnet broadcast address (returned 1 extra pings).
Host 66.216.68.1 appears to be up.
Host 66.216.68.2 appears to be up.
Host 66.216.68.3 appears to be up.
Host server1.camnetsec.com (66.216.68.10) appears to be up.
Host akqa.com (66.216.68.15) appears to be up.
Host asria.org (66.216.68.18) appears to be up.
Host webcubic.net (66.216.68.19) appears to be up.
Host dizzy.yellowdog.com (66.216.68.22) appears to be up.
Host www.outdoorwire.com (66.216.68.23) appears to be up.
Host www.inspectorhosting.com (66.216.68.24) appears to be up.
Host jwebmedia.com (66.216.68.25) appears to be up.
[...]
Host rs.lwn.net (66.216.68.48) appears to be up.
Host 66.216.68.52 appears to be up.
Host cuttlefish.laughingsquid.net (66.216.68.53) appears to be up.
[...]
Nmap run completed -- 256 IP addresses (105 hosts up) scanned in 12.691 seconds
```

This example only took 13 seconds, but provides valuable information. In that class C sized address range, 105 hosts are up. From the unrelated domain names all packed into such a small IP space, it is clear that LWN uses a colocation or dedicated server provider. If the LWN machines turned out to be highly secure, an attacker might go after one of those neighbor machines and then perform a local ethernet attack with tools such as Ettercap or Dsniff. A white-hat use of this data would be a network administrator considering moving machines to this provider. He might e-mail a few of the listed organizations and ask their opinion of the service before signing a long-term contract or making the expensive and disruptive datacenter move.

The `-sP` option sends an ICMP echo request and a TCP packet to port 80 by default (except when executed by an unprivileged UNIX user). It can be combined with any of the techniques discussed in the next section for greater flexibility. If any of those probe type and port number options are used, these default probes are overridden. When strict firewalls are in place between the source host running Nmap and the target network, using those advanced techniques is recommended. Otherwise hosts could be missed when the firewall drops probes or their responses.

### 3.3.3. Disable Ping (-P0)

Another option is to skip the Nmap enumeration stage altogether. Normally, Nmap uses this stage to determine active machines for heavier scanning. By default, Nmap only performs heavy probing such as port scans, version detection, or OS detection against hosts that are found to be up. Disabling host enumeration with `-P0` causes Nmap to attempt the requested scanning functions against *every* target IP address specified. So if a class B sized target address space (/16) is specified on the command line, all 65,536 IP addresses are scanned. That second option character in `-P0` is a

zero and not the letter O. Proper host enumeration is skipped as with the list scan, but instead of stopping and printing the target list, Nmap continues to perform requested functions as if each target IP is active.

There are many reasons for disabling the Nmap ping tests. One of the most common is intrusive vulnerability assessments. One can specify dozens of different ping probes in an attempt to elicit a response from all available hosts, but it is still possible that an active yet heavily firewalled machine might not reply to any of the probes. So to avoid missing anything, auditors frequently perform intense scans, such as for all 65,536 TCP ports, against every IP on the target network. It may seem wasteful to send hundreds of thousands of packets to IP addresses that probably have no host listening, and it can slow scan times by an order of magnitude or more. Nmap must send retransmissions to every port in case the original probe was dropped in transit, and Nmap must spend substantial time waiting for responses because it has no round-trip-time (RTT) estimate for these non-responsive IP addresses. But serious penetration testers are willing to pay this price to avoid even a slight risk of missing active machines. They can always do a quick scan as well, leaving the massive `-P0` scan to run in the background while they work. Chapter 6 provides substantial performance advice.

Another frequent reason for using `-P0` is that the tester has a list of machines that are already known to be up. There is no point wasting time with the host enumeration stage, the reasoning goes. The user creates their own list of active hosts and then passes it to Nmap using the `-iL` (take input from list) option. This strategy is rarely beneficial from a time-saving perspective. Even one unresponsive IP address in a large list will often take more time to scan than a whole ping scanning stage would have, due to the retransmission and RTT estimate issues discussed in the previous paragraph. In addition, the ping stage allows Nmap to gather RTT samples that can speed up the following port scan, particularly if the target host has strict firewall rules. While specifying `-P0` is rarely helpful as a time saver, it is important if some of the machines on your list block all of the enumeration techniques that would otherwise be specified. Users must strike a balance between scan speed and the possibility of missing a heavily cloaked machine.

## 3.4. Host Enumeration Techniques

There was a day when finding whether an IP address was registered to an active host was easy. Simply send an ICMP echo request ("ping") packet and wait for a response. Firewalls rarely blocked these requests, and the vast majority of hosts obediently responded. Such a response has been required since 1989 by RFC 1122 (<http://www.rfc-editor.org/rfc/rfc1122.txt>), which clearly states that "Every host MUST implement an ICMP Echo server function that receives Echo Requests and sends corresponding Echo Replies".

Unfortunately for network explorers, many administrators have decided that security concerns trump RFC requirements and have blocked ICMP ping messages. Example 3-2 uses an ICMP-only Nmap ping scan against six popular Web sites, but receives only two responses. This demonstrates that hosts can no longer be assumed unavailable based on failure to elicit an ICMP ping response. The `-sP -PE` options specify an ICMP-only ping scan and will soon be discussed. `-R` tells Nmap to perform reverse-DNS resolution against all hosts, even down ones.

### Example 3-2. Attempts to ping popular Internet hosts

```
# nmap -sP -PE -R -v microsoft.com ebay.com citibank.com google.com slashdot.org yahoo.com

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Host origin2.microsoft.com (207.46.250.252) appears to be down.
Host pages.ebay.com (66.135.192.87) appears to be down.
Host ld1-www.citicorp.com (192.193.195.132) appears to be down.
Host 216.239.57.99 appears to be up.
Host slashdot.org (66.35.250.150) appears to be down.
```

```
Host w3.rc.dcn.yahoo.com (216.109.127.30) appears to be up.
Nmap run completed -- 6 IP addresses (2 hosts up) scanned in 3.762 seconds
```

Fortunately, Nmap offers a wide variety of host enumeration techniques beyond the standard ICMP echo request. They are described in the following sections.

### 3.4.1. TCP SYN Ping (-PS[portlist])

This option sends an empty TCP packet with the SYN flag set. The default destination port is 80 (configurable at compile time by changing DEFAULT\_TCP\_PROBE\_PORT in `nmap.h`), but an alternate port can be specified as a parameter. A comma separated list of ports can even be specified (e.g. `-PS22,23,25,80,113,1050,35000`), in which case probes will be attempted against each port in parallel.

The SYN flag suggests to the remote system that you are attempting to establish a connection. Normally the destination port will be closed, and a RST (reset) packet sent back. If the port happens to be open, the target will take the second step of a TCP 3-way-handshake by responding with a SYN|ACK TCP packet. The machine running Nmap then tears down the nascent connection by responding with a RST rather than sending an ACK packet which would complete the 3-way-handshake and establish a full connection.

Nmap does not care whether the port is open or closed. Either the RST or SYN|ACK response discussed previously tell Nmap that the host is available and responsive. However, Nmap does note the distinction in certain cases, allowing for a "turbo-mode" single-port sweep discussed in Chapter 4.

On UNIX boxes, only the privileged user `root` is generally able to send and receive raw TCP packets. For unprivileged users, a workaround is automatically employed whereby the `connect()` system call is initiated against each target port. This has the effect of sending a SYN packet to the target host, in an attempt to establish a connection. If `connect()` returns with a quick success or an ECONNREFUSED failure, the underlying TCP stack must have received a SYN|ACK or RST and the host is marked available. If the connection attempt is left hanging until a timeout is reached, the host is marked as down. This workaround is also used for IPv6 connections, as raw IPv6 packet building support is not yet available in Nmap.

Example 3-2 failed to detect four out of six machines because they did not respond to ICMP echo requests. Repeating the experiment using a SYN probe to port 80 (`http`) garners responses from all six, as shown in Example 3-3.

#### Example 3-3. Retry Host Enumeration using port 80 SYN probes

```
# nmap -sP -PS80 -R -v microsoft.com ebay.com citibank.com google.com slashdot.org yahoo.com

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Host origin2.microsoft.com (207.46.249.252) appears to be up.
Host pages.ebay.com (66.135.192.87) appears to be up.
Host ld1-www.citicorp.com (192.193.195.132) appears to be up.
Host 216.239.57.99 appears to be up.
Host slashdot.org (66.35.250.150) appears to be up.
Host w3.rc.dcn.yahoo.com (216.109.127.30) appears to be up.
Nmap run completed -- 6 IP addresses (6 hosts up) scanned in 0.479 seconds
```

In addition to detecting all six machines, the second run is much faster. It takes less than half a second because the machines are scanned in parallel and it never times out waiting for a response. This test is not entirely fair because these are all popular web servers and thus can be expected to listen on port 80. However, it demonstrates the point that different types of hosts respond to different probe types. Nmap supports the usage of many scan types in parallel to enable effective scanning of diverse networks.

### 3.4.2. TCP ACK Ping (-PA[portlist])

The TCP ACK ping is quite similar to the just-discussed SYN ping. The difference, as you could likely guess, is that the TCP ACK flag is set instead of the SYN flag. Such an ACK packet purports to be acknowledging data over an established TCP connection, but no such connection exists. So remote hosts should always respond with a RST packet, disclosing their existence in the process.

The -PA option uses the same default port as the SYN probe (80) and can also take a list of destination ports in the same format. If an unprivileged user tries this, or an IPv6 target is specified, the connect() workaround discussed previously is used. This workaround is imperfect because connect() is actually sending a SYN packet.

The reason for offering both SYN and ACK ping probes is to maximize the chances of bypassing firewalls. Many administrators configure routers and other simple firewalls to block incoming SYN packets except for those destined for public services like the company web site or mail server. This prevents other incoming connections to the organization, while allowing users to make unobstructed outgoing connections to the Internet. This non-stateful approach takes up few resources on the firewall/router and is widely supported by hardware and software filters. As just one example of the prevalence of this method, the Linux Netfilter/iptables firewall software offers the --syn convenience option, which the man page describes as follows.

“ Only match TCP packets with the SYN bit set and the ACK and RST bits cleared. Such packets are used to request TCP connection initiation; for example, blocking such packets coming in an interface will prevent incoming TCP connections, but outgoing TCP connections will be unaffected. It is equivalent to --tcp-flags SYN,RST,ACK SYN. ”

When firewall rules such as this are in place, SYN ping probes (-PS) are likely to be blocked when sent to closed target ports. In such cases, the ACK probe shines as it cuts right through these rules.

Another common type of firewall uses stateful rules that drop unexpected packets. This feature was initially found mostly on high-end firewalls, though it has become much more common over the years. The Linux Netfilter/iptables system supports this through the --state option, which categorizes packets based on connection state as described in the following man page excerpt.

“ Possible states are INVALID meaning that the packet is associated with no known connection, ESTABLISHED meaning that the packet is associated with a connection which has seen packets in both directions, NEW meaning that the packet has started a new connection, or otherwise associated with a connection which has not seen packets in both directions, and RELATED meaning that the packet is starting a new connection, but is associated with an existing connection, such as an FTP data transfer, or an ICMP error. ”

The ACK probe is unlikely to work against firewalls taking this approach, as such an unexpected packet will be classified in the INVALID state and probably dropped. Example 3-4 shows an attempted ACK ping against Microsoft. Their stateful firewall drops the packet, leading Nmap to wrongly conclude that the host is down. The SYN probe has a much better chance of working in such cases. This begs the question of which technique to use when the firewall rules of the target networks are unknown or inconsistent. The proper answer is usually both. Nmap can send SYN and ACK probes to many ports in parallel, as well as performing other host enumeration techniques at the same time. This is further discussed in Section 3.5.

#### Example 3-4. Attempted ACK ping against Microsoft

```
# nmap -sP -PA www.microsoft.com
Starting nmap 3.51-TEST4 ( http://www.insecure.org/nmap/ )
```

```
Note: Host seems down. If it is really up, but blocking our ping probes, try -PO
Nmap run completed -- 1 IP address (0 hosts up) scanned in 37.949 seconds
```

### **3.4.3. UDP Ping (-PU[portlist])**

Another host enumeration option is the UDP ping, which sends an empty (unless `--data_length` is specified) UDP packet to the given ports. The portlist takes the same format as with the previously discussed `-PS` and `-PA` options. If no ports are specified, the default is 31338. This default can be configured at compile-time by changing `DEFAULT_UDP_PROBE_PORT` in `nmap.h`. A highly uncommon port is used by default because sending to open ports is often undesirable for this particular scan type.

Upon hitting a closed port on the target machine, the UDP probe should elicit an ICMP port unreachable packet in return. This signifies to Nmap that the machine is up and available. Many other types of ICMP errors, such as host/network unreachables or TTL exceeded are indicative of a down or unreachable host. A lack of response is also interpreted this way. If an open port is reached, most services simply ignore the empty packet and fail to return any response. This is why the default probe port is 31338, which is highly unlikely to be in use. A few services, such as chargen, will respond to an empty UDP packet, and thus disclose to Nmap that the machine is available.

The primary advantage of this scan type is that it bypasses firewalls and filters that only screen TCP. For example, I once owned a Linksys BEFW11S4 wireless broadband router. The external interface of this device filtered all TCP ports by default, but UDP probes would still elicit port unreachable messages and thus give away the device.

### **3.4.4. ICMP Ping Types (-PE, -PP, and -PM)**

In addition to the unusual TCP and UDP host enumeration types discussed previously, Nmap can send the standard packets sent by the ubiquitous ping program. Nmap sends an ICMP type 8 (echo request) packet to the target IP addresses, expecting a type 0 (Echo Reply) in return from available hosts. As noted at the beginning of this chapter, many hosts and firewalls now block these packets, rather than responding as required by RFC 1122. For this reason, ICMP-only scans are rarely reliable enough against unknown targets over the Internet. But for system administrators monitoring an internal network, this can be a practical and efficient approach. Use the `-PE` option to enable this echo request behavior.

While echo request is the standard ICMP ping query, Nmap does not stop there. The ICMP standard (RFC 792 (<http://www.rfc-editor.org/rfc/rfc792.txt>)) also specifies timestamp request, information request, and address mask request packets as codes 13, 15, and 17, respectively. While the ostensible purpose for these queries is to learn information such as address masks and current times, they can easily be used for host enumeration. A system that replies is up and available. Nmap does not currently implement information request packets, as they are not widely supported. RFC 1122 insists that "a host **SHOULD NOT** implement these messages". Timestamp and address mask queries can be sent with the `-PP` and `-PM` options, respectively. A timestamp reply (ICMP code 14) or address mask reply (code 18) discloses that the host is available. These two queries can be valuable when admins specifically block echo request packets, but forget that other ICMP queries can be used for the same purpose.

### **3.4.5. Default Combination (-PB)**

If none of these host enumeration techniques are chosen, Nmap uses a default which is equivalent to the `-PA -PE` arguments for Windows or privileged (root) UNIX users. Attentive readers know that this means a TCP ACK packet to port 80 and an ICMP Echo Request query are sent to each machine. For unprivileged UNIX shell users, the default

is equivalent to `-PS` (a TCP connect() call against port 80 of the target hosts). For security auditing, I recommend using a more comprehensive set of ping types, such as those discussed in Section 3.5.2.4.

### 3.4.6. ARP Scan (`-P?`)

This scan *does not yet exist*, but implementing it is high on the desired feature priority list. It sends an ethernet ARP request for every target IP given. If a response is received, that host is available. Of course this only works for targets on a local ethernet network, but that covers a substantial portion of Nmap usage. This scan should be much faster and even a little more reliable than other ping scan types under these circumstances. The technique and implementation plans are described further in Chapter 13.

## 3.5. Putting it All Together: Host Enumeration Strategies

### 3.5.1. Related Options

Previous sections describe the major options used to control the Nmap host enumeration phase and customize the techniques used. However, there are many more general Nmap options which are relevant here. This section provides a brief description of how these option flags relate to ping scanning. See the Nmap Reference Guide (Chapter 14) for complete descriptions of each option.

`-v` (same as `--verbose`)

By default, Nmap usually only prints active, responsive hosts. Verbose mode causes Nmap to print down hosts, as well as extra information about active ones.

`--source_port <portnum>`(same as `-g`)

Setting a constant source port works for ping scanning (TCP and UDP) as it does with other Nmap features. Some naive firewall administrators make a ruleset exception in order keep DNS (port 53) or FTP-DATA (port 20) working. Of course this opens a hole big enough to drive an Nmap ping scan through. Chapter 9 provides further details on this technique.

`-n, -R`

The `-n` option disables all DNS resolution, while the `-R` option enables DNS queries for all hosts, even down ones. The default behavior is to limit DNS resolution to active hosts. These options are particularly important for ping scanning because DNS resolution can greatly affect scan times.

`--data_length <length>`

This option adds `length` random bytes of data to every packet, and works with the TCP, UDP, and ICMP ping scan types (for privileged users scanning IPv4). This helps make the scan less conspicuous and more like the packets generated by the ubiquitous ping diagnostics program. Several intrusion detection systems (IDS), including Snort, have alerts for zero-byte ping packets. This option evades those alerts. An option value of 32 makes an echo request look more like it came from Windows, while 56 simulates the default Linux ping.

--ttl

Setting the outgoing TTL is supported for privileged users doing IPv4 ping scans. This could be useful as a safety precaution to ensure a scan does not propagate beyond the local network. It can also be used to simulate a native ping program even more convincingly.

Canned timing options (-T3, -T4, -T5, etc.)

As with Nmap functions in general, higher -T values speed up scanning. With a moderately fast and reliable connection between the source and target networks (i.e. anything more than a dial-up modem), the -T4 option is recommended.

--max\_parallelism, --min\_parallelism

These affect how many probes may be outstanding at once. With the default ping type (2-probes), the parallelism value is roughly the number of machines scanned in parallel. Reducing the ping techniques to one probe per host (e.g. -PE) will double the number of hosts scanned at once for a given parallelism level, while increasing to four probes per host (e.g. -PE -PS22,113,50000) halves it. Most users simply stick to the canned timing options such as -T4.

--min\_rtt\_timeout, --max\_rtt\_timeout, --initial\_rtt\_timeout

These options control how long Nmap waits for a ping response.

Input options (-iL, -iR)

Host input options are supported as in the rest of Nmap. Users often combine the input-from-list (-iL) option with -P0 to avoid ping-scanning hosts that are already known to be up. Read Section 3.3.3 before doing this in an attempt to save time. The -iR chooses hosts at random from allocated Internet IP space. It takes as an argument the number of random hosts you wish to scan. Use zero for a never-ending (until you abort or kill the Nmap process) scan.

Output options (-oA, -oN, -oG, -oX, etc.)

All of the Nmap output types (normal, grepable, and XML) support ping scanning. Chapter 11 further describes how they work.

--randomize\_hosts (same as -rH)

Shuffling the host scan order with this option may make the scan less conspicuous, though it also can make the scan output a bit more difficult to follow.

--packet\_trace

The normal Nmap output indicates whether a host is up or not, but does not describe which enumeration test(s) the host responded to. This is because Nmap uses a short-circuit algorithm for performance reasons. As soon as it receives any one response from a host, it stops listening for more. Printing the response might mislead users into thinking that the host only responded to one certain test, when the reality is that Nmap stopped paying attention after that point. Scanning several times might produce different results, depending on which response comes in first. To avoid this confusion, Nmap omits the ping response type altogether. Users who really need that information can rescan with --packet\_trace and see exactly what is going on at the packet level.

-D

Decoys are fully supported for privileged IPv4 ping scans, camouflaging the true attacker. Decoys are not used in DNS requests, so -n may be advisable for ultra-sensitive scans.

-6

The TCP connect()-based ping scans (-PS) support the IPv6 protocol, including multi-port mode.

-S <source IP address>, -e <sending device name>

As with other functions of Nmap, the source address and sending device can be specified with these options.

#### General options

By default, or if -P0 is specified, Nmap moves onto more intrusive scanning after the host enumeration stage. Thus many dozens of general port scanning, OS detection, and version detection options can be used. See the reference guide or relevant chapters for further information.

### 3.5.2. Choosing and Combining Ping Options

Effective scanning requires more than knowing all of the options described in this and previous sections. Users must understand how and when to use them to suit the target network topology and scanning goals.

#### 3.5.2.1. TCP probe and port selection

The TCP ping options are some of the most powerful enumeration techniques in Nmap. An administrator may be able to get away with blocking ICMP echo request packets without affecting most users, but a server absolutely must respond to SYN packets sent to the public services it provides. Meanwhile, ACK packets often get through non-stateful firewalls. I would recommend using both of SYN and ACK probes, using lists of ports based on any knowledge you might have of the target networks as well as more generally popular ports. A quick scan of more than 10,000 IP addresses across the Internet showed the ports in Table 3-1 to be particularly valuable. Of hosts with a default-drop filter (the hardest type to reach), these are the ports most likely to be accessible (open or closed).

**Table 3-1. Valuable TCP probe ports, in descending order of accessibility.**

Port number / Service	Reasoning
80/http	The prevalence of Web servers on the Internet leads many newbies to believe that the Web <i>is</i> the Internet.
25/smtp	Mail is another Internet "killer app" that companies allow through their firewalls.
22/ssh	SSH seems to have finally surpassed telnet as the standard for remote terminal administration.
443/https	SSL is a popular way for web sites to protect confidential information.
21/ftp	This file transfer protocol lives on, though many firewall administrators would not mourn its passing.

Port number / Service	Reasoning
113/auth	The auth (identd) service allows servers (usually mail or IRC) to request the username of clients connected to them. Administrators often leave this port unfiltered to avoid long timeouts that can occur when firewall rules prevent servers from connecting back to port 113. Using this port for ping scanning can sometimes lead to false positives, as some admins have been known to configure their firewalls to forge RST packets back in response to auth queries to any IP on their network, even when no machine exists at that IP. Administrators do this to avoid server timeouts while still preventing the ports from being accessed.
23/telnet	Many devices still offer this administrative interface, though it is a security nightmare.
53/domain	Domain Name servers are extremely widespread.
554/rtsp	Real Time Stream Control Protocol is used by media servers, including Quicktime and RealServer.
3389/ms-term-server	Microsoft Terminal Services
1723/pptp	Point-to-Point Tunneling Protocol is often used to implement VPN solutions on Microsoft Windows.
389/ldap	The Lightweight Directory Access Protocol is often used to store contact directories and the like.
636/ldapssl	LDAP over SSL is popular for accessing confidential information.
256/FW1-secureremote	Checkpoint Firewall-1 devices often have this administration port open.

In addition to popular ports such as the ones in the list above, choosing at least one high-numbered port is recommended. Many poorly configured firewalls only have default-deny for the "reserved ports", meaning those below 1024. I usually pick a high numbered port out of the air, such 40,000 or 10,042, to catch machines behind this sort of firewall.

In choosing the ports to probe, remember to emphasize platform diversity. If you are limiting your ping scan to two ports, http (80) and ssh (22) are probably better than http and https (443) because the latter two are related web services, and many machines that have https will often have http available anyway. Finding two accessible ports on the same machine is no better for ping scanning purposes than finding one. Choosing ports so that a broad set of hosts will match at least one of them is the goal.

Note that the valuable port table does not include many client-oriented ports such as the ubiquitous Windows SMB port 135. The primary reason is that this table only looked at hosts behind default-deny firewalls, where the vast majority of ports are filtered. In those situations, Windows ports such as 135-139 and 445 are usually blocked. When these machines are not behind a firewall, the open ports are unimportant for ping scanning because the thousands of closed ports work just as well.

### 3.5.2.2. UDP port selection

In selecting UDP ports, remember that an open port is unlikely to respond to the probes. Unfiltered ports are desired. To avoid open ports, you might consider excluding common UDP services like DNS (port 53) and SNMP (161). On the other hand, firewall rules are often so broad that those probes (particularly to port 53) might get through and hit a closed port. So I would recommend choosing at least port 53 and an arbitrarily selected high-numbered port.

### 3.5.2.3. ICMP probe selection

For ICMP, the standard ping (echo request) is usually worth trying. Many administrators specifically allows this because it is useful for debugging or because RFC 1122 requires it. I would also use at least one of the address mask or timestamp requests. These are valuable for networks where administrators intentionally block echo request packets, but forget about other ICMP queries.

### 3.5.2.4. Designing the ideal combinations of probes

How all of these ping types are combined into a ping scan strategy depends on characteristics of the target network and on the scan goals. For internal networks, the default ping type usually works well. The default is also fine for most casual scanning, where missing an occasional host is no big deal. Adding more probes can help catch those occasional stealthy machines, at the expense of making the ping scan take a bit longer. Time taken is roughly proportional to the number of probes sent to each machine. For security scans of target networks over the Internet, adding more probes is usually advisable. Try to include a diverse set of the techniques discussed previously. Here is a set of ping options that should catch the vast majority of hosts: `-PE -PT -PS21,22,23,25,80,113,31339 -PA80,113,443,10042`. Adding in `--source_port 53` might be worthwhile as well. How much better will the results be, and how much longer will it take? That depends on the target network, of course, but the Nmap random target selection option (`-iR`) makes it easy to perform a quick test. Example 3-5 shows Nmap generating 50,000 random IP addresses and then performing a default ping scan. You should remember that the default is a TCP ACK packet to port 80, and an ICMP echo request packet.

#### Example 3-5. Generating 50,000 IP Addresses, then ping scanning with default options

```
#nmap -n -sL -iR 50000 -oN - | grep "not scanned" | awk '{print $2}' > 50K_Test_IPs
# head -5 50K_Test_IPs
186.247.186.175
57.190.183.219
152.249.87.150
208.149.189.242
43.210.154.84
# nmap -sP -T4 -iL 50K_Test_IPs -oA 50KHosts_Defaultping

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Host 64.38.217.78 appears to be up.
Host pD954B8C2.dip.t-dialin.net (217.84.184.194) appears to be up.
Host 218.88.159.224 appears to be up.
[ Thousands of lines cut ]
Host d84.public.swarthmore.edu (130.58.248.84) appears to be up.
Host ip24-250-44-170.ri.ri.cox.net (24.250.44.170) appears to be up.
Host host121-52.apgea.army.mil (131.92.121.52) appears to be up.
Nmap run completed -- 50000 IP addresses (1732 hosts up) scanned in 3008.070 seconds
```

Scanning the 50,000 address took fifty minutes, and 1,732 hosts were detected. Most of the DNS names were already in cache due to a previous scratch run, though it still would have likely been much faster had DNS resolution been disabled with `-n`. To determine the effects of using a wider range of ping techniques, the same 50K hosts were rescanned with 13 probes per port rather than the default of two. As shown in Example 3-6, Nmap was able to detect 396 more hosts (23%). It took 45 minutes (90%) longer, but that is acceptable in many cases. Note that not all of the new hosts may be legitimate. Increasing the number of ping probes increases the chances that Nmap will hit network artifacts that make a non-existent host appear to be active. Firewalls that return a RST for SYN or ACK packets to port 113 are one example of this.

#### **Example 3-6. Repeating ping scan with extra probes**

```
# nmap -sP -PE -PT -PS21,22,23,25,80,113,31339 -PA80,113,443,10042 -T4 \
--source_port 53 -iL 50K_Test_IPs -oA 50KHosts_extendedping

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Host 64.38.217.78 appears to be up.
Host pD954B8C2.dip.t-dialin.net (217.84.184.194) appears to be up.
Host YahooBB220053236002.bbtec.net (220.53.236.2) appears to be up.
[ Thousands of lines cut ]
Host d84.public.swarthmore.edu (130.58.248.84) appears to be up.
Host ip24-250-44-170.ri.ri.cox.net (24.250.44.170) appears to be up.
Host sdn-ap-007castocP0414.dialsprint.net (63.187.65.160) appears to be up.
Host host121-52.apgea.army.mil (131.92.121.52) appears to be up.
Nmap run completed -- 50000 IP addresses (2128 hosts up) scanned in 5709.445 seconds
```

When performing security audits for clients, I normally start with port scan against about 1700 common ports (the default) with comprehensive ping scan options like those shown in Example 3-6. Such a scan does not take particularly long, allowing me to quickly start working. I also launch `-P0` (ping disabled) scans against all 65K ports in the background while I work. When they finish, which may be days later, I compare them to my initial quick scan and investigate any new ports or machines found.

## **3.6. Finding an Organization's IP addresses to Scan**

\* Need to actually write this section

## **3.7. Host Enumeration Code Algorithms**

One of the greatest benefits of Open Source software like Nmap is that curious users are always able to study the source code when they want answers about its operation. In the case of host enumeration, almost all of the important algorithms are contained in `targets.cc`. The highest level ping scanning function is `nexthost()`, which calls `massping()` to coordinate the actual packet-level techniques chosen. `massping()`, in turn, relies on lower level functions such as aptly named `sendrawtcpudppingqueries()`, `sendpingqueries()`, and `get_connecttcpscan_results()`. Unlike port scanning, which has numerous algorithms based on the technique chosen (such as SYN scan vs. FIN scan), host enumeration is all handled the same way at a high level.

While source code analysis is the only way to truly get the complete picture of Nmap operation down to every trivial detail, it is not always the easiest approach to understanding Nmap. In many cases, the most effective way to quickly

peek at Nmap's behavior given a set of command-line options is to add the `--packet_trace` option, which prints out all of the packets sent and received by Nmap.

Because these are excellent resources for learning the nitty-gritty details of Nmap operation, I'll only discuss the host enumeration algorithm at a high level here. When Nmap is executed, it may be passed networks containing hundreds of thousands or even millions of hosts. So Nmap breaks them into blocks that are small enough to deal with at one time (hundreds up to a couple thousand hosts). The ping scanner then pulls out a group of the first dozen or so hosts from the block. The exact initial group size depends on Nmap parameters used. The probes requested by the user are then sent to each member of the group in one spurt, and Nmap begins waiting for responses. When a conclusive response is received, that host is marked as up or down as appropriate, and Nmap resumes waiting for further responses. Nmap waits until it receives a conclusive response from every group member (unlikely for large groups), or it times out. Upon timeout, Nmap tests whether any group members have already been through the maximum number of retransmissions. If so, they are marked as down. All of the hosts which left the group because of a response or because Nmap gave up on retransmissions are then replaced by new members from the block. Nmap starts the cycle again, sending initial probes to the new group members and retransmissions to the existing ones. Eventually, Nmap runs out of new hosts in the block and the group size dwindles to zero as retransmissions complete. The ping scanning subsystem returns the results so that Nmap can begin port scanning or any other requested probing of the target machines. When Nmap finishes with them, it passes the next block to the ping scanner.

This parallelization allows the Nmap ping scanning subsystem to work very quickly. Multiple hosts, usually with multiple probes per host, are handled in parallel. The group size and timeout periods are modified in real-time based on packet latency timers and dropped packet detection. Most other components of Nmap can handle just one target host at a time. Upgrading the DNS resolver, port scanners, and possibly even OS detection to deal with multiple hosts at once, like the ping scanner and version detection can, is an ongoing project.

## Notes

1. Classless Inter-Domain Routing (CIDR) notation is a method for describing networks with more granularity than class A (CIDR /8), class B (CIDR /16), or class C (CIDR /24) notation. An excellent description is available at <http://public.pacbell.net/dedicated/cidr.html> .

# Chapter 4. Port Scanning Overview

## 4.1. Introduction to Port Scanning

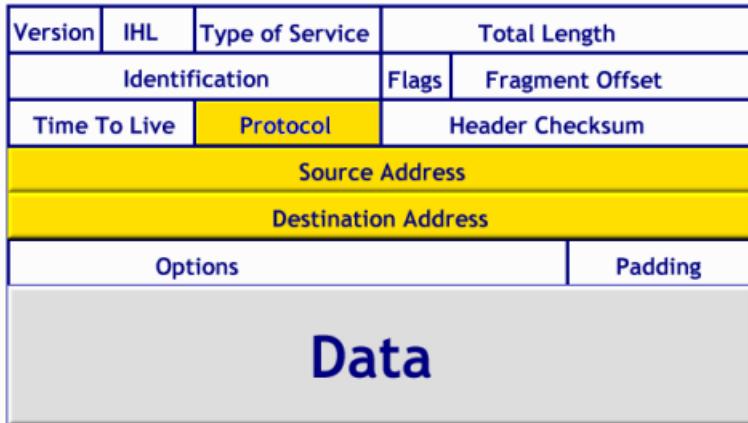
While Nmap has grown in functionality over the years, it began as an efficient port scanner, and that remains its core function. The simple command `nmap target` scans more than 1660 TCP ports on the host `target`, classifying each port into the state open, closed, or filtered.

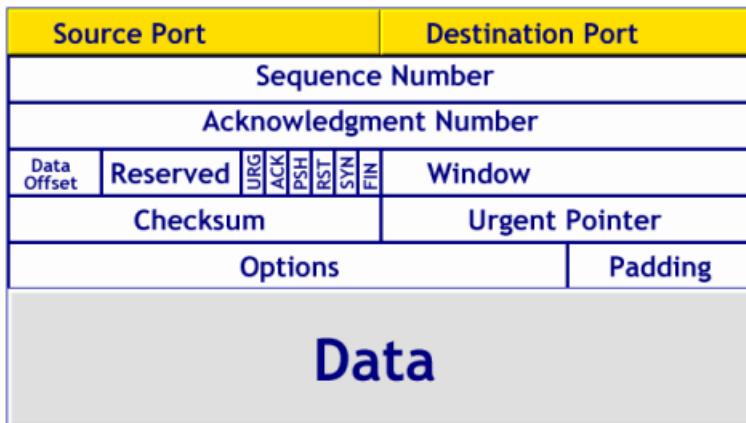
### 4.1.1. What exactly is a port?

Ports are simply a software abstraction, used to distinguish between communication channels. Similar to the way IP addresses are used to identify machines on the Internet, ports identify specific applications in use on a single machine. For example, your web browser will by default connect to TCP port 80 of machines in http URLs. If you specify the secure https protocol instead, the browser will try port 443 by default.

Nmap works with two protocols that use ports: TCP and UDP. A connection for each protocol is uniquely identified by four elements: source and destination IP addresses and corresponding source and destination ports. All of these elements are simply numbers placed in the headers of each packet sent between hosts. The protocol is an 8-bit field, which specifies what type of packet is contained in the IP data (payload) section. For example, TCP is protocol number 6, and UDP is 17. IPv4 addresses at 32-bits wide (128 with IPv6), and ports are each 16-bits long. The following figures, which are courtesy of Linux-France.Org (<http://www.linux-france.org/>), display the header layout.

Figure 4-1. IPv4 Header Layout



**Figure 4-2. TCP Header Layout****Figure 4-3. UDP Header Layout**

\* I highlighted IP protocol myself in quick, cheesy way. Should fix, or redo the whole images. Maybe include ECN bits. Images from <http://www.linux-france.org/prj/inetdoc/articles/transport/protocoles.transport.html> (GNU FDL). Maybe remove Data section, or make it smaller. Specify bit positions on top (32-bits wide). Nice 3-D eye candy :). Maybe make it clearer that TCP or UDP header goes in IP data section.

Because most popular services are registered to a well-known port number, one can often guess what services open ports represent. Nmap includes an `nmap-services` (<http://www.insecure.org/nmap/data/nmap-services>) file, containing the well-known service for registered port and protocol numbers, as well as common ports for trojan backdoors and other applications that don't bother registering with the Internet Assigned Numbers Authority (IANA). Nmap prints this service name for reference along with the port number.

Because the port number field is 16-bits wide, values can reach 65,535. The lowest possible value, zero, is invalid. The Berkeley sockets API, which defines how programs are usually written for network communication, does not allow port zero to be used as such. Instead, it interprets a port zero request as a wildcard, meaning that the programmer does not care which is used. The system then chooses an available port number. For example, programmers rarely care what source port number is used for an outgoing connection. So they set it to zero and let the operating system choose one.

While port zero is invalid, nothing stops someone from specifying it in the header field. Some malicious backdoor trojans listen on port zero of compromised systems as a stealthy way to offer illegitimate access without appearing on most port scans. To combat this, Nmap does allow scanning of port zero when it is specified explicitly (e.g. `-p0-65535`).

The first class of valid ports, numbers one through 1023, are known as reserved ports. UNIX systems (unlike Windows) require that applications have special (root) privileges in order to bind to and listen on these ports. The idea is to allow remote users to trust that they are connecting to a valid service started by an administrator and not by some wicked, unprivileged user. If the well-known port for ssh was 2222 instead of 22, a malicious user could start up a rogue ssh daemon on that port, collecting passwords of anyone who connects. As most common server applications listen on reserved ports, these are often the most fruitful to scan. So Nmap scans all 1023 reserved ports by default.

The ephemeral port range is another class of ports. This pool of ports is available by the system for allocation as needed. When an application specifies port zero ("any port"), the system chooses a port from this range. The range varies by operating system, and is usually configurable. It should contain at least a couple thousand ports to avoid running out when many concurrent connections are open. The Nmap connect() scan can use hundreds at a time as it scans every specified port on each target machine. On Linux, you can view or set the range using the file `/proc/sys/net/ipv4/ip_local_port_range`. Example 4-1 shows that on my Linux system, the range is 32,768 to 61,000. Such a large range should be sufficient in almost all cases, but I expand it just to demonstrate how to do so.

#### **Example 4-1. Viewing and increasing the ephemeral port range on Linux**

```
felix/# cat /proc/sys/net/ipv4/ip_local_port_range
32768   61000
felix/# echo "10000 65000" > /proc/sys/net/ipv4/ip_local_port_range
felix/# cat /proc/sys/net/ipv4/ip_local_port_range
10000   65000
felix/#
```

By default, Nmap only scans ports over 1024 if they are registered to a service in `nmap-services`. Specify `-p0-65535` to scan every single port. SunRPC ports are often found in the ephemeral range. Other applications open ephemeral ports temporarily for a file transfer or other event. FTP clients often do this when requesting an active mode transfer. Some P2P and instant messaging clients do so as well.

The IANA has their own port classification scheme, which differs slightly from vernacular of this book. Their authoritative port list at <http://www.iana.org/assignments/port-numbers> divides the space into the following three classes:

##### **well known ports**

These are reserved ports (within the range 1 to 1023, as discussed above) which have been registered with the IANA for a certain service. Familiar examples are ports 22, 25, and 80 for the services ssh, smtp, and http, respectively.

##### **registered ports**

These are ports fall within the range 1024 to 49,151 and have been registered with the IANA in the same way the well known ports have. Most of these are not as commonly used as the well known ports. The key difference is that unprivileged users can bind to these ports and thus run the services on their registered port. Users cannot do so on most platforms for well known ports, since they reside in the reserved port range.

##### **dynamic and/or private ports**

The IANA reserves the port numbers from 49152 through 65535 for dynamic uses such as those discussed in the ephemeral ports section. Proprietary services that are only used within a company may also use these ports.

When this book mentions registered or well known ports without any reference to the IANA, it usually means ports registered with Nmap in the `nmap-services` file, regardless of whether they fall in the reserved port range.

### **4.1.2. What is port scanning?**

Port scanning is the act of remotely testing numerous ports to determine what state they are in. The most interesting state is usually open, meaning that an application is listening and accepting connections on the port. Many techniques are available for conducting such a scan. Chapter 5 explains the circumstances under which each is most appropriate.

While many port scanners have traditionally lumped all ports into the open or closed states, Nmap is much more granular. It divides ports into five states. These states are not intrinsic properties of the port itself, but describe how Nmap sees them. For example, an Nmap scan from the same network as the target may show port 135/tcp as open, while a scan at the same time with the same options from across the Internet might show that port as filtered.

## **The five port states recognized by Nmap**

### **open**

An application is actively accepting TCP connections or UDP packets on this port. Finding these is often the primary goal of port scanning. Security-minded people know that each open port is an avenue for attack.

Attackers and pen-testers want to exploit the open ports, while administrators try to close or protect them with firewalls without thwarting legitimate users. Open ports are also interesting for non-security scans because they show services available for use on the network.

### **closed**

A closed port is accessible (it receives and responds to Nmap probe packets), but there is no application listening on it. They can be helpful in showing that a host is up on an IP address (host enumeration, or ping scanning), and as part of OS detection. Because closed ports are reachable, it may be worth scanning later in case some open up. Administrators may want to consider blocking such ports with a firewall. Then they would appear in the filtered state, discussed next.

### **filtered**

Nmap cannot determine whether the port is open because packet filtering prevents its probes from reaching the port. The filtering could be from a dedicated firewall device, router rules, or host-based firewall software. These ports frustrate attackers because they provide so little information. Sometimes they respond with ICMP error messages such as type 3 code 13 (destination unreachable: communication administratively prohibited), but filters that simply drop probes without responding are far more common. This forces Nmap to retry several times just in case the probe was dropped due to network congestion rather than filtering. It slows down the scan dramatically, further adding to the attacker's frustration.

### **unfiltered**

The unfiltered state means that a port is accessible, but Nmap is unable to determine whether it is open or closed. Only the ACK scan, which is used to map firewall rulesets, classifies ports into this state. Scanning unfiltered ports with other scan types such as Window scan, SYN scan, or FIN scan, may help resolve whether the port is open.

**open|filtered**

Nmap places ports in this state when it is unable to determine whether a port is open or filtered. This occurs for scan types in which open ports give no response. Of course the lack of response could also mean that a packet filter dropped the probe or any response it elicited. So Nmap does not know for sure whether the port is open or being filtered. The scans UDP, IP Protocol, FIN, Null, and Xmas scan classify ports this way.

**closed|filtered**

This state is used when Nmap is unable to determine whether a port is closed or filtered. It is only used for the IPID Idle scan discussed in Section 5.10.

While Nmap attempts to produce accurate results, keep in mind that all of its insights are based on packets returned by the target machines (or firewalls in front of them). Such hosts may be untrustworthy and send responses intended to confuse or mislead Nmap. Much more common are non-rfc-compliant hosts that do not respond as they should to Nmap probes. FIN, Null, and Xmas scans are particularly susceptible to this problem. Such issues are specific to certain scan types (particularly FIN, Null, and Xmas scans) and so are discussed in the relevant sections of Chapter 5.

### **4.1.3. Why scan ports?**

Port scanning is not done only for fun and amusement. There are numerous practical benefits to regularly scanning your networks. Foremost among these is security. One of the central tenants of network security is that reducing the number and complexity of services offered reduces the opportunity for attackers to break in. Most remote network compromises come from exploiting a server application listening on a TCP or UDP port. In many cases, the exploited application is not even used by the targeted organization, but was enabled by default when the machine was set up. Had that service been disabled, or protected by a firewall, the attack would have been thwarted.

Realizing that every open port is an opportunity for compromise, attackers regularly scan targets, taking an inventory of all open ports. They compare this list of listening services with their list of favorite exploits for vulnerable software. It takes just one match to compromise a machine, creating a foothold that is often used to infest the whole network. Attackers who are less discriminate about who they target will often scan for just the default port of an exploitable application. This is much faster than scanning every port, though the service will be missed when running on a non-default port. Such attackers are often derided as “script kiddies”, because they often know little more about security than how to run an exploit script written by someone more skilled. Across many organizations, such attackers are bound to find vulnerable hosts. They can be quite a nuisance, though their sheer numbers and relentless pounding against Internet-accessible machines often drive people to patch systems quickly. This reduces the likelihood of more serious, targeted attacks succeeding.

An important defense against these crackers is for systems administrators to scan their own networks regularly with tools such as Nmap. Take the list of open ports, and shut down any services that aren’t used. Ensure that those which must remain available are fully patched and that you are on the vendor’s security notification list. Firewall rules should be added where possible, limiting access to only legitimate users. Hardening instructions are available on the web for most popular applications, reducing the cracker’s opportunity even further. Nmap cannot do most of this for you, but it creates the list of available services to start out with. Some admins try to use netstat instead, but that doesn’t scale well. It requires access to every machine, and some mobile machines are easy to miss. Plus, you can’t run netstat on your average wireless access point, VOIP phone, or printer. There is also always the risk that a compromised machine will have a trojaned netstat which gives out false information. Most of the modern rootkits installed by attackers include this functionality. Relying solely on Nmap is a mistake too. A combination of careful design, configuration auditing, and regular scanning is well advised.

While security is the most common reason for port scanning, administrators often find that it suits other purposes as well. Creating an inventory of machines and the services they offer can be useful for asset tracking, network design, policy compliance checks, software license tracking, availability testing, network debugging, and more.

## 4.2. A Quick Port Scanning Tutorial

One of my goals in developing Nmap is to keep the most common usage simple, while retaining the flexibility for custom and advanced scans. This is accomplished with the command-line interface by offering dozens of options, but choosing sane defaults when they are not specified. A newbie can start out with a command as simple as **nmap *targetname***. Meanwhile, advanced users sometimes specify so many options that their terminal line wraps around.

A similar balance must be struck with command output. The most important results should stick out even to the occasional user who hasn't even read the man page. Yet the output should be comprehensive and concise enough to suit professional penetration testers who run Nmap against thousands of machines daily. Users smart enough to read this book or the Nmap source code benefit from greater control of the scanner and insights into what Nmap output really means.

This tutorial demonstrates some common Nmap port scanning scenarios and explains the output. Rather than attempt to be comprehensive, the goal is simply to acquaint new users well enough to understand the rest of this chapter.

The simplest Nmap command is simply **nmap** by itself. This prints a cheat sheet of common Nmap options and syntax. A more interesting command is **nmap *targetname***, which does the following:

1. Converts *targetname* from a hostname into an IPv4 address using DNS. I could have specified an IP address instead to skip this step.
2. Pings the host, by default with an ICMP echo request packet and a TCP ACK packet to port 80, to determine whether it is up and running. If not, Nmap reports that fact and exits. I could have specified **-P0** to skip this test. See Chapter 3.
3. Converts the target IP address back to the name using a reverse-DNS query. Because of the way DNS works, the reverse name may not be the same as the *targetname* specified on the command-line. This query can be skipped with the **-n** option to improve speed and stealthiness.
4. Launches a TCP port scan of ports 1-1024, plus all ports above 1024 which are registered in **nmap-services**. About 1660 ports are scanned if the default **nmap-services** is used. A SYN stealth scan is usually used, but **connect()** scan is substituted instead for non-root UNIX users who lack the privileges necessary to send raw packets.
5. Prints the results to standard output in normal human-readable format, and exits. Other output formats and locations (files) can be specified, as described in Chapter 11. Example 4-2 displays the results where **scanme.nmap.org** is used as *targetname*.

### Example 4-2. Simple scan: nmap scanme.nmap.org

```
# nmap scanme.nmap.org

Starting nmap 3.70 ( http://www.insecure.org/nmap/ ) at 2004-09-17 22:21 PDT
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 1655 ports scanned but not shown below are in state: filtered)
PORT      STATE      SERVICE
```

```

22/tcp  open  ssh
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
113/tcp closed auth

Nmap run completed -- 1 IP address (1 host up) scanned in 20.596 seconds

```

The first output line in Example 4-2 simply gives the Nmap version number, URL for downloading it, and the time Nmap started. The Nmap version number is important for interpreting the results, as Nmap behavior and output does change occasionally. The time is critical, since Nmap only captures a snapshot of the network during the period in which it runs. If a new host plugs in or a port opens two minutes later, it obviously won't be included in the results until the next Nmap run. Times are removed from most examples to avoid line wrapping. The version number betrays the rough timeframe anyway.

The next line provides the target IP address (IPv4 in this case), and reverse DNS name (also known as the PTR record) if it is available. Nmap promises to show the "Interesting ports", though all ports scanned are accounted for. The ports considered most interesting because they are open or in a rarely-seen state for that host are itemized individually. When many ports are in a single non-open state, they are considered a default state, and aggregated onto a single line to avoid diluting the results with thousands of uninteresting entries. In this case, Nmap notes that 1,655 ports are filtered.

The interesting ports table comes next, and provides the key scan results. The columns vary depending on options used, but in this case provide the port number and protocol, state, and service protocol for each port. The service here is just a guess made by looking up the port in `nmap-services`. The service would be listed as unknown if any of the ports were not registered in that file. Four of these ports are open, with the remaining one being closed.

Finally, Nmap reports some basic timing stats before it exits. These stats are the number of targets specified, the number of those that the ping scan found to be up, and the total time taken.

While this simple command is often all that is needed, advanced users often go much further. In Example 4-3, the scan is modified with four options. `-p0-` asks Nmap to scan every possible TCP port, `-v` asks Nmap to be verbose about it, `-A` enables aggressive tests such as remote OS and service/version detection, and `-T4` enables a more aggressive timing policy to speed up the scan.

### **Example 4-3. More complex: nmap -p0- -v -A -T4 scanme.nmap.org**

```

# nmap -p0- -v -A -T4 scanme.nmap.org

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Initiating SYN Scan against scanme.nmap.org (205.217.153.55) [65536 ports] at 23:15
Discovered open port 80/tcp on 205.217.153.55
Discovered open port 22/tcp on 205.217.153.55
Discovered open port 25/tcp on 205.217.153.55
Discovered open port 53/tcp on 205.217.153.55
SYN Stealth Scan Timing: About 4.58% done; ETC: 23:26 (0:10:25 remaining)
The SYN Stealth Scan took 680.40s to scan 65536 total ports.
Initiating service scan against 4 services on scanme.nmap.org (205.217.153.55) at 23:26
The service scan took 5.14s to scan 4 services on 1 host.
For OSScan assuming port 22 is open, port 113 closed, and neither are firewalled
Host scanme.nmap.org (205.217.153.55) appears to be up ... good.
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 65531 ports scanned but not shown below are in state: filtered)

```

```

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.1p1 (protocol 1.99)
25/tcp    open  smtp    qmail smptd
53/tcp    open  domain  ISC Bind 9.2.1
80/tcp    open  http    Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.4.20
Uptime 158.050 days (since Mon Apr 12 22:14:55 2004)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=3296835 (Good luck!)
IPID Sequence Generation: All zeros

Nmap run completed -- 1 IP address (1 host up) scanned in 689.127 seconds

```

Nmap certainly provided the requested verbosity in Example 4-3! Fortunately the extra output is easy to understand. The first eleven new lines are runtime information letting the user know what is happening as she stares expectantly at the terminal, hoping for good news. What constitutes good news depends on whether she is a systems administrator who has to fix problems, a pen-tester who needs some issues to report on, or a black-hat cracker trying to exploit them. The "discovered open port" lines provide as-it-happens notification of open ports so that she can start banging on them before the scan even finishes. The "scan timing" line provides a completion time estimate, so she knows whether to keep staring at the screen or have lunch. Because network conditions (latency, congestion, bandwidth, etc.) and packet filtering rules vary so much, the same scan options may take 30 seconds to complete against one host and 45 minutes against another.

The port table shows no new ports. All the extra ports scanned are in the filtered state, raising the filtered port total from 1,655 to 65,531. While there are no new itemized ports, the entries have changed. A new VERSION column provides the application name and (in three of the four cases) version number of each open port. This comes from service detection, one of the features enabled by `-A`. Another feature of service detection is that all of the service protocols in the SERVICE column have actually been verified. In the previous scan, they were based on the relatively flimsy heuristic of an `nmap-services` lookup. That table lookup happened to be correct this time, but it won't always be.

The remaining new lines come from OS detection (also enabled by `-A`), which is discussed in depth in Chapter 8. The final line shows that all this extra info came at a price -- the scan took thirty times longer than Example 4-2 to complete.

## 4.3. Command-line flags

While the tutorial showed how simple executing an Nmap port scan can be, dozens of command-line flags are available to make the system more powerful and flexible. This section covers only options that relate to port scans, and often describes only the port-scanning-related functionality of those options. See Chapter 15 for a comprehensive list of option flags and everything they do.

### 4.3.1. Selecting scan techniques

One of the first considerations when contemplating a port scan is deciding what techniques to use. Nmap offers about a dozen such methods. This section provides a brief summary of them, and full coverage comes in the next chapter.

Only one scan method may be used at a time, except that UDP scan (`-sU`) may be combined with any one of the TCP scan types. As a memory aid, port scan type options are of the form `-sC`, where *C* is a prominent character in the scan name, usually the first. The one exception to this is the deprecated FTP bounce scan (`-b`). By default, Nmap performs a SYN Scan, though it substitutes a Connect() scan if the user does not have proper privileges to send raw packets (requires root access on UNIX) or if IPv6 targets were specified.

## **Port scanning methods supported by Nmap**

### TCP SYN Stealth (-`sS`)

This is far and away the most popular scan type because it is the fastest way to scan ports of the most popular protocol (TCP). It is stealthier than connect() scan, and it works against all functional TCP stacks (unlike some special-purpose scans such as FIN scan).

### TCP Connect() (-`sT`)

Connect() scan uses the system call of the same name to scan machines, rather than relying on raw packets as most of the other methods do. It is usually used by unprivileged UNIX users and against IPv6 targets because SYN scan doesn't work in those cases.

### UDP (-`sU`)

Don't forget UDP ports -- they offer plenty of security holes too.

### TCP FIN, Xmas, and Null (-`sF`, -`sX`, -`sN`)

These special purpose scan types are adept at sneaking past firewalls to explore the systems behind them. Unfortunately they rely on target behavior that some systems (particularly Windows variants) don't exhibit.

### TCP ACK (-`sA`)

ACK scan is commonly used to map out firewall rulesets. In particular, it helps understand whether firewall rules are stateful or not. The downside is that it cannot distinguish open from closed ports.

### TCP Window (-`sW`)

Window scan is like ACK scan, except that it is able to detect open versus closed ports against certain machines.

### TCP Maimon (-`sM`)

Another obscure firewall-evading scan type. It is similar to a FIN scan, but includes the ACK flag as well. This allows it to get by more packet filtering firewalls, with the downside that it works against even fewer systems than FIN scan.

### TCP Idle (-`sI <zombie host>`)

The stealthiest scan type of all, even if it is slow and complex. Can exploit trusted IP address relationships.

### IP protocol (-`sO`)

Determines which IP protocols (TCP, ICMP, IGMP, etc.) are supported by the target machine. This isn't technically a port scan, since it cycles through IP protocol numbers rather than TCP or UDP port numbers. Yet it still uses the `-p` option to select scanned protocol numbers, reports its results with the normal port table format, and even uses the same underlying scan engine as the true port scanning methods. So it is close enough to a port scan that it belongs here.

TCP FTP bounce (-b <FTP bounce proxy>)

A way to trick FTP servers into performing a port scan by proxy. Unfortunately, most FTP servers are now patched to prevent this. It is a good way to sneak through restrictive firewalls when it works.

### 4.3.2. Selecting ports to scan

By default, Nmap scans ports 1-1024, plus every higher port that is registered in the `nmap-services` file. The total is about 1475 UDP ports and 1660 TCP ports. The `-F` (stands for fast) option will scan only those registered ports regardless of whether they are reserved (under 1024). The speed difference is not dramatic because this still leaves about 1000 UDP ports and 1200 TCP. One solution is to specify your own `nmap-services` file, as described in Chapter 12, though specifying the desired ports on the command-line with the `-p` option may be a better approach. The syntax of the `-p` option can be complex, and is best described with examples.

#### Port selection examples with the `-p` option

`-p22`

Scan a single port (in this case port 22) by specifying just that number as the `-p` argument.

`-p22,25,80`

Multiple ports may be separated with commas. Note that no protocol is specified, so these same port numbers will be used for whatever scan methods are specified on the command-line. If a TCP scan such as SYN scan (`-sS`) is specified, TCP ports 22, 25, and 80 are scanned. Those correspond to the services ssh, smtp, and http, respectively. If a UDP scan is selected (`-sU`), those three UDP ports are scanned. If both are specified, those three ports are scanned for each protocol, for a total of six scanned ports. With IP protocol scan (`-sO`), those three IP protocols (corresponding to xns-idp, leaf-1, and iso-ip) are scanned.

`-p80-85,443,8000-8005,8080-8085`

Port ranges may be specified by separating the beginning and end port with a hyphen. Multiple ranges or individual ports can be specified with commas. This option scans ports 80, 81, 82, 83, 84, 85, 443, 8000, etc. Based on the port numbers, this user is probably scanning TCP and looking for web servers.

`-p100,60000-`

You can omit the beginning of a range to imply port one, or the end to imply the last port possible (65535 for TCP and UDP, 255 for protocol scan). This example scans ports one through 100, and all ports greater or equal to 60,000.

`-p-`

Omit beginning and end numbers to scan the whole range (excluding zero).

`-pT:21,23,110,U:53,111,137,161`

Separate lists of TCP and UDP ports can be given by preceding the lists with T: (for TCP) or U:. This example scans three TCP ports (ftp, telnet, and pop3), and four UDP services (DNS, rpcbind, netbios, and snmp). Specifying both TCP and UDP ports only matters if you also tell Nmap to do a UDP scan (`-sU`) and one of the TCP scan methods, such as `-sS`, `-sA`, or `-sF`.

### 4.3.3. Timing-related options

Port scanning often takes more time than all of the other elements in a comprehensive Nmap scan (version detection, OS detection, ping scanning, DNS resolution, etc.) put together. Optimizing with the timing options can help substantially. This list summarizes the options that affect port scan timing. Chapter 6 offers a much more complete treatment.

`--min_rtt_timeout, --max_rtt_timeout, --initial_rtt_timeout`

The minimum, maximum, and initial amount of time in milliseconds that Nmap will wait for a port scan probe response.

`--min_hostgroup, --max_hostgroup`

Sets the minimum and maximum number of hosts that Nmap will port scan in parallel.

`--min_parallelism, --max_parallelism`

Limits the minimum or maximum number of port scan probes (across all hosts scanned concurrently) that Nmap may have outstanding.

`--host_timeout`

Asks Nmap to give up on hosts that take more than a given number of milliseconds to scan.

`--scan_delay, --max_scan_delay`

Asks Nmap to wait at least the given number of milliseconds between sending probes to any individual host. The scan delay can grow as Nmap detects packet loss, so a maximum may be specified with `--max_scan_delay`.

`-T0 through -T5`

These timing templates affect many variables, offering a simple way to adjust overall Nmap speed from very slow (`-T0`) to extremely aggressive (`-T5`).

### 4.3.4. Output format and verbosity options

Nmap offers the ability to write its reports in its standard format, a simple line-oriented “grepable” format, or XML. These reports are enabled with the `-oN` (normal), `-oG` (grepable), and `-oX` (XML) options. Each option takes a filename, and they may be combined to output in several formats at once. Several options are also available to increase output verbosity. These options are summarized in the following list, and fully covered in Chapter 11. That chapter also documents the output formats themselves.

`-v`

Increases the verbosity level, causing Nmap to print more information about the scan in progress. Open ports are shown as they are found and completion time estimates are provided when Nmap thinks a scan will take more than a few minutes. Use it twice for even greater verbosity. Using it more than twice has no effect.

`-d`

Increases the debugging level, causing Nmap to print out details about its operation that can be useful in tracking down bugs or simply understanding how it works. Higher levels result in massive amounts of data. Using the option once sets the debugging level to one, and it is incremented for each additional `-d`. Or you may

follow the `-d` with the desired level, as in `-d5`. If you don't see enough information, try a higher level. The maximum effective level is 9. If your screen is flooded with too much debugging data, reduce the level. Redusing scan intensity, such as the number of ports or targets and the features used, can also help to isolate only the debug messages you want.

#### `--packet_trace`

Causes Nmap to print a summary of every packet sent or received. This is often used for debugging, but is also a valuable way for new users to understand exactly what Nmap is doing under the covers. To avoid printing thousands of lines, you may want to specify a limited number of ports to scan, such as `-p20-30`.

#### `-oN <filename>`

Write output in Nmap's normal format to `filename`. This format is roughly the same as the standard output printed by Nmap at runtime.

#### `-oX <filename>`

Write output in Nmap's XML format to `filename`. Normal (human readable) output will still be printed to stdout unless you ask for XML to be directed there by specifying `-` as `filename`. This is the preferred format for use by scripts and programs that process Nmap results.

#### `-oG <filename>`

Write output in Nmap's so-called grepable format to `filename`. This tabular format fits the output of each host on a single line, making it easy to grep for open ports, certain operating systems, application names, or other data. Normal output will still be printed to stdout unless you ask for the grepable output to be directed there by specifying `-` as `filename`. While this format works well for parsing with simple grep and awk command-lines, significant scripts and programs should use the XML output instead. The XML format contains substantial information that grepable format has no place for, and extensibility makes XML easier to update with new information without breaking tools that rely on it.

#### `--resume <filename>`

Resume an aborted scan by specifying the normal (`-oN`) or grepable (`-oG`) output file which was created during the ill-fated scan. Don't use any options other than `--resume`, as Nmap will use the ones specified in the output file. It then parses the file and resumes scanning (and logging to the file) at the host which the previous Nmap execution was working on when it ceased.

#### `--append_output`

Tells Nmap to append scan results to any output files specified (with arguments such as `-oN` or `-oX`) rather than overwriting them.

### 4.3.5. Firewall and IDS evasion options

Nmap offers many options for sneaking past IDSs undetected or evading firewall rules. They are discussed in depth in Chapter 9, and this list gives a quick summary. Some of these options (particularly `-S` and `-e`) are useful for more mundane purposes as well.

**-f**

Asks Nmap to fragment the packets it uses for a port scan. This is usually done in an attempt to evade firewall or IDS systems. Unfortunately the option does not work when Nmap is running on recent versions of Linux. See Section 9.4.6 for a discussion of this technique.

**-D <decoy1[,decoy2][,ME],...>**

Enables decoys which hide the real attacker amongst a flurry of decoy IP addresses. See Section 9.5.3.1 for decoy scanning examples and suggestions.

**-S <IP Address>**

Sets the source address of port scan packets. This can be used on hosts with many IP addresses to select the one that packets are sent from. Or it can be used for more sinister purposes -- to spoof the scan so that some other party takes the blame. This sort of spoofing is described in Section 9.5.3.2.

**-e**

Tells Nmap which interface to send and receive packets on. This may be required if the -S option is used to spoof someone else's IP address. It can also be useful on multi-homed hosts to select the most desirable interface when several can route to the target networks.

**--source\_port (-g)**

Sets the source port used in scans. This is usually done to bypass poorly-implemented firewalls, as described in Section 9.4.2.

**--data\_length <numbytes>**

Rather than send packet headers with empty data sections as port scan probes, this option causes each probe packet to be padded with the given number of random data bytes.

### 4.3.6. Specifying targets

To scan a single host (or a few of them), simply add their names or IP addresses to the end of your Nmap command line. Nmap also has a structured syntax to make scanning large networks easy. You can give Nmap a file listing targets, or even ask Nmap to generate them randomly. This is all described in Section 3.2.

### 4.3.7. Miscellaneous options

Here are some options that can be quite handy even though they don't fit into specific categories. The descriptions focus on how each option relates to port scanning. See the Nmap Reference Guide in Chapter 15 for more comprehensive coverage.

**-6**

Asks Nmap to scan the target using the IPv6 protocol. This process is described in Section 4.4.

**-r**

Nmap randomizes the port scan order by default to make detection slightly harder. The -r option causes them to be scanned in numerical order instead.

```
--ttl <numHops>
```

Sets the IP time-to-live to the given number of hops. This can be used to avoid scanning hosts beyond a limited network. It can also be useful as a sort of poor man's traceroute to discover network topology, though that is usually easier to accomplish with hping2 (<http://www.hping.org>).

```
-P0
```

Tells Nmap to skip the ping test and simply scan every target host provided. Other options for controlling host enumeration are described in Chapter 3.

## 4.4. IPv6 Scanning [-6]

Since 2002, Nmap has offered IPv6 support for its most popular features. In particular, ping scanning (TCP-only), connect() scanning, and version detection all support IPv6. The command syntax is the same as usual except that you also add the `-6` option. Of course, you must use IPv6 syntax if you specify an address rather than a hostname. An address might look like `3ffe:501:4819:2000:210:f3ff:fe03:4d0`, so hostnames are recommended. Example 4-4 shows a typical port scanning session. The output looks the same as it usually does, with the IPv6 address on the “interesting ports” line being the only IPv6 give away.

### Example 4-4. A simple IPv6 scan

```
# nmap -6 -sV www.eurov6.org

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Interesting ports on ns1.euro6ix.com (2001:800:40:2a03::3):
(The 1656 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Pure-FTPd
22/tcp    open  ssh      OpenSSH 3.5p1 (protocol 2.0)
53/tcp    open  domain   ISC Bind 9.2.1
80/tcp    open  http     Apache httpd

Nmap run completed -- 1 IP address (1 host up) scanned in 56.782 seconds
```

While IPv6 hasn't exactly taken the world by storm, it gets significant use in some (usually Asian) countries and most modern operating systems support it. To use the Nmap `-6` feature, both the source and target of your scan must be configured for IPv6. If your ISP (like most of them) does not allocate IPv6 addresses to you, free tunnel brokers are widely available and work fine with Nmap. One of the better ones is run by BT Exact at <https://tb.ipv6.btexact.com/>. I have also used one that Hurricane Electric provides at <http://ipv6tb.he.net/>. 6to4 tunnels are another popular, free approach.

Systems that support IPv6 don't always have their IPv4 and IPv6 firewall rules in sync. Section 9.4.3 shows a real-life example of reaching ports through IPv6 that are filtered in IPv4.

## 4.5. [RECIPE] Scanning a large network for a certain open TCP port

### 4.5.1. Problem

You wish to quickly find all machines on a network that have a certain TCP port open. For example, after a new Microsoft IIS vulnerability is found, you might want to scan for all machines with TCP port 80 open and ensure that they aren't running a vulnerable version of that software. Or if you investigate a compromised box and find that the attacker left a backdoor running on port 31337, scanning your whole network for that port might quickly identify other compromised systems. A full scan would be done later.

### 4.5.2. Solution

The straightforward way is to run:

```
nmap -P0 -p<portnumber> -oG <logfilename.gnmap> <target networks>
```

Here is a concrete example of searching 4096 IPs for web servers (port 80 open):

```
nmap -P0 -p80 -oG logs/pb-port80scan-092304.gnmap 216.163.128.0/20
```

While this works, a little effort choosing appropriate timing values for the network being scanned reduces scan time substantially. The scan above took 1,236 seconds, while the optimized version below provided the same results in 869 seconds:

```
nmap -T4 -P0 -p80 --max_rtt_timeout 200 --initial_rtt_timeout 150 --min_hostgroup 512 -oG  
logs/pb-port80scan2-092304.gnmap 216.163.128.0/20
```

And much of that time is spent doing reverse-DNS resolution. Excluding that by adding `-n` to the command-line above reduces the 4096-host scan time to 193 seconds. Being patient for 3 minutes is far easier than for the 21 minutes taken before.

The commands above store grepable-format results in the specified file. A simple egrep command will then find the machines with port 80 open:

```
egrep '[^0-9]80/open' logs/pb-port80scan2-092304.gnmap
```

The egrep pattern is preceded with `[^0-9]` to avoid bogus matching ports such as 3180. Of course that can't happen since we are only scanning port 80, but it is a good practice to remember for many-port scans. If you only want the IP addresses and nothing else, pipe the egrep output to `awk '{print $2}'`.

### 4.5.3. Discussion

Sometimes a story is the best way to understand decisions, so this is how I decided upon the command lines in the solution section. I was bored at home, and finding myself curious as to whether the popular magazine *Playboy* had any secret (unadvertised) web servers on their network. Such web servers might offer exciting free content, such as Linux distribution ISOs! Those really turn me on. The way to find out is a single-port scan across their network for hosts with TCP port 80 open.

The first step is determining which IP addresses to scan. I perform a whois search of the American Registry for Internet Numbers for organizations named *Playboy*. The results are shown in Example 4-5.

**Example 4-5. Discovering Playboy's IP space**

```
core~> whois -h whois.arin.net n playboy
[Querying whois.arin.net]
[whois.arin.net]

OrgName:      Playboy
OrgID:        PLAYBO
Address:      680 N. Lake Shore Drive
City:         Chicago
StateProv:    IL
PostalCode:   60611
Country:      US

NetRange:     216.163.128.0 - 216.163.143.255
CIDR:         216.163.128.0/20
NetName:      PLAYBOY-BLK-1
NetHandle:    NET-216-163-128-0-1
Parent:       NET-216-0-0-0-0
NetType:      Direct Assignment
NameServer:   NS1-CHI.PLAYBOY.COM
NameServer:   NS2-CHI.PLAYBOY.COM
[...]
```

This shows 4096 IPs (the net range 216.163.128.0/20) registered to Playboy. Using techniques discussed in Section 3.6 I could have found many more netblocks they control, but 4096 IPs are sufficient for this example.

Next I want to estimate latency to these machines, so that Nmap will know what to expect. This isn't required, but feeding Nmap appropriate timing values can speed it up. This is particularly true for single-port -P0 scans, such as this one. Nmap does not receive enough responses from each host to accurately estimate latency and packet drop rate, so I will help it out on the command line. My first thought is to ping their main web server, as shown in Example 4-6.

**Example 4-6. Pinging Playboy's Web Server for a Latency Estimate**

```
# ping -c5 www.playboy.com
PING www.phat.playboy.com (209.247.228.201) from 205.217.153.56 : 56(84) bytes of data.
64 bytes from free-chi.playboy.com (209.247.228.201): icmp_seq=1 ttl=245 time=57.5 ms
64 bytes from free-chi.playboy.com (209.247.228.201): icmp_seq=2 ttl=245 time=56.7 ms
64 bytes from free-chi.playboy.com (209.247.228.201): icmp_seq=3 ttl=245 time=56.9 ms
64 bytes from free-chi.playboy.com (209.247.228.201): icmp_seq=4 ttl=245 time=57.0 ms
64 bytes from free-chi.playboy.com (209.247.228.201): icmp_seq=5 ttl=245 time=56.6 ms

--- www.phat.playboy.com ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 4047ms
rtt min/avg/max/mdev = 56.652/57.004/57.522/0.333 ms
```

The maximum round trip time is 58 milliseconds. Unfortunately, this IP address (209.247.228.201) is not within the 216.163.128.0/20 netblock I wish to scan. I would normally add this new netblock to the target list, but have already decided to limit my scan to the original 4096 IPs. These times are probably perfectly fine to use, but finding actual values from IPs on the target network would be even better. I use dig to obtain Playboy's public DNS records from a nameserver shown in the previous whois query. The output is shown in Example 4-7.

**Example 4-7. Digging through Playboy's DNS records**

```

core<~>dig @ns1-chi.playboy.com playboy.com. any
; <>> DiG 8.3 <>> @ns1-chi.playboy.com playboy.com. any
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6
;; flags: qr aa rd; QUERY: 1, ANSWER: 9, AUTHORITY: 0, ADDITIONAL: 4
;; QUERY SECTION:
;;      playboy.com, type = ANY, class = IN

;; ANSWER SECTION:
playboy.com.          1D IN A      209.247.228.201
playboy.com.          1D IN MX     10 mx.la.playboy.com.
playboy.com.          1D IN MX     5 mx.chi.playboy.com.
playboy.com.          1D IN NS      ns15.customer.level3.net.
playboy.com.          1D IN NS      ns21.customer.level3.net.
playboy.com.          1D IN NS      ns29.customer.level3.net.
playboy.com.          1D IN NS      ns1-chi.playboy.com.
playboy.com.          1D IN NS      ns2-chi.playboy.com.
playboy.com.          1D IN SOA     ns1-chi.playboy.com. dns.playboy.com. (
2004092010           ; serial
12H                  ; refresh
2h30m                ; retry
2wld                ; expiry
1D )                 ; minimum

;; ADDITIONAL SECTION:
mx.chi.playboy.com.   1D IN A      216.163.143.4
mx.la.playboy.com.    1D IN A      216.163.128.15
ns1-chi.playboy.com.  1D IN A      209.247.228.135
ns2-chi.playboy.com.  1D IN A      64.202.105.36

;; Total query time: 107 msec

```

The DNS query reveals two MX (mail) servers within the target 216.163.128.0/20 netblock. Since the names mx.chi and mx.la imply that they are in different regions (Chicago and Los Angeles), I decide to test them both for latency. The ping results are shown in Example 4-8.

**Example 4-8. Pinging the MX servers**

```

core~> ping -c5 mx.chi.playboy.com
PING mx.chi.playboy.com (216.163.143.4) 56(84) bytes of data.

--- mx.chi.playboy.com ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4000ms

core~> ping -c5 mx.la.playboy.com
PING mx.la.playboy.com (216.163.128.15) 56(84) bytes of data.

--- mx.la.playboy.com ping statistics ---

```

```
5 packets transmitted, 0 received, 100% packet loss, time 4011ms
```

Well, that attempt was a miserable failure. The hosts seem to be blocking ICMP ping packets. Since they are mail servers, they must have TCP port 25 open, so I try again using hping2 (<http://www.hping2.org>) to perform a TCP ping against port 25, as demonstrated in Example 4-9.

### Example 4-9. TCP Pinging the MX servers

```
core# hping2 --syn -p 25 -c 5 mx.chi.playboy.com
eth0 default routing interface selected (according to /proc)
HPING mx.chi.playboy.com (eth0 216.163.143.4): S set, 40 headers + 0 data bytes
46 bytes from 216.163.143.4: flags=SA seq=0 ttl=51 id=14221 win=65535 rtt=56.8 ms
46 bytes from 216.163.143.4: flags=SA seq=1 ttl=51 id=14244 win=65535 rtt=56.9 ms
46 bytes from 216.163.143.4: flags=SA seq=2 ttl=51 id=14274 win=65535 rtt=56.9 ms
46 bytes from 216.163.143.4: flags=SA seq=3 ttl=51 id=14383 win=65535 rtt=61.8 ms
46 bytes from 216.163.143.4: flags=SA seq=4 ttl=51 id=14387 win=65535 rtt=57.5 ms

--- mx.chi.playboy.com hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 56.8/58.0/61.8 ms

core# hping2 --syn -p 25 -c 5 mx.la.playboy.com
eth0 default routing interface selected (according to /proc)
HPING mx.la.playboy.com (eth0 216.163.128.15): S set, 40 headers + 0 data bytes
46 bytes from 216.163.128.15: flags=SA seq=0 ttl=52 id=58728 win=57344 rtt=16.0 ms
46 bytes from 216.163.128.15: flags=SA seq=1 ttl=52 id=58753 win=57344 rtt=15.4 ms
46 bytes from 216.163.128.15: flags=SA seq=2 ttl=52 id=58790 win=57344 rtt=15.5 ms
46 bytes from 216.163.128.15: flags=SA seq=3 ttl=52 id=58870 win=57344 rtt=16.4 ms
46 bytes from 216.163.128.15: flags=SA seq=4 ttl=52 id=58907 win=57344 rtt=15.5 ms

--- mx.la.playboy.com hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 15.4/15.8/16.4 ms
```

These are the results I was looking for. The LA host never takes more than 16 milliseconds to respond, while the Chicago one takes up to 62 milliseconds. This is not surprising, given that I am probing from a machine in California. It pays to be cautious, and latency can increase during heavy scanning, so I decide to let Nmap wait up to 200 milliseconds for responses. I'll have it start with a timeout of 150ms. So I pass it the options `--max_rtt_timeout 200 --initial_rtt_timeout 150`. To set a generally aggressive timing mode, I specify `-T4` at the beginning of the line. It is important the `-T4` comes before those other timing options, or the `-T4` canned RTT values (500ms initial rtt timeout, 1250ms max) will override the ones I explicitly specified.

Since I value minimizing completion time of the whole scan over minimizing the amount of time before the first batch of host results is returned, I specify a large scan group size. The option `--min_hostgroup 512` is specified so that at least 512 IPs will be scanned in parallel (when possible). Using an exact factor of the target network size (4096) prevents the small and less efficient 96-host block which would occur at the end if I specified `--min_hostgroup 500`. All of these timing issues are explained in much more depth in Chapter 6.

There is no need to waste time with a prior ping stage, since a ping would take as long as the single-port scan itself. So `-P0` is specified to disable that stage. Substantial time is saved by skipping reverse-DNS resolution with the `-n` argument. Otherwise, with ping scanning disabled, Nmap would try to look up all 4096 IPs. Nmap does not yet offer parallelized DNS subsystem, so that would be painfully slow. I am searching for webservers, so I request port eighty

with `-p80`. Of course I will miss any http servers running on non-standard ports such as 81 or 8080. SSL servers on port 443 won't be found either. One could add them to the `-p` option, but even one more port would double the scan time, which is roughly proportional to the number of ports scanned.

The final option is `-oG` followed by the filename in which I want grepable results stored. I append the target network to the command, then press enter to execute Nmap. The output is shown in Example 4-10.

#### **Example 4-10. Launching the scan**

```
# nmap -T4 -p80 -P0 --max_rtt_timeout 200 --initial_rtt_timeout 150 \
--min_hostgroup 512 -n -oG pb-port80scan-092304.gnmap 216.163.128.0/20
Warning: You specified a highly aggressive --min_hostgroup.
Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Interesting ports on 216.163.128.0:
PORT      STATE      SERVICE
80/tcp     filtered  http

Interesting ports on 216.163.128.1:
PORT      STATE      SERVICE
80/tcp     filtered  http

Interesting ports on 216.163.128.2:
PORT      STATE      SERVICE
80/tcp     filtered  http

Interesting ports on 216.163.128.3:
PORT      STATE      SERVICE
80/tcp     filtered  http
[ ... ]
Interesting ports on 216.163.143.255:
PORT      STATE      SERVICE
80/tcp     filtered  http

Nmap run completed -- 4096 IP addresses (4096 hosts up) scanned in 192.968 second
```

Nmap scans all 4096 IPs in about three minutes. The normal output shows a bunch of ports in the `filtered` state. Most of those IPs are probably not active hosts -- the port simply appears filtered because Nmap receives no response to its SYN probes. I obtain the list of web servers with a simple egrep on the output file, as shown in Example 4-11.

#### **Example 4-11. Egrep for open ports**

```
# egrep '[^0-9]80/open' pb-port80scan-092304.gnmap
Host: 216.163.140.20 () Ports: 80/open/tcp//http///
Host: 216.163.142.135 ()      Ports: 80/open/tcp//http///
```

After all that effort, only two accessible web servers are found out of 4096 IPs! Sometimes that happens. The first one, 216.163.140.20 (no reverse DNS name) brings me to a Microsoft Outlook Web Access (webmail) server. That might excite me if I was trying to compromise their network, but it isn't gratifying now. The next server (reverse name `mirrors.playboy.com`) is much better. It offers those Linux ISOs I was hoping for, as well as substantial FreeBSD, CPAN, and Apache archives! I download the latest Fedora Core ISOs at a smoking-fast 4Mbps. I suppose

an abundance of bandwidth at Playboy is not surprising. Later I scan other Playboy netblocks, finding dozens more web servers, though some of their content is inappropriate for this book.

While this is an unusual reason for port scanning, single port sweeps are common for many other purposes expressed previously. The techniques described here can be easily applied to any single-port TCP sweep.

#### **4.5.4. See Also**

Version detection can be used to find specific applications listening on a network. For example, you could seek a certain vulnerable version of OpenSSH rather than find all hosts with port 22 open. This is also useful for single-port UDP scans, as the techniques in this recipe only work well for TCP. Instructions are provided in Section 7.8.

Chapter 6 looks at scan speed optimization in much more depth.

# Chapter 5. Port Scanning Techniques and Algorithms

## 5.1. Introduction

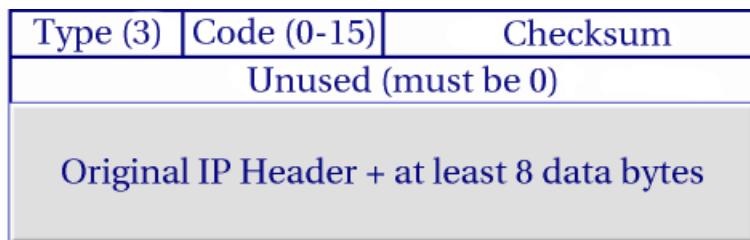
As a novice performing automotive repair, I can struggle for hours trying to fit my rudimentary tools (hammer, duct tape, wrench, etc.) to the task at hand. When I fail miserably and tow my jalopy to a real mechanic, he invariably fishes around in a huge tool chest until pulling out the perfect gizmo which makes the job seem effortless. The art of port scanning is similar. Experts understand the dozens of scan techniques and choose the appropriate one (or combination) for a given task. Inexperienced users and script kiddies, on the other hand, try to solve every problem with the default SYN scan. Since Nmap is free, the only barrier to port scanning mastery is knowledge. That certainly beats the automotive world, where it may take great skill to determine that you need a strut spring compressor, then you still have to pay thousands of dollars for it.

The previous chapter described port scanning with Nmap in general terms, including a brief summary of Nmap's supported scan types in Section 4.3.1. This chapter describes each of those scan types in depth. Typical usage scenarios and instructions are given for each scan type, as are on-the-wire packet traces illustrating how they work. Then the `ultra_scan` algorithm (which most scan methods use) is discussed, with an emphasis on aspects that can be tweaked to improve performance.

Most of the scan types are only available to privileged users. This is because they send and receive raw packets, which requires root access on UNIX systems. Using an administrator account on Windows is recommended, though it sometimes works for unprivileged users on that platform when Winpcap has already been loaded into the OS. Requiring root privileges was a serious limitation when Nmap was released in 1997, as many users only had access to shared shell accounts. Now, the world is different. Computers are cheaper, far more people have always-on direct Internet access, and desktop UNIX systems (including Linux and MAC OS X) are prevalent. A Windows version of Nmap is now available, allowing it to run on even more desktops. For all these reasons, users have less need to run Nmap from limited shared shell accounts. This is fortunate, as the privileged options make Nmap far more powerful and flexible.

When discussing how Nmap handles probe responses, many sections discuss ICMP error messages by their type and code numbers. The type and code are each 8-bit fields in ICMP headers that describe the message's purpose. Nmap port scanning techniques are concerned only with ICMP type 3, which are destination unreachable messages. Figure 5-1 shows the ICMP header layout of such a packet (it is encapsulated in the data section of an IP packet, as shown in Figure 4-1).

**Figure 5-1. ICMPv4 Destination Unreachable Header Layout**



\* This needs to be redone in the same fashion as the headers in previous chapter.

There are sixteen codes representing different destination unreachable messages. They are all shown in Table 5-1, though Nmap only cares about codes 0-3, 9, 10, and 13, which are marked with an asterisk.

**Table 5-1. ICMP destination unreachable (type 3) code values**

Code	Description
0*	Network unreachable
1*	Host unreachable
2*	Protocol unreachable
3*	Port unreachable
4	Fragmentation needed but don't-fragment bit set
5	Source route failed
6	Destination network unknown
7	Destination host unknown
8	Source host isolated (obsolete)
9*	Destination network administratively prohibited
10*	Destination host administratively prohibited
11	Network unreachable for type of service (TOS)
12	Host unreachable for TOS
13*	Communication administratively prohibited by filtering
14	Host precedence violation
15	Precedence cutoff in effect

## 5.2. TCP SYN (Stealth) Scan

SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls. SYN scan is relatively unobtrusive and stealthy, since it never completes TCP connections. It also works against any compliant TCP stack rather than depending on idiosyncrasies of specific platforms as Nmap's Fin/Null/Xmas, Maimon and Idle scans do. It also allows clear, reliable differentiation between open, closed, and filtered states.

SYN scan may be requested by passing the `-sS` option to Nmap. It requires raw-packet privileges, and is the default TCP scan when they are available. So when running Nmap as root or Administrator, `-sS` is usually omitted. This default SYN scan behavior is shown in Example 5-1, which finds a port in each of the three major states.

### Example 5-1. A SYN Scan showing three port states

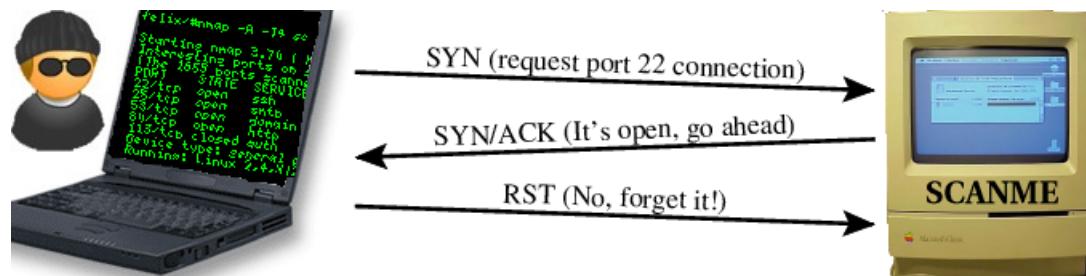
```
krad# nmap -p22,113,139 scanme.nmap.org

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
PORT      STATE      SERVICE
22/tcp    open       ssh
113/tcp   closed    auth
139/tcp   filtered  netbios-ssn
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 1.345 seconds
```

While SYN scan is pretty easy to use without any low-level TCP (<http://www.rfc-editor.org/rfc/rfc793.txt>) knowledge, understanding the technique helps when interpreting unusual results. Fortunately for us, the fearsome black-hat cracker Ereet Hagiwara has taken a break from terrorizing Japanese Windows users ([http://www.microsoft.com/japan/security/security\\_bulletins/MS04-003e.asp](http://www.microsoft.com/japan/security/security_bulletins/MS04-003e.asp)) to illustrate the Example 5-1 SYN scan for us at the packet level. First, the behavior against open port 22 is shown in Figure 5-2.

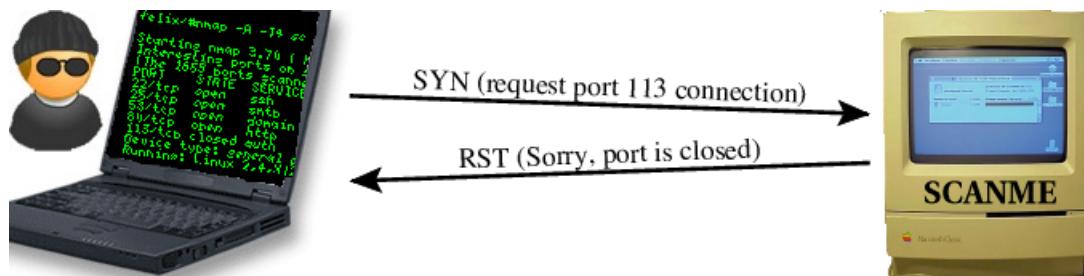
**Figure 5-2. SYN scan of open port 22**



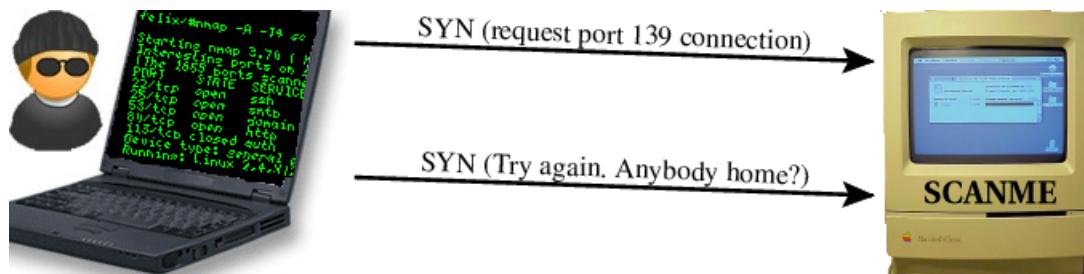
\* When illustrators create final versions of these, Ereet may have to be redrawn for copyright reasons. And the hostname should be krad.

As this example shows, Nmap starts by sending a TCP packet with the SYN flag set (see Figure 4-2 if you have forgotten what packet headers look like) to port 22. This is the first step in the TCP three-way handshake that any legitimate connection attempt takes. Since the target port is open, Scanme takes the second step by sending a response with the SYN and ACK flags back. In a normal connection, Ereet's machine (named krad) would complete the three-way handshake by sending an ACK packet acknowledging the SYN/ACK. Nmap does not need to do this, since the SYN/ACK response already told it that the port is open. If Nmap completed the connection, it would then have to worry about closing it. This usually involves another three-way handshake, using FIN packets rather than SYN. So an ACK is a bad idea, yet something still has to be done. If the SYN/ACK is ignored completely, Scanme will assume it was dropped and keep resending it. The proper response, since we don't want to make a full connection, is a RST packet as shown in the diagram. This tells Scanme to forget about (reset) the attempted connection. Nmap could send this RST packet easily enough, but it actually doesn't need to. The OS running on krad also receives the the SYN/ACK, which it doesn't expect because Nmap crafted the SYN probe itself. So the OS responds to the unexpected SYN/ACK with a RST packet. All RST packets described in this chapter also have the ACK bit set because they are always sent in response to (and acknowledge) a received packet. So that bit is not shown explicitly for RST packets. Because the three-way handshake is never completed, SYN scan is sometimes called half-open scanning.

Figure 5-3 shows how Nmap determines that port 113 is closed. This is even simpler than the open case. The first step is always the same -- Nmap sends the SYN probe to Scanme. But instead of receiving a SYN/ACK back, a RST is returned. That settles it -- the port is closed. No more communication regarding this port is necessary.

**Figure 5-3. SYN scan of closed port 113**

Finally, Ereet shows us how a filtered port appears to Nmap in Figure 5-4. The initial SYN is sent first, as usual, but Nmap sees no reply. The response could simply be slow. From previous responses (or timing defaults), Nmap knows how long to wait and eventually gives up on receiving one. A nonresponsive port is usually filtered (blocked by a firewall device, or perhaps the host is down), but this one test is not conclusive. Perhaps the port is open but the probe or response were simply dropped. Networks can be pretty flaky. So Nmap tries again, sending another SYN probe. After yet another timeout period, Nmap gives up and marks the port `filtered`. In this case, only one retransmission was attempted. As described in Section 5.13, Nmap keeps careful packet loss statistics and will attempt more retransmissions when scanning less reliable networks.

**Figure 5-4. SYN scan of filtered port 139**

Nmap will also consider a port `filtered` if it receives certain ICMP error messages back. Table 5-2 shows how Nmap assigns port states based on responses to a SYN probe.

**Table 5-2. How Nmap interprets responses to a SYN probe**

Probe Response	Assigned State
TCP SYN/ACK response	open
TCP RST response	closed
No response received	filtered (if probe retransmissions also fail to elicit responses)
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

While the pretty illustrations in this section are useful when you have them, Nmap reports exactly what it is doing at the packet level when you specify the `--packet_trace` option in addition to any other desired options. This is a great way for newbies to understand Nmap's behavior when Ereet is not around to help. Even advanced users find it

handy when Nmap produces results they don't expect. You may want to increase the debug level with `-d` (or even `-d5`) as well. Then scan the minimum number of ports and hosts necessary for your purpose or you could end up with literally millions of output lines. Example 5-2 repeats Ereet's 3-port SYN scan with packet tracing enabled (output edited for brevity). Read the command-line, then test yourself by figuring out what packets will be sent before reading on. Then once you read the trace up to "The SYN Stealth Scan took 1.25s", you should know from the RCVD lines what the port state table will look like before continuing on to read it.

### Example 5-2. Using `--packet_trace` to understand a SYN scan

```
krad# nmap -d --packet_trace -p22,113,139 scanme.nmap.org

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
SENT (0.0130s) ICMP krad > scanme Echo request (type=8/code=0) ttl=52 id=1829
SENT (0.0160s) TCP krad:63541 > scanme:80 A iplen=40 seq=3191911070 ack=2499850910
RCVD (0.0280s) ICMP scanme > krad Echo reply (type=0/code=0) iplen=28
We got a ping packet back from scanme: id = 48821 seq = 714 checksum = 16000
massping done: num_hosts: 1 num_responses: 1
Initiating SYN Stealth Scan against scanme.nmap.org (scanme) [3 ports] at 00:53
SENT (0.1340s) TCP krad:63517 > scanme:113 S iplen=40 seq=1610438635
SENT (0.1370s) TCP krad:63517 > scanme:22 S iplen=40 seq=1610438635
SENT (0.1400s) TCP krad:63517 > scanme:139 S iplen=40 seq=1610438635
RCVD (0.1460s) TCP scanme:113 > krad:63517 RA iplen=40 seq=0 ack=1610438636
RCVD (0.1510s) TCP scanme:22 > krad:63517 SA iplen=44 seq=4275897108 ack=1610438636
SENT (1.2550s) TCP krad:63518 > scanme:139 S iplen=40 seq=1610373098 win=3072
The SYN Stealth Scan took 1.25s to scan 3 total ports.
Interesting ports on scanme.nmap.org (205.217.153.55):
PORT      STATE      SERVICE
22/tcp     open       ssh
113/tcp    closed    auth
139/tcp    filtered  netbios-ssn

Nmap run completed -- 1 IP address (1 host up) scanned in 1.403 seconds
```

SYN scan has long been called the stealth scan because it is subtler than TCP connect() scan (discussed next), which was the most common scan type before Nmap was released. Despite that moniker, don't count on a default SYN scan slipping undetected through sensitive networks. Widely deployed intrusion detection systems, personal firewalls, and similar systems are all quite capable of detecting default SYN scans. More effective techniques for stealthy scanning are demonstrated in Chapter 9.

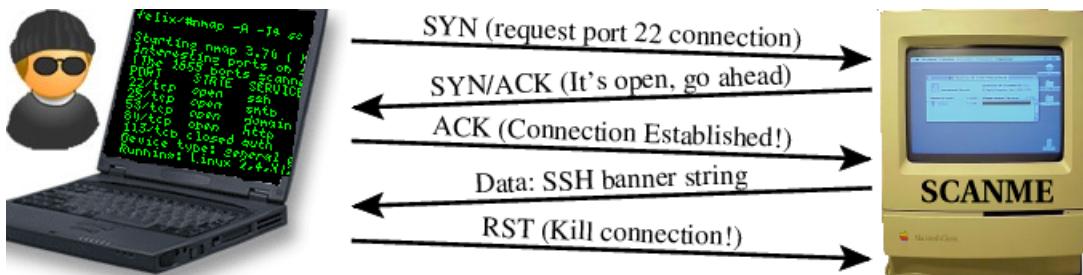
## 5.3. TCP Connect() Scan

TCP Connect() scan is the default TCP scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges or is scanning IPv6 networks. Instead of writing raw packets as most other scan types do, Nmap asks the underlying operating system to establish a connection with the target machine and port by issuing the `connect()` system call. This is the same high-level system call that web browsers, P2P clients, and most other network-enabled applications use to establish a connection. It is part of a programming interface known as the Berkeley Sockets API. Rather than read raw packet responses off the wire, Nmap uses this API to obtain status information on each connection attempt. This and the FTP bounce scan (Section 5.12) are the only scan types available to unprivileged users.

When SYN scan is available, it is usually a better choice. Nmap has less control over the high level `connect()` call than with raw packets, making it less efficient. The system call completes connections to open target ports rather than performing the half-open reset that SYN scan does. Not only does this take longer and require more packets to obtain the same information, but target machines are more likely to log the connection. A decent IDS will catch either, but most machines have no such alarm system. Many services on your average UNIX system will add a note to syslog, and sometimes a cryptic error message, when Nmap connects and then closes the connection without sending data. Truly pathetic services crash when this happens, though that is uncommon. An administrator who sees a bunch of connection attempts in his logs from a single system should know that he has been `connect()` scanned.

Figure 5-5 shows a `connect()` scan in action against open port 22 of `scanme.nmap.org`. Recall that this only required three packets for the SYN scan in Example 5-1. The exact behavior against an open port depends on the platform Nmap runs on and the service listening at the other end, but this six packet example is typical.

**Figure 5-5. Connect scan of open port 22 (nmap -sT -p22 scanme.nmap.org)**



The first two steps (SYN and SYN/ACK) are exactly the same as with a SYN scan. Then, instead of aborting the half-open connection with a RST packet, krad acknowledges the SYN/ACK with its own ACK packet, completing the connection. In this case, Scanme even had time to send its SSH banner string (`SSH-1.99-OpenSSH_3.1p1\\n`) through the now-open connection. As soon as Nmap hears from its host OS that the connection was successful, it terminates the connection. TCP connections usually end with another three-way handshake involving the FIN flag, but Nmap asks the host OS to terminate the connection immediately with a RST packet.

While this `connect()` scan example took twice as many packets as a SYN scan, the bandwidth differences are rarely so substantial. The vast majority of ports in a large scan will be closed or filtered. The packet traces for those are the same as described for SYN scan in Figure 5-3 and Figure 5-4. Only open ports generate more network traffic.

The output of a `connect()` scan doesn't differ significantly from a SYN scan. Example 5-3 shows a `connect()` scan of Scanme. The `-sT` option could have been omitted since Nmap is being run from a non-privileged account so `connect()` scan is the default type. This scan takes 30-seconds, while a SYN scan performed afterward between the two machines took only 20 seconds.

### Example 5-3. Connect scan example

```
krad~> nmap -T4 -sT scanme.nmap.org

Starting nmap 3.75 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 1658 ports scanned but not shown below are in state: filtered)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    open     smtp
53/tcp    open     domain
```

```

80/tcp  open  http
113/tcp closed auth

Nmap run completed -- 1 IP address (1 host up) scanned in 30.205 seconds

```

## 5.4. UDP Scan

While most popular services on the Internet run over the TCP protocol, UDP (<http://www.rfc-editor.org/rfc/rfc768.txt>) services are not uncommon. DNS, SNMP, and DHCP (registered ports 53, 161/162, and 67/68) are three of the most common. Because UDP scanning is generally slower and more difficult than TCP, some security auditors ignore these ports. This is a mistake, as exploitable UDP services are quite common and attackers certainly don't ignore the whole protocol. Fortunately, Nmap can help inventory UDP ports.

UDP scan is activated with the `-sU` option. It can be combined with a TCP scan type such as SYN scan (`-sS`) to check both protocols during the same run.

UDP scan works by sending an empty (no data) UDP header to every targeted port. Based on the response, or lack thereof, the port is assigned to one of four states, as shown in Table 5-3.

**Table 5-3. How Nmap interprets responses to a UDP probe**

Probe Response	Assigned State
Any UDP response from target port (unusual)	open
No response received	open filtered (if probe retransmissions also fail to elicit responses)
ICMP port unreachable error (type 3, code 3)	closed
Other ICMP unreachable errors (type 3, code 1, 2, 9, 10, or 13)	filtered

The most curious element of this table may be the `open|filtered` state. It is a symptom of the biggest challenges with UDP scanning: open ports rarely respond to these probes. The target TCP/IP stack simply passes the (empty) packet up to the listening application, which usually discards it immediately as invalid. If ports in all other states would respond, then open ports could all be deduced by elimination. Unfortunately, firewalls and filtering devices are *also* known to drop packets without responding. So when Nmap receives no response after several attempts, it cannot determine whether the port is `open` or `filtered`. When Nmap was released, filtering devices were rare enough that Nmap could (and did) simply assume that the port was `open`. The Internet is better guarded now, so Nmap changed in 2004 (version 3.70) to report nonresponsive UDP ports as `open|filtered` instead. We can see that in Example 5-4, which shows Ereet scanning a Linux box named Felix.

### Example 5-4. UDP scan example

```

krad# nmap -sU -v -F felix

Starting nmap 3.75 ( http://www.insecure.org/nmap/ )
Interesting ports on felix.yuma.net (192.168.0.42):
(The 1005 ports scanned but not shown below are in state: closed)
PORT      STATE          SERVICE
53/udp    open|filtered domain

```

```

67/udp open|filtered dhcpserver
111/udp open|filtered rpcbind
MAC Address: 00:02:E3:14:11:02 (Lite-on Communications)

Nmap run completed -- 1 IP address (1 host up) scanned in 999.250 seconds

```

This scan of Felix demonstrates the `open|filtered` ambiguity issue as well as another problem: UDP scanning can be *slow*. Scanning a thousand ports took almost 17 minutes in this case. Nmap provides ways to work around both problems, as described by the following two sections.

### 5.4.1. Disambiguating open from filtered UDP ports

In the case of the Felix scan, all but the three `open|filtered` ports were `closed`. So the scan was still successful in narrowing down potentially open ports to a handful. That is not always the case. Example 5-5 shows a UDP scan against the heavily filtered site Scanme.

#### Example 5-5. UDP scan example

```

krad# nmap -sU -F scanme.nmap.org

Starting nmap 3.75 ( http://www.insecure.org/nmap/ )
All 1008 scanned ports on scanme.nmap.org (205.217.153.55) are: open|filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 23.187 seconds

```

In this case, the scan didn't narrow down the open ports at all. All 1008 are `open|filtered`. A new strategy is called for.

Table 5-3 shows that the `open|filtered` state occurs when Nmap fails to receive any responses from its UDP probes to a particular port. Yet it also shows that, on rare occasions, the UDP service listening on a port will respond in kind, proving that the port is open. The reason these services don't respond often is that the empty packets Nmap sends are considered invalid. Unfortunately, UDP services generally define their own packet structure rather than adhering to some common general format that Nmap could always send. An SNMP packet looks completely different than a SunRPC, NFS, or DNS request packet.

To send the proper packet for every popular UDP service, Nmap would need a large database defining their probe formats. Fortunately, Nmap has that in the form of `nmap-versions`, which is part of the service and version detection subsystem described in Chapter 7.

When version scanning is enabled with `-sV` (or `-A`), it will send UDP probes to every `open|filtered` port (as well as known open ones). If any of the probes elicit a response from an `open|filtered` port, the state is changed to `open`. The results of adding `-sV` to the Felix scan are shown in Example 5-6.

#### Example 5-6. Improving Felix's UDP scan results with version detection

```

krad# nmap -sUV -F felix.yuma.net

Starting nmap 3.75 ( http://www.insecure.org/nmap/ )
Interesting ports on felix.yuma.net (192.168.0.42):
(The 1005 ports scanned but not shown below are in state: closed)
PORT      STATE         SERVICE      VERSION
53/udp    open          domain      ISC Bind 9.2.1

```

```

67/udp open|filtered dhcpserver
111/udp open rpcbind 2 (rpc #100000)
MAC Address: 00:02:E3:14:11:02 (Lite-on Communications)

Nmap run completed -- 1 IP address (1 host up) scanned in 1037.570 seconds

```

This new scan shows that port 111 and 53 are definitely open. The system isn't perfect though -- port 67 is still open|filtered. In this particular case, the port is open but Nmap does not have a working version probe for dhcp. Another tough service is SNMP, which usually only responds when the correct community string is given. Many devices are configured with the community string public, but not all are. While these results aren't perfect, learning the true state of two out of three tested ports is still helpful.

After the success in disambiguating Felix results, Ereet turns his attention back to Scanme, which listed all ports as open|filtered last time. He tries again with version detection, as shown in Example 5-7.

### **Example 5-7. Improving Scanme's UDP scan results with version detection**

```

krad# nmap -sUV -F scanme.nmap.org

Starting nmap 3.75 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 1007 ports scanned but not shown below are in state: open|filtered)
PORT      STATE SERVICE VERSION
53/udp    open  domain  ISC Bind 9.2.1

Nmap run completed -- 1 IP address (1 host up) scanned in 3053.411 seconds

```

This result took 50 minutes, versus 23 seconds for the previous Scanme scan, but these results are actually useful. Ereet's smile widens and eyes sparkle at this evidence of an open ISC Bind nameserver on a machine he wants to compromise. That software has a long history of security holes, so perhaps he can find a flaw in this recent version.

While Ereet will focus his UDP attacks on port 53 since it is confirmed open, he does not forget about the other ports. Those 1007 are listed as open|filtered. As we witnessed with the dhcpserver port on Felix, certain open UDP services can hide even from Nmap version detection. He has also only scanned the default ports so far, there are 64529 others that could possibly be open. For the record, 53 is the only open UDP port on Scanme.

While this version detection technique is the only way for Nmap to automatically disambiguate open|filtered ports, there are a couple tricks that can be tried manually. Sometimes a specialized traceroute can help. You could do a traceroute against a known-open TCP or UDP port with a tool such as hping2 (<http://www.hping.org>). Then try the same against the questionable UDP port. Differences in hop counts can differentiate open from filtered ports. Ereet attempts this against Scanme in Example 5-8. The first hping2 command does a UDP traceroute against known-open port 53. The -t 8 option tells hping2 to start at hop 8 and is only used here to save space. The second command does the same thing against presumed-closed port 54.

### **Example 5-8. Attempting to disambiguate UDP ports with TTL discrepancies**

```

krad# hping2 --udp --traceroute -t 8 -p 53 scanme.nmap.org
HPING scanme.nmap.org (ppp0): udp mode set, 28 headers + 0 data bytes
hop=8 TTL 0 during transit from ip=206.24.211.77 name=dcr2.SanFranciscosfo.savvis.net
hop=9 TTL 0 during transit from ip=208.172.147.94 name=bpr2.PaloAltoPaix.savvis.net
hop=10 TTL 0 during transit from ip=206.24.240.194 name=meernet.PaloAltoPaix.savvis.net
hop=11 TTL 0 during transit from ip=205.217.152.21 name=vlan21.sv.meer.net

```

```

--- scanme.nmap.org hping statistic ---
12 packets transmitted, 4 packets received, 67% packet loss
round-trip min/avg/max = 13.4/13.8/14.1 ms

krad# hping2 --udp --traceroute -t 8 -p 54 scanme.nmap.org
HPING scanme.nmap.org (ppp0): udp mode set, 28 headers + 0 data bytes
hop=8 TTL 0 during transit from ip=206.24.211.77 name=dcr2.SanFranciscosfo.savvis.net
hop=9 TTL 0 during transit from ip=208.172.147.94 name=bpr2.PaloAltoPaix.savvis.net
hop=10 TTL 0 during transit from ip=206.24.240.194 name=meernet.PaloAltoPaix.savvis.net
hop=11 TTL 0 during transit from ip=205.217.152.21 name=vlan21.sv.meer.net

--- scanme.nmap.org hping statistic ---
12 packets transmitted, 4 packets received, 67% packet loss
round-trip min/avg/max = 12.5/13.6/14.7 ms

```

In this example, Ereet was only able to reach hop eleven of both the open and closed ports. So these results can't be used to distinguish port states against this host. It was worth a try, and does work in a significant number of cases. It is more likely to work in situations where the screening firewall is at least a hop or two before the target host. Scanme, on the other hand, is running its own Linux iptables host-based firewall. So there is no difference in hopcount between filtered and open ports.

Another technique is to try application-specific tools against common ports. For example, a brute force SNMP community string cracker could be tried against port 161. As Nmap's version detection probe database grows, the need to augment its results with external specialized tools is reduced. They will still be useful for special cases, such as SNMP devices with a custom community string.

### 5.4.2. Speeding up UDP scans

The other big challenge with UDP scanning is doing so quickly. Open and filtered ports rarely send any response, leaving Nmap to time out and then conduct retransmissions just in case the probe or response were lost. Closed ports are often an even bigger problem. They usually send back an ICMP port unreachable error. But unlike the RST packets sent by closed TCP ports in response to a SYN or Connect scan, many hosts rate limit ICMP port unreachable messages by default. Linux and Solaris are particularly strict about this. For example, the Linux 2.4.20 kernel on Felix limits destination unreachable messages to one per second (in `net/ipv4/icmp.c`). This explains why the scan in Example 5-4 is so slow.

Nmap detects rate limiting and slows down accordingly to avoid flooding the network with useless packets that the target machine will drop. Unfortunately, a Linux-style limit of one packet per second makes a 65,536-port scan take more than 18 hours. Here are some suggestions specific to this problem. Also read Chapter 6 for more detailed discussion and general advise.

Increase host parallelism

If Nmap receives just one port unreachable error from a single target host per second, it could receive 100/second just by scanning 100 such hosts at once. Implement this by passing a large value (such as 100) to `--min_hostgroup`.

Scan popular ports first

Very few UDP port numbers are commonly used. A scan of a hundred common ports will go quite quickly. You can then investigate those results while you launch a multi-day 65K-port sweep of the network in the background.

Scan from behind the firewall

As with TCP, packet filters can slow down scans dramatically. Many modern firewalls make setting packet rate limits easy. If you can bypass that problem by launching the scan from behind the firewall rather than across it, do so.

Use `-v` and chill out

With verbosity (`-v`) enabled, Nmap provides estimated time for scan completion of each host. There is no need to watch it closely. Get some sleep, head to your favorite pub, read a book, finish other work, or otherwise amuse yourself while Nmap tirelessly scans on your behalf.

## 5.5. TCP Null, FIN, and Xmas Scans

These three scan types (even more are possible with the `--scanflags` option described in the next section) exploit a subtle loophole in the TCP RFC (<http://www.rfc-editor.org/rfc/rfc793.txt>) to differentiate between open and closed ports. Page 65 says that “if the [destination] port state is CLOSED .... an incoming segment not containing a RST causes a RST to be sent in response.” Then the next page discusses packets sent to open ports without the SYN, RST, or ACK bits set, stating that: “you are unlikely to get here, but if you do, drop the segment, and return.”

When scanning systems compliant with this RFC text, any packet not containing SYN, RST, or ACK bits will result in a returned RST if the port is closed and no response at all if the port is open. As long as none of those three bits are included, any combination of the other three (FIN, PSH, and URG) are OK. Nmap exploits this with three scan types:

Null scan (`-sN`)

Does not set any bits (tcp flag header is 0)

FIN scan (`-sF`)

Sets just the TCP FIN bit.

Xmas scan (`-sX`)

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

These three scan types are exactly the same in behavior except for the TCP flags set in probe packets. Responses are treated as shown in Table 5-4.

**Table 5-4. How Nmap interprets responses to a Null, FIN, or Xmas scan probe**

Probe Response	Assigned State
No response received	open filtered (if probe retransmissions also fail to elicit responses)
TCP RST packet	closed

Probe Response	Assigned State
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

The key advantage to these scan types is that they can sneak through certain non-stateful firewalls and packet filtering routers. Such firewalls try to prevent incoming TCP connections (while allowing outbound ones) by blocking any TCP packets with the SYN bit set and ACK cleared. This configuration is common enough that the Linux iptables firewall command offers a special `--syn` option to implement it. The Null, FIN, and Xmas scans clear the SYN bit and thus fly right through those rules.

Another advantage is that these scan types are a little more stealthy than even a SYN scan. Don't count on this though -- most modern IDS products can be configured to detect them.

The big downside is that not all systems follow RFC 793 to the letter. A number of systems send RST responses to the probes regardless of whether the port is open or not. This causes all of the ports to be labeled `closed`. Major operating systems that do this are Microsoft Windows, many Cisco devices, BSDI, and IBM OS/400. This scan does work against most UNIX-based systems though. Since Nmap OS detection tests for this quirk, you can learn whether the scan works against a particular type of system by examining the `nmap-os-fingerprints` file. Test T2 sends a NULL packet to an open port. So if you see a line like `T2 (Resp=N)`, that system seems to support the RFC and one of these scans should work against it. If the T2 line is longer, the system violated the RFC by sending a response and these scans won't work. Chapter 8 explains OS fingerprinting in further detail.

Another downside of these scans is that they can't distinguish open ports from certain filtered ones. If the packet filter sends an ICMP destination prohibited error, Nmap knows that a port is filtered. But most filters simply drop banned probes without any response, making the ports appear open. Since Nmap cannot be sure which is the case, it marks nonresponsive ports as `open|filtered`. Adding version detection (`-sV`) can disambiguate as it does with UDP scans, but that defeats much of the stealthy nature of this scan. If you are willing and able to connect to the ports anyway, you might as well use a SYN scan.

Using these scan methods is simple. Just add the `-sN`, `-sF`, or `-sX` options to specify the scan type. Example 5-9 shows two examples. The first one, a FIN scan against Para, identifies all 5 open ports (as `open|filtered`). The next execution, an Xmas scan against `scanme.nmap.org` doesn't work so well. Since it is unable to differentiate the 1658 filtered ports from the 4 open ones, all 1662 are listed as `open|filtered`. This demonstrates why Nmap offers so many scan methods. No single technique is preferable in all cases. Ereet will simply have to try another method to learn more about Scanme.

### Example 5-9. Example FIN and Xmas scans

```
krad# nmap -sF -T4 para

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on para (192.168.10.191):
(The 1658 ports scanned but not shown below are in state: closed)
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
53/tcp    open|filtered domain
111/tcp   open|filtered rpcbind
515/tcp   open|filtered printer
6000/tcp  open|filtered X11
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 4.644 seconds
```

```
krad# nmap -sX -T4 scanme.nmap.org
```

```
Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 1662 ports scanned but not shown below are in state: open|filtered)
PORT      STATE SERVICE
113/tcp    closed auth
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 23.112 seconds
```

Demonstrating the full, firewall-bypassing power of these scans requires a rather lame target firewall configuration. Unfortunately, those aren't hard to find. Example 5-10 shows a SYN scan of a SCO/Caldera machine named Docsrv.

#### **Example 5-10. SYN scan of docsrv.caldera.com**

```
# nmap -sS -T4 docsrv.caldera.com
```

```
Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on docsrv.caldera.com (216.250.128.247):
(The 1660 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed auth
507/tcp   open  crs
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 28.624 seconds
```

This example looks OK. Only two ports are open and the rest (except for 113) are filtered. With a modern stateful firewall, a FIN scan should not produce any extra information. Yet I try it anyway, obtaining the output in Example 5-11.

#### **Example 5-11. FIN scan of docsrv.caldera.com**

```
# nmap -sF -T4 docsrv.caldera.com
```

```
Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on docsrv.caldera.com (216.250.128.247):
(The 1624 ports scanned but not shown below are in state: closed)
PORT      STATE      SERVICE
7/tcp     open|filtered echo
9/tcp     open|filtered discard
11/tcp    open|filtered systat
13/tcp    open|filtered daytime
15/tcp    open|filtered netstat
19/tcp    open|filtered chargen
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
23/tcp    open|filtered telnet
25/tcp    open|filtered smtp
```

```

37/tcp    open|filtered time
79/tcp    open|filtered finger
80/tcp    open|filtered http
110/tcp   open|filtered pop3
111/tcp   open|filtered rpcbind
135/tcp   open|filtered msrpc
143/tcp   open|filtered imap
360/tcp   open|filtered scoi2odialog
389/tcp   open|filtered ldap
465/tcp   open|filtered smtps
507/tcp   open|filtered crs
512/tcp   open|filtered exec
513/tcp   open|filtered login
514/tcp   open|filtered shell
515/tcp   open|filtered printer
636/tcp   open|filtered ldapssl
712/tcp   open|filtered unknown
955/tcp   open|filtered unknown
993/tcp   open|filtered imaps
995/tcp   open|filtered pop3s
1434/tcp  open|filtered ms-sql-m
2000/tcp  open|filtered callbook
2766/tcp  open|filtered listen
3000/tcp  open|filtered ppp
3306/tcp  open|filtered mysql
6112/tcp  open|filtered dtspc
32770/tcp open|filtered sometimes-rpc3
32771/tcp open|filtered sometimes-rpc5
32772/tcp open|filtered sometimes-rpc7

```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 7.635 seconds
```

Wow! That is a lot of apparently open ports. Most of them are probably open, because having just these 39 filtered and the other 1624 closed (sending a RST packet) would be unusual. Yet it is still possible that some or all are filtered instead of open. FIN scan cannot determine for sure. We will revisit this case and learn more later in this chapter.

## 5.6. Custom scan types with `--scanflags`

Truly advanced Nmap users need not limit themselves to the canned scanned types offered. The `--scanflags` allows you to design your own scan by specifying arbitrary TCP flags. Let your creative juices flow, while evading intrusion detection systems whose vendors simply paged through the Nmap man page adding specific rules!

The `--scanflags` argument can be a numerical flag value such as 9 (PSH and FIN), but using symbolic names is easier. Just mash together any combination of URG, ACK, PSH, RST, SYN, and FIN. For example, `--scanflags URGACKPSHRSTSYNFIN` sets everything, though it's not very useful for scanning. The order these are specified in is irrelevant.

In addition to specifying the desired flags, you can specify a TCP scan type (such as `-sA` or `-sF`). That base type tells Nmap how to interpret responses. For example, a SYN scan considers no-response to indicate an `filtered` port, while a FIN scan treats the same as `open|filtered`. Nmap will behave the same way it does for the base scan type, except that it will use the TCP flags you specify instead. If you don't specify a base type, SYN scan is used.

### 5.6.1. Custom SYN/FIN scan

One interesting custom scan type is SYN/FIN. Sometimes a firewall admin or device manufacturer will attempt to block incoming connections with a rule such as “drop any incoming packets with only the SYN flag set”. They limit it to *only* the SYN flag because they don’t want to block the SYN/ACK packets which are returned as the second step of an outgoing connection.

The problem with this approach is that most end systems will accept initial SYN packets that contain other (non-ACK) flags as well. For example, the Nmap OS fingerprinting system sends a SYN/FIN/URG/PSH packet to an open port. More than half of the fingerprints in the database respond with a SYN/ACK. Thus they allow port scanning with this packet and generally allow making a full TCP connection too. Some systems have even been known to respond with SYN/ACK to a SYN/RST packet! The TCP RFC is ambiguous as to which flags are acceptable in an initial SYN packet, though SYN/RST certainly seems bogus.

Example 5-12 shows Ereet conducting a successful SYN/FIN scan of Google. Apparently he is getting bored with scanme.nmap.org.

#### Example 5-12. A SYN/FIN scan of Google

```
krad# nmap -sS --scanflags SYNFIN -T4 www.google.com

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on www.google.com (216.239.57.103):
(The 1660 ports scanned but not shown below are in state: filtered)
PORT      STATE    SERVICE
80/tcp    open     http
179/tcp   closed   bgp
443/tcp   open     https

Nmap run completed -- 1 IP address (1 host up) scanned in 22.914 seconds
```

Similar scan types, such as SYN/URG or SYN/PSH/URG/FIN will generally work as well. If you aren’t getting through, don’t forget the already mentioned SYN/RST option.

### 5.6.2. PSH scan

Section 5.5 noted that RFC-compliant systems allow one to scan ports using any combination of the FIN, PSH, and URG flags. While there are eight possible permutations, Nmap only offers three canned modes (Null, FIN, and Xmas). Show some personal flair by trying a PSH/URG or FIN/PSH scan instead. Results rarely differ from the three canned modes, but there is a small chance of evading scan detection systems.

To perform such a scan, just specify your desired flags with `--scanflags` and specify FIN scan (`-sF`) as the base type (choosing Null or Xmas would make no difference). Example 5-13 demonstrates a PSH scan against a Linux machine on my local network.

#### Example 5-13. A custom PSH scan

```
krad# nmap -sF --scanflags PSH  para

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on para (192.168.10.191):
(The 1658 ports scanned but not shown below are in state: closed)
```

```

PORT      STATE           SERVICE
22/tcp    open|filtered ssh
53/tcp    open|filtered domain
111/tcp   open|filtered rpcbind
515/tcp   open|filtered printer
6000/tcp  open|filtered X11
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap run completed -- 1 IP address (1 host up) scanned in 5.953 seconds

```

Because these scans all work the same way, I could keep just one of `-sF`, `-sN`, and `-sX` options, letting users emulate the others with `--scanflags`. There are no plans to do this because the shortcut options are easier to remember and use. You can still try the emulated approach to show off your Nmap skills. Execute `nmap -sF --scanflags FINPSHURG target` rather than the more mundane `nmap -sX target`.

### Warning

In my experience, needlessly complex Nmap command-lines don't impress girls. They usually respond with a condescending sneer, presumably because they recognize that the command is redundant.

## 5.7. TCP ACK Scan

This scan is different than the others discussed so far in that it never determines open (or even `open|filtered`) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

ACK scan is enabled by specifying the `-sA` option. Its probe packet has only the ACK flag set (unless you use `--scanflags`). When scanning unfiltered systems, open and closed ports will both return a RST packet. Nmap then labels them as unfiltered, meaning that they are reachable by the ACK packet, but whether they are open or closed is undetermined. Ports that don't respond, or send certain ICMP error messages back, are labeled filtered. Table 5-5 provides the full details.

**Table 5-5. How Nmap interprets responses to an ACK scan probe**

Probe Response	Assigned State
TCP RST response	unfiltered
No response received	filtered (if probe retransmissions also fail to elicit responses)
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

ACK scan usage is similar to most other scan types in that you simply add a single option flag, `-sA` in this case. Example 5-14 shows an ACK scan against Scanme.

#### Example 5-14. A Typical ACK Scan

```
krad# nmap -sA -T4 scanme.nmap.org
```

```

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 1658 ports scanned but not shown below are in state: filtered)
PORT      STATE      SERVICE
22/tcp    UNfiltered ssh
25/tcp    UNfiltered smtp
53/tcp    UNfiltered domain
80/tcp    UNfiltered http
113/tcp   UNfiltered auth

Nmap run completed -- 1 IP address (1 host up) scanned in 19.823 seconds

```

One of the most interesting uses of ACK scanning is to differentiate between stateful and stateless firewalls. Section 9.3.2 describes how to do this and why you would want to.

Sometimes a combination of scan types can be used to glean extra information from a system. As an example, start by reviewing the FIN scan of Docsvr in Example 5-11. Nmap finds the closed ports in that case, but 39 of them are listed as open|filtered because Nmap cannot determine between those two states with a FIN scan. Now look at the ACK scan of the same host in Example 5-15. Two of those 39 previously unidentified ports are shown to be filtered. The other 37 (based on the default port line above the table) are in the state unfiltered. That means open or closed. If one scan type identifies a port as open or filtered and another identifies it as open or closed, logic dictates that it must be open. By combining both scan types, we have learned that 37 ports on Docsvr are open, 2 are filtered, and 1624 are closed. While logical deduction worked well here to determine port states, that technique can't always be counted on. It assumes that different scan types always return a consistent state for the same port, which is inaccurate. Firewalls and TCP stack properties can cause different scans against the same machine to differ markedly. Against Docsvr, we have seen that a SYN scan considers the SSH port (tcp/22) filtered, while an ACK scan considers it unfiltered. When exploring boundary conditions and strangely configured networks, interpreting Nmap results is an art that benefits from experience and intuition.

### Example 5-15. An ACK scan of Docsvr

```

# nmap -sA -T4 docsvr.caldera.com

Starting nmap 3.77 ( http://www.insecure.org/nmap/ )
Interesting ports on docsvr.caldera.com (216.250.128.247):
(The 1661 ports scanned but not shown below are in state: UNfiltered)
PORT      STATE      SERVICE
135/tcp   filtered msrpc
1434/tcp  filtered ms-sql-m

Nmap run completed -- 1 IP address (1 host up) scanned in 7.207 seconds

```

## 5.8. TCP Window Scan

Window scan is exactly the same as ACK scan except that it exploits an implementation detail of certain systems to differentiate open ports from closed ones, rather than always printing UNfiltered when a RST is returned. It does this by examining the TCP Window value of the RST packets returned. On some systems, open ports use a positive window size (even for RST packets) while closed ones have a zero window. Window scan sends the same bare ACK probe as ACK scan, interpreting the results as shown in Table 5-6.

**Table 5-6. How Nmap interprets responses to a Window scan ACK probe**

Probe Response	Assigned State
TCP RST response with non-zero window field	open
TCP RST response with zero window field	closed
No response received	filtered (if probe retransmissions also fail to elicit responses)
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

This scan relies on an implementation detail of a minority of systems out on the Internet, so you can't always trust it. Systems that don't support it will usually return all ports `closed`. Of course, it is possible that the machine really has no open ports. If most scanned ports are `closed` but a few common port numbers (such as 22, 25, 53) are `filtered`, the system is most likely susceptible. Occasionally, systems will even show the exact opposite behavior. If your scan shows 1000 open ports and 3 closed or filtered ports, then those three may very well be the truly open ones.

While this scan is not suited for every situation, it can be quite useful on occasion. Recall Example 5-11, which shows many `open|filtered` ports not found in a basic SYN scan. The problem is that we can't distinguish between open and filtered ports with that FIN scan. The previous section showed that we could distinguish them by combining FIN and ACK scan results. In this case, a Window scan makes it even easier by not requiring the FIN scan results, as shown in Example 5-16.

#### Example 5-16. Window scan of docsrv.caldera.com

```
# nmap -sW -T4 docsrv.caldera.com

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on docsrv.caldera.com (216.250.128.247):
(The 1624 ports scanned but not shown below are in state: closed)
PORT      STATE     SERVICE
7/tcp      open      echo
9/tcp      open      discard
11/tcp     open      systat
13/tcp     open      daytime
15/tcp     open      netstat
19/tcp     open      chargen
21/tcp     open      ftp
22/tcp     open      ssh
23/tcp     open      telnet
25/tcp     open      smtp
37/tcp     open      time
79/tcp     open      finger
80/tcp     open      http
110/tcp    open      pop3
111/tcp    open      rpcbind
135/tcp    filtered msrpc
143/tcp    open      imap
360/tcp    open      scoi2odialog
389/tcp    open      ldap
465/tcp    open      smtps
507/tcp    open      crs
```

```

512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
515/tcp  open  printer
636/tcp  open  ldapssl
712/tcp  open  unknown
955/tcp  open  unknown
993/tcp  open  imaps
995/tcp  open  pop3s
1434/tcp filtered ms-sql-m
2000/tcp open  callbook
2766/tcp open  listen
3000/tcp open  ppp
3306/tcp open  mysql
6112/tcp open  dtspc
32770/tcp open  sometimes-rpc3
32771/tcp open  sometimes-rpc5
32772/tcp open  sometimes-rpc7

```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 7.304 seconds
```

These results are exactly what we wanted! The same 39 interesting ports are shown as with the FIN scan, but this time it distinguishes between the two filtered ports (MS-SQL and MSRPC) and the 37 that are actually open. These are the same results we obtained by combining FIN and ACK scan results together in the previous section. Verifying results for consistency is another good reason for trying multiple scan types against a target network.

## 5.9. TCP Maimon Scan

The Maimon scan is named after its discoverer, Uriel Maimon. He described the technique in Phrack Magazine issue #49 (November 1996). Nmap, which included this technique, was released two issues later. This technique is exactly the same as Null, FIN, and Xmas scan, except that the probe is FIN/ACK. According to RFC 793 (TCP), a RST packet should be generated in response to such a probe whether the port is open or closed. However, Uriel noticed that many BSD-derived systems simply drop the packet if the port is open. Nmap takes advantage of this to determine open ports, as shown in Table 5-7.

**Table 5-7. How Nmap interprets responses to a Maimon scan probe**

Probe Response	Assigned State
No response received	open filtered (if probe retransmissions also fail to elicit responses)
TCP RST packet	closed
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

The Nmap flag for a Maimon scan is `-sM`. While this option was quite useful in 1996, modern systems rarely exhibit this bug. They send a RST back for all ports, making every port appear closed. This result is shown in Example 5-17

**Example 5-17. A failed Maimon scan**

```
# nmap -sM -T4 para

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
All 1663 scanned ports on para (192.168.10.191) are: closed
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap run completed -- 1 IP address (1 host up) scanned in 4.189 seconds
```

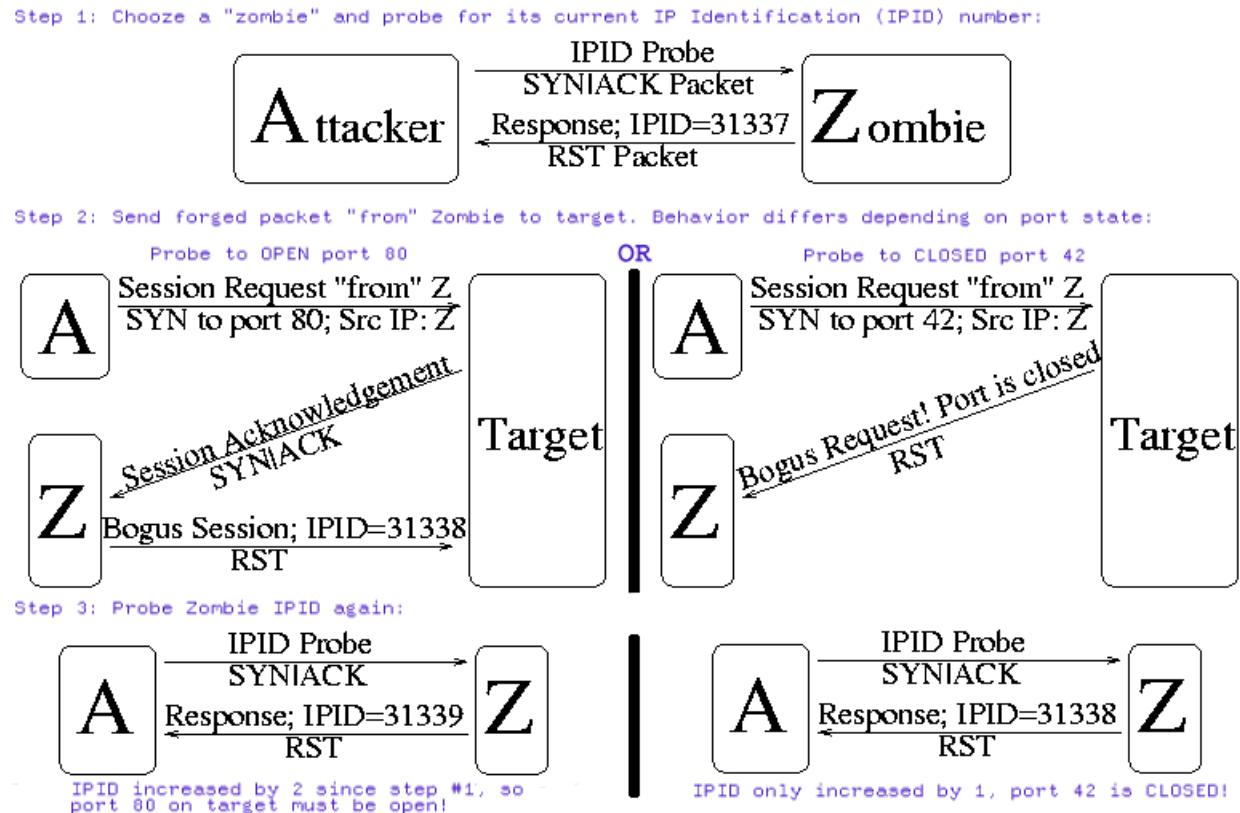
## 5.10. TCP Idle Scan

In 1998, security researcher Antirez (who also wrote the hping2 tool frequently used in this book) posted to the Bugtraq mailing list an ingenious new port scanning technique. Idle scan, as it has become known, allows for completely blind port scanning. Attackers can actually scan a target without sending a single packet to the target from their own IP address! Instead, a clever side-channel attack allows for the scan to be bounced off a dumb "zombie" host. Intrusion detection system (IDS) reports will finger the innocent zombie as the attacker. Besides being extraordinarily stealthy, this scan type permits mapping out IP-based trust relationships between machines.

While Idle scanning is more complex than any of the techniques discussed so far, you don't need to be a TCP/IP expert to understand it. It can be put together from these basic TCP/IP facts:

- One way to determine whether a TCP port is open is to send a SYN (session establishment) packet to the port. The target machine will respond with a SYN/ACK (session request acknowledgment) packet if the port is open, and RST (reset) if the port is closed. This is the basis of the previously discussed SYN scan.
- A machine which receives an unsolicited SYN|ACK packet will respond with a RST. An unsolicited RST will be ignored.
- Every IP packet on the Internet has a fragment identification number (IPID). Many operating systems simply increment this number for each packet they send. So probing for this number can tell an attacker how many packets have been sent since the last probe.

By combining these traits, it is possible to scan a target network while forging your identity so that it looks like an innocent "zombie" machine did the scanning. This technique is easiest to describe with a diagram. In Figure 5-6, an attacker, A, is scanning a Target machine, while blaming the scan on some Zombie, Z. The boxes represent machines, and the lines represent packets. Brief English descriptions of the packets are printed on top of the lines, while actual TCP flags and distinctive packet information is printed below them.

**Figure 5-6. Idle Scan Technique (Simplified)**

\* When this figure is redone, it should either show a filtered port case, or at least note at the bottom-right that port 42 is closed or filtered.

As this diagram demonstrates, the target hosts respond differently to the zombie depending on port state. If the probed port is open, the target sends a SYN/ACK to the zombie. The zombie does not expect this SYN/ACK, so it sends a RST back. By sending the RST, the zombie causes its IPID sequence number to increment. If the port is closed, the target sends a RST to the zombie. Zombies ignore this unsolicited RST packet and do not increment their IPID sequence number. In step three, the attacker simply probes for the Zombie's latest IPID. If the IPID value is just one higher than the previous probe, the new response accounts for that increment and the target port must be closed or filtered. Nmap versions starting with 3.78 label such a port as `closed|filtered`, while previous versions considered it `closed`. If the IPID value increased by two, that extra increment was due to the zombie sending back a RST to the target and so the port is open.

Idlescan is the ultimate stealth scan. Nmap offers decoy scanning (`-D`) to help users shield their identity, but that (unlike Idle scan) still requires an attacker to send some packets to the target from his real IP address to get scan results back. One upshot of Idle scan is that intrusion detection systems will generally send alerts claiming that the zombie machine has launched a scan against them. So it can be used to frame some other party for a scan. Keep this possibility in mind when reading alerts from your IDS.

A unique advantage of Idle scan is that it can be used to defeat certain packet filtering firewalls and routers. IP source address filtering is a common (though weak) security mechanism for limiting machines that may connect to a sensitive host or network. For example, a company database server might only allow connections from the public web server which accesses it. Or a home user might only allow ssh (interactive login) connections from his work

machines.

A more disturbing scenario occurs when some company bigwig demands that network administrators open a firewall hole so he can access internal network resources from his home IP address. This can happen when executives are unwilling or unable to use secure VPN alternatives.

Idle scanning can sometimes be used to map out these trust relationships. The key factor is that Idlescan results list open ports from the zombie host's perspective. A normal scan against the aforementioned database server might show no ports open, but performing an Idle scan while using the web server's IP as the zombie could expose the trust relationship by showing the database-related service ports open.

Mapping out these trust relationships can be very useful to attackers for prioritizing targets. The web server discussed above may seem mundane to an attacker until she notices its special database access.

A disadvantage to Idle scanning is that it takes far longer than most other scan types. Despite the optimized algorithms described in Section 5.10.3, A 15-second SYN scan could take 15 minutes or more as an Idle scan. Another issue is that you must be able to spoof packets as if they are coming from the zombie and have them reach the target machine. Many ISPs (particularly dialup and residential broadband providers) now implement egress filtering to prevent this sort of packet spoofing. Higher end providers (such as colocation and T1 service) are much less likely to do this. If this filtering is in effect, Nmap will print a quick error message for every zombie you try. If changing ISPs is not an option, you might try using another IP on the same ISP network. Sometimes the filtering only blocks spoofing of IP addresses that are *outside* the range used by customers. Another challenge with idle scan is that you must find a working zombie host, as described in the next section.

### 5.10.1. Finding a working idle scan zombie host

The first step in executing an IPID Idle scan is to find an appropriate zombie. It needs to assign IPID packets incrementally on a global (rather than per-host it communicates with) basis. It should be idle (hence the scan name), as extraneous traffic will bump up its IPID sequence, confusing the scan logic. The lower the latency between the attacker and the zombie, and between the zombie and the target, the faster the scan will proceed.

When an Idle scan is attempted, Nmap tests the proposed Zombie and reports any problems with it. If one doesn't work, try another. Enough Internet hosts are vulnerable that zombie candidates aren't hard to find. Since the hosts need to be idle, choosing a well-known host such as [www.yahoo.com](http://www.yahoo.com) or [google.com](http://google.com) will almost never work.

A common approach is to simply execute a Nmap ping scan of some network. You could use Nmap's random IP selection mode (`-iR`), but that is likely to result in far away zombies with substantial latency. Choosing a network near your source address, or near the target, should produce better results. You can try an Idle scan using each available host from the ping scan results until you find one that works. As usual, it is best to ask permission before using someone's machines for unexpected purposes such as idle scanning.

Performing a port scan and OS identification (`-O`) on the zombie candidate network rather than just a ping scan helps in selecting a good zombie. As long as verbose mode (`-v`) is enabled, OS detection will usually determine the IPID sequence generation method and print a line such as "IPID Sequence Generation: Incremental". If the type is given as Incremental or Broken little-endian incremental, the machine is a good zombie candidate. That is still no guarantee that it will work, as Solaris and some other systems create a new IPID sequence for each host they communicate with. The host could also be too busy. OS detection and the open port list can also help in identifying systems that are likely to be idle.

While identifying a suitable zombie takes some initial work, you can keep re-using the good ones.

### 5.10.2. Executing an Idle scan

Once a suitable zombie has been found, performing a scan is easy. Simply specify the zombie hostname to the `-sI` option and Nmap does the rest. Example 5-18 shows an example of Ereet scanning the Recording Industry Association of America by bouncing an Idle scan off an Adobe machine named Kiosk.

#### Example 5-18. An Idle scan against the RIAA

```
# nmap -P0 -p- -sI kiosk.adobe.com www.riaa.com

Starting nmap V. 3.10ALPHA3 ( www.insecure.org/nmap/ )
Idlescan using zombie kiosk.adobe.com (192.150.13.111:80); Class: Incremental
Interesting ports on 208.225.90.120:
(The 65522 ports scanned but not shown below are in state: closed)
Port      State       Service
21/tcp    open        ftp
25/tcp    open        smtp
80/tcp    open        http
111/tcp   open        sunrpc
135/tcp   open        loc-srv
443/tcp   open        https
1027/tcp  open        IIS
1030/tcp  open        iad1
2306/tcp  open        unknown
5631/tcp  open        pcanywheredata
7937/tcp  open        unknown
7938/tcp  open        unknown
36890/tcp open        unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 2594.472 seconds
```

From the scan above, we learn that the RIAA is not very security conscious (note the open PC Anywhere, portmapper, and Legato nsexec ports). Since they apparently have no firewall, it is unlikely that they have an IDS. But if they do, it will show kiosk.adobe.com as the scan culprit. The `-P0` option prevents Nmap from sending an initial ping packet to the RIAA machine. That would have disclosed Ereet's true address. The scan took a long time because `-p-` was specified to scan all 65K ports. Don't try to use kiosk for your scans, as it has already been removed.

By default, Nmap forges probes to the target from the source port 80 of the zombie. You can choose a different port by appending a colon and port number to the zombie name (e.g. `-sI kiosk.adobe.com:113`). The chosen port must not be filtered from the attacker or the target. A SYN scan of the zombie should show the port in the open or closed state.

### 5.10.3. Idle scan implementation algorithms

While Figure 5-6 describes Idle scan at the fundamental level, the Nmap implementation is far more complex. Key differences are parallelism for quick execution and redundancy to reduce false positives.

Parallelizing idle scan is trickier than with other scan techniques due to indirect method of deducing port states. If Nmap sends probes to many ports on the target and then checks the new IPID value of the zombie, the number of IPID increments will expose how many target ports are open, but not which ones. This isn't actually a major

problem, as the vast majority of ports in a large scan will be `closed|filtered`. Since only open ports cause the IPID value to increment, Nmap will see no intervening increments and can mark the whole group of ports as `closed|filtered`. Nmap can scan groups of up to 100 ports in parallel. If Nmap probes a group then finds that the zombie IPID has increased  $N$  times, there must be  $N$  open ports among that group. Nmap then finds the open ports with a binary search. It splits the group into two and separately sends probes to each. If a subgroup shows zero open ports, that group's ports are all marked `closed|filtered`. If a subgroup shows one or more open ports, it is divided again and the process continues until those ports are identified. While this technique adds complexity, it can reduce scan times by an order of magnitude over scanning just one port at a time.

Reliability is another major idle scanning concern. If the zombie host sends packets to any unrelated machines during the scan, its IPID increments. This causes Nmap to think it has found an open port. Fortunately, parallel scanning helps here too. If Nmap scans 100 ports in a group and the IPID increase signals two open ports, Nmap splits the group into two fifty-port subgroups. When Nmap does an IPID scan on both subgroups, the total zombie IPID increase better be two again! Otherwise, Nmap will detect the inconsistency and rescan the groups. It also modifies group size and scan timing based on the detected reliability rate of the zombie. If Nmap detects too many inconsistent results, it will quit and ask the user to provide a better zombie.

Sometimes a packet trace is the best way to understand complex algorithms and techniques such as these. Once again, the Nmap `--packet_trace` makes these trivial to produce when desired. Example 5-19 provides an annotated packet trace of an actual seven port idle scan. The IP addresses have been changed to Attacker, Zombie, and Target (as in Figure 5-6) and some irrelevant aspects of the trace lines (such as TCP window size) have been removed for clarity.

#### **Example 5-19. IPID scan packet trace**

```
Attacker# nmap -sI Zombie -P0 -p20-25,110 -r --packet_trace -v Target
```

*-P0 is necessary for stealth, otherwise ping packets would be sent to the target from Attacker's real address. Version scanning would also expose the true address, and so -sV is not specified. -r (turns off port randomization) is only used to make this example easier to follow.*

```
Starting nmap 3.78 ( http://www.insecure.org/nmap/ )
```

*Nmap firsts tests the Zombie IPID sequence generation by sending 6 SYN/ACK to it and analyzing the responses. This helps Nmap immediately weed out bad zombies. It is also necessary because some systems (usually Microsoft Windows machines, though not all Windows boxes do this) increment the IPID by 256 for each packet sent rather than by one. This happens on little-endian machines when they don't convert the IPID to network byte order (big-endian). Nmap uses these initial probes to detect and work around this problem.*

```
SENT (0.0060s) TCP Attacker:51824 > Zombie:80 SA id=35996
SENT (0.0900s) TCP Attacker:51825 > Zombie:80 SA id=25914
SENT (0.1800s) TCP Attacker:51826 > Zombie:80 SA id=39591
RCVD (0.1550s) TCP Zombie:80 > Attacker:51824 R id=15669
SENT (0.2700s) TCP Attacker:51827 > Zombie:80 SA id=43604
RCVD (0.2380s) TCP Zombie:80 > Attacker:51825 R id=15670
SENT (0.3600s) TCP Attacker:51828 > Zombie:80 SA id=34186
```

```
RCVD (0.3280s) TCP Zombie:80 > Attacker:51826 R id=15671
SENT (0.4510s) TCP Attacker:51829 > Zombie:80 SA id=27949
RCVD (0.4190s) TCP Zombie:80 > Attacker:51827 R id=15672
RCVD (0.5090s) TCP Zombie:80 > Attacker:51828 R id=15673
RCVD (0.5990s) TCP Zombie:80 > Attacker:51829 R id=15674
Idlescan using zombie Zombie (Zombie:80); Class: Incremental
```

*For this next test, Nmap spoofs four packets to Zombie as if they are coming from Target. Then it probes the zombie to insure that the IPID increased. If it hasn't, then it is likely that either the attacker's ISP is blocking the spoofed packets or the zombie uses a separate IPID sequence counter for each host it communicates with. Both are common occurrences, so Nmap always performs this test. The last-known Zombie IPID was 15674, as shown above.*

```
SENT (0.5990s) TCP Target:51823 > Zombie:80 SA id=1390
SENT (0.6510s) TCP Target:51823 > Zombie:80 SA id=24025
SENT (0.7110s) TCP Target:51823 > Zombie:80 SA id=15046
SENT (0.7710s) TCP Target:51823 > Zombie:80 SA id=48658
SENT (1.0800s) TCP Attacker:51987 > Zombie:80 SA id=27659
RCVD (1.2290s) TCP Zombie:80 > Attacker:51987 R id=15679
```

*The four spoofed packets coupled with the probe from Attacker caused the Zombie to increase its IPID from 15674 to 15679. Perfect! Now the real scanning begins. Remember that 15679 is the latest Zombie IPID.*

```
Initiating Idlescan against Target
SENT (1.2290s) TCP Zombie:80 > Target:20 S id=13200
SENT (1.2290s) TCP Zombie:80 > Target:21 S id=3737
SENT (1.2290s) TCP Zombie:80 > Target:22 S id=65290
SENT (1.2290s) TCP Zombie:80 > Target:23 S id=10516
SENT (1.4610s) TCP Attacker:52050 > Zombie:80 SA id=33202
RCVD (1.6090s) TCP Zombie:80 > Attacker:52050 R id=15680
```

*Nmap probes ports 20-23. Then it probes Zombie and finds that the new IPID is 15680, only one higher than the previous value of 15679. There were no IPID increments in between those two known packets, meaning ports 20-23 are probably closed/filtered. It is also possible that a SYN/ACK from a Target port has simply not arrived yet. In that case, Zombie has not responded with a RST and thus its IPID has not incremented. To ensure accuracy, Nmap will try these ports again later.*

```
SENT (1.8510s) TCP Attacker:51986 > Zombie:80 SA id=49278
RCVD (1.9990s) TCP Zombie:80 > Attacker:51986 R id=15681
```

*Nmap probes again because four tenths of a second has gone by since the last probe it sent. The Zombie (if not truly idle) could have communicated with other hosts during this period, which would screw up later results if not detected here. Fortunately, that has not happened: the next IPID is 15681 as expected.*

```

SENT (2.0000s) TCP Zombie:80 > Target:24 S id=23928
SENT (2.0000s) TCP Zombie:80 > Target:25 S id=50425
SENT (2.0000s) TCP Zombie:80 > Target:110 S id=14207
SENT (2.2300s) TCP Attacker:52026 > Zombie:80 SA id=26941
RCVD (2.3800s) TCP Zombie:80 > Attacker:52026 R id=15684

```

*Nmap probes ports 24, 25, and 110 then queries the Zombie IPID. It has jumped from 15681 to 15684. It skipped 15682 and 15683, meaning that two of those three ports are likely open. Nmap cannot tell which two are open, and it could also be a false positive. So Nmap drills down deeper, dividing the scan into subgroups.*

```

SENT (2.6210s) TCP Attacker:51867 > Zombie:80 SA id=18869
RCVD (2.7690s) TCP Zombie:80 > Attacker:51867 R id=15685
SENT (2.7690s) TCP Zombie:80 > Target:24 S id=30023
SENT (2.7690s) TCP Zombie:80 > Target:25 S id=47253
SENT (3.0000s) TCP Attacker:51979 > Zombie:80 SA id=12077
RCVD (3.1480s) TCP Zombie:80 > Attacker:51979 R id=15687

```

*The first subgroup is ports 24 and 25. The IPID jumps from 15685 to 15687, meaning that one of these two ports is most likely open. Nmap tries the divide and conquer approach again, probing each port separately.*

```

SENT (3.3910s) TCP Attacker:51826 > Zombie:80 SA id=32515
RCVD (3.5390s) TCP Zombie:80 > Attacker:51826 R id=15688
SENT (3.5390s) TCP Zombie:80 > Target:24 S id=47868
SENT (3.7710s) TCP Attacker:52012 > Zombie:80 SA id=14042
RCVD (3.9190s) TCP Zombie:80 > Attacker:52012 R id=15689

```

*A port 24 probe shows no jump in the IPID. So that port is closed. From the results so far, Nmap has tentatively determined:*

- 1) Ports 20-23 are closed/filtered
- 2) Two of the ports 24, 25, and 110 are open
- 3) One of the ports 24 and 25 are open
- 4) Port 24 is closed/filtered

*Stare at this puzzle long enough and you'll find only one solution: ports 25 and 110 are open while the other five are closed/filtered. Using this logic, Nmap could cease scanning and print results now. It used to do so, but that produced too many false positive open ports when the Zombie wasn't truly idle. So Nmap continues scanning to verify its results*

```

SENT (4.1600s) TCP Attacker:51858 > Zombie:80 SA id=6225
RCVD (4.3080s) TCP Zombie:80 > Attacker:51858 R id=15690
SENT (4.3080s) TCP Zombie:80 > Target:25 S id=35713
SENT (4.5410s) TCP Attacker:51856 > Zombie:80 SA id=28118
RCVD (4.6890s) TCP Zombie:80 > Attacker:51856 R id=15692
Discovered open port 25/tcp on Target
SENT (4.6900s) TCP Zombie:80 > Target:110 S id=9943
SENT (4.9210s) TCP Attacker:51836 > Zombie:80 SA id=62254

```

```
RCVD (5.0690s) TCP Zombie:80 > Attacker:51836 R id=15694
Discovered open port 110/tcp on Target
```

*Probes of ports 25 and 110 show that they are open, as we deduced previously.*

```
SENT (5.0690s) TCP Zombie:80 > Target:20 S id=8168
SENT (5.0690s) TCP Zombie:80 > Target:21 S id=36717
SENT (5.0690s) TCP Zombie:80 > Target:22 S id=4063
SENT (5.0690s) TCP Zombie:80 > Target:23 S id=54771
SENT (5.3200s) TCP Attacker:51962 > Zombie:80 SA id=38763
RCVD (5.4690s) TCP Zombie:80 > Attacker:51962 R id=15695
SENT (5.7910s) TCP Attacker:51887 > Zombie:80 SA id=61034
RCVD (5.9390s) TCP Zombie:80 > Attacker:51887 R id=15696
```

*Just to be sure, Nmap tries ports 20-23 again. A Zombie IPID query shows no sequence jump. On the off chance that a SYN/ACK from Target to Zombie came in late, Nmap tries another IPID query. This again shows no open ports. Nmap is now sufficiently confident with its results to print them.*

The Idlescan took 5 seconds to scan 7 ports.

Interesting ports on Target:

PORt	STATE	SERVICE
20/tcp	closed filtered	ftp-data
21/tcp	closed filtered	ftp
22/tcp	closed filtered	ssh
23/tcp	closed filtered	telnet
24/tcp	closed filtered	priv-mail
25/tcp	open	smtp
110/tcp	open	pop3

```
Nmap run completed -- 1 IP address (1 host up) scanned in 5.949 seconds
```

For complete details on the Nmap idle scan implementation, read `idle_scan.cc` from the Nmap source code distribution.

While port scanning is a clever abuse of predictable IPID sequences, they can be exploited for many other purposes as well. Examples are peppered throughout this book, particularly in Chapter 9.

## 5.11. IP Protocol Scan

IP Protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines. This isn't technically a port scan, since it cycles through IP protocol numbers rather than TCP or UDP port numbers. Yet it still uses the `-p` option to select scanned protocol numbers, reports its results within the normal port table format, and even uses the same underlying scan engine as the true port scanning methods. So it is close enough to a port scan that it belongs here.

Besides being useful in its own right, protocol scan demonstrates the power of open source software. While the fundamental idea is pretty simple, I had not thought to add it nor received any requests for such functionality. Then in the summer of 2000, Gerhard Rieger conceived the idea, wrote an excellent patch implementing it, and sent it to the

nmap-hackers mailing list. I incorporated that patch into the Nmap tree and released a new version the next day. Few pieces of commercial software have users enthusiastic enough to design and contribute their own improvements!

Protocol scan works in a similar fashion to UDP scan. Instead of iterating through the port number field of a UDP packet, it sends IP packet headers and iterates through the 8-bit IP protocol field. The headers are usually empty, containing no data and not even the proper header for the claimed protocol. The three exceptions are TCP, UDP, and ICMP. A proper protocol header for those is included since some systems won't send them otherwise and because Nmap already has functions to create them. Instead of watching for ICMP port unreachable messages, protocol scan is on the lookout for ICMP *protocol* unreachable messages. Table 5-8 shows how responses to the IP probes are mapped to port states.

**Table 5-8. How Nmap interprets responses to an IP protocol probe**

Probe Response	Assigned State
Any response in any protocol from target host	open (for protocol used by response, not necessarily probe protocol)
ICMP protocol unreachable error (type 3, code 2)	closed
Other ICMP unreachable errors (type 3, code 1, 3, 9, 10, or 13)	filtered (though they prove ICMP is open if sent from the target machine)
No response received	open filtered (if probe retransmissions also fail to elicit responses)

Like open ports in the TCP or UDP protocols, every open protocol is a potential exploitation vector. In addition, protocol scan results help determine the purpose of a machine and what sort of packet filtering is in place. End hosts usually have little more than icmp, tcp, udp, and (sometimes) igmp open, while routers often offer much more, including routing-related protocols such as GRE and EGP. Firewalls and VPN gateways may show encryption-related protocols such as IPSec and SWIPE.

Like the ICMP port unreachable messages received during a UDP scan, ICMP protocol unreachable messages are often rate limited. For example, no more than one ICMP destination unreachable response is sent per second from a default Linux 2.4.20 box. Since there are only 256 possible protocol numbers, this is less of a problem than with a 65,536-port UDP scan. The suggestions in Section 5.4.2 apply to speeding up IP protocol scans as well.

Protocol scan is used the same way as most other scan techniques. Just specify `-sO` in addition to whatever general Nmap options please you. The normal port (`-p`) option is used to select protocol numbers. Or you can use `-F` to scan all protocols listed in the `nmap-protocols` database. By default, Nmap scans all 256 possible values. Example 5-20 shows Ereet scanning a router in Poland followed by a typical Linux box on my local network.

#### **Example 5-20. IP protocol scan of a router and a typical Linux 2.4 box**

```
# nmap -sO 62.233.173.90 para

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting protocols on ntwklan-62-233-173-90.devs.futuro.pl (62.233.173.90):
(The 240 protocols scanned but not shown below are in state: closed)
PROTOCOL STATE          SERVICE
1      open              icmp
4      open|filtered    ip
6      open              tcp
8      open|filtered    egp
```

```

9      open|filtered  igrp
17     filtered      udp
47     open|filtered gre
53     filtered      swipe
54     open|filtered narp
55     filtered      mobile
77     filtered      sun-nd
80     open|filtered iso-ip
88     open|filtered eigrp
89     open|filtered ospfigp
94     open|filtered ipip
103    filtered      pim

Interesting protocols on para (192.168.10.191):
(The 252 protocols scanned but not shown below are in state: closed)
PROTOCOL STATE          SERVICE
1      open            icmp
2      open|filtered  igmp
6      open            tcp
17     filtered       udp
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap run completed -- 2 IP addresses (2 hosts up) scanned in 458.040 seconds

```

## 5.12. TCP FTP Bounce Scan

An interesting feature of the FTP protocol (RFC 959 (<http://www.rfc-editor.org/rfc/rfc959.txt>)) is support for so-called proxy ftp connections. This allows a user to connect to one FTP server, then ask that files be sent to a third-party server. Such a feature is ripe for abuse on many levels, so most servers have ceased supporting it. One of the abuses this feature allows is causing the FTP server to port scan other hosts. Simply ask the FTP server to send a file to each interesting port of a target host in turn. The error message will describe whether the port is open or not. This is a good way to bypass firewalls because organizational FTP servers are often behind firewalls where they have more access than any old Internet host would. Nmap supports ftp bounce scan with the `-b` option. It takes an argument of the form `username:password@server:port`. *Server* is the name or IP address of a vulnerable FTP server. As with a normal URL, you may omit `username:password`, in which case anonymous login credentials (`user: anonymous password:-wwwuser@`) are used. The port number (and preceding colon) may be omitted as well, in which case the default FTP port (21) on *server* is used.

In Example 5-21, I attempt to bounce off the main Microsoft FTP server to scan Google.

### Example 5-21. Attempting an FTP bounce scan

```
# nmap -P0 -b ftp.microsoft.com google.com

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Your ftp bounce server doesn't allow privileged ports, skipping them.
Your ftp bounce server sucks, it won't let us feed bogus ports!
```

Frequent users of the FTP bounce scan better get used to that error message. This vulnerability was widespread in 1997 when Nmap was released, but has largely been fixed. Vulnerable servers are still around, so it is worth trying

when all else fails. If bypassing a firewall is your goal, scan the target network for open port 21 (or even for any ftp services if you scan all ports with version detection), then try a bounce scan using each. Nmap will tell you whether the host is vulnerable or not. If you are just trying to cover your tracks, you don't need to (and, in fact, shouldn't) limit yourself to hosts on the target network. Before you go scanning random Internet addresses for vulnerable FTP servers, consider that sysadmins may not appreciate you abusing their servers in this way.

Example 5-22 shows a successful bounce scan against a few interesting ports on Scanme. The verbose option (-v) was given to provide extra detail. The given server type of "JD FTP Server" means that this is an HP JetDirect print server.

### **Example 5-22. Successful FTP bounce scan**

```
krad~> nmap -p 22,25,135 -P0 -v -b XXX.YY.111.2 scanme.nmap.org

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Attempting connection to ftp://anonymous:-wwwuser@XXX.YY.111.2:21
Connected:220 JD FTP Server Ready
Login credentials accepted by ftp server!
Initiating TCP ftp bounce scan against scanme.nmap.org (205.217.153.55)
Adding open port 22/tcp
Adding open port 25/tcp
Scanned 3 ports in 12 seconds via the Bounce scan.
Interesting ports on scanme.nmap.org (205.217.153.55):
PORT      STATE      SERVICE
22/tcp    open       ssh
25/tcp    open       smtp
135/tcp   filtered  msrpc

Nmap run completed -- 1 IP address (1 host up) scanned in 21.790 seconds
```

## **5.13. Scan Code and Algorithms**

In 2004, Nmap's primary port scanning engine was rewritten for greater performance and accuracy. The new engine, known as `ultra_scan` after its function name, handles SYN, Connect, UDP, Null, FIN, Xmas, ACK, Window, Maimon, and IP Protocol scans. That leaves only Idle scan and FTP bounce scan using their own engines.

While the diagrams throughout this chapter show how each scan type works, the Nmap implementation is far more complex since it has to worry about port and host parallelization, latency estimation, packet loss detection, timing profiles, abnormal network conditions, packet filters, response rate limits, and much more.

This section doesn't provide every low-level detail of the `ultra_scan` engine. If you are inquisitive enough to want that, you are better off getting it from the source. You can find `ultra_scan()` and its high-level helper functions defined in `scan_engine.cc` from the Nmap tarball. Here I cover the most important algorithmic features. Understanding these helps in optimizing your scans for better performance, as described in Chapter 6.

### **5.13.1. Network condition monitoring**

Some authors brag that their scanners are faster than Nmap because of stateless operation. They simply blast out a flood packets then listen for responses and hope for the best. While this may have value for quick surveys and other cases where speed is more important than comprehensiveness and accuracy, I don't find it appropriate for security

scanning. A stateless scanner cannot detect dropped packets in order to retransmit and throttle its send rate. If a busy router half way along the network path drops 80% of the scanner's packet flood, the scanner will still consider the run successful and print results that are woefully incomplete. Nmap, on the other hand, saves extensive state in RAM while it runs. There is usually plenty of memory available, even on a PDA. Nmap marks each probe with sequence numbers, source or destination ports, ID fields, or other aspects (depending on probe type) which allow it to recognize responses (and thus drops). It then adjusts its speed appropriately to stay as fast as the network (and given command-line options) allow without crossing the line and suffering inaccuracy or unfairly hogging the shared network. Some administrators who have not installed an IDS might not notice an Nmap SYN scan of their whole network. But you better believe the admin will investigate if you use a brute packet flooding scanner that affects his Quake ping time!

### **5.13.2. Host and port parallelization**

Most of the diagrams in this chapter illustrate using a technique to determine the state of a single port. Sending a probe and receiving the response requires a round trip time (rtt) between the source and target machines. If your rtt is 200ms and you are scanning 65,536 ports on a machine, handling them serially would take at least 3.6 hours. Scan a network of 20,000 machines that way and the wait balloons to more than 8 years. Clearly, this is unacceptable. So Nmap parallelizes its scans, and is capable of scanning hundreds of ports on each of dozens of machines at the same time. This improves speeds by several orders of magnitude. The number of hosts and ports it scans at a time is dependent on arguments described in Chapter 6, such as `--min_hostgroup`, `--min_parallelism`, `-T4`, and `--max_rtt_timeout`, among many others. It also depends on network conditions detected by Nmap.

When scanning multiple machines, Nmap tries to efficiently spread the load between them. If a machine appears overwhelmed (drops packets or its latency increases), Nmap slows down for that host while continuing against others at full speed.

### **5.13.3. Round trip time estimation**

Every time a probe response is received, Nmap calculates the microseconds elapsed since the probe was sent. We'll call this the instanceRTT, and Nmap uses it to keep a running tally of three crucial timing-related values: srtt, rttvar, and timeout. Nmap keeps separate values for each host and also merged values for a whole group of hosts scanned in parallel. They are calculated as follows:

srtt

The smoothed average round trip time. This is what Nmap uses as its most accurate rtt guess. Rather than use a true arithmetic mean, the formula favors more recent results because network conditions change frequently. The formula is:  $\text{newsrtt} = \text{oldsrtt} + (\text{instanceRTT} - \text{oldsrtt}) / 8$

rttvar

This is the observed variance or deviation in the round trip time. The idea is that if rtt values are quite consistent, Nmap can give up shortly after waiting the srtt. If the variance is quite high, Nmap must wait much longer than the srtt before giving up on a probe because relatively slow responses are common. The formula is:  $\text{newrttvar} = \text{AbsoluteValue}(\text{instanceRTT} - \text{oldsrtt}) - \text{oldrttvar}$

timeout

This is the amount of time Nmap is willing to wait before giving up on a probe. It is calculated as: timeout = newsrtt + newrttvar \* 4

When a probe times out, Nmap may retransmit the probe or assign a port state such as `filtered` (depending on scan type). Nmap keeps some state information even after a timeout just in case a late response arrives while the overall scan is still in progress.

\* What does O'Reilly want to do with these formulas? Keep ghetto ASCII or display them nicely? MathML?

These simple time estimation formulas seem to work quite well. I did not make them up, but found them in networking literature. TCP implementations use very similar techniques, as discussed in RFC2988 -- Computing TCP's Retransmission Timer (<http://www.rfc-editor.org/rfc/rfc2988.txt>).

#### 5.13.4. Congestion control

Retransmission timers are far from the only technique Nmap gleaned from TCP. Since Nmap is most commonly used with TCP, it is only fair to follow many of the same rules. Particularly since those rules are the result of substantial research into maximizing throughput without degrading into a tragedy of the commons where everyone selfishly hogs the Network. With its default options, Nmap is reasonably polite. Three reasons are the congestion window, exponential backoff, and slow start algorithms. The congestion window controls how many probes Nmap may have outstanding at once. If the window is full, Nmap won't send any more until a response is received or a probe times out. Exponential backoff means that Nmap slows itself down dramatically when it detects dropped packets. The congestion window is usually reduced to one whenever drops are detected. Slow start is an algorithm for gradually increasing the scan speed to determine the performance limits of the network.

All of these techniques are described in RFC 2581 -- TCP Congestion Control (<http://www.rfc-editor.org/rfc/rfc2581.txt>). That document was written by networking gurus Richard Stevens, Vern Paxson, and Mark Almman. It is only 10 pages long and anyone interested in implementing efficient TCP stacks (or other network protocols, or port scanners) should find it fascinating.

#### 5.13.5. Port scan pings

Every technique discussed in this algorithms section involves (at some level) network monitoring to detect and estimate network packet loss and latency. That really is critical to obtaining fast scan times. Unfortunately, good data is often difficult to come by when scanning heavily firewalled systems. These filters often drop the overwhelming majority of packets without any response. Nmap may have to send 20,000 probes or more to find one responsive port, making it difficult to monitor network conditions.

To combat this problem, Nmap 3.70 introduced the idea of port scan pings. If Nmap has found at least one port responsive on a heavily filtered host, it will send a probe to that port every five seconds that it goes without receiving responses from any other ports. This allows Nmap to conduct a sufficient level of monitoring to speed up or slow down its scans as network conditions allow.

### **5.13.6. Inferred neighbor times**

Sometimes even port scan pings won't help because no responsive ports at all have been found. The machine could be down (and scanned with `-P0`), or every single port could be filtered. Or perhaps the target does have a couple responsive ports, but Nmap has not been lucky enough to find them yet. In these cases, Nmap uses timing values that it maintains for the whole group of machines it is scanning at the same time. As long as at least one response has been received from any machine in the group, Nmap has something to work with. Of course Nmap cannot assume that hosts in a group always share similar timing characteristics. So Nmap tracks the timing variances between responsive hosts in a group. If they differ wildly, Nmap infers long timeouts for neighboring hosts to be on the safe side.

### **5.13.7. Adaptive retransmission**

The simplest of scanners (and the stateless ones) generally don't retransmit probes at all. They simply send a probe to each port and report based on the response or lack thereof. Slightly more complex scanners will retransmit a set number of times. Nmap tries to be smarter by keeping careful packet loss statistics for each scan against a target. If no packet loss is detect, Nmap may retransmit only once when it fails to receive a probe response. When massive packet loss is evident, Nmap may retransmit ten or more times. This allows Nmap to scan hosts on fast, reliable networks quickly, while preserving accuracy (at the expense of some speed) when scanning problematic networks or machines. Even Nmap's patience isn't unlimited though. At a certain point (twelve retransmissions with Nmap 3.75), Nmap will print a warning and give up on further retransmissions. This prevents malicious hosts from slowing Nmap down too much with intentional packet drops, slow responses, and similar responses. Such an attack is known as tarpitting and is commonly used against spammers.

### **5.13.8. Scan delay**

Packet response rate limiting is perhaps the most pernicious problem faced by port scanners such as Nmap. For example, Linux 2.4 kernels limit ICMP error messages returned during a UDP (`-sU`) or IP protocol (`-sO`) scan to one per second. If Nmap counted these as normal drops, it would be continually slowing down (remember exponential backoff) but still end up having the vast majority of its probes dropped. Instead, Nmap tries to detect this situation. When a large proportion of packets are being dropped, it implements a short delay (as little as 5 milliseconds) between each probe sent to a single target. If drops continue to be a major problem, Nmap will keep doubling the delay until the drops cease or Nmap hits the maximum allowed scan delay. The maximum scan delay defaults to one second between probes. The scan delay is sometimes enabled when a slow host can't keep up, even when that host has no explicit rate limiting rules. This can reduce total network traffic substantially by reducing wasted (dropped) probe packets. Unfortunately even small scan delay values can make a scan takes several times as long. Nmap is conservative by default, allowing second-long scan delays for TCP and UDP probes. If your priorities differ, you can configure maximum scan delays as discussed in Chapter 5.

## **Chapter 6. Optimizing Nmap Performance**

# Chapter 7. Service and Application Version Detection

## 7.1. Introduction

Previous chapters discussed many techniques for port scanning -- determining the TCP or UDP port numbers that are listening for connections on a system. Point Nmap at a remote machine, and it might tell you that ports 25/tcp, 80/tcp, and 53/udp are open. Using its nmap-services database of more than 2,200 well-known services, Nmap would report that those ports probably correspond to a mail server (SMTP), web server (HTTP), and name server (DNS) respectively. This lookup is usually accurate -- the vast majority of daemons listening on TCP port 25 are, in fact, mail servers. However, you should not bet your security on this! People can and do run services on strange ports. Perhaps their main web server was already on port 80, so they picked a different port for a staging or test server. Maybe they think hiding a vulnerable service on some obscure port prevents "evil hackers" from finding it. Even more common lately is that people choose ports based not on the service they want to run, but on what gets through the firewall. When ISPs blocked port 80 after major Microsoft IIS worms CodeRed and Nimda, hordes of users responded by moving their personal web servers to another port. When companies block telnet access due to its horrific security risks, I have seen users simply run telnetd on the Secure Shell (SSH) port instead.

Even if Nmap is right, and the hypothetical server above is running SMTP, HTTP, and DNS servers, that is not a lot of information. When doing vulnerability assessments (or even simple network inventories) of your companies or clients, you really want to know which mail and DNS servers and versions are running. Having an accurate version number helps dramatically in determining which exploits a server is vulnerable to. Do keep in mind that security fixes are often backported to earlier versions of software, so you cannot rely solely on the version number to prove a service is vulnerable.

Another good reason for determining the service types and version numbers is that many services share the same port number. For example, port 258/tcp is used by both the Checkpoint Firewall-1 GUI management interface and the yak Windows chat client. This makes a guess based on the nmap-services table even less accurate. Anyone who has done much scanning knows that you also often find services listening on unregistered ports - these are a complete mystery without version detection. A final problem is that filtered UDP ports often look the same to a simple port scanner as open ports (see Chapter 3 - Mainstream Port Scanning Techniques). But if they respond to the service-specific probes sent by Nmap version detection, you know for sure that they are open (and often exactly what is running).

The Nmap version scanning subsystem (introduced in version 3.45) tries to answer all these questions by connecting to open ports and interrogating them for further information using probes that the specific services understand. This allows Nmap to give a detailed assessment of what is really running, rather than just what port numbers are open. Example 7-1 shows the actual output.

### Example 7-1. Simple usage of version detection

```
# nmap -A -T4 -F www.insecure.org

Starting nmap 3.40PVT16 ( http://www.insecure.org/nmap/ )
Interesting ports on www.insecure.org (205.217.153.53):
(The 1206 ports scanned but not shown below are in state: filtered)
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh      OpenSSH 3.1pl1 (protocol 1.99)
```

```

25/tcp  open  smtp    Qmail smptd
53/tcp  open  domain  ISC Bind 9.2.1
80/tcp  open  http    Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)
113/tcp closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 108.307 days (since Wed May 21 12:27:44 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 34.962 seconds

```

Nmap version detection offers the following advanced features (fully described later):

- High speed, parallel operation via non-blocking sockets and a probe/match definition grammar designed for efficient yet powerful implementation.
- Determines the application name and version number where available -- not just the service protocol.
- Supports both the TCP and UDP protocols, as well as both textual ASCII and packed binary services.
- Multi-platform support, including Linux, Windows, Mac OS X, FreeBSD/NetBSD/OpenBSD, Solaris, and all the other platforms on which Nmap is known to work.
- If SSL is detected, Nmap connects using OpenSSL (if available) and tries to determine what service is listening behind the encryption. This allows it to discover services like https, pop3s, imaps, etc. as well as providing version details.
- If a SunRPC service is discovered, Nmap launches its brute-force RPC grinder to find the program number, name, and version number.
- IPv6 is supported, including TCP, UDP, and SSL over TCP.
- Community contributions - If Nmap gets data back from a service that it does not recognize, a "service fingerprint" is printed along with a submission URL. This system is patterned after the extremely successful Nmap OS Detection (Chapter 7) fingerprint submission process. New probes and corrections can also be submitted.
- Comprehensive database - Nmap recognizes more than one thousand service signatures, covering more than 180 unique service protocols from acap, afp, and aim to xml-rpc, zebadee, and zebra.

## 7.2. Usage/Examples

Before delving into the technical details of how version detection is implemented, here are some examples demonstrating its usage and capabilities. To enable version detection, just add `-sv` to whatever Nmap flags you normally use. Or use the `-A` option, which also turns on OS detection (`-O`, Chapter 7) and may enable other advanced and aggressive features later. It is really that simple, as shown in Example 7-2.

### Example 7-2. Version detection against WWW.Microsoft.Com

```

# nmap -A -T4 -F www.microsoft.com

Starting nmap 3.40PVT16 ( http://www.insecure.org/nmap/ )
Interesting ports on 80.67.68.30:
(The 1208 ports scanned but not shown below are in state: closed)

```

```

PORT      STATE     SERVICE      VERSION
22/tcp    open      ssh          Akamai-I SSH (protocol 1.5)
80/tcp    open      http         AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
443/tcp   open      ssl/http    AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
Device type: general purpose
Running: Linux 2.1.X|2.2.X
OS details: Linux 2.1.19 - 2.2.25
Uptime 22.924 days (since Fri Aug 15 03:34:27 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 19.223 seconds

```

This preceding scan demonstrates a couple things. First of all, it is gratifying to see WWW.Microsoft.Com served off one of Akamai's Linux boxes. More relevant to this chapter is that the "service" for port 443 is "ssl/http". That means that service detection first discovered that the port was SSL, then it loaded up OpenSSL and performed service detection again through SSL connections to discover a web server running AkamiGHost behind the encryption. Recall that -T4 causes Nmap to go faster (more aggressive timing) and -F tells Nmap to scan only ports registered in nmap-services.

Example 7-3 is a longer and more diverse example.

### Example 7-3. Complex version detection

```

./nmap -A -T4 localhost

Starting nmap 3.40PVT16 ( http://www.insecure.org/nmap/ )
Interesting ports on felix (127.0.0.1):
(The 1640 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          WU-FTPD wu-2.6.1-20
22/tcp    open  ssh          OpenSSH 3.1pl1 (protocol 1.99)
53/tcp    open  domain       ISC Bind 9.2.1
79/tcp    open  finger       Linux fingerd
111/tcp   open  rpcbind     2 (rpc #100000)
443/tcp   open  ssl/http    Apache httpd 2.0.39 ((Unix) mod_perl/1.99_04-dev [cut])
515/tcp   open  printer      CUPS 1.1
631/tcp   open  ipp          CUPS 1.1
953/tcp   open  rndc?       -
5000/tcp   open  ssl/ftp     WU-FTPD wu-2.6.1-20
5001/tcp   open  ssl/ssh     OpenSSH 3.1pl1 (protocol 1.99)
5002/tcp   open  ssl/domain ISC Bind 9.2.1
5003/tcp   open  ssl/finger  Linux fingerd
6000/tcp   open  X11         (access denied)
8000/tcp   open  http-proxy  Junkbuster webproxy
8080/tcp   open  http        Apache httpd 2.0.39 ((Unix) mod_perl/1.99_04-dev [cut])
8081/tcp   open  http        Apache httpd 2.0.39 ((Unix) mod_perl/1.99_04-dev [cut])
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 8.653 days (since Fri Aug 29 11:16:40 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 42.494 seconds

```

You can see here the way RPC services are treated, with the brute force RPC scanner being used to determine that port 111 is rpcbind version 2. You may also notice that port 515 gives the service as "printer", but that version column is empty. This means that Nmap did determine the service name via its probing, but was not able to determine anything else. On the other hand, port 953 gives the service as "rndc?". The question mark tells us that Nmap was not even able to determine the service name through probing. As a fallback, rndc is mentioned because that has port 953 registered in `nmap-services`. Unfortunately, none of Nmap's probes elicited any sort of response from rndc. If they had, Nmap would have printed a service fingerprint and a submission URL so that it could be recognized in the next version. As it is, Nmap requires a special probe. One might even be available by the time you read this. The upcoming "community contributions" section provides details on writing your own probes.

It is also worth noting that some services provide much more information than just the version number. Examples above include whether X11 permits connections, the SSH protocol number, and the Apache module versions list. Some of the Apache modules even had to be cut from the output to fit on this page.

A few early reviewers questioned the sanity of running services such as SSH and finger over SSL. This was actually just fun with stunnel (<http://www.stunnel.org/>), in part to ensure that parallel SSL scans actually work.

### 7.3. Technique Described

Nmap version scanning is actually rather straightforward. It was designed to be as simple as possible while still being scalable, fast, and accurate. The truly nitty-gritty details are best discovered by downloading and reviewing the source code, but a synopsis of the techniques used follows.

Nmap first does a port scan as per your instructions, and then passes all the open TCP and/or UDP ports to the service scanning module. Those ports are then interrogated in parallel, although a single port is described here for simplicity.

1. If the port is TCP, Nmap starts by connecting to it.
2. Once the TCP connection is made, Nmap listens for roughly 5 seconds. Many common services, including most ftp, ssh, smtp, telnet, pop3, and imap servers, identify themselves in an initial welcome banner. Nmap refers to this as the "NULL probe", because Nmap just listens for responses without sending any probe data. If any data is received, Nmap compares it to hundreds of signature regular expressions in its `nmap-service-probes` file (described in Section 7.6). If the service is fully identified, we are done with that port! The regular expression includes substrings that can be used to pick version numbers out of the response. In some cases, Nmap gets a "soft match" on the service type, but no version info. In that case, Nmap continues but only send probes that are known to recognize the soft-matched service type.
3. At this point, Nmap UDP probes start, and TCP connections end up here if the NULL probe above fails or soft-matches. Since the reality is that most ports are used by the service they are registered to in `nmap-services`, every probe has a list of port numbers that are considered "good bets". For example, the probe called GetRequest that recognizes web servers (among other services) lists 80-85, 8000-8010, and 8080-8085 as probable ports. Nmap sequentially executes the probe(s) that match the port number being scanned. Each probe includes a probe string (which can be arbitrary ASCII text or \xHH escaped binary), which is sent to the port. Responses that come back are compared to a list of regular expressions of the same type as discussed in the NULL probe description above. As with the NULL probe, these tests can either result in a full match (ends processing for the remote service), a soft match (limits future probes to those which match a certain service), or no match at all.
4. In most cases, the "NULL probe" or the probable port probe(s) (there is usually only one) described above matches the service. Since the NULL "probe" shares its connection with the probable port probe, this allows

service detection to be done with only one brief connection in most cases. With UDP only one packet is usually required. But should the NULL probe and probable port probe(s) fail, Nmap goes through all of the existing probes sequentially. In the case of TCP, Nmap must make a new connection for each probe to avoid having previous probes corrupt the results. This worst-case scenario can take a bit of time, although the pain is limited by making most probes generic enough to match many services. For example, the GenericLines probe sends two blank lines ("r\nr\n") to the service. This matches daemons of 13 service types (so far), including ftp, ident, pop3, uucp, postgres, and whois. The GetRequest probe matches even more service types. Other examples include "help\r\n" and generic RPC and MS SMB probes. In addition, any softmatch reduces the number of tried probes dramatically.

5. One of the probes tests whether the target port is running SSL. If so (and if OpenSSL is available), Nmap connects back via SSL and restart the service scan to determine what is listening behind the encryption. A special directive allows different probable ports for normal and SSL tunneled connections. For example, Nmap should start against port 443 (https) with an SSL probe. But after SSL is detected and enabled, Nmap should try the GetRequest probe against port 443 because that port usually has a web server listening behind SSL encryption.
6. Another generic probe identifies RPC-based services. When these are found, the Nmap RPC Grinder (discussed later) is initiated to brute force the RPC program number/name and supported version numbers. Similarly, an SMB postprocessor for fingerprinting Windows services may be added eventually.
7. If at least one of the probes elicits some sort of response, yet Nmap is unable to recognize the service, the response content is printed to the user in the form of a "fingerprint" that can be submitted at a provided URL for the next version of Nmap.

## 7.4. Technique Demonstrated

If the English description above is not clear enough, you can see for yourself how it works by adding the `--version_trace` (and usually `-d` (debugging)) options to your Nmap command line. This shows all the connection and data read/write activity of the service scan. Example 7-4 is a real annotated example (output slightly modified for readability).

### Example 7-4. Detailed trace of version detection

```
# nmap -sSV -T4 -F -d --version_trace www.insecure.org

Starting nmap 3.48 ( http://www.insecure.org/nmap/ )
Host www.insecure.org (205.217.153.53) appears to be up ... good.
Initiating SYN Stealth Scan against www.insecure.org (205.217.153.53) at 19:53
Initiating service scan against 4 services on 1 host at 19:53
```

*The SYN scan has found 4 open ports - now we are beginning a service scan against each of them in parallel. We start with a TCP connection for the NULL probe:*

```
Starting probes against new service: 205.217.153.53:22 (tcp)
NSOCK (2.0750s) TCP connection requested to 205.217.153.53:22 (IOD #1) EID 8
Starting probes against new service: 205.217.153.53:25 (tcp)
NSOCK (2.0770s) TCP connection requested to 205.217.153.53:25 (IOD #2) EID 16
Starting probes against new service: 205.217.153.53:53 (tcp)
NSOCK (2.0830s) TCP connection requested to 205.217.153.53:53 (IOD #3) EID 24
```

```

Starting probes against new service: 205.217.153.53:80 (tcp)
NSOCK (2.0860s) TCP connection requested to 205.217.153.53:80 (IOD #4) EID 32
NSOCK (2.0870s) Callback: CONNECT SUCCESS for EID 32 [205.217.153.53:80]
NSOCK (2.0870s) Read request from IOD #4 [205.217.153.53:80] (timeout: 5000ms) EID 42
NSOCK (2.0870s) Callback: CONNECT SUCCESS for EID 24 [205.217.153.53:53]
NSOCK (2.0870s) Read request from IOD #3 [205.217.153.53:53] (timeout: 5000ms) EID 50
NSOCK (2.0870s) Callback: CONNECT SUCCESS for EID 16 [205.217.153.53:25]
NSOCK (2.0870s) Read request from IOD #2 [205.217.153.53:25] (timeout: 5000ms) EID 58
NSOCK (2.0870s) Callback: CONNECT SUCCESS for EID 8 [205.217.153.53:22]
NSOCK (2.0870s) Read request from IOD #1 [205.217.153.53:22] (timeout: 5000ms) EID 66

```

*At this point, "Null probe" connections have successfully been made to all four services. It starts at 2 seconds because that is how long the ping and SYN scans took.*

```

NSOCK (2.0880s) Callback: READ SUCCESS for EID 66 [205.217.153.53:22] (23 bytes): SSH-1.99-OpenSSH_3
Service scan match: www.insecure.org (205.217.153.53):22 is ssh. Version: |OpenSSH|3.1p1|protocol 1

```

*SSH was nice enough to fully identify itself immediately upon connection as OpenSSH 3.1p1. One down, three to go.*

```

NSOCK (2.0880s) Callback: READ SUCCESS for EID 58 [205.217.153.53:25] (27 bytes): 220 core.lnxnet.ne
Service scan soft match: www.insecure.org (205.217.153.53):25 is smtp

```

*The mail server on port 25 also gave us a useful banner. We do not know what type of mail server it is, but starting with "220 " and including the word "ESMTP" tells us it is a mail (SMTP) server. So Nmap softmatches smtp, meaning that only probes able to match SMTP servers are tried from now on. Note that non-printable characters are represented by dots -- so the ".." after ESMTP is really the "\r\n" line termination sequence.*

```

NSOCK (2.0880s) Read request from IOD #2 [205.217.153.53:25] (timeout: 4996ms) EID 74
NSOCK (7.0880s) Callback: READ TIMEOUT for EID 74 [205.217.153.53:25]
NSOCK (7.0880s) Write request for 6 bytes to IOD #2 EID 83 [205.217.153.53:25]: HELP..
NSOCK (7.0880s) Read request from IOD #2 [205.217.153.53:25] (timeout: 5000ms) EID 90

```

*Nmap listens a little longer on the SMTP connection, just in case the server has more to say. The read request times out after 5 seconds. Nmap then finds the next probe which is registered to port 25 and has smtp signatures. That probe simply consists of "HELP\r\n", which Nmap writes into the connection.*

```

NSOCK (7.0880s) Callback: READ TIMEOUT for EID 50 [205.217.153.53:53]
NSOCK (7.0880s) Write request for 32 bytes to IOD #3 EID 99 [205.217.153.53:53]: ....vers
NSOCK (7.0880s) Read request from IOD #3 [205.217.153.53:53] (timeout: 5000ms) EID 106

```

*The DNS server on port 53 does not return anything at all. The first probe registered to port 53 in nmap-service-probes is DNSVersionBindReq, which queries a DNS server for its version number. This is sent onto the wire.*

```

NSOCK (7.0880s) Callback: READ TIMEOUT for EID 42 [205.217.153.53:80]

```

NSOCK (7.0880s) Write request for 18 bytes to IOD #4 EID 115 [205.217.153.53:80]: GET / HTTP/1.0....  
NSOCK (7.0880s) Read request from IOD #4 [205.217.153.53:80] (timeout: 5000ms) EID 122

The port 80 NULL Probe also failed to return any data. An HTTP GET request is sent, since that probe is registered to port 80.

NSOCK (7.0920s) Callback: READ SUCCESS for EID 122 [205.217.153.53:80] [EOF](15858 bytes)  
Service scan match: www.insecure.org (205.217.153.53):80 is http. Version: |Apache httpd|2.0.39|(Un

*Apache returned a huge (15KB) response, so it is not printed. That response provided detailed configuration information, which Nmap picks out of the response. There are no other probes registered for port 80. So if this had failed, Nmap would have tried the first TCP probe in nmap-service-probes. That probe simply sends blank lines ("r\nr\n"). A new connection would have been made in case the GET probe confused the service.*

NSOCK (7.0920s) Callback: READ SUCCESS for EID 106 [205.217.153.53:53] (50 bytes): .0.....ve  
Service scan match: www.insecure.org (205.217.153.53):53 is domain. Version: |ISC Bind|9.2.1||

*Port 53 responded to our DNS version request. Most of the response (as with the probe) is binary, but you can clearly see the version 9.2.1 there. If this probe had failed, the next probe registered to port 53 is a DNS server status request (14 bytes: "\0\x0C\0\0\x10\0\0\0\0\0\0\0\0\0"). Having this backup probe helps because many more servers respond to a status request than a version number request.*

NSOCK (7.0920s) Callback: READ SUCCESS for EID 90 [205.217.153.53:25] (55 bytes): 214 qmail home pag Service scan match: www.insecure.org (205.217.153.53):25 is smtp. Version: |qmail smtpd|||

Port 25 gives a very helpful response to the "Help" probe. Other SMTP servers such as Postfix, Courier, and Exim can often be identified by this probe as well. If the response did not match, Nmap would have given up on this service because it had already softmatched smtp and there are no more smtp probes in nmap-service-probes.

The service scan took 5 seconds to scan 4 services on 1 host.

*This service scan run went pretty well. No service required more than one connection. It took five seconds because Qmail and Apache hit the 5-second NULL probe timeout before Nmap sent the first real probes. Here is the reward for these efforts:*

```
Interesting ports on www.insecure.org (205.217.153.53):
(The 1212 ports scanned but not shown below are in state: closed)

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.1p1 (protocol 1.99)
25/tcp    open  smtp    qmail smtpd
53/tcp    open  domain  ISC Bind 9.2.1
80/tcp    open  http    Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)
```

Nmap run completed -- 1 IP address (1 host up) scanned in 7.104 seconds

## 7.5. Post-processors

Nmap is usually finished working on a port once it has deduced the service and version information as demonstrated above. However, there are certain services for which Nmap performs additional work. These post-processors are presently available for RPC and SSL services, and Windows SMB interrogation is under consideration.

### 7.5.1. RPC Grinding

SunRPC (Sun Remote Procedure Call) is a common UNIX protocol used to implement many services including NFS. Nmap ships with an `nmap-rpc` database of almost 600 RPC programs. Many RPC services use high-numbered ports and/or the UDP transport protocol, making them available through many poorly configured firewalls. RPC programs (and the infrastructure libraries themselves) also have a long history of serious remotely exploitable security holes. So network admins and security auditors often wish to learn more about any RPC programs on their networks.

If the portmapper (`rpcbind`) service (UDP or TCP port 111) is available, RPC services can be enumerated with the UNIX `rpcinfo` command. Example 7-5 demonstrates this against a default Solaris 9 server.

#### Example 7-5. Enumerating RPC services with `rpcinfo`

```
> rpcinfo -p ultra
   program vers proto   port
    100000    4   tcp    111  rpcbind
    100000    4   udp    111  rpcbind
    100232   10   udp   32777  sadmind
    100083    1   tcp   32775  ttdbserverd
    100221    1   tcp   32777  kcms_server
    100068    5   udp   32778  cmsd
    100229    1   tcp   32779  metad
    100230    1   tcp   32781  metamhd
    100242    1   tcp   32783  rpc.metamedd
    100001    4   udp   32780  rstatd
    100002    3   udp   32782  rusersd
    100002    3   tcp   32785  rusersd
    100008    1   udp   32784  walld
    100012    1   udp   32786  sprayd
    100011    1   udp   32788  rquotad
    100024    1   udp   32790  status
    100024    1   tcp   32787  status
    100133    1   udp   32790  nsm_addrand
    100133    1   tcp   32787  nsm_addrand
[ Dozens of lines cut for brevity ]
```

This example shows that hosts frequently offer many RPC services, which increases the probability that one is exploitable. You should also notice that most of the services are on strange high-numbered ports (which may change for any number of reasons) and split between UDP and TCP transport protocols.

Because the RPC information is so sensitive, many administrators try to obscure this information by blocking the portmapper port (111). Unfortunately, this does not close the hole. Nmap can determine all of the same info by directly communicating with open RPC ports through a 3-step process

1. The TCP and/or UDP port scan finds all of the open ports

2. Version detection determines which of the open ports use the SunRPC protocol
3. The RPC brute force engine determines the program identity of each rpc port by trying a "NULL command" against each of the 600 programs numbers in `nmap-rpc`. Most of the time Nmap guesses wrong and receives an error message stating that the requested program number is not listening on the port. Nmap continues trying each number in its list until success is returned for one of them. Nmap gives up in the unlikely event that it exhausts all of its known program numbers or if the port sends malformed responses that suggest it is not really RPC.

\* Should I provide a diagram showing an actual RPC probe packet and the responses to expect?

The RPC program identification probes are done in parallel, and retransmissions are handled for UDP ports. This feature is automatically activated whenever version detection finds any RPC ports. Or it can be performed without version detection by specifying the `-sR` option. Example 7-6 demonstrates direct RPC scanning done as part of version detection.

#### **Example 7-6. Nmap direct RPC scan**

```
# nmap -F -A -sSU ultra

Starting nmap 3.48 ( http://www.insecure.org/nmap/ )
Interesting ports on ultra.yuma.net (192.168.0.50):
* I should change the domain name of my internal home network to
one I actually own, such as Nmap.Org

(The 2171 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE          VERSION
[A whole bunch of ports cut for brevity]
32776/tcp open  kcms_server      1 (rpc #100221)
32776/udp open  sadmind         10 (rpc #100232)
32777/tcp open  kcms_server      1 (rpc #100221)
32777/udp open  sadmind         10 (rpc #100232)
32778/tcp open  metad           1 (rpc #100229)
32778/udp open  cmsd            2-5 (rpc #100068)
32779/tcp open  metad           1 (rpc #100229)
32779/udp open  rstatd          2-4 (rpc #100001)
32780/tcp open  metamhd         1 (rpc #100230)
32780/udp open  rstatd          2-4 (rpc #100001)
32786/tcp open  status           1 (rpc #100024)
32786/udp open  sprayd          1 (rpc #100012)
32787/tcp open  status           1 (rpc #100024)
32787/udp open  rquotad         1 (rpc #100011)
Device type: general purpose
Running: Sun Solaris 9
OS details: Sun Solaris 9
Uptime 0.120 days (since Sun Nov 16 21:38:16 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 252.701 seconds
```

### 7.5.2. SSL Post-processor notes

As discussed in the technique section, Nmap has the ability to detect the SSL encryption protocol and then launch an encrypted session through which it executes normal version detection. As with the RPC grinder discussed previously, the SSL postprocessor is automatically executed whenever an appropriate (SSL) port is detected. This is demonstrated by Example 7-7.

#### **Example 7-7. Version scanning through SSL**

```
nmap -P0 -sSV -T4 -F www.amazon.com

Starting nmap 3.48 ( http://www.insecure.org/nmap/ )
Interesting ports on 207-171-184-16.amazon.com (207.171.184.16):
(The 1214 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache Stronghold httpd 2.4.2 (based on Apache 1.3.6)
443/tcp   open  ssl/http  Apache Stronghold httpd 2.4.2 (based on Apache 1.3.6)

Nmap run completed -- 1 IP address (1 host up) scanned in 35.038 seconds
```

Note that the version information is the same for each of the two open ports, but the service is `http` on port 80 and `ssl/http` on port 443. The common case of `https` on port 443 is not hardcoded - Nmap should be able to detect SSL on any port and determine the underlying protocol for any service that Nmap can detect in cleartext. If Nmap had not detected the server listening behind SSL, the service listed would be "ssl/unknown". If Nmap had not been built with SSL support, the service listed would have simply been "ssl". The "version" column would be blank in both of these cases.

The SSL support for Nmap depends on the free OpenSSL library (<http://www.openssl.org>) and has not been tested on Windows. Nor is it included in the Linux RPM binaries, to avoid breaking systems which lack these libraries. The Nmap source code distribution attempts to detect OpenSSL on a system and link to it when available. See chapter one for details on customizing the build process to include or exclude OpenSSL.

## 7.6. nmap-service-probes File Format

As with remote OS detection (-O), Nmap uses a flat file to store the version detection probes and match strings. While the version of `nmap-services` distributed with Nmap is sufficient for most users, understanding the file format allows advanced Nmap hackers to add their own services to the detection engine. Like many UNIX files, `nmap-service-probes` is line-oriented. Lines starting with a hash (#) are treated as comments and ignored by the parser. Blank lines are ignored as well. Other lines must contain one of the directives described below. Some readers prefer to peek at the examples in Section 7.6.6 before tackling the following dissection.

### 7.6.1. The `probe` directive

Syntax: Probe <protocol><probename><probesendstring>

Examples:

```
Probe TCP NULL q||
```

The probe directive tells Nmap what string to send to recognize various services. All of the directives discussed later operate on the most recent Probe statement. The arguments are as follows:

#### protocol

This must be either TCP or UDP. Nmap only uses probes that match the protocol of the service it is trying to scan.

#### probename

This is a plain English name for the probe. It is used in service fingerprints to describe which probes elicited responses.

#### probestring

Tells Nmap what to send. It must start with a q, then a delimiter character which begins and ends the string. Between the delimiter characters is the string that is actually sent. It is formatted similarly to a C or Perl string in that it allows the following standard escape characters: \\ \0, \a, \b, \f, \n, \r, \t, \v, \xHH. One Probe line in nmap-service-probes has an empty probestring, as shown in the third example above. This is the TCP NULL probe which just listens for the initial banners that many services send.

## 7.6.2. The match directive

Syntax: match <service> <pattern> [versioninfo]

Examples:

```
match ftp m/^220.*Welcome to PureFTPD (\d\S+)/ v/PureFTPD/$1//  
match ssh m/^SSH-(.\d+)-OpenSSH_(\S+)/ v/OpenSSH/$2/protocol $1/  
match mysql m/^.\0\0\0\n(4.[-\w]+)\0...0/s v/MySQL/$1//  
match ssc-agent m|^0\x1e0\x060\t0\$| v/Novell Netware ssc-agent///  
match chargen m@ABCDEFGHIJKLMNPQRSTUVWXYZ|  
match netbios-ssn m+^\0\0\0.\xffSMB\0.*([^\0]|([\^\w]\0))(([-\w]\0){2,50})+ v/Samba smbd/3.X/workgro
```

The match directive tells Nmap how to recognize services based on responses to the string sent by the previous Probe directive. A single Probe line may be followed by dozens or hundreds of match statements. If the given pattern matches, an optional version specifier builds the application name, version number, and additional info for Nmap to report. The arguments to this directive follow:

#### service

This is simply the service name that the pattern matches. Examples would be ssh, smtp, http, or snmp.

#### pattern

This pattern is used to determine whether the response received matches the service given in the previous parameter. The format is like Perl, with the syntax being "m/[regex]/[opts]". The "m" tells Nmap that a match string is beginning. The forward slash (/) is a delimiter, which can be substituted by almost any printable character as long as the second slash is also replaced to match. The regex is a Perl-style regular expression (<http://www.perldoc.com/perl5.8.0/pod/perlre.html>). This is made possible by the excellent Perl Compatible Regular Expressions (PCRE) library (<http://www.pcre.org>). The only options currently supported are 'i', which makes a match case-insensitive and 's' which includes newlines in the '.' specifier. As you might expect, these

two options have the same semantics as in Perl. Subexpressions to be captured (such as version numbers) are surrounded by parenthesis as shown in most of the examples above.

#### versioninfo

This field is of the form v/vendorproductname/version/info/ where the slash can be replaced by any delimiter character. Any of the 3 fields can be empty, and the whole argument can be omitted if no further information on the service is available. The vendorproductname includes the vendor and often service name when relevant and is of the form "Sun Solaris rexecd", "ISC Bind named", or "Apache httpd". The version string is the version "number" (may include non-numeric characters, and even multiple words), while "info" is miscellaneous further information that was immediately available and might be useful (like whether an X server is open, or the protocol number of ssh servers). Any of the version fields can include numbered strings such as \$1 or \$2, which are replaced (in a Perl-like fashion) with the corresponding parenthesized substring in the *pattern*. In rare cases, a helper function can be applied to the replacement text before insertion. The \$P(3) expression in the example netbios-ssn match string above is one such example. The P() function includes only printable characters from the captured string. For netbios-ssn, a string such as "W\00\0R\0K\0G\0R\0O\0U\0P\0" is decoded to simply "WORKGROUP".

### 7.6.3. The softmatch directive

Syntax: softmatch <service> <pattern>

Examples:

```
softmatch ftp m|^220 [-.\w ]+ftp.*\r\n$/i
softmatch smtp m|^220 [-.\w ]+SMTP.*\r\n|
softmatch pop3 m|^+OK [-[\[]\(\)! ,/+:<>@\.\w ]+\r\n$|
```

The softmatch directive is similar in format to the match directive discussed above. The main difference is that scanning continues after a softmatch, but it is limited to probes that are known to match the given service. This allows for a normal ("hard") match to be found later, which may provide useful version information. See Section 7.3 for more details on how this works. Arguments are not defined here because they are the same as for 'match' above, except that there is never a *versioninfo* argument. Also as with match, many softmatch statements can exist within a single Probe

### 7.6.4. The ports and sslports directives

Syntax: ports <portlist>

Examples:

```
ports 21,43,110,113,199,505,540,1248,5432,30444
ports 111,4045,32750-32810,38978
```

This line tells Nmap what ports the services identified by this Probe are commonly found on. It should only be used once within each Probe section. The syntax is a slightly simplified version of that taken by the Nmap -p option. See the examples above. More details on how this works are in Section 7.3

Syntax: sslports <portlist>

Example:

```
sslports 443
```

This is the same as 'ports' directive described above, except that these ports are often used to wrap a service in SSL. For example, the HTTP probe declares 'sslports 443' and SMTP-detecting probes have an 'sslports 465' line because those are the standard ports for https and smtps respectively. The *portlist* format is the same as with ports. This optional directive cannot appear more than once per Probe.

### 7.6.5. The `totalwaitms` directive

Syntax: `totalwaitms <milliseconds>`

Example:

```
totalwaitms 5000
```

This rarely necessary directive specifies the amount of time Nmap should wait before giving up on the most recently defined Probe against a particular service. The Nmap default is usually fine.

### 7.6.6. Putting it all together

Here are some examples from `nmap-service-probes` which put this all together (to save space many lines have been skipped). After reading this far into the section, the following should be understood.

```
# This is the NULL probe that just compares any banners given to us
#####
#NEXT PROBE#####
Probe TCP NULL q||

# Wait for at least 5 seconds for data. Otherwise an Nmap default is used.
totalwaitms 5000
# Windows 2003
match ftp m/^220[ -]Microsoft FTP Service\r\n/ v/Microsoft ftpd///
match ftp m/^220 ProFTPD (\d\S+) Server/ v/ProFTPD/$1///
softmatch ftp m/^220 [-.\w ]+ftp.*\r\n$/i
match ident m|^flock()\ on closed filehandle .*midentd| v/midentd//broken/
match imap m|^* OK Welcome to Binc IMAP v(\d[-.\w+])| v/Binc IMAPd/$1///
softmatch imap m|^* OK [-.\w ]+imap[-.\w ]+\r\n$/i
match lucent-fwadm m|^0001;2$| v/Lucent Secure Management Server///
match meetingmaker m/^xc1,$/ v/Meeting Maker calendaring///
# lopster 1.2.0.1 on Linux 1.1
match napster m|^1$| v/Lopster Napster P2P client///

Probe UDP Help q|help\r\n\r\n|
ports 7,13,37
match chargen m|@ABCDEFGHIJKLMNOPQRSTUVWXYZ|
match echo m|^help\r\n\r\n$|
# Will last until 0xC5FFFF, in April 2005 - need to shift in advance.
match time m|^[\xc0-\xc5]...$|
```

## 7.7. Community Contributions

No matter how technically advanced a service detection framework is, it would be nearly useless without a comprehensive database of services against which to match. This is where the open source nature of Nmap really shines. The Insecure.Org lab is pretty substantial by geek standards, but it can never hope to run more than a tiny percentage of machine types and services that are out there. Fortunately experience with OS detection fingerprints has shown that Nmap users together run all of the common stuff, plus a staggering array of bizarre equipment as well. The Nmap OS Fingerprint Database contains more than a thousand entries, including all sorts of switches, WAPs, VoIP phones, game consoles, UNIX boxes, Windows hosts, printers, routers, PDAs, firewalls, etc. Version detection also supports user submissions, and Nmap users have contributed thousands of services. There are three primary ways that the Nmap community helps to make this an exceptional database:

- Submit service fingerprints* -- If a service responds to one or more of Nmap's probes and yet Nmap is unable to identify that service, Nmap prints a "service fingerprint" like this one:

```
SF-Port21-TCP:V=3.40PVT16%D=9/6%Time=3F5A961C%r(NULL,3F,"220\x20stage\x20F
SF:TP\x20server\x20\Version\x202\.1WU\(1\)\+SCO-2\.6\.1\+-sec\)\x20ready\
SF:.\r\n")%r(GenericLines,81,"220\x20stage\x20FTP\x20server\x20\Version\x
SF:202\.1WU\(1\)\+SCO-2\.6\.1\+-sec\)\x20ready\.\r\n500\x20":\x20command\
SF:x20not\x20understood\.\r\n500\x20":\x20command\x20not\x20understood\.\
SF:r\n");
```

If you receive such a fingerprint, and are sure you know what daemon version is running on the target host, please submit the fingerprint at the URL Nmap gives you. The whole submission process is anonymous (unless you choose to provide identifying info) and should not take more than a couple minutes. If you are feeling particularly helpful, scan the system again using -d (Nmap sometimes gives longer fingerprints that way) and paste both fingerprints into the fingerprint box on the submission form. Sometimes people read the file format section and submit their own working match lines. This is OK, but please submit the service fingerprint(s) as well because existing scripts make integrating and testing them relatively easy.

For those who care, the information in the fingerprint above is port number (21), protocol (TCP), Nmap version (3.40PVT16), date (September 6), UNIX time in hex, and a sequence of probe responses in the form  
`r({probename}, {response length}, "{responsestring}")`

- Submit corrections* -- This is another easy way to help improve the database. When integrating a service fingerprint submitted for "chargen on Windows XP" or "FooBar FTP server 3.9.213", it is difficult to determine how general the match is. Will it also match chargen on Solaris or FooBar FTP 2.7? There is no good way to tell. So a very specific name is used in the hope that people will report when the match needs to be generalized. If you scan a host and the service fingerprint gives an incorrect OS, version number, application name, or even service type, please mail the full Nmap output and correct information to <fyodor@insecure.org> and Nmap will be updated appropriately.
- Submit new probes* -- Suppose Nmap fails to detect a service. If it received a response to any probes at all, it should provide a fingerprint that can be submitted as described in #1 above. But what if there is no response and thus a fingerprint is not available? Create and submit your own probe! These are very welcome. The following steps describe the process.

### Steps for creating a new version detection probe

- Download the latest version of Nmap from <http://www.insecure.org/nmap/> and try again. You would feel a bit silly spending time developing a new probe just to find out that it has already been added. Make sure no

- fingerprint is available, as it is better to recognize services using existing probes if possible than to create too many new ones. If the service does not respond to any of the existing probes, there is no other choice.
- b. Decide on a good probe string for recognizing the service. An ideal probe should elicit a response from as many instances of the service as possible, and ideally the responses should be unique enough to differentiate between them. This step is easiest if you understand the protocol very well, so consider reading the relevant RFCs and product documentation. One simple approach is to simply start a client for the given service and watch what initial handshaking is done by sniffing the network with Ethereal or Tcpdump, or connecting to a listening Netcat.
  - c. Once you have decided on the proper string, add the appropriate new Probe line to Nmap (see Section 7.3 and Section 7.6). Do not put in any match lines at first, although a ‘ports’ directive to make this new test go first against the registered ports is OK. Then scan the service with Nmap a few times. You should get a fingerprint back showing the service’s response to your new probe. Send the new probe line and the fingerprints (against different machines if possible, but even a few against the same daemon helps to note differences) to Fyodor at fyodor@insecure.org. It will likely then be integrated into future versions of Nmap. Any details you can provide on the nature of your probe string is helpful as well. For custom services that only appear on your network, it is better to simply add them to your own nmap-service-probes rather than the global Nmap

## 7.8. [RECIPE] Find all servers running an insecure or nonstandard version of an application

\* *I need to actually write this recipe*

## 7.9. [RECIPE] Hack version detection to suit custom needs, such as open proxy detection

\* *I need to actually write this recipe*

# **Chapter 8. OS Fingerprinting**

# Chapter 9. Detecting and Subverting Firewalls and Intrusion Detection Systems

## 9.1. Introduction

Many Internet pioneers envisioned a global open network with a universal IP address space allowing virtual connections between any two nodes. This allows hosts to act as true peers, serving and retrieving information from each other. People could access all of their home systems from work, changing the climate control settings or unlocking the doors for early guests. This vision of universal connectivity has been stifled by address space shortages and security concerns. In the early 1990s, organizations began deploying firewalls for the express purpose of reducing connectivity. Huge networks were cordoned off from the unfiltered Internet by application proxies, network address translation, and packet filters. The unrestricted flow of information gave way to tight regulation of approved communication channels and the content that passes over them.

Network obstructions such as firewalls can make mapping a network exceedingly difficult. It will not get any easier, as stifling casual reconnaissance is often a key goal of implementing the devices. Nevertheless, Nmap offers many features to help understand these complex networks, and to verify that filters are working as intended. It even supports mechanisms for bypassing poorly implemented defenses. One of the best methods of understanding your network security posture is to try to defeat it. Place yourself in the mindset of an attacker, and deploy techniques from this chapter against your networks. Launch an FTP bounce scan, Idle scan, fragmentation attack, or try to tunnel through one of your own proxies.

In addition to restricting network activity, companies are increasingly monitoring traffic with intrusion detection systems (IDS). All of the major IDSs ship with rules designed to detect Nmap scans because scans are sometimes a precursor to attacks. Many of these products have recently morphed into intrusion *prevention* systems (IPS) that actively block traffic deemed malicious. Unfortunately for network administrators and IDS vendors, reliably detecting bad intentions by analyzing packet data is a tough problem. Attackers with patience, skill, and the help of certain Nmap options can usually pass by IDSs undetected. Meanwhile, administrators must cope with large numbers of "false positive" results where innocent activity is misdiagnosed and alerted on or blocked.

## 9.2. Why would whitehats ever do this?

Some of you whitehat readers may be tempted to skip this chapter. For authorized use against your own networks, why would you ever want to evade your own security systems? Because it helps in understanding the danger of real attackers. If you can sneak around a blocked portmapper port using Nmap direct RPC scanning, then so can the bad guys. It is easy to make a mistake in configuring complex firewalls and other devices. Many of them even come with glaring security holes which conscientious users must find and close. Regular network scanning can help find the dangerous implicit rules of your Checkpoint Firewall-1 or Windows IPsec filters before attackers do.

There are good reasons for evading IDSs as well. The most common is to evaluate IDS performance. If attackers can slide under the radar by simply adding an Nmap flag or two, the system is not offering much protection. It may still catch the script kiddies and worms, but they are usually blazingly obvious anyway.

Occasionally people suggest that Nmap should not offer features for evading firewall rules or sneaking past IDSs. They argue that these features are just as likely to be misused by attackers as used by administrators to enhance security. The problem with this logic is that these methods would still be used by attackers, who would just find other tools or patch the functionality into Nmap. Meanwhile, administrators would find it that much harder to do their jobs.

Deploying only modern, patched FTP servers is a far more powerful defense than trying to prevent the distribution of tools implementing the FTP bounce attack.

## **9.3. Determining Firewall Rules**

The first step toward bypassing firewall rules is to understand them. Where possible, Nmap distinguishes between ports that are reachable but closed, and those that are actively filtered. An effective technique is to start with a normal SYN port scan, then move on to more exotic techniques such as ACK scan and IPID sequencing to gain a better understanding of the network.

### **9.3.1. Standard SYN scan**

One helpful feature of the TCP protocol is that systems are required by RFC 793 (<http://www.rfc-editor.org/rfc/rfc793.txt>) to send a negative response to unexpected connection requests in the form of a TCP RST (reset) packet. The RST packet makes closed ports easy for Nmap to recognize. Filtering devices such as firewalls, on the other hand, tend to drop packets destined for disallowed ports. In some cases they send ICMP error messages (usually port unreachable) instead. Because dropped packets and ICMP errors are easily distinguishable from RST packets, Nmap can reliably detect filtered TCP ports from open or closed ones, and it does so automatically. This is shown in Example 9-1.

#### **Example 9-1. Detection of closed and filtered TCP ports**

```
# nmap -sS -T4 scanme.nmap.org

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 1655 ports scanned but not shown below are in state: filtered)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    open     smtp
53/tcp    open     domain
80/tcp    open     http
113/tcp   closed   auth

Nmap run completed -- 1 IP address (1 host up) scanned in 31.669 seconds
```

One of the most important lines in Example 9-1 is the parenthetical note that “the 1655 ports scanned but not shown below are in state: filtered”. In other words, this host has a proper deny-by-default firewall policy. Only those ports the administrator explicitly allowed are reachable, while the default action is to deny (filter) them. Four of the enumerated ports are in the open state, while the auth port (113) is closed. 1655 out of 1660 tested ports are unreachable by this standard scan. Leaving port 113 closed but unfiltered is a common practice on the Internet due to widespread use of the auth (often called ident) protocol. If that port is filtered instead of open or closed, some mail and IRC servers will spend a long time trying to connect back to their client’s ident port until the connection times out. A forged RST packet from the firewall causes the server to give up on ident quickly.

#### **9.3.1.1. Sneaky firewalls that return RST**

While the Nmap distinction between closed ports (which return a RST packet) and filtered ports (returning nothing or an ICMP error) is usually accurate, many firewall devices are now capable of forging RST packets as though they

are coming from the destination host and claiming that the port is closed. One example of this capability is the Linux iptables system, which offers many methods for rejecting undesired packets. The iptables man page documents this feature as follows:

--reject-with *type*

The *type* given can be icmp-net-unreachable, icmp-host-unreachable, icmp-port-unreachable, icmp-proto-unreachable, icmp-net-prohibited or icmp-host-prohibited, which return the appropriate ICMP error message (port-unreachable is the default). The option tcp-reset can be used on rules which only match the TCP protocol: this causes a TCP RST packet to be sent back. This is mainly useful for blocking ident (113/tcp) probes which frequently occur when sending mail to broken mail hosts (which won't accept your mail otherwise).

Forging RST packets by firewalls and IDS/IPS is not particularly common outside of port 113, as it can be confusing to legitimate network operators and it also allows scanners to move on to the next port immediately without waiting on the timeout caused by dropped packets. Nevertheless, it does happen. Such forgery can usually be detected by careful analysis of the RST packet in comparison with other packets sent by the machine. Section 9.6 describes effective techniques for doing so.

### 9.3.2. ACK scan

As described in depth in Chapter 5, the ACK scan sends TCP packets with only the ACK bit set. Whether ports are open or closed, the target is required by RFC 793 (<http://www.rfc-editor.org/rfc/rfc793.txt>) to respond with a RST packet. Firewalls that block the probe, on the other hand, usually make no response or send back an ICMP destination unreachable error. This distinction allows Nmap to report whether the ACK packets are being filtered. The set of filtered ports reported by an Nmap ACK scan is often less than for a SYN scan against the same machine because ACK scans are more difficult to filter. Many networks allow nearly unrestricted outbound connections, but wish to block Internet hosts from initiating connections back to them. Blocking incoming SYN packets (without the ACK bit set) is an easy way to do this, but it still allows any ACK packets through. Blocking those ACK packets is more difficult, because they do not tell which side started the connection. To block unsolicited ACK packets (as sent by the Nmap ACK scan), while allowing ACK packets belonging to legitimate connections, firewalls must statefully watch every established connection to determine whether a given ACK is appropriate. These stateful firewalls are usually more secure because they can be more restrictive. Blocking ACK scans is one extra available restriction. The downsides are that they require more resources to function, and a stateful firewall reboot can cause a device to lose state and terminate all established connections passing through it.

While stateful firewalls are widespread and rising in popularity, the stateless approach is still quite common. For example, the Linux Netfilter/iptables system supports the --syn convenience option to make the stateless approach described above easy to implement.

In the previous section, a SYN scan showed that all but 5 of 1660 common ports on scanme.nmap.org were in the filtered state. Example 9-2 demonstrates an ACK scan against the same host to determine whether it is using a stateful firewall.

#### Example 9-2. ACK scan against Scanme

```
# nmap -sA -T4 scanme.nmap.org
Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
```

```
(The 1655 ports scanned but not shown below are in state: filtered)
PORT      STATE     SERVICE
22/tcp    UNfiltered ssh
25/tcp    UNfiltered smtp
53/tcp    UNfiltered domain
80/tcp    UNfiltered http
113/tcp   UNfiltered auth
```

Nmap run completed -- 1 IP address (1 host up) scanned in 31.389 seconds

The same five ports displayed in the SYN scan are shown here. The other 1655 are still filtered. This is because Scanme is protected by this stateful iptables directive: **iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT**. This only accepts packets that are part of or related to an established connection. Unsolicited ACK packets sent by Nmap are dropped, except to the five special ports shown. Special rules allow all packets to the open ports 22, 25, 53, and 80, as well as sending a RST packet in response to port 113 probes. Note that the five shown ports are in the unfiltered state, since the ACK scan cannot further divide them into open (22, 25, 53, and 80) or closed (113).

Now let us look at another example. A Linux host named Para on my local network uses the following (simplified to save space) firewall script:

```
#!/bin/sh
#
# A simple, stateless, host-based firewall script.

# First of all, flush & delete any existing tables
iptables -F
iptables -X

# Deny by default (input/forward)
iptables --policy INPUT DROP
iptables --policy OUTPUT ACCEPT
iptables --policy FORWARD DROP

# I want to make ssh and www accessible from outside
iptables -A INPUT -m multiport -p tcp --destination-port 22,80 -j ACCEPT

# Allow responses to outgoing TCP requests
iptables -A INPUT --proto tcp ! --syn -j ACCEPT
```

This firewall is stateless, as there is no sign of the --state option or the -m state module request. Example 9-3 shows SYN and ACK scans against this host.

### Example 9-3. Contrasting SYN and ACK scans against Para

```
# nmap -sS -p1-100 -T4 para

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on para (192.168.10.191):
(The 98 ports scanned but not shown below are in state: filtered)
PORT      STATE     SERVICE
22/tcp    open      ssh
```

```
80/tcp closed http
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap run completed -- 1 IP address (1 host up) scanned in 3.810 seconds

# nmap -sA -p1-100 -T4 para

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
All 100 scanned ports on para (192.168.10.191) are: UNfiltered
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap run completed -- 1 IP address (1 host up) scanned in 0.695 seconds
```

In the SYN scan, 98 of 100 ports are filtered. Yet the ACK scan shows every scanned port being unfiltered. In other words, all of the ACK packets are sneaking through unhindered and eliciting RST responses. These responses also make the scan more than five times as fast, since it does not have to wait on timeouts.

Now we know how to distinguish between stateful and stateless firewalls, but what good is that? The ACK scan of Para shows that some packets are probably reaching the destination host. I say probably because firewall forgery is always possible. While you may not be able to establish TCP connections to those ports, they can be useful for determining which IP addresses are in use, OS detection tests, certain IPID shenanigans, and as a channel for tunneling commands to rootkits installed on those machines. Other scan types, such as FIN scan, may even be able to determine which ports are open and thus infer the purpose of the hosts. Such hosts may be useful as zombies for an IPID idle scan.

This pair of scans also demonstrates that what we are calling a port state is not solely a property of the port itself. Here, the same port number is considered *filtered* by one scan type and *unfiltered* by another. What IP address you scan from, the rules of any filtering devices along the way, and which interface of the target machine you access can all affect how Nmap sees the ports. The port table only reflects what Nmap saw when running from a particular machine, with a defined set of options, at the given time.

### **9.3.3. IPID tricks**

The humble identification field within IP headers can divulge a surprising amount of information. Later in this chapter it will be used for port scanning (Idle scan technique) and to detect when firewall and intrusion detection systems are forging RST packets as though they come from protected hosts. Another neat trick is to discern what source addresses make it through the firewall. There is no point spending hours on a blind spoofing attack "from" 192.168.0.1 if some firewall along the way drops all such packets.

I usually test this condition with the free network probing tool hping2 (<http://www.hping.org>). This is a rather complex technique, but it can be valuable sometimes. Here are the steps I take.

1. Find at least one accessible (open or closed) port of one machine on the internal network. Routers, printers, and Windows boxes often work well. Recent releases of Linux, Solaris, and OpenBSD have largely resolved the issue of predictable IPID sequence numbers and will not work. The machine chosen should not be heavily trafficked.
2. Verify that the machine has predictable IPID sequences. The following command tests a Windows XP machine named playground. The hping2 options request that 5 SYN packets be sent to port 80, one second apart.

```
# hping2 -c 5 -i 1 -p 80 -S playground
HPING playground (eth0 192.168.0.40): S set, 40 headers + 0 data bytes
```

```

len=46 ip=192.168.0.40 ttl=128 id=64473 sport=80 flags=RA seq=0 rtt=0.7 ms
len=46 ip=192.168.0.40 ttl=128 id=64474 sport=80 flags=RA seq=1 rtt=0.3 ms
len=46 ip=192.168.0.40 ttl=128 id=64475 sport=80 flags=RA seq=2 rtt=0.3 ms
len=46 ip=192.168.0.40 ttl=128 id=64476 sport=80 flags=RA seq=3 rtt=0.3 ms
len=46 ip=192.168.0.40 ttl=128 id=64477 sport=80 flags=RA seq=4 rtt=0.3 ms

--- playground hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.3/0.7 ms

```

Since the IPID fields are perfectly sequential, we can move on to the next test. If they were random or very far apart, we would have to find a new accessible host.

3. Start a flood of probes to the target from a host near your own (just about any host will do). An example command is **hping2 --spoof scanme.nmap.org --fast -p 80 -c 10000 -S playground**. Replace scanme.nmap.org with some other host of your choosing, and playground with your target host. Getting replies back is not necessary, because the goal is simply to increment the IPID sequences. Do not use the real address of the machine you are running hping2 from. Using a machine nearby on the network is advised to reduce the probability that your own ISP will block the packets.

While this is going on, redo the test from the previous step against your target machine.

```

# hping2 -c 5 -i 1 -p 80 -S playground
HPING playground (eth0 192.168.0.40): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.40 ttl=128 id=64672 sport=80 flags=RA seq=0 rtt=0.6 ms
len=46 ip=192.168.0.40 ttl=128 id=64683 sport=80 flags=RA seq=1 rtt=0.2 ms
len=46 ip=192.168.0.40 ttl=128 id=64694 sport=80 flags=RA seq=2 rtt=0.2 ms
len=46 ip=192.168.0.40 ttl=128 id=64705 sport=80 flags=RA seq=3 rtt=0.2 ms
len=46 ip=192.168.0.40 ttl=128 id=64716 sport=80 flags=RA seq=4 rtt=0.2 ms

--- playground hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.3/0.6 ms

```

This time, the IPIDs are increasing by roughly 11 a second instead of one. The target is receiving our 10 forged packets per second, and responding to each. Each response increments the IPID. Some hosts use a unique IPID sequence for each IP address they communicate with. If that had been the case, we would not have seen the IPID leaping like this and we would have looked for a different target host on the network.

4. Repeat step 3 using spoofed addresses that you suspect may be allowed through the firewall or trusted. Try addresses from within their firewall, as well as the RFC 1918 (<http://www.rfc-editor.org/rfc/rfc1918.txt>) blessed private networks such as 10.0.0.0/8, 192.168.0.0/16, and 172.16.0.0/12. Also try localhost (127.0.0.1) and maybe another address from 127.0.0.0/8 to detect cases where 127.0.0.1 is hard coded in. There have been many security holes related to spoofed localhost packets, including the infamous Land denial of service attack. Misconfigured systems sometimes trust these addresses without checking whether they came in through the localhost interface. If a source address gets through to the end host, the IPID will jump as seen in step 3. If it continues to increment slowly as in step 2, the packets were likely dropped by a firewall or router.

The end result of this technique is a list of source address netblocks that are permitted through the firewall, and those that are blocked. This information is valuable for several reasons. The IP addresses a company chooses to block or allow may give clues as to what addresses are used internally or trusted. For example, machines on a company's

production network might trust IP addresses on the corporate network, or trust a system administrator's personal machine. Machines on the same production network also sometimes trust each other, or trust localhost. Common IP-based trust relationships are seen in nfs exports, host firewall rules, tcp wrappers, custom applications, rlogin, etc. Before spending substantial time trying to find and exploit these problems, use the test described here to determine whether the spoofed packets even get through.

A concrete example of this trusted-source-address problem is that I once found that a company's custom UDP service allowed users to skip authentication if they came from special netblocks entered into a configuration file. These netblocks corresponded to different corporate locations. Their internet-facing firewall smartly tried to block those addresses, as actual employees could access production from a private link. But by using the techniques described in this section, I found that the firewall was not perfectly synced with the config file. There were a few addresses from which I could successfully forge the UDP control messages and take over their application.

This technique of mapping out the firewall rules does not use Nmap, but the results are valuable for future runs. For example, this test can show whether to use certain decoys (-D). The best decoys will make it all the way to the target system. In addition, forged packets must get through for the IPID Idle scan (discussed later) to work. Testing potential source IPs with this technique is usually easier than finding and testing every potential Idle proxy machine on a network. Potential Idle proxies need only be tested if they pass step number two, above.

### **9.3.4. UDP version scanning**

The previous sections have all focused on the prevalent TCP protocol. Working with UDP is often more difficult, because the protocol does not provide acknowledgment of open ports like TCP does. Many UDP applications will simply ignore unexpected packets, leaving Nmap unsure whether the port is open or filtered. So Nmap places them in the open|filtered state, as shown in Example 9-4.

#### **Example 9-4. UDP scan against firewalled host**

```
# #nmap -sU -p50-59 scanme.nmap.org

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
PORT      STATE            SERVICE
50/udp    open|filtered   re-mail-ck
51/udp    open|filtered   la-maint
52/udp    open|filtered   xns-time
53/udp    open|filtered   domain
54/udp    open|filtered   xns-ch
55/udp    open|filtered   isi-gl
56/udp    open|filtered   xns-auth
57/udp    open|filtered   priv-term
58/udp    open|filtered   xns-mail
59/udp    open|filtered   priv-file

Nmap run completed -- 1 IP address (1 host up) scanned in 1.400 seconds
```

This 10-port scan was not very helpful. No port responded to the probe packets, and so they are all listed as open or filtered. One way to better understand which ports are actually open is to send a whole bunch of UDP probes for dozens of different known UDP services in the hope of eliciting a response from any open ports. Nmap version

detection (chapter 7) does exactly that. Example 9-5 shows the same scan with the addition of version detection (`-sV`).

**Example 9-5. UDP version scan against firewalled host**

```
# nmap -sV -sU -p50-59 scanme.nmap.org

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
PORT      STATE      SERVICE      VERSION
50/udp    open|filtered re-mail-ck
51/udp    open|filtered la-maint
52/udp    open|filtered xns-time
53/udp    open          domain      ISC Bind 9.2.1
54/udp    open|filtered xns-ch
55/udp    open|filtered isi-gl
56/udp    open|filtered xns-auth
57/udp    open|filtered priv-term
58/udp    open|filtered xns-mail
59/udp    open|filtered priv-file

Nmap run completed -- 1 IP address (1 host up) scanned in 31.380 seconds
```

Version detection shows beyond a doubt that port 53 (domain) is open, and even what it is running. The other are still in `open|filtered` because they did not respond to any of the probes. They are probably filtered, though this is not guaranteed. They could be running a service like SNMP, which only responds to packets with the correct community string. Or they could be running an obscure or custom UDP service for which no Nmap version detection probe exists. Also note that this scan took 15 times longer than the previous one. Sending all of those probes to each port is a relatively slow process.

## 9.4. Bypassing Firewall Rules

While mapping out firewall rules can be valuable, bypassing rules is often the primary goal. Nmap implements many techniques for doing this, though most are only effective against poorly configured networks. Unfortunately, those are common. Individual techniques may each have a low probability of success, so try as many different methods as possible. The attacker need only find one misconfiguration to succeed, while the network defenders must close every hole.

### 9.4.1. Exotic scan flags

The previous section discussed using an ACK scan to map out which target network ports are filtered. However, it could not determine which of the accessible ports were open or closed. Nmap offers several scan methods that are good at sneaking past firewalls while still providing the desired port state information. FIN scan is one such technique. In Section 9.3.2, SYN and ACK scans were run against a machine named Para. The SYN scan showed only 2 open ports, perhaps due to firewall restrictions. Meanwhile, the ACK scan is unable to recognize open ports from closed ones. Example 9-6 shows another scan attempt against this machine, this time using a FIN scan. Because a naked FIN packet is being set, this packet flies past the rules blocking SYN packets. While a SYN scan only found one open port below 100, the FIN scan finds both of them.

**Example 9-6. FIN scan against stateless firewall**

```
# nmap -sF -p1-100 -T4 para

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on para (192.168.10.191):
(The 98 ports scanned but not shown below are in state: closed)
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
53/tcp    open|filtered domain
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap run completed -- 1 IP address (1 host up) scanned in 1.612 seconds
```

Many other scan types are worth trying, since the target firewall rules and target host type determine which techniques will work. Some particularly valuable scan types are FIN, Maimon, Window, SYN|FIN, and NULL scans. These are all described in Chapter 5.

#### **9.4.2. Source port manipulation**

One surprisingly common misconfiguration is to trust traffic based only on the source port number. It is easy to understand how this comes about. An administrator will set up a shiny new firewall, only to be flooded with complaints from ungrateful users whose applications stopped working. In particular, DNS may be broken because the UDP DNS replies from external servers can no longer enter the network. FTP is another common example. In active FTP transfers, the remote server tries to establish a connection back to the client to transfer the requested file.

Secure solutions to these problems exist, often in the form of application-level proxies or protocol-parsing firewall modules. Unfortunately there are also easier, insecure solutions. Noting that DNS replies come from port 53 and active ftp from port 20, many admins have fallen into the trap of simply allowing incoming traffic from those ports. They often assume that no attacker would notice and exploit such firewall holes. In other cases, admins consider this a short-term stop-gap measure until they can implement a more secure solution. Then they forget the security upgrade.

Overworked network administrators are not the only ones to fall into this trap. Numerous products have shipped with these insecure rules. Even Microsoft has been guilty. The IPsec filters that ship with Windows 2000 and Windows XP contain an implicit rule that allows all TCP or UDP traffic from port 88 (Kerberos). In another well-known case, versions of the Zone Alarm personal firewall up to 2.1.25 allowed incoming UDP packets with the source port 53 (DNS) or 67 (DHCP).

Nmap offers the `-g` option to exploit these weaknesses. Simply provide a port number, and Nmap will send packets from that port where possible. Nmap must use different port numbers for certain OS detection tests to work properly, and DNS requests ignore the `-g` flag because Nmap relies on system libraries to handle those. Most TCP scans, including SYN scan, support the option completely, as does UDP scan. In May 2004, JJ Gray posted example Nmap scans to Bugtraq that demonstrate exploitation of the Windows IPsec source port 88 bug against one of his clients. A normal scan, followed by a `-g 88` scan are shown in Example 9-7. Some output has been removed for brevity and clarity.

**Example 9-7. Bypassing Windows IPsec filter using source port 88**

```
# nmap -sS -v -v -P0 172.25.0.14
```

```
Starting nmap 3.50 ( http://www.insecure.org/nmap/ )
Interesting ports on 172.25.0.14:
(The 1658 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE
88/tcp    closed  kerberos-sec

Nmap run completed -- 1 IP address (1 host up) scanned in 7.017 seconds

# nmap -sS -v -v -P0 -g 88 172.25.0.14

Starting nmap 3.50 ( http://www.insecure.org/nmap/ )
Interesting ports on 172.25.0.14:
(The 1653 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
445/tcp   open   microsoft-ds
1025/tcp  open   NFS-or-IIS
1027/tcp  open   IIS
1433/tcp  open   ms-sql-s

Nmap run completed -- 1 IP address (1 host up) scanned in 0.367 seconds
```

Note that the closed port 88 was the hint that led JJ to try using it as a source port. For further information on this vulnerability, see Microsoft Knowledge Base Article 811832  
(<http://support.microsoft.com/default.aspx?scid=kb;EN-US;811832>)

#### **9.4.3. IPv6 attacks**

While IPv6 has not exactly taken the world by storm, it is reasonably popular in Japan and certain other regions. When organizations adopt this protocol, they often forget to lock it down as they have instinctively learned to do with IPv4. Or they may try to, but find that their hardware does not support IPv6 filtering rules. Filtering IPv6 can sometimes be more critical than IPv4 because the expanded address space often allows the allocation of globally addressable IPv6 addresses to hosts that would normally have to use the RFC1918-blessed private IPv4 addresses.

Performing an IPv6 scan rather than the IPv4 default is often as easy as adding `-6` to the command line. Certain features such as OS detection and UDP scanning are not yet supported for this protocol, but the most popular features work. Example 9-8 demonstrates IPv4 and IPv6 scans, performed in 2002, of a well-known IPv6 development and advocacy organization.

#### **Example 9-8. Comparing IPv4 and IPv6 scans**

```
> nmap www.kame.net

Starting nmap V. 3.10ALPHA1 ( www.insecure.org/nmap/ )
Interesting ports on kame220.kame.net (203.178.141.220):
(The 1585 ports scanned but not shown below are in state: closed)
Port      State      Service
19/tcp    filtered  chargen
21/tcp    open       ftp
22/tcp    open       ssh
```

```

53/tcp      open     domain
80/tcp      open     http
111/tcp     filtered sunrpc
137/tcp     filtered netbios-ns
138/tcp     filtered netbios-dgm
139/tcp     filtered netbios-ssn
513/tcp     filtered login
514/tcp     filtered shell
2049/tcp    filtered nfs
2401/tcp    open     cvspserver
5999/tcp    open     ncd-conf
7597/tcp    filtered qaz
31337/tcp   filtered Elite

```

Nmap run completed -- 1 IP address (1 host up) scanned in 34 seconds

```
> nmap -6 www.kame.net
```

```

Starting nmap V. 3.10ALPHA1 ( www.insecure.org/nmap/ )
Interesting ports on 3ffe:501:4819:2000:210:f3ff:fe03:4d0:
(The 1595 ports scanned but not shown below are in state: closed)
Port      State       Service
21/tcp    open        ftp
22/tcp    open        ssh
53/tcp    open        domain
80/tcp    open        http
111/tcp   open        sunrpc
2401/tcp  open        cvspserver

```

Nmap run completed -- 1 IP address (1 host up) scanned in 19 seconds

The first scan shows numerous filtered ports, including frequently exploitable services such as sunrpc, Windows NetBIOS, and NFS. Yet scanning the same host with IPv6 shows no filtered ports! Suddenly SunRPC (port 111) is available, and waiting to be queried by an IPv6-enabled rpcinfo or by Nmap version detection, which supports IPv6. They fixed the issue shortly after I notified them of it.

In order to perform an IPv6 scan, a system must be configured for IPv6. It must have an IPv6 address and routing information. Since my ISPs do not provide an IPv6 address, I use a free ipv6 tunnel broker service. One of the better free tunnel brokers is run by BT Exact at <https://tb.ipv6.btexact.com/>. I have also used one that Hurricane Electric provides at <http://ipv6tb.he.net/>. 6to4 tunnels are another popular, free approach. Of course, this technique also requires that the target use IPv6.

#### **9.4.4. IPID Idle Scanning**

The IPID Idle Scan has a reputation for being one of the most stealthy scan types, since no packets are sent to the target from your real address. Open ports are inferred from the IPID sequences of a chosen zombie machine. A less recognized feature of Idle scan is that the results obtained are actually those you would get if the zombie was to scan the target host directly. In a similar way that the `-g` option allows exploitation of trusted source ports, Idle Scan can sometimes exploit trusted source IP addresses. This ingenious scan type, which was originally conceived by security researcher Antirez, is described fully in Chapter 5.

### 9.4.5. Multiple ping probes

A common issue when trying to scan through firewalled networks is that dropped ping probes can lead to missed hosts. To reduce this problem, Nmap allows a very wide variety of probes to be sent in parallel. Hopefully at least one will get through. Chapter three discusses these techniques in depth, including empirical data on the best firewall-busting techniques.

### 9.4.6. Fragmentation

Some packet filters have trouble dealing with IP packet fragments. They could reassemble the packets themselves, but that requires extra resources. There is also the possibility that fragments will take different paths, preventing reassembly. Due to this complexity, some filters ignore all fragments, while others automatically pass all but the first fragment. Interesting things can happen if the first fragment is not long enough to contain the whole TCP header, or if the second packet partially overwrites it. The number of filtering devices vulnerable to these problems is shrinking, though it never hurts to try. An Nmap scan will use tiny IP fragments if the `-f` is specified. Run a sniffer like ethereal or tcpdump the first time you use this option, to ensure packets leave your machine fragmented. Some overly helpful hosts will defragment the packets before they even leave the device. Linux 2.4 kernels are particularly prone to this.

It might be nice if Nmap could send fragments out of order or with configurable length. The RFCs allow IP packets with only 8 bytes of data after the IP header. So a 20-byte TCP packet could be split into three packets (the final packet may be smaller still). Because certain Linux versions and other operating systems restrict sending tiny or out-of-order IP fragments over raw sockets, Nmap breaks the 20-byte TCP header into a 16-byte segment and a four-byte segment, which it then sends in order.

If a fragmented port scan gets through, a tool such as Fragroute (<http://www.monkey.org/~dugsong/fragroute/>) can be used to fragment other tools and exploits used to attack the host.

### 9.4.7. Proxies

Application-level proxies, particularly for the web, have become popular due to perceived security and network efficiency (through caching) benefits. Like firewalls and IDS, misconfigured proxies can cause far more security problems than they solve. The most frequent problem is a failure to set appropriate access controls. Hundreds of thousands of wide-open proxy machines exist on the Internet, allowing anyone to use them as an anonymous hopping points to other Internet sites. Dozens of organizations use automated scanners to find these open proxies and distribute the IP addresses. Occasionally the proxies are used for arguably positive things, such as escaping the draconian censorship imposed by the Chinese government on its residents. This "great firewall of China" has been known to block the New York Times website as well as other news, political, and spiritual sites that the government disagrees with. Unfortunately, the open proxies are more frequently abused by more sinister folks who want to anonymously crack into sites, commit credit card fraud, or flood the Internet with spam.

While hosting a wide-open proxy to Internet resources can cause numerous problems, a more serious condition is when the open proxies allow connections back into the protected network. Administrators who decide that internal hosts must use a proxy to access Internet resources often inadvertently allow traffic in the opposite direction as well. The hacker Adrian Lamo is famous for breaking into Microsoft, Excite, Yahoo, WorldCom, the New York Times, and other large networks, usually by exploiting this reverse-proxy technique.

Nmap does not presently offer a proxy scan-through option, though it is high on the priority list. Chapter 7 discusses a way to find open proxies using Nmap version detection.

\* I still need to add that section.

In addition, plenty of dedicated free proxy scanners are available on Internet sites such as Packet Storm (<http://packetstormsecurity.nl/>). Lists of thousands of open proxies are widespread as well.

#### **9.4.8. Source routing**

This old-school technique is still effective in some cases. If a particular router on the path is causing you trouble, try to find a route around it. Effectiveness of this technique is limited because packet filtering problems usually occur on or near the target network. Those machines are likely to either drop all source routed packets or to be the only way into the network. Nmap does not presently support source routing, so I use Hobbit's Netcat ([http://www.atstake.com/research/tools/network\\_utilities/](http://www.atstake.com/research/tools/network_utilities/)), with the `-g` option, when I find it necessary.

#### **9.4.9. FTP Bounce Scan**

While only a small percentage of FTP servers are still vulnerable, it is worth checking whether all of your clients' systems for this problem. At a minimum, it allows outside attackers to utilize vulnerable systems to scan other parties. Worse configurations even allow attackers to bypass the organization's firewalls. Details and examples of this technique are provided in Section 5.12. Example 9-9 shows an HP printer being used to relay a port scan. If this printer is behind the organization's firewall, it can be used to scan normally inaccessible (to the attacker) internal addresses as well.

##### **Example 9-9. Exploiting a printer with the FTP bounce scan**

```
felix~> nmap -p 22,25,135 -P0 -v -b XXX.YY.111.2 scanme.nmap.org

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Attempting connection to ftp://anonymous:-wwwuser@XXX.YY.111.2:21
Connected:220 JD FTP Server Ready
Login credentials accepted by ftp server!
Initiating TCP ftp bounce scan against scanme.nmap.org (205.217.153.55)
Adding open port 22/tcp
Adding open port 25/tcp
Scanned 3 ports in 12 seconds via the Bounce scan.
Interesting ports on scanme.nmap.org (205.217.153.55):
PORT      STATE     SERVICE
22/tcp    open      ssh
25/tcp    open      smtp
135/tcp   filtered msrpc

Nmap run completed -- 1 IP address (1 host up) scanned in 21.790 seconds
```

#### **9.4.10. Take an alternative path**

I hate to overuse the “think outside the box” cliche, but continually banging on the front door of a well-secured network is not always the best approach. Look for other ways in. Wardial their phone lines, attack subsidiaries who may have special network access, or show up at their offices with Wi-Fi sniffing equipment, or even sneak in and plug into a convenient ethernet jack. Nmap works well through all of these connections. Just make sure that your

penetration-testing contract covers these methods before your client catches you in a ninja suit grappling onto their datacenter rooftop.

## **9.5. Subverting Intrusion Detection Systems**

Firewalls are not the only obstacle that modern attackers face. Intrusion detection and prevention systems can be problematic as well. Network administration staff do not always take well to a flood of 2 A.M. intrusion alert pages from the IDS. Considerate hackers take pains to prevent their actions from causing all of these alerts in the first place. A first step is to detect whether an IDS is even present -- many small companies do not use them. If an IDS is suspected or detected, there are many effective techniques for subverting it. They fall into three categories that vary by intrusiveness: avoiding the IDS as if the attacker is not there, confusing the IDS with misleading data, and exploiting the IDS to gain further network privilege or just to shut it down. Alternatively, attackers who are not concerned with stealth can ignore the IDS completely as they pound away at the target network.

### **9.5.1. Intrusion detection system detection**

Early the never-ending battle between network administrators and malicious hackers, admins defended their turf by hardening systems and even installing firewalls to act as a perimeter barrier. Hackers developed new tools to penetrate or sneak around the firewalls and exploit vulnerable hosts. The arms race escalated with admins introducing intrusion detection systems that constantly watch for devious activity. Attackers responded, of course, by devising systems for detecting and deceiving the IDS. While intrusion detection systems are meant to be passive devices, many can be detected by attackers over the network.

The least conspicuous IDS is one that passively listens to network traffic without ever transmitting. Special network tap hardware devices are available to ensure that the IDS *cannot* transmit, even if it is compromised by attackers. Despite the security advantages of such a setup, it is not widely deployed due to practical considerations. Modern IDSs expect to be able send alerts to central management controls and the like. If this was all the IDS transmitted, the risk would be minimal. But to provide more extensive data on the alert, they often initiate probes that may be seen by attackers.

#### **9.5.1.1. Reverse probes**

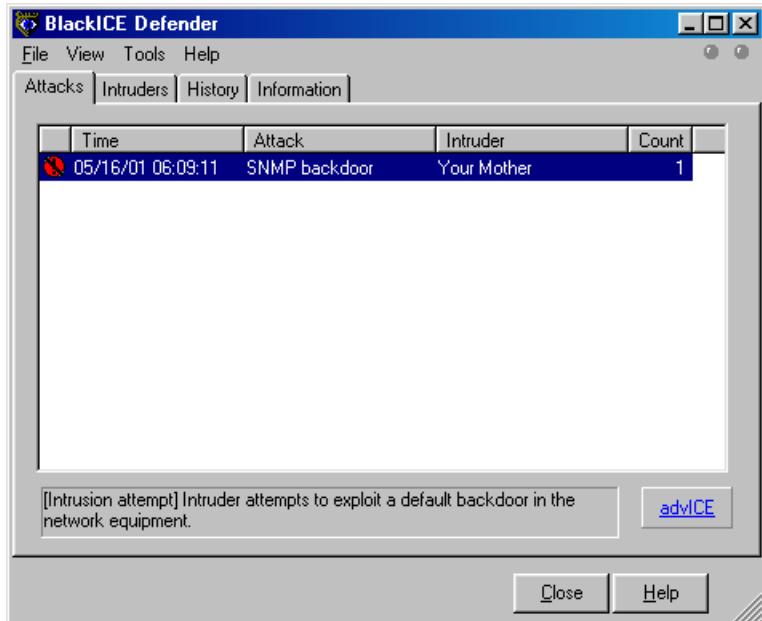
One probe commonly initiated by IDSs is reverse DNS query of the attacker's IP address. A domain name in an alert is more valuable than just an IP address, after all. Unfortunately, attackers who control their own rDNS (quite common) can watch the logs in real time and learn that they have been detected. This is a good time for attackers to feed misinformation, such as bogus names and cache entries to the requesting IDS.

Some IDSs go much further, and send more intrusive probes to the apparent attackers. When an attacker sees his target port scan him back, there is no question that he has set off alarms. Some IDSs send Windows NetBIOS information requests back to the attacker. ISS BlackIce Defender is one vendor that does (or at least did) this by default. I wrote a small tool called icepick which sends a simple packet that generates an alert from listening BlackIce instances. Then it watches for telltale NetBIOS queries and reports any BlackIce installations found. One could easily scan large networks looking for this IDS and then attempt to exploit them using holes discussed later in this chapter.

Not content with simply locating BlackIce installations or detecting them during penetration tests, I wrote a simple UNIX program called windentd which replies to the probe with misinformation. Figure 9-1 shows a BlackIce

console where the Intruder is listed as "Your Mother" thanks to windentd and icepick. Those simple tools are available from <http://www.insecure.org/presentations/CanSecWest01/>, though they are not supported.

**Figure 9-1. BlackIce discovers an unusual intruder**



### 9.5.1.2. Sudden firewall changes and suspicious packets

Many intrusion detection systems have lately morphed into what marketing departments label intrusion prevention systems. The best of these systems are inline on the network so that they can restrict packet flow when suspicious activity is detected. For example, they may block any further traffic from an IP address that they believe has port scanned them, or that has attempted a buffer overflow exploit. Attackers are likely to notice this if they port scan a system, then are unable to connect to the reported open ports. Attackers can confirm that they are blocked by trying to connect from another IP address.

Suspicious response packets can also be a tip-off that an attacker's actions have been flagged by an IDS. In particular, many IDSs that are *not* inline on the network will forge RST packets in an attempt to tear down connections. Ways to determine that these packets are forged are covered in Section 9.6.

### 9.5.1.3. Naming conventions

Naming conventions can be another giveaway of IDS presence. If an Nmap list scan returns host names such as realsecure, ids-monitor, or dragon-ids, you may have found an intrusion detection system. The admins might have given away that information inadvertently, or they may think of it like the alarm stickers on house and car windows. Perhaps they think that the script kiddies will be scared away by IDS-related names. It could also be misinformation. You can never fully trust DNS names. For example, you might assume that bugzilla.securityfocus.com is a web server running the popular Bugzilla web-based bug tracking software. Not so. The Nmap scan in Example 9-10 shows that it is probably a Symantec Raptor firewall instead. No web server is accessible.

**Example 9-10. Host names can be deceiving**

```
# nmap -sS -sV -T4 -p1-24 bugzilla.securityfocus.com

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Interesting ports on 205.206.231.82:
(The 21 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp-proxy   Symantec Enterprise Firewall FTP proxy
22/tcp    open  ssh?        Symantec Raptor firewall secure gateway telnetd
23/tcp    open  telnet     Symantec Raptor firewall secure gateway telnetd

Nmap run completed -- 1 IP address (1 host up) scanned in 0.935 seconds
```

**9.5.1.4. Unexplained TTL jumps**

One more way to detect certain IDSs is to watch for unexplained gaps (or suspicious machines) in traceroutes. In Example 9-11, which was contrived for simplicity, traceroute locates nothing at hop 5. That may be an inline IDS or firewall protecting the target company. Of course, this can only detect inline IDSs. Even some of the inline devices may fail to decrement the TTL or may refuse to pass ICMP ttl-exceeded messages back from the protected network.

**Example 9-11. Noting TTL gaps with traceroute**

```
# traceroute www.target.com
traceroute to orestes.red.target.com (10.0.0.6), 30 hops max, 38 byte packets
 1 gw (205.217.153.49)  0.694 ms  0.641 ms  0.587 ms
 2 metrol-ge-152.pa.meer.net (205.217.152.1)  1.972 ms  1.413 ms  1.947 ms
 3 208.185.168.171 (208.185.168.171)  1.294 ms  1.853 ms  1.325 ms
 4 p4-2-0-0.r06.plalca01.us.bb.verio.net (129.250.9.129)  1.596 ms  1.779 ms  1.467 ms
 5 * * *
 6 orestes.red.target.com (10.0.0.6)  76.200 ms  76.180 ms  76.747 ms
#
```

**9.5.2. Avoiding intrusion detection systems**

The most subtle way to defeat intrusion detection systems is to avoid their watchful gaze entirely. The reality is that rules governing IDSs are pretty brittle in that they can often be defeated by manipulating the attack slightly. Attackers have dozens of techniques, from URL encoding to polymorphic shellcode generators for escaping IDS detection of their exploits. This section focuses on stealthy port scanning, which is even easier than stealthily exploiting vulnerabilities.

**9.5.2.1. Slow down**

When it comes to avoiding IDS alerts, patience is a virtue. Port scan detection is usually threshold based. The system watches for a given number of probes in a certain timeframe. This helps prevent false positives from innocent users. It is also essential to save resources -- saving connection probes forever would consume memory and make realtime list searching too slow. The downside to this threshold approach is that attackers can evade it by keeping their scan rate just below the threshold. Nmap offers several canned timing modes that can be selected with the `-T` option to

accomplish this. For example, the `-T paranoid` option causes Nmap to send just one probe at a time, waiting five minutes between them. A large scan may take weeks, but at least it probably will not be detected. The `-T sneaky` option is similar, but it only waits 15 seconds between probes.

Rather than specify canned timing modes such as `sneaky`, timing variables can be customized precisely with options such as `--max_parallelism`, `--min_rtt_timeout`, and `--scan_delay`. Chapter 6 describes these in depth.

#### 9.5.2.1.1. A practical example: bypassing default Snort 2.2.0 rules

Examining the handy open-source IDS Snort provides a lesson on sneaking under the radar. Snort has had several generations of port scan detectors. The latest, Flow-portscan, is quite formidable. A scan that slips by this is likely to escape detection by many other IDSS as well.

Flow-portscan is made up of two detection systems that can work in concert (or be enabled individually) to detect port scanners. The system and its dozens of configuration variables are documented in `docs/README.flow-portscan` (<http://cvs.snort.org/viewcvs.cgi/snort/doc/README.flow-portscan?rev=HEAD>) in the Snort distribution, but I'll provide a quick summary.

The simpler detection method in Flow-portscan is known as the *fixed time scale*. This simply watches for scanner-fixed-threshold probe packets in scanner-fixed-window seconds. Those two variables, which are set in `snort.conf`, each default to 15. Note that the counter includes any probes sent from a single machine to any host on the protected network. So quickly scanning a single port on each of 15 protected machines will generate an alert just as surely as scanning 15 ports on a single machine.

If this were the only detection method, the solution would be pretty easy. Pass the `--scan_delay 1075` option to ensure that Nmap waits 1.075 seconds between sending probes. The intuitive choice might be a one second wait between packets to avoid 15 packets in 15 seconds, but that is not enough. There are only 14 weights between sending the first packet and the fifteenth, so the wait must be at least  $15/14$ , or 1.07143 seconds. Some poor sap who chooses `--scan_delay 1000` would slow the scan down dramatically, while still triggering the alarm. If multiple hosts on the network are being probed, they must be scanned separately to avoid triggering the alarm. The option `--max_hostgroup 1` would insure that only one host at a time is scanned, but is not completely safe because it will not enforce the `--scan_delay` between the last probe sent to one host, and the first sent to the next. As long as at least 15 ports per host are being scanned, you could compensate by making the `--scan_delay` at least 1155ms, or simply start single-target Nmap instances from a shell script, waiting 1075ms between them. Example 9-12 shows such a stealthy scan of several machines on a network. Multiple Nmap instances are handled using the tcsh shell syntax. Here the IPs are specified manually. If many targets were desired, they could be enumerated into a file with the `-iL` (list scan) option, then Nmap started against each using a normal shell loop. The reason these scans took more than 1.075 seconds per port is that retransmissions were required for the filtered ports to ensure that they were not dropped due to network congestion.

#### Example 9-12. Slow scan to bypass the default Snort 2.2.0 Flow-portscan fixed time scan detection method

```

felix~# foreach target (205.217.153.53 205.217.153.54 205.217.153.55)
foreach? nmap --scan_delay 1075 -p21,22,23,25,53 $target
foreach? usleep 1075000
foreach? end

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Interesting ports on www.insecure.org (205.217.153.53):
PORT      STATE      SERVICE
21/tcp     filtered  ftp

```

```

22/tcp open      ssh
23/tcp filtered telnet
25/tcp open      smtp
53/tcp open      domain

```

Nmap run completed -- 1 IP address (1 host up) scanned in 10.746 seconds

```

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Interesting ports on lists.insecure.org (205.217.153.54):
PORT      STATE      SERVICE
21/tcp     filtered  ftp
22/tcp     open       ssh
23/tcp     filtered  telnet
25/tcp     open       smtp
53/tcp     open       domain

```

Nmap run completed -- 1 IP address (1 host up) scanned in 10.781 seconds

```

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
PORT      STATE      SERVICE
21/tcp     filtered  ftp
22/tcp     open       ssh
23/tcp     filtered  telnet
25/tcp     open       smtp
53/tcp     open       domain

```

Nmap run completed -- 1 IP address (1 host up) scanned in 10.804 seconds

Unfortunately for port scanning enthusiasts, defeating Snort is not so simple. It has another method, known as *sliding time scale*. This method is similar to the fixed-window method just discussed, except that it increases the window whenever a new probe from a host is detected. An alarm is raised if scanner-sliding-threshold probes are detected during the window. The window starts at scanner-sliding-window seconds, and increases for each probe detected by the amount of time elapsed so far in the window times scanner-sliding-scale-factor. Those three variables default to 40 probes, 20 seconds, and a factor of 0.5 in snort.conf.

The sliding scale is rather insidious in the way it grows continually as new packets come in. The simplest (if slow) solution would be to send one probe every 20.1 seconds. This would evade both the default fixed and sliding scales. This could be done just as in Example 9-12, but using a higher value. You could speed this up by an order of magnitude by sending 14 packets really fast, waiting 20 seconds for the window to expire, then repeating with another 14 probes. You may be able to do this with a shell script controlling Nmap, but writing your own simple SYN scanning program for this custom job may be preferable.

### 9.5.2.2. Fragment packets

IP fragments can be a major problem for intrusion detection systems, particularly because the handling of oddities such as overlapping fragments and fragmentation assembly timeouts are ambiguous and differ substantially between platforms. So the IDS often has to guess at how the remote system will interpret a packet. Fragment assembly can also be resource intensive. For these reasons, many intrusion detection systems still do not support fragmentation very well. An Nmap scan will use tiny IP fragments if the `-f` is specified. Because some hosts do not handle

fragmented packets properly, run a sniffer like ethereal or tcpdump the first time you use this option to verify that packets leave your machine fragmented. Some overly helpful hosts will defragment the packets before they even leave the device.

### **9.5.2.3. Evade specific rules**

Most IDS vendors brag about how many alerts they support, but many (if not most) are easy to bypass. The most popular IDS among Nmap users is the open source Snort (<http://www.snort.org>). Example 9-13 shows all of the default rules in Snort 2.0.0 that reference Nmap.

#### **Example 9-13. Default Snort rules referencing Nmap**

```
felix~/src/snort-2.0.0/rules>grep -i nmap *
icmp.rules:alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING NMAP";
  dsize:0;itype: 8;reference:arachnids,162;classtype:attempted-recon;sid:469;rev:1;)
scan.rules:alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN nmap XMAS";
  flags:FPU; reference:arachnids,30; classtype:attempted-recon; sid:1228;rev:1;)
scan.rules:alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN nmap TCP";
  flags:A;ack:0; reference:arachnids,28; classtype:attempted-recon; sid:628;rev:1;)
scan.rules:alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN nmap fingerprint attempt";
  flags:SFP; reference:arachnids,05; classtype:attempted-recon; sid:629; rev:1;)
web-attacks.rules:alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
  (msg:"WEB-ATTACKS nmap command attempt"; flow:to_server,established;content:"nmap%20";
  nocase;sid:1361;classtype:web-application-attack; rev:4;)
```

Now let us look at these rules through the eyes of an attacker. The first rule looks for an ICMP ping packet without any payload (dsize:0). Simply specifying a non-zero --data\_length option, as discussed in Chapter 3, will defeat that rule. Or the user could specify a different type of ping scan entirely, such as TCP SYN ping.

The next rule searches for TCP packets with the FIN, PSH, and URG flags set (flags:FPU) and signals an Nmap XMAS scan alert. Adding the option --scanflags FINPSH to the XMAS scan flag will remove the URG flag. The scan will still work as expected, but the rule will fail to trigger.

The third rule in the list looks for TCP packets with the ACK bit set but an acknowledgment number of zero (flags:A;ack:0). Ancient versions of Nmap did this, but it was fixed in 1999 in response to the Snort rule.

Rule number four looks for TCP packets with the SYN, FIN, PSH, and URG flags set (flags:SFP). It then declares an Nmap OS Fingerprinting attempt. An attacker can avoid flagging this by omitting the -o flag. If he really wishes to do OS detection, that single test can be commented out in `osscan.cc`. The OS detection will still be quite accurate, but the IDS alert will not flag.

The final rule looks for people sending the string "nmap " to web servers. They are looking for attempts to execute commands through the web server. An attacker could defeat this by renaming Nmap, using a tab character instead of a space, or connecting with SSL encryption if available.

Of course there are other relevant rules that do not have Nmap in the name but could still be flagged by intrusive port scans. Advanced attackers install the IDS they are concerned with on their own network, then alter and test scans in advance to ensure that they do not trigger alarms.

Snort was only chosen for this example because its rules database is public and it is a fellow open source network security tool. Commercial IDSs suffer from similar issues.

#### **9.5.2.4. Avoid easily detected Nmap features**

Some features of Nmap are more conspicuous than others. In particular, version detection connects to many different services, which will often leave logs on those machines and set off alarms on intrusion detection systems. OS detection is also easy to spot by intrusion detection systems, because a few of the tests use rather unusual packets and packet sequences. The Snort rules shown in Example 9-13 demonstrate a typical Nmap OS detection signature.

One solution for pen-testers who wish to remain stealthy is to skip these conspicuous probes entirely. Service and OS detection are valuable, but not essential for a successful attack. They can also be used on a case-by-case basis against machines or ports that look interesting, rather than flooding the whole target network with them.

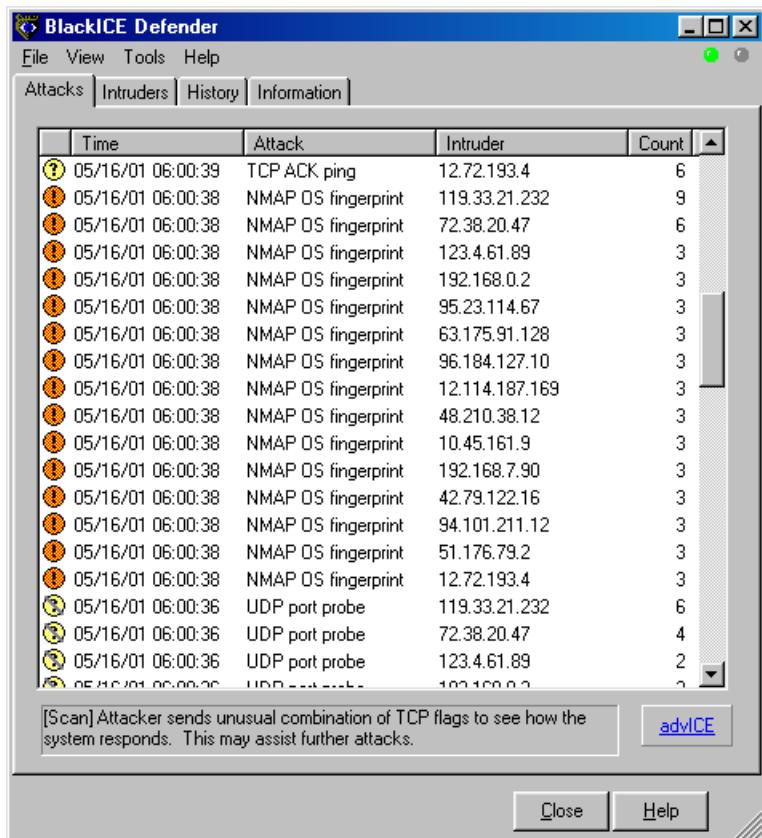
### **9.5.3. Misleading intrusion detection systems**

The previous section discussed using subtlety to avoid the watchful eye of intrusion detection systems. An alternative approach is to actively mislead or confuse the IDS with packet forgery. Nmap offers numerous options for effecting this.

#### **9.5.3.1. Decoys**

Street criminals know that one effective means for avoiding authorities after a crime is to melt into any nearby crowds. The cops may not be able to tell the purse snatcher from all of the innocent passersby. In the network realm, Nmap can construct a scan that appears to be coming from dozens of hosts across the world. The target will have trouble determining which host represents the attackers, and which ones are innocent decoys. While this can be defeated through router path tracing, response-dropping, and other "active" mechanisms, it is generally an extremely effective technique for hiding the scan source. Figure 9-2 shows a BlackICE report screen that is inundated with decoys. The administrator cannot complain to the providers for every ISP on the list. It would take a long time, and all but one of the hosts are innocent.

**Figure 9-2.** An attacker masked by dozens of decoys



Decoys are added with the `-D` option. The argument is a list of hosts, separated by commas. The string `ME` can be used as one of the decoys to represent where the true source host should appear in the scan order. Otherwise it will be a random position. Including `ME` in the 6th position or further in the list prevents some common port scan detectors from reporting the activity. For example, Solar Designer's excellent Scanlogd only reports the first five scan sources to avoid flooding its logs with decoys.

Note that the hosts used as decoys should be up and running. It would be pretty easy to determine which host is scanning if only one is actually up on the network. Using too many down decoys can also cause target ports to become temporarily unresponsive, due to a condition known as a SYN flood. Using IP addresses instead of names is advised to avoid appearing in the decoy networks' nameserver logs. The targets themselves should ideally be expressed by IP addresses too.

Decoys are used both in the initial ping scan (using ICMP, SYN, ACK, or whatever) and during the actual port scanning phase. Decoys are also used during remote OS detection. They are not used for DNS queries or service/version detection. Using too many decoys can slow a scan dramatically, and sometimes even make it less accurate. Many retail (dialup, cable modem, DSL, etc.) ISPs filter out most spoofed packets, though spoofed packets from the same network range as yours may get through. Do some tests first against some machine you control across the Internet, or you could even test this against 3rd party servers using IPID tricks similar to those discussed in Section 9.3.3.

### 9.5.3.2. Port scan spoofing

While a huge group of decoys is quite effective at hiding the true source of a port scan, the IDS alerts will make it obvious that someone is using decoys. A more subtle, but limited, approach is to spoof a port scan from a single address. Specify the `-s` followed by a source IP, and Nmap will launch the requested port scan from that given source. No useful Nmap results will be available, since the target will respond to the spoofed IP, which Nmap will not see. IDS alarms at the target will blame the spoofed source for the scan. You may have to specify `-e interfacename` to select the proper interface name (such as `eth0`, `ppp0`, etc.) for Nmap to send the spoofed packets through. This can be useful for framing innocent parties, casting doubt in the administrator's mind about the accuracy of his IDS, and denial of service attacks that will be discussed in Section 9.5.3.4.

### 9.5.3.3. Idlescan

Idlescan is a clever technique that allows for spoofing the source IP address, as discussed in the previous section, while still obtaining accurate TCP port scan results. This is done by abusing properties of the IP identification field as implemented by many systems. It is described in much more depth in Chapter 5.

### 9.5.3.4. DOS attacks against reactive systems

Many vendors are pushing what they call intrusion *prevention* systems. These are basically IDSs that can actively block traffic and reset established connections that are deemed malicious. These are usually inline on the network or host-based, for greater control over network activity. Other (non-inline) systems listen promiscuously and try to deal with suspicious connections by forging TCP RST packets. In addition to the traditional IPS vendors that try to block a wide range of suspicious activity, many popular small programs such as Port Sentry (<http://sourceforge.net/projects/sentrytools/>) are designed specifically to block port scanners.

While blocking port scanners may at first seem like a good idea, there are many problems with this approach. The most obvious one is that port scans are usually quite easy to forge, as previous sections have demonstrated. It is often easy for attackers to tell when this sort of software is in place, because they will not be able to connect to purportedly open ports after doing a port scan. They will try again from another system and successfully connect, confirming that the original IP was blocked. Attackers can then use the host spoofing techniques discussed previously (`-s` option) to cause the target host to block any systems the attacker desires. This may include important DNS servers, major web sites, software update archives, mail servers, and the like. It probably would not take long to annoy the legitimate administrator enough to disable reactive blocking. While most such products offer a whitelist option to prevent blocking certain important hosts, enumerating them all is extraordinarily difficult. Attackers can usually find a new commonly used host to block, annoying users until the admin determines the problem and adjusts the whitelist accordingly.

## 9.5.4. Exploiting intrusion detection systems

The most audacious way to subvert intrusion detection systems is to hack them. Many commercial and open source vendors have pitiful security records of product exploitability. Internet Security System's flagship RealSecure and BlackICE IDS products had a vulnerability which allowed the Witty worm to compromise more than ten thousand installations, then attempted to disable them by random filesystem corruption. Other IDS and firewall vendors such as Cisco, Checkpoint, Netgear, and Symantec have suffered serious remotely exploitable vulnerabilities as well. Open source sniffers have not done much better, with exploitable bugs found in Snort, Ethereal, TCPdump, fakebo,

and many others. Denial of service attacks that crash the IDS (often with a single packet) are even more common than these privilege escalation vulnerabilities. A crashed IDS will not detect any Nmap scans.

Given all of these vulnerabilities, exploiting the IDS may be the most viable way into the target network. A nice aspect of this approach is that you do not even have to find the IDS. Sending a rogue packet to any "protected" machine on the network is usually enough to trigger these IDS bugs.

### **9.5.5. Ignoring intrusion detection systems**

While advanced attackers will often employ IDS subversion techniques described in this chapter, the much more common novice attackers (script kiddies) rarely concern themselves with IDSs. Many companies do not even deploy an IDS, and those that do often have them misconfigured or pay little attention to the alerts. An Internet-facing IDS will see so many attacks from script kiddies and worms that a few Nmap scans to locate a vulnerable service are unlikely to raise any flags.

Even if such an attacker compromises the network, is detected by a monitored IDS, and then kicked out of the systems, that is a small loss. Hacking is often a numbers game for them, so losing one compromised network out of thousands is inconsequential. Such a well-patrolled network would have likely quickly noticed their planned usage (such as denial of service attacks, mass scanning, or spam sending) quickly and shut them down anyway. They want to compromise negligently administered and poorly monitored networks that will long-lasting nodes of criminal activity.

Being tracked down and prosecuted is rarely a concern of the IDS-ignoring set. They usually launch attacks from other compromised networks, which are often several globe-spanning hops away from their true location. Or they may use anonymous connectivity such as provided by some Internet cafes, school computer labs, or the prevalent open wireless access points. Throwaway dialup accounts are also commonly used. Even if they get kicked off, signing up again with another (or the same) provider takes only minutes. Many attackers come from Romania, China, South Korea, and other countries where prosecution is highly unlikely.

Internet worms are another class of attack that rarely bothers with IDS evasion. As with script kiddies, the brute force and shameless scanning of millions of IP addresses often leads to more compromises per hour than a careful, targeted approach that emphasizes stealth.

While most attacks make no effort at stealth, the fact that most intrusion detection systems are so easily subverted is a major concern. Skilled attackers are a small minority, but are often the greatest threat. Do not be lulled into complacency by the large number of alerts spewed from IDSs. They cannot detect everything, and often miss what is most important.

Even skilled hackers sometimes ignore IDS concerns for initial reconnaissance. They simply scan away from some untraceable IP address, hoping to blend in with all of the other attackers and probe traffic on the Internet. After analyzing the results, they may launch more careful, stealthy attacks from other systems.

## **9.6. Detecting packet forgery by firewall and intrusion detection systems**

Previous sections mentioned that some firewall and intrusion detection systems can be configured to forge packets as if they came from one of the protected systems behind the device. TCP RST packets are a frequent example. Load balancers, SSL accelerators, network address translation, and certain honeynets can also lead to confusing or inconsistent results. Understanding how Nmap interprets responses helps a great deal in piecing together complex

remote network topologies. When Nmap reports unusual or unexpected results, you can add the `--packet_trace` option to see the raw packets upon which Nmap based its conclusions. In perplexing situations, you may have to go even further and launch custom probes and analyze packets with other tools such as hping2 and ethereal. The goal is often to find inconsistencies that help you understand the actual network setup. The following sections describe several useful techniques for doing so. While most of these tests do not involve Nmap directly, they can be useful for interpreting unexpected Nmap results.

### 9.6.1. Look for TTL consistency

Firewalls, load balancers, NAT gateways, and similar devices are usually located one or more hops in front of the machines they are protecting. In this case, packets can be created with a TTL such that they reach the network device but not the end host. If a RST is received from such a probe, it must have been sent by the device.

During one informal assessment, I scanned the network of a large magazine publisher over the Internet. Almost every IP address showed port 113 closed. Suspecting RST forgery by a firewall, I dug a bit deeper. Because it contained open, closed, and filtered ports, I decided to focus on this host in particular<sup>1</sup>:

```
# nmap -sS -P0 -T4 -F mx.chi.example.com
Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Interesting ports on mx.chi.example.com (xx.yy.143.4):
(The 1216 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE
25/tcp    open  smtp
113/tcp   closed auth

Nmap run completed -- 1 IP address (1 host up) scanned in 53.196 seconds
```

Is port 113 really closed, or is the firewall spoofing RST packets? I counted the distance (in network hops) to ports 25 and 113 using the custom traceroute mode of the free hping2 utility, as shown in Example 9-14. I could have used the Nmap `--ttl` option to do this, but hping2 is designed for this exact purpose.

#### Example 9-14. Detection of closed and filtered TCP ports

```
# hping2 -t 5 --traceroute -p 25 -S mx.chi.example.com
[ combined with results from hping2 -i 1 --ttl \* -p 25 -S mx.chi.example.com ]
5->TTL 0 during transit from 64.159.2.97 (ae0-54.mp2.SanJose1.Level3.net)
6->TTL 0 during transit from 64.159.1.34 (so-3-0-0.mp2.Chicago1.Level3.net)
7->TTL 0 during transit from 200.247.10.170 (pos9-0.core1.Chicago1.level3.net)
8->TTL 0 during transit from 200.244.8.42 (gige6-0.ipcolo1.Chicago1.Level3.net)
9->TTL 0 during transit from XX.YY.73.205 (ge1-0.br1.ord.example.net)
10->TTL 0 during transit from XX.YY.228.247 (f0-0.bl.chi.example.com)
11->No response
12->TTL 0 during transit from XX.YY.143.130 (fw.chi.example.com)
13->46 bytes from XX.YY.143.4: flags=SA seq=0 ttl=52 id=48957 rtt=75.8 ms

# hping2 -t 5 --traceroute -p 113 -S mx.chi.example.com
[ results augmented again ]
5->TTL 0 during transit from 64.159.2.97 (ae0-54.mp2.SanJose1.Level3.net)
6->TTL 0 during transit from 64.159.1.34 (so-3-0-0.mp2.Chicago1.Level3.net)
7->TTL 0 during transit from 200.247.10.170 (pos9-0.core1.Chicago1.level3.net)
8->TTL 0 during transit from 200.244.8.42 (gige6-0.ipcolo1.Chicago1.Level3.net)
9->TTL 0 during transit from XX.YY.73.205 (ge1-0.br1.ord.example.net)
```

```
10->TTL 0 during transit from XX.YY.228.247 (f0-0.b1.chi.example.com)
11->Nothing
12->46 bytes from XX.YY.143.4: flags=RA seq=0 ttl=48 id=53414 rtt=75.0 ms
```

This custom traceroute shows that reaching open port 25 requires 13 hops. 12 hops away is a firewall in Chicago, helpfully named fw.chi.example.com. One would expect different ports on the same machine to be the same hop-distance away. Yet port 113 responds with a RST after only 12 hops. That RST is being forged by fw.chi.example.com. Since the firewall is known to forge port 113 responses, those packets should not be taken as an indicator that a host is available at a given IP address. I found available hosts by ping scanning the network again, using common probe types such as ICMP echo requests (-PE) and SYN packets to ports 22 and 80 (-PS22,80), but omitting any ping probes involving TCP port 113.

### **9.6.2. Look for IPID and sequence number consistency**

Every IP packet contains a 16-bit identification field that is used for defragmentation. It can also be exploited to gain a surprising amount of information on remote hosts. This includes port scanning using the Nmap Idle Scan technique, traffic estimation, host alias detection, and much more. It can also help to detect many network devices, such as load balancers. I once noticed strange OS detection results when scanning beta.search.microsoft.com. So I launched hping2 SYN probes against TCP port 80 to learn what was going on. Example 9-15 shows the results.

#### **Example 9-15. Testing IPID sequence number consistency**

```
hping2 -c 10 -i 1 -p 80 -S beta.search.microsoft.com.
HPING beta.search.microsoft.com. (eth0 207.46.197.115): S set, 40 headers
46 bytes from 207.46.197.115: flags=SA seq=0 ttl=56 id=57645 win=16616 rtt=21.2 ms
46 bytes from 207.46.197.115: flags=SA seq=1 ttl=56 id=57650 win=16616 rtt=21.4 ms
46 bytes from 207.46.197.115: flags=RA seq=2 ttl=56 id=18574 win=0 rtt=21.3 ms
46 bytes from 207.46.197.115: flags=RA seq=3 ttl=56 id=18587 win=0 rtt=21.1 ms
46 bytes from 207.46.197.115: flags=RA seq=4 ttl=56 id=18588 win=0 rtt=21.2 ms
46 bytes from 207.46.197.115: flags=SA seq=5 ttl=56 id=57741 win=16616 rtt=21.2 ms
46 bytes from 207.46.197.115: flags=RA seq=6 ttl=56 id=18589 win=0 rtt=21.2 ms
46 bytes from 207.46.197.115: flags=SA seq=7 ttl=56 id=57742 win=16616 rtt=21.7 ms
46 bytes from 207.46.197.115: flags=SA seq=8 ttl=56 id=57743 win=16616 rtt=21.6 ms
46 bytes from 207.46.197.115: flags=SA seq=9 ttl=56 id=57744 win=16616 rtt=21.3 ms
```

Looking at the sequence of IPID numbers (in bold), it is clear that there are really 2 machines sharing this IP address through some sort of load balancer. One has IPID sequences in the range of 57K, while the other is using 18K. Given this information, it is no wonder that Nmap had trouble settling on a single operating system guess. They may be running on very different systems.

Similar tests can be performed on other numeric fields, such as the TCP timestamp option or the initial sequence number returned by open ports.

### **9.6.3. The Bogus Checksum trick**

Another handy trick for determining whether an IDS or Firewall is spoofing response packets is to send probes with a bogus checksum. Essentially all end hosts check the checksum before further processing and will not respond to these corrupt packets. Firewalls, on the other hand, often omit this check. Packets returned from corrupt-checksum

probes can be assumed spoofed. This technique is further described in Phrack 60, article 12 (<http://www.phrack.org/phrack/60/p60-0x0c.txt>).

#### **9.6.4. Close Analysis of packet headers and contents**

It is surprising how many elements can differ in even a small TCP header. Refer to Chapter 8 for dozens of subtle details that can be indicative of a different OS. For example, different systems respond with different TCP options, RST packet text, type of service, etc. If there are several systems behind a load balancer, or the packets are being sent by firewall or intrusion detection systems, the packets will rarely match exactly.

#### **9.6.5. Unusual network uniformity**

When response packets are sent by a firewall, they are often more uniform than would be expected from clusters of individual machines. While scanning the large magazine company discussed in the previous TTL-checking section, I found that hundreds of sequential-IP machines responded with a RST to port 113. In a real cluster of machines, you would expect at least a couple to be out at a given time. Additionally, I was unable to elicit any other type of response from most of these addresses. This suspicious result led me to do the TTL tests which showed that fw.chi.example.com was actually spoofing the RST packets.

## **Notes**

1. Host names and IPs have been disguised slightly

# Chapter 10. Defenses against Nmap

## 10.1. Introduction

Chapter 9 discussed the myriad ways that Nmap (along with a few other open source security tools) can be used to slip through firewalls and outsmart intrusion detection systems. Now we look at the situation from the other side of the fence. How technology such as firewalls and IDSs can defend against Nmap. Possible defenses include blocking the probes, restricting information returned, slowing down the Nmap scan, and returning misleading information. The dangers of some defenses are covered as well. Obfuscating your network to the extent that attackers cannot understand what is going on is not a net win if your administrators no longer understand it either. Similarly, defensive software meant to confuse or block port scanners is not beneficial if it opens up more serious vulnerabilities itself. Many of the techniques described herein protect against active probes in general, not just those produced with Nmap.

## 10.2. Proactive Scanning

It is often said that the best defense is a good offense. An excellent way to defend against attackers is to think like them. Scan your networks regularly, and carefully analyze the output for vulnerabilities. Use crontab on UNIX, or the Task Scheduler on Windows, with a system such as NDiff or Nmap-report (see Section 1.2.3)

- \* Consider changing reference to section on automating scans and tracking differences between them, if and when available to notify you of any changes.

Proactive scanning provides the opportunity to find and fix vulnerabilities before attackers do. It also makes you better aware of what information attackers can obtain. When you have reviewed the results yourself for weaknesses and are comfortable with your security posture, port scanners become much less threatening. The people who are most paranoid about port scanners and employ the most defensive and detection software are often those with the least confidence in their network security. I do not want to dissuade anyone from using the techniques described throughout this chapter, but only to suggest that they first seek out and fix any existing network vulnerabilities. Fixing a hole is far more effective than trying to hide it. That approach is also less stressful than constantly worrying that attackers may find the vulnerabilities. Once known holes are patched and proactive scanning is in place, further defensive technology may be warranted to protect against zero-day exploits, internal threats, and any holes that your vulnerability analysis system may miss.

Remember that some poorly implemented and tested systems may react adversely to port scans, OS detection, or version detection. This is rarely a problem when scanning over the Internet, because machines that crash when scanned do not last long in the hostile Internet. Internal machines are often more fragile. When beginning a proactive scanning program, ensure that it is approved and communicated to affected parties in advance. Start with a relatively small part of the network and insure there are no problems, then take it further in stages. You may want to start with simple port scanning, then move on to OS detection or version detection later as desired.

## 10.3. Blocking and Slowing Nmap with Firewalls

One of the best defensive measures against scanning is a well-configured firewall. Rather than simply obfuscate the network configuration, as some techniques described later do, well-configured firewalls can effectively block many avenues of attack.

Any decent firewall book emphasizes this cardinal rule: deny by default. Rather than trying to block suspected malicious traffic, block everything first, then specifically override that to allow essential traffic. It is much easier to overlook blocking something malicious than to accidentally explicitly allow the same. Additionally, failing to block bad traffic may not be noticed until it is exploited by an attacker, while failing to allow legitimate traffic is usually quickly discovered by the affected users. And they will keep reminding you until it is fixed.

The two preceding reasons should be enough to convince anyone to go with deny-by-default, but there are other benefits as well. One is to slow down large scale reconnaissance from tools like Nmap. When an Nmap TCP SYN scan encounters a closed port, the target machine sends back a RST packet and that port status is determined in only one round-trip-time. That is under a quarter of a second even across the world from my webserver in California to an ISP in Moscow. If a firewall filters the port, on the other hand, Nmap has to wait for a worst-case timeout before giving up. Nmap then makes several retransmissions just in case the packet was dropped by some router due to overcapacity rather than by a firewall rule. In large-scale scans, the difference can be quite significant. For example, a 1660-port TCP SYN scan against a machine on my wireless network (**nmap -sS -T4 para**) takes only 5 seconds when all ports are open or closed. Filtering a dozen or so commonly exploited ports increases the scan time to 12 seconds. Moving to default-deny (filtering all ports except the 5 open ones) nearly triples the scan time to 33 seconds. A 28-second difference may not sound meaningful, but it can add up to extra days for large-scale scans.

Filtered ports are even more frustrating to attackers when the UDP protocol is used. When firewalling is not involved, virtually all systems respond with an ICMP port unreachable when Nmap probes a closed port. Open ports usually do not respond at all. So if a deny-by-default firewall drops a probe packet, Nmap cannot tell if the port is open or filtered. Retransmissions do not help here, as the port will never respond. Attackers must then resort to slower and much more conspicuous techniques such as Nmap version detection and SNMP community string brute forcing to make sense of the UDP ports.

To actually slow Nmap down, make sure the firewall is dropping the packets rather than responding with an ICMP error. Otherwise Nmap will run just as fast and accurately as if the ports were closed, though you still reap the benefit of blocking the probes. As an example of this distinction, the Linux iptables firewall offers the target actions DROP and REJECT. As the names imply, DROP does nothing beyond blocking the packet, while REJECT sends an error message back. The former is better for slowing down reconnaissance and is usually recommended, though REJECT can ease network trouble diagnosis by making it crystal clear that the firewall is blocking certain traffic.

Another tenet of firewalls is *defense in depth*. Even though ports are blocked by the firewall, make sure they are closed (no application is listening) anyway. Assume that a determined attacker will eventually breach the firewall. Even if they get through using a technique from Chapter 9, the individual machines should be locked down to present a strong defense. This leaves more room for mistakes, which everyone makes on occasion. Attackers will need to find weaknesses in both the firewall and individual machines. A port scanner is pretty impotent against ports that are both closed and filtered. Using private address space (such as with network address translation) and additional firewalls provide even more protection.

## 10.4. Detecting Nmap Scans

Some people believe that detecting port scans is a waste of time. They are so common that any organization connected to the Internet will be regularly scanned. Very few of these represent targeted attacks. Many are Internet worms endlessly pounding away seeking some Windows vulnerability or another. Some scans come from Internet research projects, others from curious or bored individuals exploring the Internet. I scanned tens of thousands of IPs seeking good examples and empirical data for this book. Other scans actually are malicious. Script kiddies regularly scan huge ranges for systems susceptible to their exploit du jour. While these folks have bad intentions, they are likely to move along on their own after finding no vulnerable services on your network. The biggest threat are

attackers specifically targeting your organization, though those represent such a small percentage of detected scans that they are extremely tough to distinguish. So many admins do not even bother recording port scans.

Other administrators take a different view. They contend that port scans are often precursors to attacks, and should at least be logged if not responded to. They often place detection systems on internal networks to reduce the flood of Internet port scan activity. The logs are sometimes analyzed for trends, or submitted to 3rd parties such as Dshield for world-wide correlation and analysis. Sometimes extensive logs and scary graphs measuring attacks are submitted to management to justify adequate budgets.

System logs alone are rarely sufficient for detecting port scans. Usually only scan types that establish full TCP connections are logged, while the default Nmap SYN scan sneaks through. Even full TCP connections are only logged if the particular application explicitly does so. Such error messages, when available, are often cryptic. However, a bunch of different services spouting error messages at the same time is a common indicator of scanning activity. Intrusive scans, particularly those using Nmap version detection, can often be detected by this means. But only if the administrators actually read the system logs regularly. The vast majority of log messages go forever unread. Log monitoring tools such as Logwatch (<http://www.logwatch.org>) and Swatch (<http://swatch.sourceforge.net/>) can certainly help, but the reality is that system logs are only marginally effective at detecting Nmap activity.

Special purpose port scan detectors are a more effective approach to detecting Nmap activity. Two common examples are PortSentry (<http://sourceforge.net/projects/sentrytools/>) and Scanlogd (<http://www.openwall.com/scanlogd/>). Scanlogd has been around since 1998 and was carefully designed for security. No vulnerabilities have been reported during its lifetime. PortSentry offers similar features, as well as a reactive capability that blocks the source IP of suspected scanners. Note that this reactive technique can be dangerous, as demonstrated in Section 10.5.6.

Despite being subject to threshold-based attacks discussed in Chapter 9, these port scan detection tools work pretty well. Yet the type of administrator who cares enough to keep tabs on port scans will also want to know about more serious attacks such as exploit attempts and installed backdoors. For this reason, intrusion detection systems that alert on a wide range of suspicious behavior are more popular than these special-purpose tools.

Many vendors now sell intrusion detection systems, but Nmap users gravitate to an open source lightweight IDS named Snort. It ranked as the third most popular security tool among a survey group of 1800 Nmap users.

\* *Note favorite tools appendix if I decide to add it.*

Like Nmap, Snort is improved by a global community of developers. It supports more than two thousand rules for detecting all sorts of suspicious activity, including port scans.

A properly installed and monitored IDS can be a tremendous security asset, but do not forget the risks discussed in Chapter 9. Snort has had multiple remotely exploitable vulnerabilities, and so have many of its commercial competitors. Additionally, a skilled attacker can defeat most IDS rules, so do not let your guard down. IDSs too often lead to a false sense of security.

## 10.5. Clever Trickery

Nmap, like other active probing tools, obtains its information by sending out packets to target systems and then trying to interpret and organize any responses into useful reports. Nmap must rely on information from systems and networks that may be downright hostile environments. Some administrators take offense at being scanned, and a small percentage try to confuse or slow Nmap with active measures beyond the firewall and IDS techniques discussed previously.

Many of these active response methods are quite clever. I would argue that many are too clever, causing more problems than they solve. One such problem is exploitability. Much of this custom active response software is just a

quick hack, written without careful security consideration. For example, an administrator friend of mine named Paul was quite proud of installing FakeBO on his machine. He laughed at the prospect of fooling script kiddies into thinking they found a Back Orifice infected machine to commandeer, when Paul was really just logging their attempts. The joke was on Paul when a FakeBO buffer overflow was discovered and an attacker used it to compromise his box and install a real backdoor.

The other major risk common to these technologies is displacement of time that is better spent elsewhere. Confusing attackers can be fun and gratifying, and in some cases even hampers attacks. But in the end, these techniques are mostly security by obscurity. That can still be beneficial, but is not as important as more resilient technologies such as firewalls and vulnerability patching. Advanced attackers will likely see through the obfuscation anyway, and the script kiddies and worms rarely bother with reconnaissance. The daily attempted ISS exploits against my Apache webserver are testament to that. These techniques should be considered only when you are already highly confident of your security posture. Too many people use them as a substitute to truly securing their networks.

### 10.5.1. Hiding Services on Obscure Ports

Occasionally administrators advocate running services on unusual ports to make it harder for attackers to find them. In particular, they note the frequency of single-port sweeps across their address space from attackers seeking out a vulnerable version of some software. Autonomous worms frequently do the same thing.

It is true that this sort of obfuscation may prevent some worms and script kiddies from finding services, but they are rarely more than a marginal threat to companies that quickly patch vulnerabilities. And companies who do not patch quickly will not be saved by this simple port obfuscation. Proponents often argue that even more skillful attackers will fall for this. Some have even posted to security lists that scanning all 65,536 TCP ports is inconceivable. They are wrong. Attackers can and do scan all TCP ports. In addition, techniques such as Nmap version detection make it easy to determine what service is listening on an unusual port. Example 10-1 shows such a scan. Notable is that it only takes 8 minutes, and this is from a slow residential aDSL line in another state. From a faster machine, the same scan takes only 3 minutes. If the default state had been filtered, the scan would have been slower but not unreasonably so. Even if a scan takes 10 or 20 minutes, an attacker does not have to sit around watching. A targeted attack against a company can easily be left overnight, and mass attackers may leave a scanner running for weeks, periodically downloading the latest data files.

#### Example 10-1. An all-tcp-port version scan

```
# nmap -sSV -T4 -O -p0-65535 apollo.sco.com

Starting nmap 3.50 ( http://www.insecure.org/nmap/ )
Interesting ports on apollo.sco.com (216.250.128.35):
(The 65524 ports scanned but not shown below are in state: closed)
PORT      STATE     SERVICE      VERSION
0/tcp      filtered  unknown
21/tcp     open      ftp          WU-FTPD 2.1WU(1)+SCO-2.6.1+-sec
22/tcp     open      ssh          SSH 1.2.22 (protocol 1.5)
199/tcp    open      smux?
457/tcp    open      http         NCSA httpd 1.3
615/tcp    open      http         NCSA httpd 1.5
1035/tcp   filtered unknown
1521/tcp   open      oracle-tns Oracle DB Listener 2.3.4.0.0 (for SCO System V/386)
13722/tcp  open      inetd        inetd (failed exec /usr/openv/netbackup/bin/bpjjava-msvc)
13782/tcp  open      inetd        inetd (failed exec /usr/openv/netbackup/bin/bpcd)
13783/tcp  open      inetd        inetd (failed exec /usr/openv/bin/vopied)
```

```

64206/tcp open    unknown
Device type: general purpose
Running: SCO UnixWare
OS details: SCO UnixWare 7.0.0 or OpenServer 5.0.4-5.0.6

Nmap run completed -- 1 IP address (1 host up) scanned in 501.897 seconds
#

```

The biggest downside to this approach is a major inconvenience to legitimate users. Some services, such as smtp and dns, almost always have to run on their well-known ports for practical reasons. Even for services such as http and ssh that can be more easily changed, doing so means that all users must remember an unusual port number such as 52,147 whenever they connect to the service. When there are several "hidden" services, it is particularly difficult to remember which is which. Using different ports on each machine becomes even more confusing, but standardizing on unusual port mappings across the organization reduces the purported benefit of this scheme. Attackers may notice that ssh is always at 52,147. The end result is that all-port Nmap scans against your servers may increase, as frustrated legitimate users try to find where essential services are hidden. Less savvy users may flood you with phone calls instead.

### 10.5.2. Port knocking

A technique called port knocking has recently become popular as a way to hide services from potential attackers. The method is well described on the front page of <http://www.portknocking.org/>:

Port knocking is a method of establishing a connection to a networked computer that has no open ports. Before a connection is established, ports are opened using a port knock sequence, which is a series of connection attempts to closed ports. A remote host generates and sends an authentic knock sequence in order to manipulate the server's firewall rules to open one or more specific ports. These manipulations are mediated by a port knock daemon, running on the server, which monitors the firewall log file for connection attempts that can be translated into authentic knock sequences. Once the desired ports are opened, the remote host can establish a connection and begin a session. Another knock sequence may be used to trigger the closing of the port.

This method is not brand new, but it exploded in popularity in 2003 when Martin Krzywinski coined the name port knocking, wrote an implementation, created the extensive web site, and wrote articles about it for Sys Admin and Linux Journal magazines. Port Knocking adds a second layer of protection to services, though authentication is usually weaker than that provided by primary services such as ssh. Implementations are usually subject to sniffing and replay attacks, and often suffer from brute force and denial of service threats as well.

The upside is a service concealment which is much stronger than the simple and ineffective obscure ports technique described previously. A port competently hidden through port knocking is nearly impossible to discover using active probes such as those sent by Nmap. On the other hand, sniffer-based systems such as intrusion detection systems and passive network mappers trivially detect this scheme.

Deciding whether to implement port knocking requires an analysis of the benefits and costs applicable to the proposed implementation. Service concealment is only beneficial for a small set of applications. The white-hat motivation is to prevent attackers from connecting to (and exploiting) vulnerable services, while still allowing connections from authorized users all over the world. If only certain IP addresses need to connect, firewall restrictions limiting connections to those specific IPs are usually a better approach. In an ideal world, applications would securely handle authentication themselves and there would be no need to hide them to prevent exploitation. Unfortunately, even security-conscious programs such as ssh have suffered numerous remotely exploitable

pre-authentication flaws. While these bugs should be fixed as soon as possible in any case, port knocking may provide an extra window of time before a new bug is exploited. After all, some ssh exploits spread underground long before official patches were available. Then when a bug is announced, even the most conscientious administrator may require several hours or days to learn about the bug, test the fix, and locate and patch all vulnerable instances. The response time of a home computer owner may be even longer. After all, the vast majority of computer users do not subscribe to Bugtraq.

The good guys are not the only ones who benefit from service concealment. It is at least as popular (if not more so) for gray hat and downright criminal uses. Many ISPs restrict users from running any server daemons such as web or ssh services. Customers could hide a personal sshd or web server (only for very limited use, as the public could not easily connect) using port knocking technology. Similarly, my friend Tom's employer only permitted connections from home using a Windows-only VPN client. Tom responded by setting up a port knocking system (before it was called that) which, upon receiving the appropriate probes, set up a reverse ssh tunnel from his work server back to his home Linux box. This allowed him to work from home with full access to the work network and without having to suffer the indignities of using Windows. It is worth re-iterating that the service provider in both the ISP and employer examples could have detected the subterfuge using a sniffer. Segueing into even darker uses, computer criminals frequently use techniques like these to hide backdoors in systems that they have compromised. Script kiddies may just leave a blatant ssh daemon or even raw root shell listening on some high port, vulnerable to detection by the next Nmap scan. More cautious attackers use concealment techniques including port knocking in their backdoors and rootkits.

While the service concealment provided by this system can be valuable, it comes with many limitations. Services intended for public use are inappropriate, since no one is going to install a special knock client just to visit your web site. In addition, publicizing the access instructions would defeat the system's primary purpose. Non-public service should usually be blocked by a firewall rather than shielded with port knocking. When a group of people need access, VPNs are often a better solution as they offer encryption and user-level access control. VPNs are also built to handle real-world networks, where packets can be dropped, duplicated, and re-ordered. A relatively simple probe using the Portknocking.Org implementation can require more than 30 port probes, all of which must arrive at the destination in order. For this many probes, you will need a special client. Using **telnet** or a web browser is too tedious. Additionally, all firewalls in the path must allow you to connect to these unusual ports. Given these restrictions and hassles, using a VPN may be just as convenient.

An additional risk is that port knocking implementations are still immature. The best-known one, written by Martin Krzywinski, warns on the download page that "this is a prototype and includes the bare minimum to get started. Do not use this for production environments." Also remember that proactive scanning to inventory your own network will be more difficult with programs such as this installed.

Do not let this long list of limitations dissuade you from even considering port knocking. It may be appropriate for specific circumstances, particularly those related to hidden backdoors or remote administration of a personal machine.

### **10.5.3. Honeypots and Honeynets**

An increasingly popular method for confusing attackers is to place bait systems on a network and monitor them for attacks. These are known as honeypots. Your author is a member of the Honeynet Project (<http://www.honeynet.org>), which installs networks of these for research purposes. Many corporations have deployed these systems for corporate security purposes, though doing so is risky. The extensive monitoring required makes them high-maintenance and there is always a risk that attackers will break in and use the machines to commit serious crimes. Lower maintenance solutions, such as Honeyd described in the next section, or even an IDS, may be more appropriate. In any case, Honeypots are designed to catch more invasive attacks than simple Nmap scans, so they are not discussed further.

### 10.5.4. OS Spoofing

Several programs have been developed specifically to trick Nmap OS detection. They manipulate the host operating system to support custom responses to Nmap probes. In this way, a Linux PC can be made to resemble an Apple LaserWriter printer or even a webcam. IP Personality (<http://ippersonality.sourceforge.net/>), released in 2000, is one of the most popular systems. It extends the Linux Netfilter framework to support these shenanigans. Unfortunately, it has not been updated since April 2002 and may not work on kernel versions beyond 2.4.18.

Tool availability alone does not make OS spoofing a good idea. One has to justify the effort somehow. The IP Personality FAQ avoids the question “Why would you need this?” by responding that “If you ask this, then you don’t”. Nevertheless, some people find it valuable enough to write and use these tools. One reason is that specific OS information makes it easier for attackers to infer vulnerabilities on your network, and also helps decide what sort of exploit to run. Of course the vulnerability itself is the real problem there, and should be fixed. Other people run this sort of tool because they are embarrassed about the OS they run, or they are extremely privacy conscious. If your operating system is in a legal gray area because some company is claiming IP infringement and filing suits against users, OS spoofing might protect against such a nuisance suit.

One serious problem with masking a host OS this way is that it can cause security and functionality problems. Nmap tests for several important security properties, such as TCP initial sequence number and IP identification number predictability. Emulating a different system, such as a printer, may require weakening these number sequences so that they are predictable and vulnerable to all the attacks that implies. The obscurity gained by spoofing your operating system fingerprint is not worth sacrificing valuable security mechanisms. This sort of spoofing can also cripple functionality. Many Nmap OS detection tests involve asking the system what TCP options are supported. Pretending not to support certain options such as timestamps and window scaling will remove the efficiency benefits of those options. Pretending to support unavailable options can be disasterous.

In Example 10-2, Nmap is fooled by IP Personality into believing a Linux box is really a Sega Dreamcast game console. It is from a paper entitled *A practical approach for defeating Nmap OS-Fingerprinting* (<http://voodoo.somoslopeor.com/papers/nmap.html>) by David Barroso Berrueta. That excellent paper includes far more examples, as well as detailed configuration instructions. It also describes many similar systems, with handy warnings such as “the code is not very stable. I loaded the module and in a few moments my Linux box got frozen.”

#### Example 10-2. Deceiving Nmap with IP Personality

```
# nmap -sS -O -oN nmap2.log 192.168.0.19

Interesting ports on 192.168.0.19:
(The 1597 ports scanned but not shown below are in state: closed)
Port      State       Service
22/tcp    open        ssh
25/tcp    open        smtp
80/tcp    open        http
143/tcp   open        imap2
Remote operating system guess: Sega Dreamcast
Nmap run completed -- 1 IP address (1 host up) scanned in 5.886 seconds
```

A newer and more popular program for operating system spoofing (among other features) is Honeyd (<http://www.honeyd.org>). It is actively maintained by author Niels Provos and offers several major benefits over IP Personality. One is that it is much easier to configure. Almost 100 configuration lines were required for the Dreamcast spoofing above. Honeyd, on the other hand, simply reads the Nmap OS detection database (`nmap-os-fingerprints`) and emulates any OS the user chooses. Honeyd also solves the security and functionality problems of OS spoofing by creating synthetic hosts for the emulation. You can ask Honeyd to take over

hundreds of unused IP addresses in an organization. It responds to probes sent to those IPs based on its configuration. This eliminates the security and functionality risks of trying to mask a host's own TCP stack. You are creating a bunch of synthetic hosts instead, so this does not help obscure the OS of existing hosts. The synthetic hosts basically constitute a low-maintenance honeynet that can be watched for attacks. It is mostly intended for research purposes, such as using the worldwide network of Honeyd installations to identify new worms and track spammer activity.

As with other techniques in this section, I recommend experimenting with OS spoofing only when completely satisfied by your security posture. Spoofing a single OS, or even adding hundreds of decoy Honeyd instances, is no substitute for patching vulnerable systems. Many attackers (and especially worms) do not even bother with OS detection before sending exploit code.

It is also worth noting that these systems are easy to detect by skilled attackers. It is extraordinarily hard to present a convincing facade, given all of application and tcp stack differences between operating systems. Nobody will believe that the system in Example 10-2 offering imap, smtp, and ssh is really a Dreamcast running its native OS. In addition, a bug in all versions up to 0.8 allowed for simple Honeyd identification with a single probe packet. There are also many TCP characteristics that Honeyd cannot yet handle. Those can be used to detect Honeyd, though Nmap does not automate this work. If Honeyd becomes widespread, detection functionality will likely be added to Nmap.

Deception programs such as Honeyd are just one reason that Nmap users should interpret Nmap results carefully and watch for inconsistencies, particularly when scanning networks that you do not control.

### **10.5.5. Tar pits**

Rather than trick attackers, some people aim for just slowing them down. Tar pits have long been popular methods for slowing Internet worms and spammers. Some administrators use TCP techniques such as zero-sized receive windows or slowly trickling data back byte by byte. LaBrea (<http://labrea.sourceforge.net/>) is a popular implementation of this. Others use applications-level techniques such as long delays before responding to each SMTP commands. While these are mostly used by anti-spammers, similar techniques can be used to slow Nmap scans. For example, limiting the rate of RST packets sent by closed ports can dramatically slow scanners down.

### **10.5.6. Reactive port scan detection**

We previously discussed scan detection using tools such as Scanlogd. Other tools go much further than that, and actually respond to the scans. Some people propose attacking back by launching exploits or denial of service attacks against the scan source. This is a terrible idea for many reasons. For one, scans are often forged. If the source address is accurate, it may be a previous victim that the attacker is using as a scapegoat. Or the scan may be part of an Internet research survey or come from a legitimate employee or customer. Even if the source address is a computer belonging to an actual attacker, striking back may disrupt innocent systems and routers along the path. It may also be illegal.

While the idea of attacking back is widely shunned in the security community, there is much more interest in responding to detected attacks by adjusting firewall rules to block the offending IP address. The idea is to prevent them from following up on the scan with an actual attack. There are several risks in this approach. One is that you show your hand. It will be obvious to attackers that they have been blocked, and most have plenty of other IP addresses they can use to continue probing. They will then know about your reactive system, and could escalate their own attacks. A more important problem is that scans are so easily forged. Chapter nine describes several methods for doing so. When an attacker notices the block, he may spoof scans from important systems, such as major web sites and DNS servers. A target network which then blocks those IPs will be committing a denial of service attack on itself. Restricting firewall blocks to scans that initiate a full TCP connection reduces the spoofing problem, but that fails to stop even the default Nmap SYN scan.

### **10.5.7. Escalating arms race**

While the primary focus of this book is on open source tools, a number of commercial vendors have introduced products that attempt to deceive Nmap. One example is the Cisco Security Agent. The evaluation guide claims the following protections against Nmap.

Network Mapper (Nmap) identifies which devices are present on a network and what operating system and services they are running by sending out a series of network probes. The presence of a device on the network and the ports it is running are both announced by its response to Nmap probes. The pattern of error messages returned identifies the operating system. Nmap is surprisingly accurate. It is frequently used at the initial stage of an attack or investigation to determine which systems might respond to an attacker's exploits.

Expected outcome of Nmap scan against Cisco Security Agent protected systems: Nmap is unable to identify the target operating system of systems running the default server or default desktop policies. Nmap scans appear to hang while its security tests timeout. Nmap scans against systems not protected by Cisco Security Agent report results very quickly

I am investigating how CSA works, and whether Nmap can automatically detect and adjust for it. Scanning technology is an arms race. Open source and commercial companies will continue to create products designed to slow down, block, or deceive Nmap and other tools. Meanwhile, Nmap continually improves, developing resiliency in the face of these challenges.

# Chapter 11. Nmap Output Formats

## 11.1. Introduction

A common problem with open source security tools is confusing and disorganized output. They often spew out many lines of irrelevant debugging information, forcing users to dig through pages of output trying to discern important results from the noise. Program authors often devote little effort to organizing and presenting results effectively. The output messages can be difficult to understand and poorly documented. This shouldn't be too surprising -- writing clever code to exploit some TCP/IP weakness is usually more gratifying than documentation or UI work. Since open source authors are rarely paid, they do what they enjoy.

At the risk of offending my friend Dan Kaminsky, I'll name his scanrand (<http://www.doxpara.com/>) port scanner as an example of a program that was clearly developed with far more emphasis on neat technical tricks than a user friendly UI. The sample output in Example 11-1 is from the Scanrand documentation page.

### Example 11-1. Scanrand output against a local network

```
bash-2.05a# scanrand 10.0.1.1-254:quick
UP:      10.0.1.38:80      [01]  0.003s
UP:      10.0.1.110:443    [01]  0.017s
UP:      10.0.1.254:443    [01]  0.021s
UP:      10.0.1.57:445     [01]  0.024s
UP:      10.0.1.59:445     [01]  0.024s
UP:      10.0.1.38:22      [01]  0.047s
UP:      10.0.1.110:22      [01]  0.058s
UP:      10.0.1.110:23      [01]  0.058s
UP:      10.0.1.254:22      [01]  0.077s
UP:      10.0.1.254:23      [01]  0.077s
UP:      10.0.1.25:135     [01]  0.088s
UP:      10.0.1.57:135     [01]  0.089s
UP:      10.0.1.59:135     [01]  0.090s
UP:      10.0.1.25:139     [01]  0.097s
UP:      10.0.1.27:139     [01]  0.098s
UP:      10.0.1.57:139     [01]  0.099s
UP:      10.0.1.59:139     [01]  0.099s
UP:      10.0.1.38:111     [01]  0.127s
UP:      10.0.1.57:1025    [01]  0.147s
UP:      10.0.1.59:1025    [01]  0.147s
UP:      10.0.1.57:5000    [01]  0.156s
UP:      10.0.1.59:5000    [01]  0.157s
UP:      10.0.1.53:111     [01]  0.182s
bash-2.05a#
```

While this does get the job done, it is difficult to interpret. Output is printed based on when the response was received, without any option for sorting the port numbers or even grouping all open ports on a target host together. A bunch of space is wasted near the beginning of each line and no summary of results is provided.

Nmap's output is also far from perfect, though I do try pretty hard to make it readable, well-organized, and flexible. Given the number of ways Nmap is used by people and other software, no single format can please everyone. So

Nmap offers several formats, including the interactive mode for humans to read directly and XML for easy parsing by software.

In addition to offering different output formats, Nmap offers options for controlling the verbosity of output as well as debugging messages. Output types may be sent to standard output or to named files, which Nmap can append to or clobber. Output files may also be used to resume aborted scans. This chapter includes full details on these options and every output format. chapter.

## 11.2. Command-line flags

As with almost all other Nmap capabilities, output behavior is controlled by command-line flags. These flags are grouped by category and described in the following sections.

### 11.2.1. Controlling output type

The most fundamental output control is designating the format(s) of output you would like. Nmap offers five types, as summarized in the following list and fully described in later sections.

#### Output formats supported by Nmap

##### Interactive output

This is the output that Nmap sends to the standard output stream (stdout) by default. So it has no special command-line option. Interactive mode caters to human users reading the results directly and it is characterized by a table of interesting ports that is shown in dozens of examples throughout this book.

##### Normal output (-oN)

This is very similar to interactive output, and is sent to the file you choose. It does differ from interactive output in several ways, which derive from the expectation that this output will be analyzed after the scan completes rather than interactively. So interactive output includes messages (depending on verbosity level specified with -v) such as scan completion time estimates and open port alerts. Normal output omits those as unnecessary once the scan completes and the final interesting ports table is printed. This output type prints the nmap command-line used and execution time and date on its first line.

##### XML output (-ox)

XML offers a stable format that is easily parsed by software. Free XML parsers are available for all major computer languages, including C/C++, Perl, Python, and Java. In almost all cases that a non-trivial application interfaces with Nmap, XML is the preferred format. This chapter also discusses how XML results can be transformed into other formats, such as HTML reports and database tables.

##### Grepable output (-oG)

This simple format is easy to manipulate on the command line with simple UNIX tools such as grep, awk, cut, and diff. Each host is listed on one line, with the tab, slash, and comma characters used to delimit output fields. While this can be handy for quickly grokking results, the XML format is preferred for more significant tasks as it is more stable and contains more information.

### sCRiPt KiDDi3 0utPU+ (-oS)

This format is provided for the 'l33t haXXorZ!'

While interactive output is the default and has no associated command-line options, the other four format options use the same syntax. They take one argument, which is the filename that results should be stored in. Multiple formats may be specified, but each format may only be specified once. For example, you may wish to save normal output for your own review while saving XML of the same scan for programmatic analysis. You might do this with the options `-oX myscan.xml -oN myscan.nmap`. While this chapter uses the simple names like `myscan.xml` for brevity, more descriptive names are generally recommended. The names chosen are a matter of personal preference, though I use long ones that incorporate the scan date and a word or two describing the scan, placed in a directory named after the company I'm scanning. As a convenience, you may specify `-oA basename` to store scan results in normal, XML, and grepable formats at once. They are stored in `basename.nmap`, `basename.xml`, and `basename.gnmap`, respectively. As with most programs, you can prefix the filenames with a directory path, such as `~/nmaplogs/foocorp/` on UNIX or `c:\hacking\sco` on Windows.

While these options save results to files, Nmap still prints interactive output to `stdout` as usual. For example, the command **nmap -oX myscan.xml target** prints XML to `myscan.xml` and fills standard output with the same interactive results it would have printed if `-oX` wasn't specified at all. You can change this by passing a hyphen character as the argument to one of the format types. This causes Nmap to deactivate interactive output, and instead print results in the format you specified to the standard output stream. So the command `nmap -oX - target` will send only XML output to `stdout`. Serious errors may still be printed to the normal error stream, `stderr`.

When you specify a filename to an output format flag such as `-oX` or `-oN`, that file is overwritten by default. If you prefer to keep the existing content of the file and append the new results, specify the `--append_output` option. All output filenames specified in that Nmap execution will then be appended to rather than clobbered.

Unlike some Nmap arguments, the space between the logfile option flag (such as `-oX`) and the filename or hyphen is mandatory. If you omit the flags and give arguments such as `-oG-` or `-oXscan.xml`, a backwards compatibility feature of Nmap will cause the creation of *normal format* output files named `G-` and `Xscan.xml` respectively.

## 11.2.2. Controlling verbosity of output

After deciding which format(s) you wish results to be saved in, you can decide how detailed those results should be. The first `-v` option enables verbosity with a level of one. Specify `-v` twice for a slightly greater effect. Verbosity levels greater than two aren't useful. Most changes only effect interactive output, and some also affect normal and script kiddie output. The other output types are meant to be processed by machines, so Nmap can give substantial detail by default in those formats without fatiguing a human user. However, there are a few changes in other modes where output size can be reduced substantially by omitting some detail. For example, a comment line in the grepable output that provides a list of all ports scanned is only printed in verbose mode because it can be quite long. The following list describes the major changes you get with at least one `-v` option.

### Scan completion time estimates

On scans that take more than a minute or two, you will see occasional updates like this in interactive output mode:

```
SYN Stealth Scan Timing: About 30.01% done; ETC: 16:04 (0:01:09 remaining)
```

New updates are given if the estimates change significantly. All port scanning techniques except for Idle scan and FTP bounce scan support completion time estimation, and so does version scanning.

#### Open ports reported when discovered

When verbosity is enabled, open ports are printed in interactive mode as they are discovered. They are still reported in the final interesting ports table as well. This allows users to begin investigating open ports before Nmap even completes. Open port alerts look like this:

```
Discovered open port 53/tcp on 205.217.153.55
```

#### Additional warnings

Nmap always prints warnings about obvious mistakes and critical problems. That standard is lowered when verbosity is enabled, allowing more warnings to be printed. There are dozens of these warnings, covering topics from targets experiencing excessive drops or extraordinarily long latency, to ports which respond to probes in unexpected ways. Rate limiting prevents these warnings from flooding the screen.

#### Additional notes

Nmap prints many extra informational notes when in verbose mode. For example, it prints out the time when each port scan is started along with the number of hosts and ports scanned. It later prints out a concluding line disclosing how long the scan took and briefly summarizing the results.

#### Extra OS detection information

With verbosity, results of the TCP ISN and IPID sequence number predictability tests are shown. These are done as a byproduct of OS detection. With verbosity greater than one, the actual OS detection fingerprint is shown in more cases.

#### Down hosts are printed in ping scan

During a ping scan with verbosity enabled, down hosts will be printed, rather than just up ones.

#### Birthday wishes

Nmap wishes itself a happy birthday when run in verbose mode on September 1.

The changes that are usually only useful until Nmap finishes and prints its report are only sent to interactive output mode. If you send normal output to a file with `-oN`, that file won't contain open port alerts or completion time estimates, though they are still printed to stdout. The assumption is that you will review the file when Nmap is done and don't want a lot of extra cruft, while you might watch Nmap's execution progress on standard output and care about runtime progress. If you really want everything printed to stdout sent to a file, use the output stream redirection provided by your shell (e.g. `nmap -v scanme.nmap.org > scanoutput.nmap`).

The dozens of small changes contingent on verbosity (mostly extra messages) are too numerous to cover here. They are also always subject to change. An effective way to see them all is to unpack the latest Nmap tarball and grep for them with a command such as `grep -A1 o.verbose *.cc`. Representative excerpts from the output are shown in Example 11-2.

**Example 11-2. Greping for verbosity conditionals**

```

felix~> grep -A1 o.verbose *.cc
idle_scan.cc: if (o.debugging || o.verbose) {
idle_scan.cc-   log_write(LOG_STDOUT, "Initiating Idlescan against %s\n", target->NameIP());
--
nmap.cc: if (o.verbose)
nmap.cc-   output_ports_to_machine_parseable_output(ports, o.TCPScan(), o.udpscan, o.ipprotscan);
--
nmap_rpc.cc: if (o.debugging || o.verbose)
nmap_rpc.cc-   gh_perror("recvfrom in get_rpc_results");
--
osscan.cc: if (o.verbose && openport != (unsigned long) -1)
osscan.cc-   log_write(LOG_STDOUT, "For OSScan assuming port %d is open, %d is closed...");
--
output.cc: if (o.verbose)
output.cc-   log_write(LOG_NORMAL|LOG_SKID|LOG_STDOUT, "IPID Sequence Generation: %s\n")

```

Example 11-3 puts all of this together by showing a normal scan followed by the same scan with verbosity enabled. Features such as the extra OS identification data, completion time estimates, open port alerts, and extra informational messages are easily identified in the latter output. This extra info is often helpful during interactive scanning, so I always specify `-v` when scanning a single machine unless I have a good reason not to.

**Example 11-3. A comparison of interactive output with and without verbosity enabled.**

```

# nmap -T4 -A -p- scanme.nmap.org

Starting nmap 3.77 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 65530 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.1p1 (protocol 1.99)
25/tcp    open  smtp     qmail smtpd
53/tcp    open  domain   ISC Bind 9.2.1
80/tcp    open  http     Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.4.20
Uptime 4.945 days (since Fri Nov 12 15:34:34 2004)

Nmap run completed -- 1 IP address (1 host up) scanned in 684.774 seconds

# nmap -v -T4 -A -p- scanme.nmap.org

Starting nmap 3.77 ( http://www.insecure.org/nmap/ )
Initiating SYN Stealth Scan against scanme.nmap.org (205.217.153.55) [65535 ports] at 3:22
Discovered open port 22/tcp on 205.217.153.55
Discovered open port 53/tcp on 205.217.153.55
Discovered open port 80/tcp on 205.217.153.55
Discovered open port 25/tcp on 205.217.153.55
SYN Stealth Scan Timing: About 4.58% done; ETC: 3:33 (0:10:24 remaining)
The SYN Stealth Scan took 679.55s to scan 65535 total ports.

```

```

Initiating service scan against 4 services on scanme.nmap.org (205.217.153.55) at 3:33
The service scan took 5.10s to scan 4 services on 1 host.
For OSScan assuming port 22 is open, 113 is closed, and neither are firewalled
Host scanme.nmap.org (205.217.153.55) appears to be up ... good.
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 65530 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.1pl1 (protocol 1.99)
25/tcp    open  smtp     qmail smtpd
53/tcp    open  domain   ISC Bind 9.2.1
80/tcp    open  http     Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.4.20
Uptime 4.916 days (since Fri Nov 12 15:34:34 2004)
TCP Sequence Prediction: Class=random positive increments
                           Difficulty=3048990 (Good luck!)
IPID Sequence Generation: All zeros

Nmap run completed -- 1 IP address (1 host up) scanned in 687.967 seconds

```

### 11.2.3. Enabling debugging output

When even verbose mode doesn't provide sufficient data for you, debugging is available to flood you with much more! As with the verbosity option (-v), debugging is enabled with a command-line flag (-d) and the debug level can be increased by specifying it multiple times. Alternatively, you can set a debug level by giving an argument to -d. For example, -d9 sets level nine. That is the highest effective level and will produce thousands of lines unless you run a very simple scan with very few ports and targets.

Debugging output is useful when a bug is suspected in Nmap, or if you are simply confused as to what Nmap is doing and why. As this feature is mostly intended for developers, debug lines aren't always self-explanatory. If you don't understand a line, your only recourse is to ignore it, look it up in the source code, or request help from the development list (nmap-dev). Other lines are self explanatory. The messages often become more obscure as the debug level is increased. Example 11-4 shows a few different debugging lines that resulted from a -d5 scan of Scanme.

#### Example 11-4. Some representative debugging lines

```

Timeout vals: srtt: 30256 rttvar: 30256 to: 151280 delta 15699
              ==> srtt: 32218 rttvar: 26616 to: 138682
RCVD (1.0710s) TCP 205.217.153.55:113 > 63.205.186.56:34538 RA ttl=241 id=0 ack=1188628258
**TIMING STATS**: IP, probes active/freshportsleft/outstanding/retranwait/onbench,
                  cwnd/ccthresh/delay, timeout/srtt/rttvar/
Groupstats (1/1 incomplete): 10/*/*/*/* 15.00/50/* 128805/49393/19853
205.217.153.55: 10/65515/15/5/0 15.00/50/0 125924/41340/21146
Discovered filtered port 38281/tcp on 205.217.153.55
Packet capture filter (device ppp0): dst host [ip] and
                                      (icmp or (tcp and src host 205.217.153.55))
The avg TCP TS HZ is: 100.624257

```

No full example is given here because debug logs are so long. In Example 11-3, a scan against Scanme used 14 lines of text without verbosity, and 28 with it. The same scan with `-d` instead of `-v` took 74 lines. With `-d2` it ballooned to 65,768 lines, and `-d5` output 242,650 lines! The debug option implicitly enables verbosity, so there is no need to specify them both.

Determining the best output level for a certain debug task is a matter of trial and error. I try a low level first to understand what is going on, then increase it as necessary. As I learn more, I may be able to better isolate the problem or question. I then try to simplify the command in order to offset some increased verbiage of the higher debug level.

Just as grep can be useful to identify the changes and levels associated with verbosity, it also helps with investigating debug output. I recommend running this command from the `nmap-VERSION` directory in the Nmap source tarball:

```
grep -A1 o.debugging *.cc
```

## 11.2.4. Enabling packet tracing

The `--packet_trace` option causes Nmap to print a summary of every packet it sends and receives. This can be extremely useful for debugging or understanding Nmap's behavior, as examples throughout this book demonstrate. Example 11-5 shows a simple ping scan of Scanme with packet tracing enabled.

### Example 11-5. Using `--packet_trace` to detail a ping scan of Scanme

```
# nmap --packet_trace -sP scanme.nmap.org

Starting nmap 3.77 ( http://www.insecure.org/nmap/ ) at 2004-11-18 15:59 PST
SENT (0.0110s) ICMP 63.205.186.56 > 205.217.153.55 Echo request (type=8/code=0)
    ttl=47 id=12401 ipLen=28
SENT (0.0130s) TCP 63.205.186.56:45425 > 205.217.153.55:80 A ttl=39 id=22911
    ipLen=40 seq=2336084894 win=4096 ack=826135454
RCVD (0.0420s) ICMP 205.217.153.55 > 63.205.186.56 Echo reply (type=0/code=0)
    ttl=50 id=56265 ipLen=28
Host scanme.nmap.org (205.217.153.55) appears to be up.
Nmap run completed -- 1 IP address (1 host up) scanned in 0.171 seconds
```

This Nmap execution shows three extra lines caused by packet tracing (each have been wrapped for readability). Each line contains several fields. The first is whether a packet is sent or received by Nmap, as abbreviated to `SENT` and `RCVD`. The next field is a time counter, providing the elapsed time since Nmap started. The time is in seconds, and in this case Nmap only required a tiny fraction of one. The next field is the protocol: TCP, UDP, or ICMP. Next comes the source and destination IP addresses, separated with a directional arrow. For TCP or UDP packets, each IP is followed by a colon and the source or destination port number.

The remainder of each line is protocol specific. As you can see, ICMP provides a human-readable type if available (`Echo request` in this case) followed by the ICMP type and code values. The ICMP packet logs end with the IP TTL, ID, and packet length field. TCP packets use a slightly different format after the destination IP and port number. First comes a list of characters representing the set TCP flags. The flag characters are SFRPUEC, which stand for SYN, FIN, RST, PSH, URG, ECE, and CWR, respectively. The latter two flags are part of TCP explicit congestion notification, described in RFC 3168 (<http://www.rfc-editor.org/rfc/rfc3168.txt>).

Because packet tracing can lead to thousands of output lines, it helps to limit scan intensity to the minimum that still serves your purpose. A scan of a single port on a single machine won't bury you in data, while the output of a

--packet\_trace scan of a whole network can be overwhelming. Packet tracing is automatically enabled when the debug level (-d) is at least three.

Sometimes --packet\_trace provides specialized data that Nmap never shows otherwise. For example, Example 11-5 shows ICMP and TCP ping packets sent to the target host. The target responds to the ICMP echo request, which can be valuable information that Nmap doesn't otherwise show. It is possible that the target host replied to the TCP packet as well -- Nmap stops listening once it receives one response to a ping scan since that is all it takes to determine that a host is online.

### 11.2.5. Resuming canceled scans

Some extensive Nmap runs take a very long time -- on the order of days. Such scans don't always run to completion. Restrictions may prevent Nmap from being run during working hours, the network could go down, the machine Nmap is running on might suffer a planned or unplanned reboot, or Nmap itself could crash. The admin running Nmap could cancel it for any other reason as well, by specifying control-C. Restarting the whole scan from the beginning may be undesirable. Fortunately, if normal (-oN) or grepable (-oG) logs were kept, the user can ask Nmap to resume scanning with the target it was working on when execution ceased. Simply specify the --resume option and pass the normal/grepable output file as its argument. No other arguments are permitted, as Nmap parses the output file to use the same ones specified previously. Simply call Nmap as **nmap --resume logfilename**. Resumption does not support the XML output format combining the two runs into one valid XML file would be difficult.

## 11.3. Interactive output

Interactive output is what Nmap prints to the stdout stream, which usually appears on the terminal window you executed Nmap from. In other circumstances, you might have redirected stdout to a file or another application such as Nessus or an Nmap GUI may be reading the results. If a larger application is interpreting the results rather than printing Nmap output directly to the user (as the Nmap X-Window frontend NmapFE does), then using the XML output discussed in Section 11.6 would be more appropriate.

This format has but one goal: to present results that will be valuable to a human reading over them. No effort is made to make these easily machine parseable or to maintain a stable format between Nmap versions. Better formats exist for these things. The toughest challenge is deciding which information is valuable enough to print. Omitting data that a user wants is a shame, though flooding the user with pages of mostly irrelevant output can be even worse. The verbosity, debugging, and packet tracing flags are available to shift this balance based on individual users' preferences.

This output format needs no extensive description here, as most Nmap examples in this book already show it. To understand Nmap's interactive output for a certain feature, see the section of this book dedicated to that feature. Typical examples of interactive output are given in Example 11-3.

## 11.4. Normal output (-oN)

Normal output is printed to a file when the -oN option is specified with a filename argument. It is similar to interactive output, except that notes which lose relevance once a scan completes are removed. It is assumed that the file will be read after Nmap completes, so estimated completion times and new open port alerts are redundant to the

actual completion time and the ordered port table. Since output may be saved a long while and reviewed among many other logs, Nmap prints the execution time, command-line arguments, and Nmap version number on the first line. A similar line at the end of a scan divulges final timing and a host count. Those two lines begin with a pound character to identify them as comments. If your application must parse normal output rather than XML/Grepable formats, ensure that it ignores comments that it doesn't recognize rather than treating them as an error and aborting. Example 11-6 is a typical example of normal output. Note that `-oN -` was used to prevent interactive output and send normal output straight to stdout.

#### **Example 11-6. A typical example of normal output**

```
# nmap -T4 -A -p- -oN - scanme.nmap.org
# nmap 3.77 scan initiated Sun Nov 21 7:55:07 2004 as: nmap -T4 -A -p- -oN - scanme.nmap.org
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 65530 ports scanned but not shown below are in state: filtered)
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh      OpenSSH 3.1p1 (protocol 1.99)
25/tcp    open     smtp     qmail smtplib
53/tcp    open     domain   ISC Bind 9.2.1
80/tcp    open     http     Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)
113/tcp   closed   auth
Device type: general purpose
Running: Linux 2.4.x|2.5.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.4.20
Uptime 9.105 days (since Fri Nov 12 5:34:59 2004)

# Nmap run completed at Sun Nov 21 8:06:07 2004 -- 1 IP address (1 host up) scanned in 660.397 seconds
```

## **11.5. \$crIpT kLddI3 OuTPut (-oS)**

Script kiddie output is like interactive output, except that it is post-processed to better suit the 'l33t HaXXorZ! They previously looked down on Nmap due to its consistent capitalization and spelling. It is best understood by example, as given in Example 11-7.

#### **Example 11-7. A typical example of \$crIpT KiDDi3 OuTPut**

```
# nmap -T4 -A -oS - scanme.nmap.org

$TArTIng nmap 3.77 ( Http://wWw.!nS3cur3.0rG/nmap/ )
|nter3st|ng poRtz on $canm3.nmap.org (205.217.153.55):
(ThE 1658 porTz scannEd but not sh0wn below ar3 in $tat3: f|lTerEd)
P0rT      $TATE    $3RV1cE v3R$ION
22/tcp    0p3n    Ssh      0p3n$$H 3.1p1 (pr0tocol 1.99)
25/tcp    0p3n    $Mtp    Qmail smTPd
53/tcp    open     d0maIn  1SC bind 9.2.1
80/tCp   0p3n    http    4pacH3 httpd 2.0.39 ((Unlx) mOd_p3rl/1.99_07-dEv P3Rl/v5.6.1)
113/tcp   CLO$eD aUth
dEv|Ce typ3: g3nEral pUrp0$e
RUnNIng: L|nux 2.4.x|2.5.X
oS dEtalz: LInux 2.4.0 - 2.5.20, L!nux 2.4.18 - 2.4.20
uptIme 9.113 Dayz (sinc3 Fr1 Nov 12 15:34:59 2004)
```

```
Nmap rUn completeD -- 1 IP addre$z (1 h0$T up) $cann3d !n 27.119 $3cONds
```

Some humor-impaired people take this option far too seriously, and scold me for catering to script kiddies. It is simply a joke *making fun* of the script kiddies. They don't actually use this mode, as far as I know.

## 11.6. XML output (-oX)

XML, the *extensible markup language*, has its share of critics as well as plenty of zealous proponents. I was long in the former group, and only grudgingly incorporated XML into Nmap after volunteers performed most of the work. Since then, I have learned to appreciate the power and flexibility that XML offers, and even wrote this book in the DocBook XML format. I strongly recommend that programmers interact with Nmap through the XML interface rather than trying to parse the normal, interactive, or grepable output. That format includes more information than the others and is extensible enough that new features can be added without breaking existing programs that use it. It can be parsed by standard XML parsers, which are available for all popular programming languages, usually for free. Editors, validators, transformation systems, and many other applications already know how to handle the format. Normal and interactive output, on the other hand, are custom to Nmap and subject to regular changes as I strive for a clearer presentation to end users. Grepable output is also Nmap-specific and tougher to extend than XML. It is considered deprecated, and many Nmap features such as MAC address detection are not presented in this output format.

An example of Nmap XML output is shown in Example 11-8. Whitespace has been adjusted for readability. In this case, XML was sent to stdout thanks to the `-oX -` construct. Some programs executing Nmap opt to read the output that way, while others specify that output be sent to a filename and then they read that file after Nmap completes.

### Example 11-8. An example of Nmap XML output

```
# nmap -T4 -A -oX - -p1-1024 scanme.nmap.org
<?xml version="1.0" ?>
<!-- nmap 3.78 scan initiated Fri Dec 10 21:40:13 2004 as:
   nmap -T4 -A -oX - -p1-1024 scanme.nmap.org -->
<nmaprun scanner="nmap" args="nmap -T4 -A -oX - -p1-1024 scanme.nmap.org"
   start="1102743613" startstr="Fri Dec 10 21:40:13 2004"
   version="3.78" xmloutputversion="1.01">
<scaninfo type="syn" protocol="tcp" numservices="1024" services="1-1024" />
<verbose level="0" />
<debugging level="0" />
<host><status state="up" />
<address addr="205.217.153.55" addrtype="ipv4" />
<hostnames><hostname name="scanme.nmap.org" type="PTR" /></hostnames>
<ports><extraports state="filtered" count="1019" />
<port protocol="tcp" portid="22"><state state="open" />
   <service name="ssh" product="OpenSSH" version="3.1p1"
      extrainfo="protocol 1.99" method="probed" conf="10" />
</port>
<port protocol="tcp" portid="25"><state state="open" />
   <service name="smtp" product="qmail smtpd" method="probed" conf="10" />
</port>
<port protocol="tcp" portid="53"><state state="open" />
```

```

<service name="domain" product="ISC Bind" version="9.2.1" method="probed"
    conf="10" />
</port>
<port protocol="tcp" portid="80"><state state="open" />
    <service name="http" product="Apache httpd" version="2.0.39"
        extrainfo="(Unix) mod_perl/1.99_07-dev" method="probed" conf="10" />
</port>
<port protocol="tcp" portid="113"><state state="closed" />
    <service name="auth" method="table" conf="3" />
</port>
</ports>
<os>
    <portused state="open" proto="tcp" portid="22" />
    <portused state="closed" proto="tcp" portid="113" />
    <osclass type="general purpose" vendor="Linux" osfamily="Linux" osgen="2.4.X" accuracy="100" />
    <osclass type="general purpose" vendor="Linux" osfamily="Linux" osgen="2.5.X" accuracy="100" />
    <osmatch name="Linux 2.4.0 - 2.5.20" accuracy="100" />
    <osmatch name="Linux 2.4.18 - 2.4.20" accuracy="100" />
</os>
<uptime seconds="813079" lastboot="Fri Nov 12 15:35:00 2004" />
<tcpsequence index="1972182" class="random positive increments" difficulty="Good luck!"
    values="E2E6D835,E32B1CB7,E3203691,E3740715,E36B40C8,E33B1621" />
<ipidsequence class="All zeros" values="0,0,0,0,0,0" />
<tcptssequence class="100HZ" values="4D8A8C7,4D8A8D3,4D8A8DF,4D8A8EB,4D8A8F7,4D8A903" />
</host>
<runstats>
    <finished time="1102743614" timestr="Fri Dec 10 21:40:14 2004" />
    <hosts up="1" down="0" total="1" />
    <!-- Nmap run completed at Fri Dec 10 21:40:14 2004;
        1 IP address (1 host up) scanned in 21.142 seconds -->
</runstats>
</nmaprun>

```

Another advantage of XML is that its verbose nature makes it easier to read and understand than other formats. Readers familiar with Nmap in general can likely understand most of the XML output in Example 11-8 without further documentation. The grepable output format, on the other hand, is tough to decipher without its own reference guide.

There are a few aspects of the example XML output which may not be self-explanatory. For example, look at the two `port` elements in Example 11-9

### Example 11-9. Nmap XML port elements

```

<port protocol="tcp" portid="22"><state state="open" />
    <service name="ssh" product="OpenSSH" version="3.1p1"
        extrainfo="protocol 1.99" method="probed" conf="10" />
</port>
<port protocol="tcp" portid="113"><state state="closed" />
    <service name="auth" method="table" conf="3" />
</port>

```

The port protocol, id (port number), state, and service name are the same as would be shown in the interactive output port table. The service product, version, and extrainfo come from version detection and are combined together into one field of the interactive output port table. The `method` and `conf` attributes aren't present in any other output types. The method can be `table`, meaning the service name was simply looked up in `nmap-services` based on the port number and protocol, or it can be `probed`, meaning that it was determined through the version detection system. The `conf` attribute measures the confidence Nmap has that the service name is correct. The values range from one (least confident) to ten. Nmap only has a confidence level of three for ports determined by table lookup, while it is highly confident (level 10) that port 22 of Example 11-9 is ssh, because Nmap connected to the port and found a server exhibiting the ssh protocol.

One other aspect that some users find confusing is that the attributes `nmaprun/start` and `finished/end` hold timestamps given in UNIX time, the number of seconds January 1, 1970. This is often easier for programs to handle. For the convenience of human readers, versions 3.78 and newer include the equivalent calendar time written out in the attributes `nmaprun/startstr` and `finished/endstr`.

\* *If anyone finds other portions of the XML output confusing, let me know and I can cover them here.*

Nmap includes a document type definition (DTD) which allows XML parsers to validate Nmap XML output. While it is primarily intended for programmatic use, it can also help humans interpret Nmap XML output. The DTD defines the legal elements of the format, and often enumerates the attributes and values they can take on. It is reproduced in Appendix A.

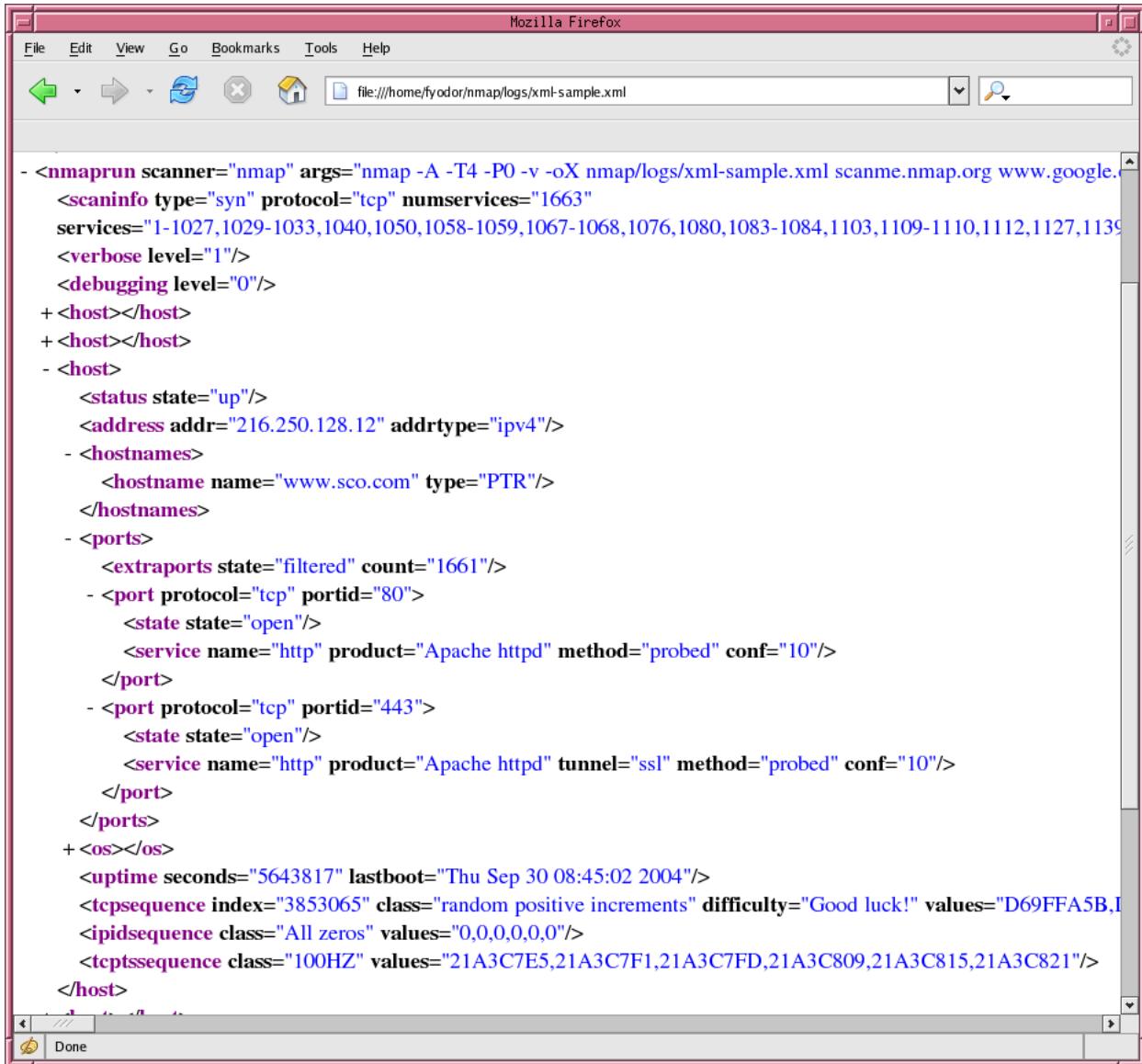
### 11.6.1. Using XML Output

The Nmap XML format can be used in many powerful ways, though few users actually take any advantage of it. I believe this is due to inexperience of many users with XML, combined with a lack of practical, solution-oriented documentation on using the Nmap XML format. This chapter provides several practical examples, including Section 11.7, Section 11.8, and Section 11.9.

A key advantage of XML is that you do not need to write your own parser as you do for specialized Nmap output types such as grepable and interactive output. Any general XML parser should do. The XML parser that people are most familiar with is the one in your web browser. Both IE and Mozilla/Firefox include capable parsers that can be used to view Nmap XML data. Using them is as simple as typing the XML filename or URL into the address bar. A document tree-view is shown, allowing you to expand and reduce elements as desired. It also provides syntax highlighting to quickly recognize key elements. If you know you'll be reading Nmap output, saving normal or interactive output as well as XML is advisable as most people find them the easiest to read and interpret. But if you only have XML output because you lost or didn't create the other forms, or because you are debugging a program that uses the XML, then reading the XML in a web browser is often preferable to using a text editor. Figure 11-1 shows Firefox rendering a tree view of Nmap XML.

\* *TODO: I may need to change this when I insert XSLT stylesheets into Nmap XML output. When that happens, you will get a pretty, rendered view automatically. Will need to change text after the figure then too.*

**Figure 11-1. Reading XML in a web browser**



Similarly, spreadsheet programs, including Microsoft Excel, are often able to import Nmap XML data directly for viewing.

A major problem with browsing Nmap XML logs directly through a web browser or spreadsheet is that the logs are treated in a generic way, just like any other XML file. The browser doesn't understand the relative importance of elements, nor how to organize the data for a more useful presentation. With the help of a stylesheet specific to Nmap, the logs can be rendered in a much more useful fashion. This is demonstrated in Section 11.9.

## 11.7. Manipulating XML output with Perl

Generic XML parsers are available for all popular programming languages, often for free. Examples are the libxml C library and the Apache Xerces parser for Java and C++ (with Perl and COM bindings). While these parsers are sufficient for handling Nmap XML output, developers have created custom modules for several languages which can make the task of interoperating with Nmap XML even easier.

The language with the best custom Nmap XML support is Perl. Max Schubert (affectionately known as Perldork) has created a module named `Nmap::Scanner` (<http://sourceforge.net/projects/nmap-scanner/>) and Anthony Persaud created one called `Nmap::Parser` (<http://www.nmapparser.com>). These two modules have many similarities: they can execute Nmap themselves or read from an output file, are well documented, come with numerous example scripts, are part of the Comprehensive Perl Archive Network (CPAN), and are popular with users. They each offer both a callback based parser for interpreting data as Nmap runs as well as an all-at-once parser for obtaining a fully parsed document once Nmap finishes executing. Their API is a bit different, as `Nmap::Scanner` relies on typesafe classes while `Nmap::Parser` relies on lighter-weight native Perl arrays. I recommend looking at each to decide which best meets your needs and preferences.

Example 11-10 is a simple demonstration of `Nmap::Parser`. It comes from the documentation (which contains many other examples) and performs a quick scan, then prints overall scan statistics as well as information on each available target host. Notice how readable it is compared to scripts using other Nmap output formats that are dominated by parsing logic and regular expressions. Even people with poor Perl skills could use this as a starting point to create simple programs to automate their Nmap scanning needs.

### Example 11-10. `Nmap::Parser` sample code

```
use Nmap::Parser;

#PARSING
my $np = new Nmap::Parser;

$nmap_exe = '/usr/bin/nmap';
$np->parsescan($nmap_exe,'-sT -p1-1023', @ips);

#or

$np->parsefile('nmap_output.xml') #using filenames

#GETTING SCAN INFORMATION

print "Scan Information:\n";
$si = $np->get_scaninfo();
#get scan information by calling methods
print
'Number of services scanned: '.$si->num_of_services()."\\n",
'Start Time: '.$si->start_time()."\\n",
'Scan Types: ',(join ' ', $si->scan_types())."\n";

#GETTING HOST INFORMATION

print "Hosts scanned:\\n";
for my $host_obj ($np->get_host_objects()){
    print
```

```
'Hostname  : '.$host_obj->hostname()."\n",
'Address   : '.$host_obj->ipv4_addr()."\n",
'OS match  : '.$host_obj->os_match()."\\n",
'Open Ports: '(join ',', $host_obj->tcp_ports('open'))."\n";
    #... you get the idea...
}

#frees memory - helpful when dealing with memory intensive scripts
$np->clean();
```

For comparison, Example 11-11 is a sample Perl script using Nmap::Scanner from its documentation. This one uses an event-driven callback approach, registering the functions `scan_started` and `port_found` to print real-time alerts when a host is found up and when each open port is discovered on the host.

### Example 11-11. Nmap::Scanner sample code

```
my $scanner = new Nmap::Scanner;
$scanner->register_scan_started_event(\&scan_started);
$scanner->register_port_found_event(\&port_found);
$scanner->scan(-ss -p 1-1024 -O --max-rtt-timeout 200 somehost.org.net.it);

sub scan_started {
    my $self      = shift;
    my $host      = shift;

    my $hostname = $host->name();
    my $addresses = join( , , map {$_->address()} $host->addresses());
    my $status   = $host->status();

    print "$hostname ($addresses) is $status\\n";
}

sub port_found {
    my $self      = shift;
    my $host      = shift;
    my $port      = shift;

    my $name = $host->name();
    my $addresses = join( , , map {$_->addr()} $host->addresses());

    print "On host $name ($addresses), found ",
        $port->state()," port ",
        join( /,$port->protocol(),$port->portid()), "\\n";
}
```

## 11.8. Output to a database

A common desire is to output Nmap results to a database for easier queries and tracking. This allows users from an individual penetration tester to an international enterprise to store all of their scan results and easily compare them. The enterprise might run large scans daily and schedule queries to mail administrators of newly open ports or available machines. The penetration tester might learn of a new vulnerability and search all of his old scan results for the affected application so that he can warn the relevant clients. Researchers may scan millions of IP addresses and keep the results in a database for easy real-time queries.

While these goals are laudable, Nmap offers no direct database output functionality. Not only are there too many different database types for me to support them all, but user's needs vary so dramatically that no single database schema is suitable. The needs of the enterprise, pen-tester, and researcher all call for different table structures.

For projects large enough to require a database, I recommend deciding on an optimal DB schema first, then writing a simple program or script to import Nmap XML data appropriately. Such scripts often take only minutes, thanks to the wide availability of XML parsers and database access modules. Perl often makes a good choice, as it offers a powerful database abstraction layer and also custom Nmap XML support. Section 11.7 shows how easily Perl scripts can make use of Nmap XML data.

Another option is to use a custom Nmap database support patch. The most popular of these is nmap-sql (<http://sourceforge.net/projects/nmssql>), which adds MySQL logging functionality into Nmap itself. The downsides are that it currently only supports the MySQL database and it must be frequently ported to new Nmap versions. An XML-based approach, on the other hand, is less likely to break when new Nmap versions are released.

## 11.9. Creating HTML reports

\* *TODO: I need to add this section once I finish deciding what to do about adding XSLT stylesheet to default XML output.*

## 11.10. Grepable output (-oG)

This output format is covered last because it is deprecated. The XML output format is far more powerful, and is nearly as convenient for experienced users. XML is a standard for which dozens of excellent parsers are available, while grepable output is my own simple hack. XML is extensible to support new Nmap features as they are released, while I often must omit those features from grepable output for lack of a place to put them.

Nevertheless, grepable output is still quite popular. It is a simple format that lists each host on one line and can be trivially searched and parsed with standard UNIX tools such as grep, awk, cut, sed, diff, and Perl. Even I usually use it for one-off tests done at the command line. Finding all the hosts with the ssh port open or that are running Solaris takes only a simple grep to identify the hosts, piped to an awk or cut command to print the desired fields. One grepable output aficionado is MadHat ([madhat@unspecific.com](mailto:madhat@unspecific.com)), who contributed to this section.

Example 11-12 shows a typical example of grepable output. Normally each host takes only one line, but I split this entry into seven lines to fit on the page. There are also three lines starting with a hash prompt (not counting the Nmap command line). Those are comments describing when Nmap started, the command line options used, and completion time and statistics. One of the comment lines enumerates the port numbers that were scanned. I shortened it to avoid wasting dozens of lines. That particular comment is only printed in verbose (-v) mode. Increasing the verbosity level beyond one -v will not further change the grepable output. The times and dates have been replaced with [time] to reduce line length.

**Example 11-12. A typical example of grepable output**

```
# nmap -oG - -T4 -A scanme.nmap.org
# nmap 3.77 scan initiated [time] as: nmap -oG - -T4 -A scanme.nmap.org
# Ports scanned: TCP(1663;1-1027,1029-1033,1040,...,65301) UDP(0;) PROTOCOLS(0;)
Host: 205.217.153.55 (scanme.nmap.org)
  Ports: 22/open/tcp//ssh//OpenSSH 3.1p1 (protocol 1.99)/,
          25/open/tcp//smtp//qmail smtpd/, 53/open/tcp//domain//ISC Bind 9.2.1/,
          80/open/tcp//http//Apache httpd 2.0.39 ((Unix) mod_perl|1.99_07-dev Perl|v5.6.1)/,
          113/closed/tcp//auth/// Ignored State: filtered (1658)
          OS: Linux 2.4.0 - 2.5.20|Linux 2.4.18 - 2.4.20 Seq Index: 3004446
          IPID Seq: All zeros
# Nmap run completed at [time] -- 1 IP address (1 host up) scanned in 27.177 seconds
```

The command-line here requested that grepable output be sent to standard output with the `-oG` argument to `-oG`. Aggressive timing (`-T4`) as well as OS and version detection (`-A`) were requested. The comment lines are self-explanatory, leaving the meat of grepable output in the `Host` line. Had I scanned more hosts, each of the available ones would have its own `Host` line.

**11.10.1. Grepable output fields**

The host line is split into fields, each of which consist of a field name followed by a colon and space, then the field content. The fields are separated by tab characters (ASCII number 9, '\t'). Example 11-12 shows six fields: Host, Ports, Ignored State, OS, Seq Index, and IPID. A Status section is included in list (`-sL`) and ping (`-sP`) scans, and a Protocols section is included in IP protocol (`-sO`) scans. The exact fields given depend on Nmap options used. For example, OS detection triggers the OS, Seq Index, and IPID fields. Because they are tab delimited, you might split up the fields with a Perl line such as:

```
@fields = split("\t", $host_line);
```

In the case of Example 11-12, the array `@fields` would contain six members. `$fields[0]` would contain “`Host : 205.217.153.55 (scanme.nmap.org)`”, and `$fields[1]` would contain the long Ports field. Scripts that parse grepable output should ignore fields they don’t recognize, as new fields may be added to support Nmap enhancements.

The eight possible fields are described in the following sections.

**11.10.1.1. Host field**

**Example:** Host: 205.217.153.55 (scanme.nmap.org)

The Host field always comes first and is included no matter what Nmap options are chosen. The contents are the IP address (an IPv6 address if `-6` was specified), a space, and then the reverse DNS name in parenthesis. If no reverse name is available, the parenthesis will be empty.

**11.10.1.2. Ports field**

**Example:** Ports: 111/open/tcp//rpcbind (rpcbind V2)/(rpcbind:100000\*2-2)/2 (rpc #100000)/, 113/closed/tcp//auth///

The Ports field is by far the most complex, as can be seen in Example 11-12. It includes entries for every interesting port (the ones which would be included in the port table in normal Nmap output). The port entries are separated with a comma and a space character. Each port entry consists of seven subfields, separated by a forward slash (/). The

subfields are: port number, state, protocol, owner, service, SunRPC info, and version info. Some subfields may be empty, particularly for basic port scans without OS or version detection. The consecutive slashes in Example 11-12 reveal empty subfields. In Perl, you might split them up as so:

```
($port, $state, $protocol, $owner, $service, $rpc_info, $version) = split('/', $ports);
```

Alternatively, you could grab the information from the command line using commands such as these:

```
cut -d/ -f<fieldnumbers>
awk -F/ '{print $<fieldnumber>}';
```

Certain subfields can contain a slash in other output modes. For example, an SSL-enabled web server would show up as `ssl/http` and the version info might contain strings such as `mod_ssl/2.8.12`. Since a slash is the subfield delimiter, this would screw up parsing. To avoid this problem, slashes are changed into the pipe character (`|`) when they would appear anywhere in the Port field.

Parsers should be written to allow more than seven slash-delimited subfields and to simply ignore the extras because future Nmap enhancements may call for new ones. The following list describes each of the seven currently defined Port subfields.

#### Port number

This is simply the numeric TCP or UDP port number.

#### State

The same port state which would appear in the normal output port table is shown here.

#### Protocol

This is `tcp` or `udp`.

#### Owner

Specifies the username that the remote service is running under if ident scan (`-I`) was requested and succeeded.

#### Service

The service name, as obtained from an `nmap-services` lookup, or (more reliably) through version detection (`-sv`) if it was requested and succeeded. With version detection enabled, compound entries such as `ssl|http` and entries with a trailing question mark may be seen. The meaning is the same as for normal output, as discussed in Chapter 7.

#### SunRPC info

If version detection (`-sv`) or RPC scan (`-sR`) were requested and the port was found to use the SunRPC protocol, the RPC program number and accepted version numbers are included here. A typical example is `"(rpcbind:100000*2-2)"`. The data is always returned inside parenthesis. It starts with the program name, then a colon and the program number, then an asterisk followed by the low and high supported version numbers separated by a hyphen. So in this example, `rpcbind` (program number 100,000) is listening on the port for `rpcbind` version 2 requests.

## Version info

If version detection is requested and succeeds, the results are provided here in the same format used in interactive output. For SunRPC ports, the RPC data is printed here too. The format for RPC results in this column is <low version number>-<high version number> (rpc #<rpc program number>). When only one version number is supported, it is printed by itself rather than as a range. A port which shows (rpcbind:100000\*2-2) in the SunRPC info subfield would show 2 (rpc #100000) in the version info subfield.

### 11.10.1.3. Protocols field

**Example:** Protocols: 1/open|icmp/, 2/open|filtered/igmp/

The IP protocol scan (-sO) has a Protocols field rather than Ports. Its contents are quite similar to the Ports field, but it has only three subfields rather than seven. They are delimited with slashes, just as with the Ports field. Any slashes that would appear in a subfield are changed into pipes (|), also as done in the Ports field. The subfields are protocol number, state, and protocol name. These correspond to the three fields shown in interactive output for a protocol scan. An example of IP protocol scan grepable output is shown in Example 11-13. The Host line is wrapped for readability.

#### Example 11-13. Grepable output for IP protocol scan

```
# nmap -v -oG - -sO localhost
# nmap 3.75 scan initiated [time] as: nmap -oG - -sO -v localhost
# Ports scanned: TCP(0;) UDP(0;) PROTOCOLS(256;0-255)
Host: 127.0.0.1 (felix) Protocols: 1/open|filtered/icmp/, 2/open|filtered/igmp/,
                                6/open|filtered/tcp/, 17/open|filtered/udp/,
                                255/open|filtered// Ignored State: closed (251)
# Nmap run completed at [time] -- 1 IP address (1 host up) scanned in 1.340 seconds
```

### 11.10.1.4. Ignored State field

**Example:** Ignored State: filtered (1658)

To save space, Nmap may omit ports in one non-open state from the list in the Ports field. Nmap does this in interactive output too. Regular Nmap users are familiar with the lines such as “The 1658 ports scanned but not shown below are in state: filtered”. For grepable mode, that state is given in the Ignored State field. Following the state name is a space, then in parenthesis is the number of ports found in that state.

### 11.10.1.5. OS field

**Example:** OS: Linux 2.4.0 - 2.5.20

Any perfect OS matches are listed here. If there are multiple matches, they are separated by a pipe character as shown in Example 11-12. Only the free-text descriptions are provided. Grepable mode does not provide the vendor, OS family, and device type classification shown in other output modes.

### 11.10.1.6. Seq Index field

**Example:** Seq Index: 3004446

This number is an estimate of the difficulty of performing TCP initial sequence number sequence prediction attacks against the remote host. These are also known as blind spoofing attacks, and they allow an attacker to forge a full TCP connection to a remote host as if it was coming from some other IP address. This can always help an attacker hide his or her tracks, and it can lead to privilege escalation against services such as rlogin that commonly grant extra privileges to trusted IP addresses. The seq index value is only available when OS detection (-O) is requested and succeeds in probing for this. It is reported in interactive output when verbosity (-v) is requested. More details on the computation and meaning of this value are provided in Chapter 8.

### 11.10.1.7. IPID field

**Example:** IPID Seq: All zeros

This simply describes the remote host's IPID generation algorithm. It is only available when OS detection (-O) is requested and succeeds in probing for it. Interactive mode reports this as well, and it is discussed in Chapter 8.

### 11.10.1.8. Status field

**Example:** Status: Up

Ping and list scans contain only two fields in grepable mode: Host and Status. Status describes the target host as either Up, Down, Smurf, or Unknown. List scan always categorizes targets as Unknown because it does not perform any tests. Ping scan lists a host as up if it responds to at least one ping probe, down if no responses are received, and smurf if ping probes sent to the target resulted in one or more responses from other hosts. In the special case of a Smurf status, the number of unique hosts responding to the ping probes is provided in parenthesis. A format example is: "Status: Smurf (72 responses)". Down hosts are only shown when verbosity is enabled with -v. Example 11-14 demonstrates a ping scan of 100 random hosts, while Example 11-15 demonstrates a list scan of five hosts.

#### Example 11-14. Ping scan grepable output

```
# nmap -sP -oG - -iR 100
# nmap 3.75 scan initiated [time] as: nmap -sP -oG - -iR 100
Host: 67.101.77.102 (h-67-101-77-102.nycmny83.covad.net)           Status: Up
Host: 219.93.164.197 () Status: Up
Host: 222.113.158.200 ()           Status: Up
Host: 66.130.155.190 (modemcable190.155-130-66.mc.videotron.ca) Status: Up
# Nmap run completed at [time] -- 100 IP addresses (4 hosts up) scanned in 13.226 seconds
```

#### Example 11-15. List scan grepable output

```
# nmap -sL -oG - -iR 5
# nmap 3.75 scan initiated [time] as: nmap -sL -oG - -iR 5
Host: 199.223.2.1 ()     Status: Unknown
Host: 191.222.112.87 () Status: Unknown
Host: 62.23.21.157 (host.157.21.23.62.rev.coltfrance.com)           Status: Unknown
Host: 138.217.47.127 (CPE-138-217-47-127.vic.bigpond.net.au)         Status: Unknown
Host: 8.118.0.91 ()       Status: Unknown
# Nmap run completed at [time] -- 5 IP addresses (0 hosts up) scanned in 1.797 seconds
```

## 11.10.2. Parsing grepable output on the command line

Grepable output really shines when you want to gather information quickly without the overhead of writing a script to parse XML output. Example 11-16 shows a typical example of this. The goal is to find all hosts on a class C sized network with port 80 open. Nmap is told to scan just that port of each host (skipping the ping stage) and to output a grepable report to stdout. The results are piped to a trivial awk command which finds lines containing /open/ and outputs fields two and three for each matching line. Those fields are the IP address and hostname (or empty parenthesis if the hostname is unavailable).

### Example 11-16. Parsing grepable output on the command line

```
> nmap -p80 -P0 -oG - 10.1.1.0/24 | awk '/open/{print $2 " " $3}'  
10.1.1.72 (userA.corp.foocompany.biz)  
10.1.1.73 (userB.corp.foocompany.biz)  
10.1.1.75 (userC.corp.foocompany.biz)  
10.1.1.149 (admin.corp.foocompany.biz)  
10.1.1.152 (printer.corp.foocompany.biz)  
10.1.1.160 (10-1-1-160.foocompany.biz)  
10.1.1.161 (10-1-1-161.foocompany.biz)  
10.1.1.201 (10-1-1-201.foocompany.biz)  
10.1.1.254 (10-1-1-254.foocompany.biz)
```

# Chapter 12. Understanding and Customizing Nmap Data Files

## 12.1. Introduction

Nmap relies for port scanning and other operations on six data files, all of which have names beginning with nmap-. One example is `nmap-services`, a registry of port names to their corresponding port number and protocol. The others, which this chapter describes one by one, are `nmap-service-probes` (version detection probe database), `nmap-rpc` (SunRPC program name to number database for direct RPC scanning), `nmap-os-fingerprints` (OS detection database), `nmap-mac-prefixes` (ethernet MAC address prefix (OUI) to vendor lookup table), and `nmap-protocols` (list of IP protocols for protocol scan). The source distribution installs these files in `/usr/local/share/nmap/` and the official Linux RPMs put them in `/usr/share/nmap/`. Other distributions may install them elsewhere.

The latest versions of these files are kept at <http://www.insecure.org/nmap/data/>, though it is strongly recommended that users upgrade to the most recent Nmap version rather than grabbing newer data files a la carte. There are no guarantees that newer files will work with older versions of Nmap (though they almost always do), and the resulting Frankenstein versions of Nmap can confuse the operating system and service fingerprint submission process.

Most users never change the data files, but it can be handy for advanced users who might want to add a version fingerprint or port assignment for a custom daemon running at their company. This section provides a description of each file and how they are commonly changed. The general mechanism for replacing Nmap data files with custom versions is then discussed. A couple of the files don't relate to port scanning directly, but they are all discussed here for convenience.

## 12.2. `nmap-services`

The `nmap-services` file is a registry of port names to their corresponding number and protocol. Most lines have a comment as well. Nmap ignores the comments, but users sometimes grep for them in the file when Nmap reports an open service of a type that the user does not recognize. Example 12-1 shows a typical excerpt from the file.

**Example 12-1. Excerpt from `nmap-services`**

```
qotd      17/tcp    # Quote of the Day
qotd      17/udp    # Quote of the Day
msp       18/tcp    # Message Send Protocol
msp       18/udp    # Message Send Protocol
chargen   19/tcp    # ttyst source Character Generator
chargen   19/udp    # ttyst source Character Generator
ftp-data  20/tcp    # File Transfer [Default Data]
ftp-data  20/udp    # File Transfer [Default Data]
ftp       21/tcp    # File Transfer [Control]
ftp       21/udp    # File Transfer [Control]
ssh       22/tcp    # Secure Shell Login
ssh       22/udp    # Secure Shell Login
telnet   23/tcp    #
telnet   23/udp    #
```

```

priv-mail      24/tcp      # any private mail system
priv-mail      24/udp      # any private mail system
smtp          25/tcp      # Simple Mail Transfer
smtp          25/udp      # Simple Mail Transfer

```

This file was originally based off the IANA assigned ports list at <http://www.iana.org/assignments/port-numbers>, though many other ports have been added over the years. The IANA does not track trojans, worms and the like, yet discovering them is important for many Nmap users.

This excerpt shows that UDP ports are often registered for tcp-only services such as ssh and ftp. This was inherited from the IANA, who tend to always register services for both protocols. Because Nmap scans ports listed in `nmap-services` by default, this aspect slows Nmap down by bloating the port list size. The `nmap-services` list will be cleaned up eventually to remove these redundant entries.

The grammar of this file is pretty simple. There are two whitespace-separated columns. The first is the service name or abbreviation, as seen in the `SERVICE` column of Nmap output. The second column gives the port number and protocol, separated by a slash. That syntax is seen in the `PORT` column of Nmap output. Nmap disregards anything beyond the second column, but most lines continue with whitespace then and a pound ('#') character, followed by a comment. Lines may be blank or contain just a pound character followed by comments.

Astute readers notice the similarity in structure between `nmap-services` and `/etc/services` (usually found at `c:\winnt\system\drivers\etc\services` on Windows). This is no coincidence. The format was kept to allow systems administrators to copy in any custom entries from their own `/etc/services`, or even to substitute their own version of that file entirely. The `/etc/services` format allows a third column providing alias names for a service. Nmap allows (but ignores) these in `nmap-services`.

Admins sometimes change this file to reflect custom services running on their network. For example, an online services company I once consulted for had dozens of different custom daemons running on high-numbered ports. Adding these port numbers to `nmap-services` ensures that they are scanned by default. If `-p1-65535` is used to scan all ports, the open ports will show up anyway. Adding them to the file is still helpful because Nmap will then print the proper names rather than unknown. Services specific to a single organization should generally stay in their own `nmap-services`, but other port registrations can benefit everyone. If you find that the default port for a major worm, trojan, filesharing application, or other service is missing from the latest `nmap-services`, please send it to me (`fyodor@insecure.org`) for inclusion in the next release. This helps all users while preventing you from having to maintain and update your own custom version of `nmap-services`.

Similarly, a certain registered port may be frequently wrong for a certain organization. `nmap-services` can only handle one service name per port number and protocol combination, yet sometimes several different types of applications end up using the same default port number. In that case, I try to choose the most popular one for `nmap-services`. Organizations which commonly use another service on such a port number may change the file accordingly.

Another common customization is to strip `nmap-services` down to only the most common, essential services for an organization. Then the Nmap `-F` option will scan only those ports and be much faster than with the original file. The file should normally be placed in a custom location accessible with the `--datadir` option rather than where Nmap will use it by default. Section 12.8 provides advice for customizing these files, including ways to prevent Nmap upgrades from wiping out your modified versions.

### 12.3. nmap-service-probes

This file contains the probes that the Nmap service/version detection system (`-sv` or `-A` options) uses during port

interrogation to determine what program is listening on a port. Example 12-2 offers a typical excerpt.

#### **Example 12-2. Excerpt from nmap-service-probes**

```
#####
# DNS Server status request: http://www.crynw.r.com/crynw/rfc1035/rfc1035.html
Probe UDP DNSStatusRequest q|\0\0\x10\0\0\0\0\0\0\0\0|
ports 53,135
match domain m|^00x90x04000000000000|
# This one below came from 2 tested Windows XP boxes
match msrpc m|^x04x060000x100000000000|
[...]
#####
# DNS Server status request: http://www.crynw.r.com/crynw/rfc1035/rfc1035.html
Probe UDP Help q|help\r\n\r\n|
ports 7,13,37
match chargen m|@ABCDEFGHIJKLMNPQRSTUVWXYZ|
match echo m|^help\r\n\r\n$|
match time m|^[\xc0-\xc5]...$|
```

The grammar of this file is fully described in Chapter 7. While `nmap-service-probes` is more complex than `nmap-services`, the benefits of improving it can also be greater. Nmap can be taught to actually recognize a company's custom services, rather than simply guessed based on `nmap-services` port registration.

Additionally, some admins have been using version detection for tasks well beyond its original intended purpose. A short probe can cause Nmap to print the title of web pages, recognize worm-infected machines, locate open proxies, and more. A recipe describing how to do this can be found in Section 7.9.

## **12.4. nmap-rpc**

As with `nmap-services`, `nmap-rpc` simply maps numbers to names. In this case, SunRPC program numbers are mapped to the program name which uses them. Example 12-3 offers a typical excerpt.

#### **Example 12-3. Excerpt from nmap-rpc**

```
rpcbind      100000  portmap sunrpc rpcbind
rstatd       100001  rstat rup perfmeter rstat_svc
rusersd      100002  rusers
nfs          100003  nfsprog nfsd
ypserv        100004  ypprog
mountd       100005  mount showmount
rpc.operd    100080  opermsg      # Sun Online-Backup
# DMFE/DAWS (Defense Automated Warning System)
#
GqsrV       200034  gqsrV
Ppt          200035  ppt
Pmt          200036  pmt
```

Nmap only cares about the first two whitespace-separated columns -- the program name and number. It doesn't look at any aliases or comments that may appear beyond that. Blank lines and those starting with pound comments are permitted. This format is the same as used by `/etc/rpc` on UNIX, so admins may use that file instead if they desire.

`nmap-rpc` is only used by the RPC grinding feature of Nmap version descriptions. That feature is covered in Section 7.5.1.

Users rarely change `nmap-rpc`. When they do, it is usually to add a custom service or a public one that is missing from the latest `nmap-rpc`. In the latter case, please send a note to me at [fyodor@insecure.org](mailto:fyodor@insecure.org) so that I can add it to the next version. As with `nmap-services`, some admins strip the file down, removing obscure RPC programs to save scan time. The same warning applies: specify your stripped `nmap-rpc` with the `--datadir` option rather than installing it where it will be used implicitly.

## 12.5. nmap-os-fingerprints

This file contains extensive data on how hundreds of different systems respond to specialized TCP and UDP queries. The data is grouped into more than a thousand structures, known as OS Fingerprints, that each contain response data for a known class of systems. When remote OS detection is requested with the `-o` option, responses received from the target system are compared with the `nmap-os-fingerprints` database. If a match is found, the corresponding description and classification likely describe the target OS as well. Example 12-4 is a typical excerpt, showing a couple fingerprints from the file.

### Example 12-4. Excerpt from `nmap-os-fingerprints`

```
Fingerprint Sega Dreamcast game console
Class Sega | embedded || game console
TSeq(Class=TD%gcd=<780%SI=<14)
T1 (DF=N%W=1D4C%ACK=S++%Flags=AS%Ops=M)
T2 (Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
T3 (Resp=Y%DF=N%W=1D4C%ACK=S++%Flags=AS%Ops=M)
T4 (DF=N%W=0%ACK=S%Flags=R%Ops=)
T5 (DF=N%W=0%ACK=S%Flags=AR%Ops=)
T6 (DF=N%W=0%ACK=S%Flags=R%Ops=)
T7 (DF=N%W=0%ACK=S++%Flags=AR%Ops=)
PU(Resp=N)

Fingerprint Linux 2.6.0 (x86)
Class Linux | Linux | 2.6.X | general purpose
TSeq(Class=RI%gcd=<6%SI=<269E81A&>62D97%IPID=Z%TS=1000HZ)
T1 (DF=Y%W=7FFF%ACK=S++%Flags=AS%Ops=MNNTNW)
T2 (Resp=N)
T3 (Resp=Y%DF=Y%W=7FFF%ACK=S++%Flags=AS%Ops=MNNTNW)
T4 (DF=Y%W=0%ACK=O%Flags=R%Ops=)
T5 (DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
T6 (DF=Y%W=0%ACK=O%Flags=R%Ops=)
T7 (DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
PU(DF=N%TOS=D0%IPLen=164%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)
```

The process of OS fingerprinting, as well as the format of this file, are fully described in Chapter 8.

`nmap-os-fingerprints` is rarely changed by users because removing fingerprints offers few advantages and creating a new fingerprint to add is a moderately complex process. When Nmap finds an unrecognized machine that appears suitable for inclusion in the DB, it prints out a fingerprint and a URL where the user may submit it for incorporation into future versions of Nmap. Some users tweak the fingerprint names if a match is not quite right (for example Linux 2.6.9 is reported as “Linux 2.6.5 - 2.6.8”). Please also notify me of such problems -- Chapter 8

describes how to do so. Global changes help everyone, and prevent you from having to maintain your own fork of the file.

## **12.6. nmap-mac-prefixes**

Users rarely modify this file, which maps MAC address prefixes to vendor names. Read on for the complete treatment.

Ethernet devices, which have become the dominant network interface type, are each programmed with a unique 42-bit identifier known as a MAC address. This address is placed in ethernet headers to identify which machine on a local network sent a packet, and which machine the packet is destined for. Humans usually represent it as a hex string, such as 00:60:1D:38:32:90.

To assure that MAC addresses are unique in a world with thousands of vendors, the IEEE assigns an Organizationally Unique Identifier (OUI) to each company manufacturing ethernet devices. The company must use its own OUI for the first three bytes of MAC addresses for equipment it produces. For example, the OUI of 00:60:1D:38:32:90 is 00601D. It can choose the remaining three bytes however it wishes, as long as they are unique. A counter is the simple approach. Companies that assign all 24 million possible values can obtain more OUIs. `nmap-mac-prefixes` maps each assigned OUI to the name of the vendor that sells them. Example 12-5 is a typical excerpt.

### **Example 12-5. Excerpt from `nmap-mac-prefixes`**

```
006017 Tokimec
006018 Stellar ONE
006019 Roche Diagnostics
00601A Keithley Instruments
00601B Mesa Electronics
00601C Telxon
00601D Lucent Technologies
00601E Softlab
00601F Stallion Technologies
006020 Pivotal Networking
006021 DSC
006022 Vicom Systems
006023 Pericom Semiconductor
006024 Gradient Technologies
006025 Active Imaging PLC
006026 Viking Components
```

The first value is the 3-byte OUI as 6 hex digits. It is followed by the company name. This file is created, using a simple perl script, from the complete list of OUIs available from <http://standards.ieee.org/regauth/oui/oui.txt>. The IEEE also offers an OUI FAQ at <http://standards.ieee.org/faqs/OUI.html>.

Nmap can determine the MAC address of hosts on a local ethernet LAN by reading the headers off the wire. It uses this table to look up and report the manufacturer name based on the OUI. This can be useful for roughly identifying the type of machine you are dealing with. A device with a Cisco, Hewlett Packard, or Sun OUI probably identifies a router, printer, or SPARCstation, respectively. Example 12-5 shows that the device at 00:60:1D:38:32:90 was made by Lucent. It is in fact the Lucent Orinoco wireless card in my laptop.

## 12.7. nmap-protocols

This file maps the 1-byte IP Protocol number in the IP header into the corresponding protocol name. Example 12-6 is a typical excerpt.

### Example 12-6. Excerpt from nmap-protocols

```

hopopt      0    HOPOPT      # IPv6 Hop-by-Hop Option
icmp        1    ICMP       # Internet Control Message
igmp        2    IGMP       # Internet Group Management
ggp         3    GGP        # Gateway-to-Gateway
ip          4    IP         # IP in IP (encapsulation)
st          5    ST         # Stream
tcp         6    TCP        # Transmission Control
cbt         7    CBT        # CBT
egp         8    EGP        # Exterior Gateway Protocol
[ ... ]
chaos       16   CHAOS      # Chaos
udp         17   UDP        # User Datagram

```

The first two fields are the protocol name or abbreviation and the number in decimal format. Nmap doesn't care about anything after the protocol number. It is used for IP protocol scanning, as described at Section 5.11. Less than 140 protocols are defined and users almost never modify this file. The raw data is made available by the IANA at <http://www.iana.org/assignments/protocol-numbers>

## 12.8. Using Customized Data Files

Any or all of the Nmap data files may be replaced with versions customized to the user's liking. They can only be replaced in whole -- you can not specify changes that will be merged with the original files at runtime. When Nmap looks for each file, it searches by name in many directories and selects the first one found. This is the analogous to the way your UNIX shell finds programs you ask to execute by searching through the directories in your \$PATH one at a time in order. The following list gives the Nmap directory search order. It shows that an `nmap-services` found in the directory specified by `--datadir` will be used in preference to one found in `~/nmap/` because the former is searched first.

### Nmap data file directory search order

1. If `--datadir` option was specified, check the directory given as its argument.
2. If the `NMAPDIR` environmental variable is set, check that directory.
3. If Nmap is not running on Windows, search in `~/nmap` of the user running Nmap. It tries the real user ID's home directory, and then the effective UID's if they differ.
4. If Nmap *is* running on Windows, check the directory in which the Nmap binary resides.
5. Check the compiled in `NMAPDATADIR` directory. That value is defined to `c:\nmap` on Windows, and `$prefix/share/nmap` on UNIX. `$prefix` is `/usr/local` for the default source build and `/usr` for the Linux RPMs. The `$prefix` can be changed by giving `./configure` the `--prefix` option when compiling the source.
6. As a last resort, the current working directory of your shell (.) is tried. This is done last for the same security reasons that . should not appear first on your shell execution \$PATH. On a shared system, a malicious user could place bogus data files in a shared directory such as `/tmp`. Those files could be malformed, causing Nmap

to complain and exit, or they could cause Nmap to skip important ports. If Nmap tried . first, other users who happened to run Nmap in that shared directory would get the bogus versions. This could also happen by accident if you inadvertently ran Nmap in a directory that happened to have a file named `nmap-services` (or one of the other ones). Users who really want Nmap to try the current directory early may set `$NMAPDIR` to . at their own risk.

This list shows the many choices users have when deciding how to replace a file with their own customized version. The option I usually recommend is to place the customized files in a special directory named appropriately for the change. For example, an `nmap-services` stripped to contain just the hundred most common ports could be placed in `~/nmap-fewports`. Then specify this directory with the `--datadir` option. This ensures that the customized files are only used intentionally. Since the Nmap output-to-file formats include the Nmap command-line used, you will know which files were used when reviewing the logs later.

Another option is to simply edit the original in `NMAPDATADIR`. This is rarely recommended, as the edited file will likely be overwritten the next time Nmap is upgraded. Additionally, this makes it hard to use the original files if you suspect that your replacements are causing a problem. This also makes it difficult to compare your version with the original to recall what you changed.

A third option is to place the customized files in your UNIX `~/nmap` directory. Of course you should only insert files that you have changed. The others will still be retrieved from `NMAPDATADIR` as usual. This is very convenient, as Nmap will use the customized files implicitly whenever you run it. That can be a disadvantage as well. Users sometimes forget the files exist. When they upgrade Nmap to a version with newer data files, the old copies in `~/nmap` will still be used, reducing the quality of results.

Setting the `$NMAPDIR` to the directory with files is another alternative. This can be useful when testing a new version of Nmap. Suppose you obtain Nmap version 3.70, notice the huge list of changes, and decide to test it out before replacing your current known-working version. You might compile it in `~/src/nmap-3.70`, but execute it there and Nmap tries to read the data files from `/usr/local/share/nmap`. Those are the old versions, since Nmap 3.70 has not yet been installed. Simply set `$NMAPDIR` to `~/src/nmap-3.70`, test to your heart's content, and then perform the **make install**. A disadvantage to using `$NMAPDIR` regularly is that the directory name is not recorded in Nmap output files like it is when `--datadir` is used instead.

## **Chapter 13. Nmap Cookbook**

## **Chapter 14. The History and Future of Nmap**

# **Chapter 15. Nmap Reference Guide**

# Appendix A. Nmap XML Output DTD

## A.1.

This document type definition (DTD) is used by XML parsers to validate Nmap XML output. The latest version is always available at <http://www.insecure.org/nmap/data/nmap.dtd>. While it is primarily intended for programmatic use, it is included here due to its value in helping humans interpret Nmap XML output. The DTD defines the legal elements of the format, and often enumerates the attributes and values they can take on. Using the DTD is discussed further in Section 11.6.

\* *TODO: Must include the most recent version before book goes to press.*

```
<!--
nmap.dtd
This is the DTD for nmap's XML output (-oX) format.
$Id: nmap.dtd,v 1.8 2004/11/24 20:13:01 fyodor Exp $
```

Originally written by:  
William McVey <[wam@cisco.com](mailto:wam@cisco.com)> <[wam+nmap@wamber.net](mailto:wam+nmap@wamber.net)>

Now maintained by Fyodor <[fyodor@insecure.org](mailto:fyodor@insecure.org)> as part of Nmap.

To validate using this file, simply add a DOCTYPE line similar to:

```
<!DOCTYPE nmaprun SYSTEM "nmap.dtd">
to the nmap output immediately below the prologue (the first line). This
should allow you to run a validating parser against the output (so long
as the dtd is in your parser's dtd search path).
```

Bugs:

Most of the elements are "locked" into the specific order that nmap generates, when there really is no need for a specific ordering.

This is primarily because I don't know the xml DTD construct to specify "one each of this list of elements, in any order". If there is a construct similar to SGML's '&' operator, please let me know.

Since the work to write this DTD was done as part of WAM's job duties for the Cisco Secure Consulting Services group (<http://www.cisco.com/go/securityconsulting>), the following copyright needs to be included in this and any other derived works.

```
# Copyright (c) 2001 by Cisco systems, Inc.
#
# Permission to use, copy, modify, and distribute modified and
# unmodified copies of this software for any purpose and without fee is
# hereby granted, provided that (a) this copyright and permission notice
# appear on all copies of the software and supporting documentation, (b)
```

```

# the name of Cisco Systems, Inc. not be used in advertising or
# publicity pertaining to distribution of the program without specific
# prior permission, and (c) notice be given in supporting documentation
# that use, modification, copying and distribution is by permission of
# Cisco Systems, Inc.
#
# Cisco Systems, Inc. makes no representations about the suitability
# of this software for any purpose. THIS SOFTWARE IS PROVIDED "AS
# IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING,
# WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND
# FITNESS FOR A PARTICULAR PURPOSE.
#
-->

<!-- parameter entities to specify common "types" used elsewhere in the DTD -->
<!ENTITY % attr_numeric "CDATA" >
<!ENTITY % attr_ipaddr "CDATA" >
<!ENTITY % attr_numeric "CDATA" >
<!ENTITY % attr_type "(ipv4 | ipv6 | mac)" >

<!ENTITY % host_states "(up|down|unknown|skipped)" >

<!-- see: nmap.c:statenum2str for list of port states -->
<!-- Maybe they should be enumerated as in scan_types below , but I -->
<!-- don't know how to escape states like open|filtered -->
<!ENTITY % port_states "CDATA" >

<!ENTITY % hostname_types "(PTR)" >

<!-- see output.c:output_xml_scaninfo_records for scan types -->
<!ENTITY % scan_types "(syn|ack|bounce|connect|null|xmas|window|maimon|fin|udp|ipproto)" >

<!-- <!ENTITY % ip_versions "(ipv4)" > -->

<!ENTITY % port_protocols "(ip|tcp|udp)" >

<!-- I don't know exactly what these are, but the values were enumerated via:
     grep "conf=" *
-->
<!ENTITY % service_confs "( 3 | 5 | 10)" >

<!-- This element was started in nmap.c:nmap_main().
     It represents to the topmost element of the output document.
-->
<!ELEMENT nmaprun (scaninfo?, verbose, debugging, host*, runstats?) >
<!ATTLIST nmaprun
    scanner (nmap) #REQUIRED

```

```

args CDATA #IMPLIED
start %attr_numeric; #IMPLIED
version CDATA #REQUIRED
xmloutputversion (1.01) #REQUIRED
>

<!-- this element is written in output.c:doscaninfo() -->
<!ELEMENT scaninfo EMPTY >
<!ATTLIST scaninfo
  type %scan_types; #REQUIRED
  protocol %port_protocols; #REQUIRED
  numservices %attr_numeric; #REQUIRED
  services CDATA #REQUIRED
>

<!-- these elements are written in nmap.c:nmap_main() -->
<!ELEMENT verbose EMPTY >
<!ATTLIST verbose level %attr_numeric; #IMPLIED >

<!ELEMENT debugging EMPTY >
<!ATTLIST debugging level %attr_numeric; #IMPLIED >

<!--
this element is started in nmap.c:nmap_main() and filled by
output.c:write_host_status(), output.c:printportoutput(), and
output.c:printosscanoutput()
-->
<!ELEMENT host ( status, address , (address | hostnames |
  smurf | ports | addport | os | uptime |
  tcpsequence | ipidsequence | tcptssequence )* ) >

<!-- these elements are written by output.c:write_xml_initial_hostinfo() -->
<!ELEMENT status EMPTY >
<!ATTLIST status state %host_states; #REQUIRED >

<!ELEMENT address EMPTY >
<!ATTLIST address
  addr %attr_ipaddr; #REQUIRED
  addrtype %attr_type; "ipv4"
  vendor CDATA #IMPLIED
>

<!ELEMENT hostnames (hostname)* >
<!ELEMENT hostname EMPTY >
<!ATTLIST hostname
  name CDATA #IMPLIED

```

```

type %hostname_types; #IMPLIED
>

<!-- this element is written by output.c:write_host_status() -->
<!ELEMENT smurf EMPTY >
<!ATTLIST smurf responses %attr_numeric; #REQUIRED >

<!-- this element is written by portlist.cc:addport() -->
<!ELEMENT addport      EMPTY >
<!ATTLIST addport
    state      %port_states;  #REQUIRED
    owner      CDATA          #IMPLIED
    portid     %attr_numeric; #REQUIRED
    protocol   %port_protocols; #REQUIRED
>

<!-- these elements are written by output.c:printportoutput() -->

<!ELEMENT ports (extraports? , port*) >

<!ELEMENT extraports EMPTY >
<!ATTLIST extraports
    state  %port_states; #REQUIRED
    count  %attr_numeric; "closed"
>

<!ELEMENT port (state , owner? , service? ) >
<!ATTLIST port
    protocol %port_protocols; #REQUIRED
    portid  %attr_numeric; #REQUIRED
>

<!ELEMENT state EMPTY >
<!ATTLIST state state %port_states; #REQUIRED >

<!ELEMENT owner EMPTY >
<!ATTLIST owner name CDATA #REQUIRED >

<!ELEMENT service EMPTY >
<!ATTLIST service
    name CDATA #REQUIRED
    conf %service_confs; #REQUIRED
        method      (table|detection|probed) #REQUIRED
        version    CDATA          #IMPLIED
        product    CDATA          #IMPLIED
        extrainfo  CDATA          #IMPLIED

```

```

proto (rpc) #IMPLIED
rpcnum %attr_numeric; #IMPLIED
lowver %attr_numeric; #IMPLIED
highver %attr_numeric; #IMPLIED
>

<!-- these elements are written by output.c: printosscanoutput() -->

<!ELEMENT os ( portused*, osclass*, osmatch* ) >

<!ELEMENT portused EMPTY >
<!ATTLIST portused
  state %port_states; #REQUIRED
  proto %port_protocols; #REQUIRED
  portid %attr_numeric; #REQUIRED
>
<!ELEMENT osclass EMPTY >
<!ATTLIST osclass
  vendor      CDATA      #REQUIRED
  osgen       CDATA      #IMPLIED
  type        CDATA      #IMPLIED
  accuracy    CDATA      #REQUIRED
  osfamily   CDATA      #REQUIRED
>

<!ELEMENT osmatch EMPTY >
<!ATTLIST osmatch
  name        CDATA      #REQUIRED
  accuracy   %attr_numeric; #REQUIRED
>

<!ELEMENT uptime EMPTY >
<!ATTLIST uptime
  seconds    %attr_numeric; #REQUIRED
  lastboot   CDATA      #IMPLIED
>

<!ELEMENT tcpsequence EMPTY >
<!ATTLIST tcpsequence
  index     %attr_numeric; #REQUIRED
  class     CDATA      #REQUIRED
  difficulty CDATA      #REQUIRED
  values    CDATA      #REQUIRED
>

<!ELEMENT ipidsequence EMPTY >

```

```
<!ATTLIST ipidsequence
  class CDATA #REQUIRED
  values CDATA #REQUIRED
>

<!ELEMENT tcptssequence EMPTY >
<!ATTLIST tcptssequence
  class CDATA #REQUIRED
  values CDATA #IMPLIED
>

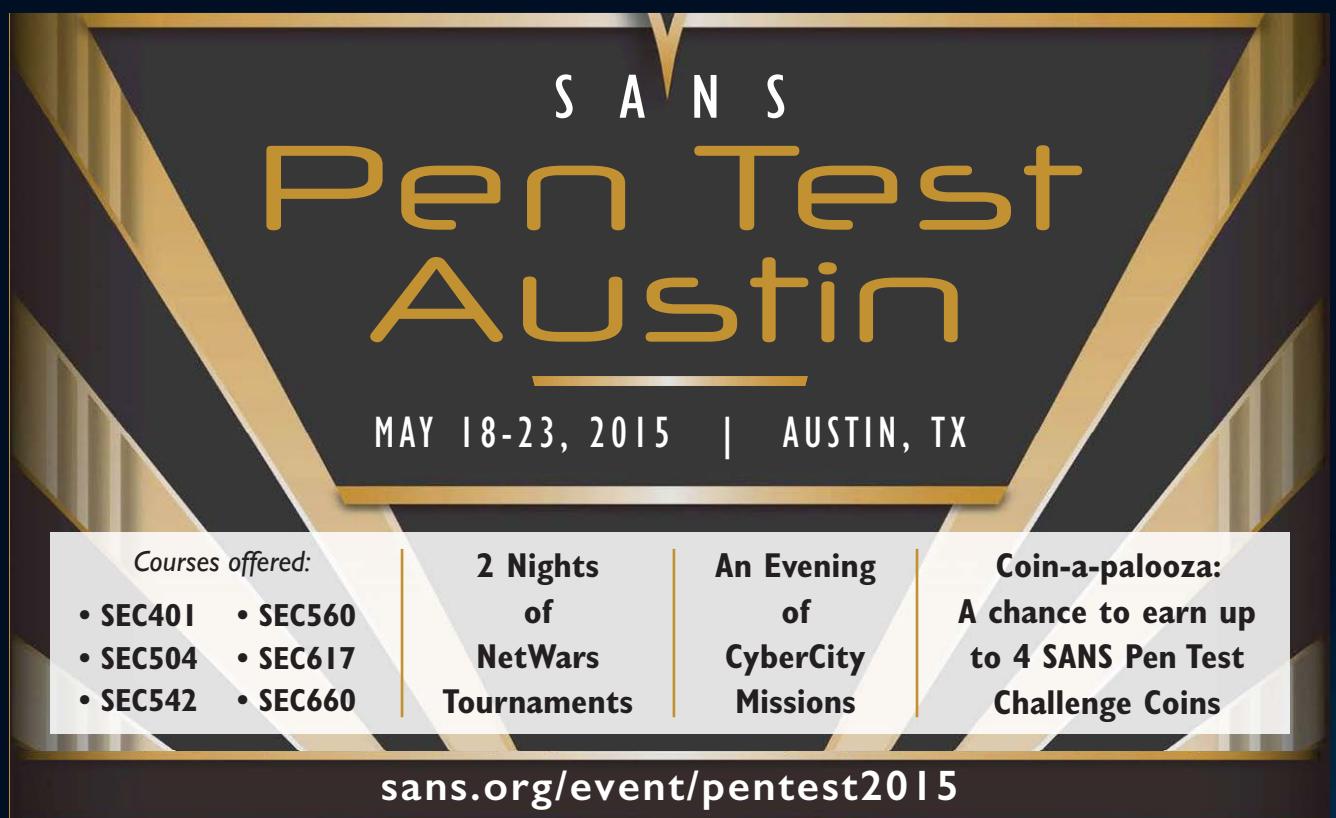
<!-- these elements are generated in output.c:printfinaloutput() -->
<!ELEMENT runstats (finished, hosts) >

<!ELEMENT finished EMPTY >
<!ATTLIST finished time %attr_numeric; #REQUIRED >

<!ELEMENT hosts EMPTY >
<!ATTLIST hosts
  up %attr_numeric; "0"
  down %attr_numeric; "0"
  skipped %attr_numeric; "0"
  total %attr_numeric; #REQUIRED
>
```

## **Appendix B. Appendix A: Complementary Tools**

## FUTURE PEN TESTING EVENTS



# S A N S

# Pen Test

# Austin

---

MAY 18-23, 2015 | AUSTIN, TX

A red-themed promotional graphic for SANS Pen Test Hackfest 2015. At the top left is a stylized knight logo with a sword. To its right, three large red arrows point rightward, each containing white text: 'STARTS WITH', 'THEN MOVES TO', and 'TWO-DAY SUMMIT TALKS'. Below these arrows is another red arrow pointing right with the text 'SIX DAYS OF TRAINING'. In the center, there's a grid of three sections: the left section shows a world map with 'NETWARS' overlaid; the middle section shows a city skyline with 'NETWARS CYBERCITY' overlaid; and the bottom section shows a circular logo for 'SANS NetWars Competition INTERACTIVE CYBER RANGE'. To the right of the middle section is text for 'Hands-On CyberCity Missions One Night'. To the right of the bottom section is text for 'Coin-a-palooza! Win up to 4 Pen Test Coins that you may have missed'. At the bottom, a large paragraph describes the event as a way to build penetration testing and vulnerability assessment skills, featuring top-rated experts sharing tips and advice. A URL at the very bottom is 'sans.org/event/sans-pen-test-hackfest-2015'.

The image is a poster for SANS Penetration Testing. At the top, the word "SANS" is written in large, white, serif capital letters. Below it, "Penetration" is in red and "Testing" is in dark blue, separated by a horizontal line. To the left of the text is a stylized illustration of a knight in armor, wearing a red cape, holding a sword. The background is dark blue at the top, transitioning to white in the middle where the text is located, and back to dark blue at the bottom. The main title "Attack Surfaces, Tools, and Techniques" is written in large, yellow, outlined sans-serif capital letters across three lines. A thin horizontal line runs across the bottom of the page.

# COIN - A - PALOOZA

Each SANS Pen Test Course includes a final full day (Day 6) of hands-on computer security challenges that hammer home the lessons taught throughout the entire course. The top winners in each course of this full-day Capture-the-Flag event receive the much-coveted challenge coin associated with the course. Each coin is unique for its associated course, with a custom logo, a special tag line, and a theme. Coins are available for the 504, 542, 560, 561, 573, 575, 617, 642, 660, and 760 courses, as well as the SANS NetWars challenge. The prize coin congratulates the victors on their great accomplishment and challenges them further to use their amazing skills to make a positive difference in their workplace and career.



# RESOURCES

**On this poster:**

- Tools and techniques that every security professional should know to maximize the value of your pen testing and vulnerability assessment work
  - In-depth network diagrams with various attack surfaces every enterprise must defend, as well as world-class pen test techniques to assess each vector
  - A detailed mind map of sites and distributions you can use to practice your skills and keep them sharp
  - A list of awesome resources for keeping your skills current
  - A description of the SANS Pen Test Challenge Coins for our Capture the Flag winners
  - An overview of the in-depth, hands-on, skill-driven courses in the SANS PenTest Curriculum

PENETRATION TESTING PRACTICE LABS

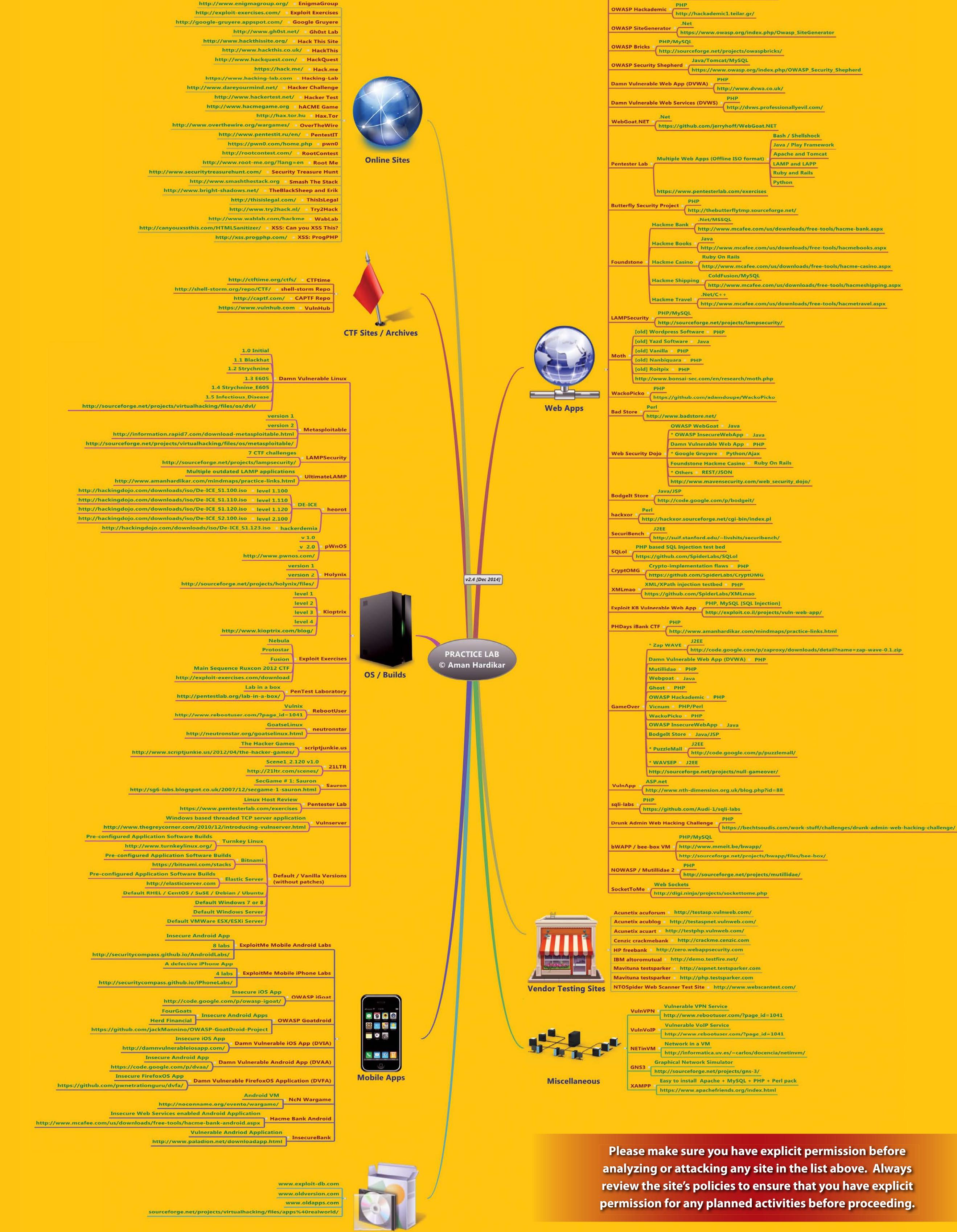
# Vulnerable Apps/Systems

*Created by Aman Hardikar .M*

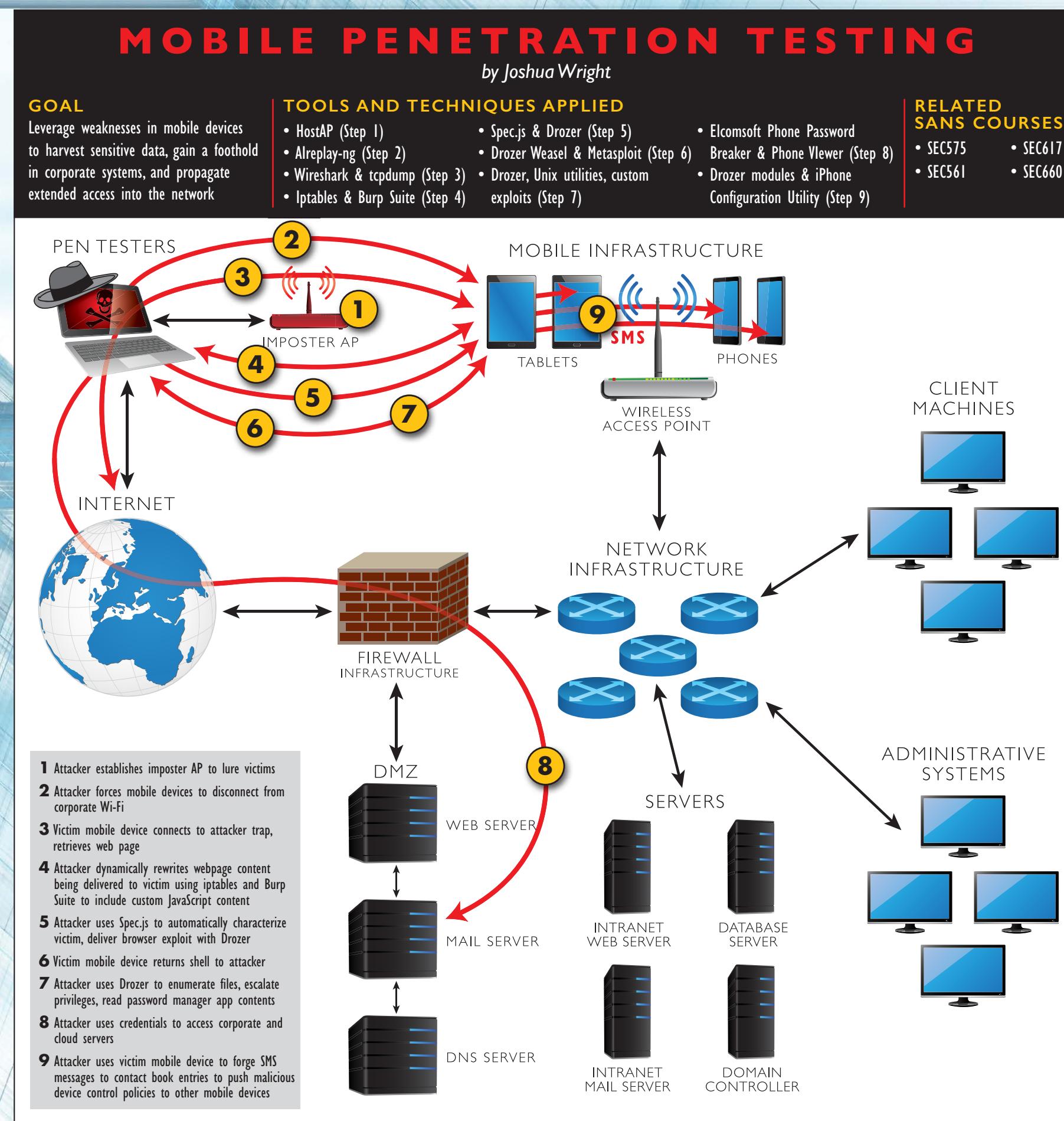
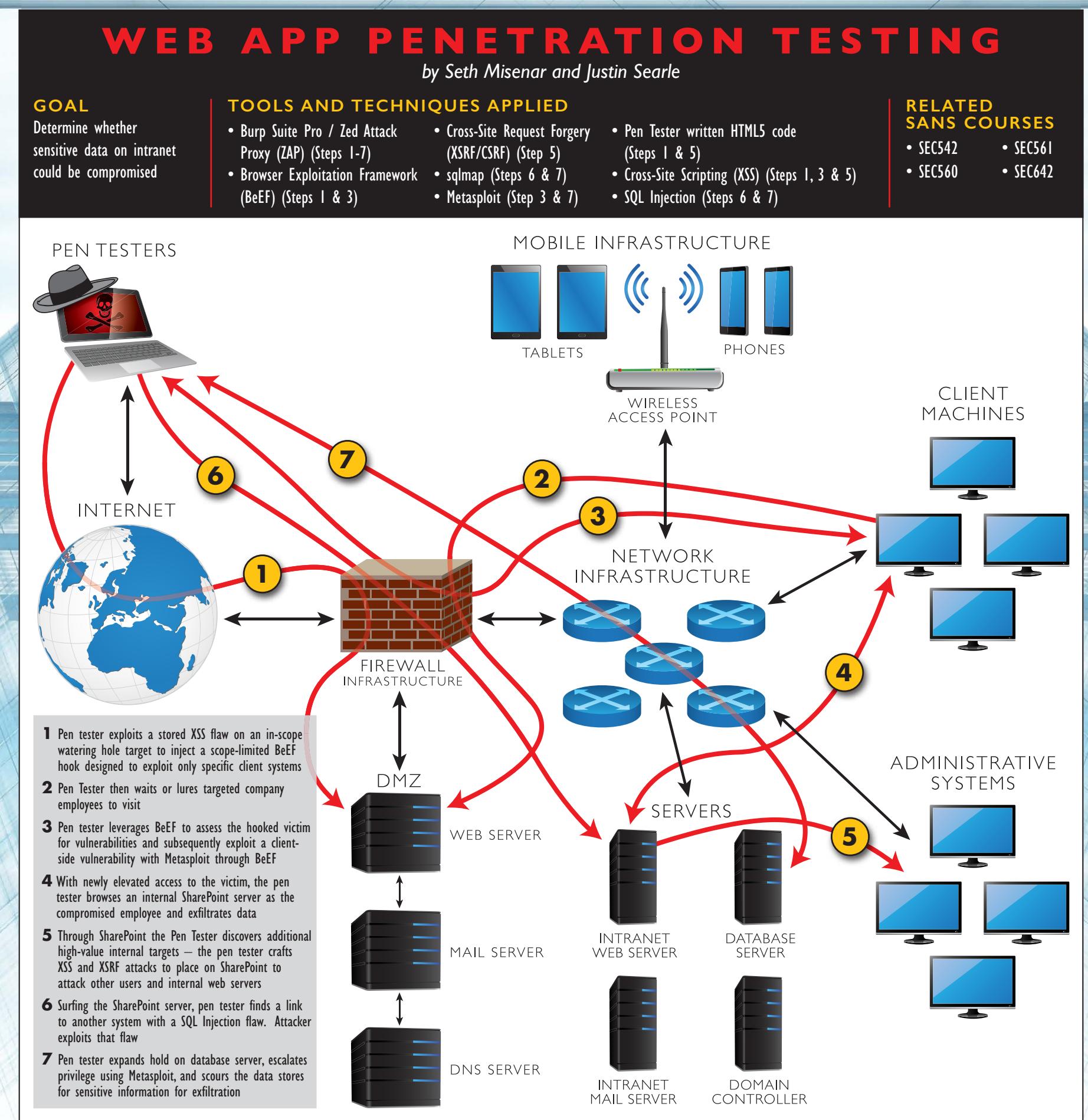
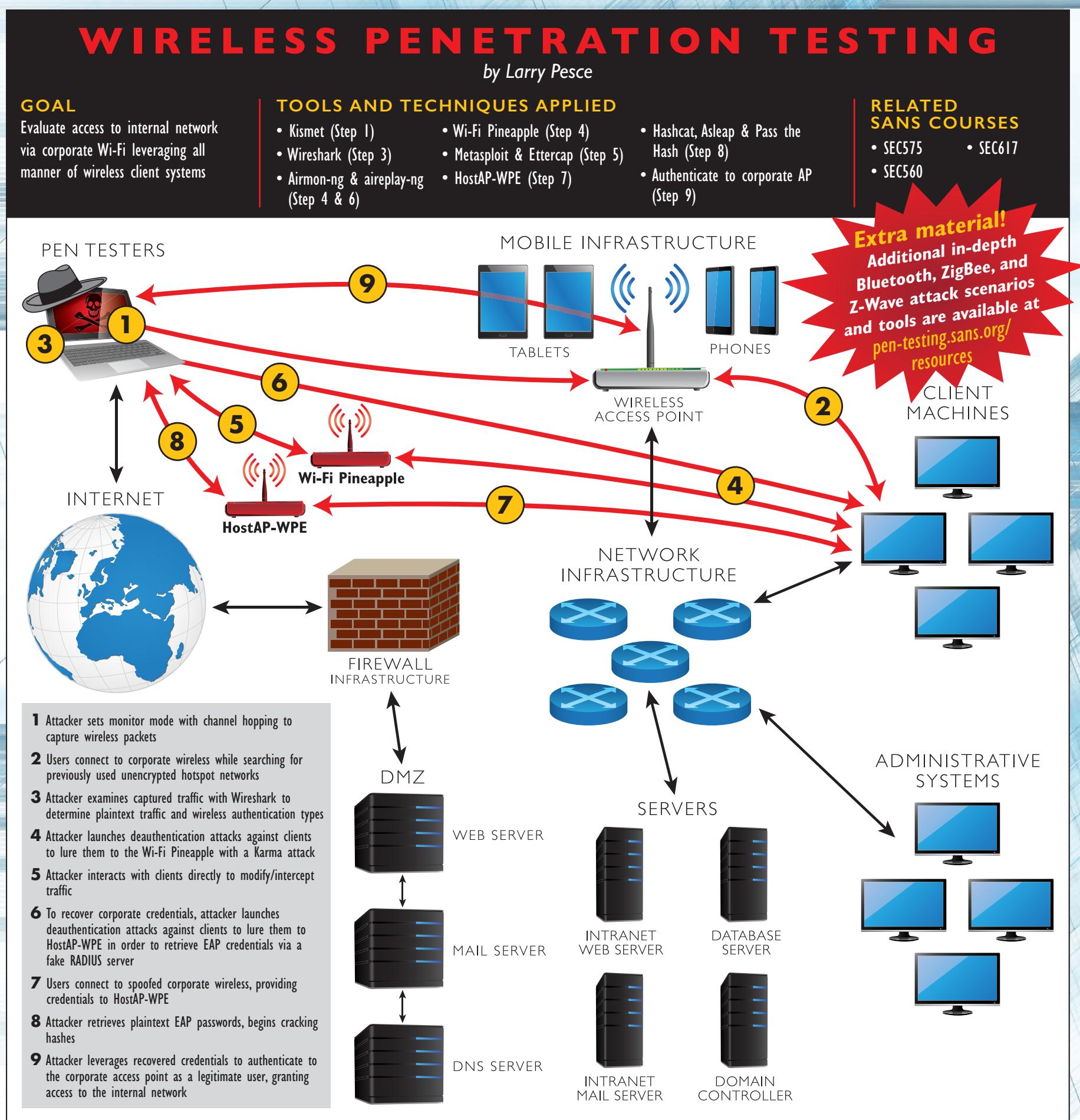
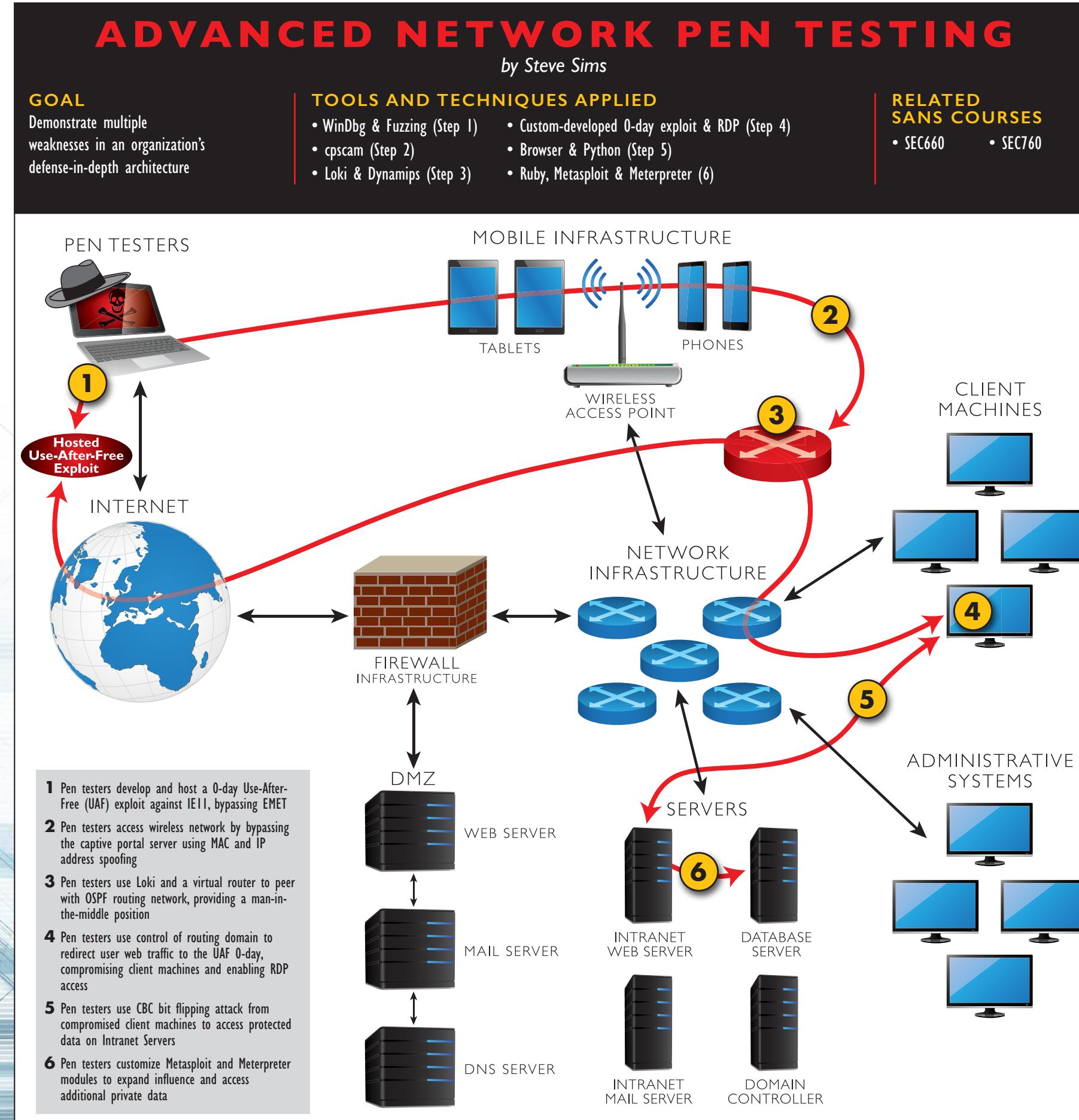
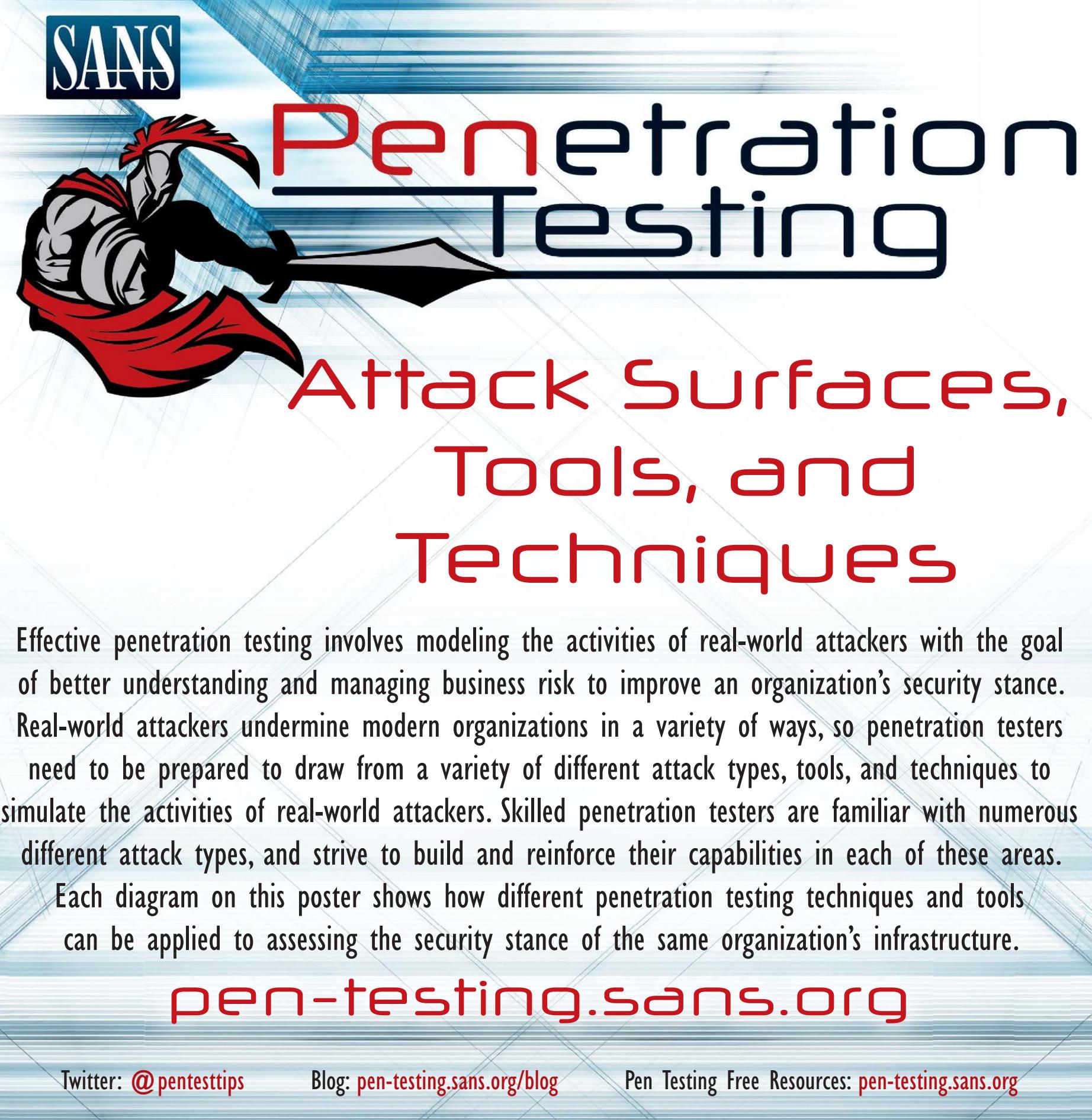
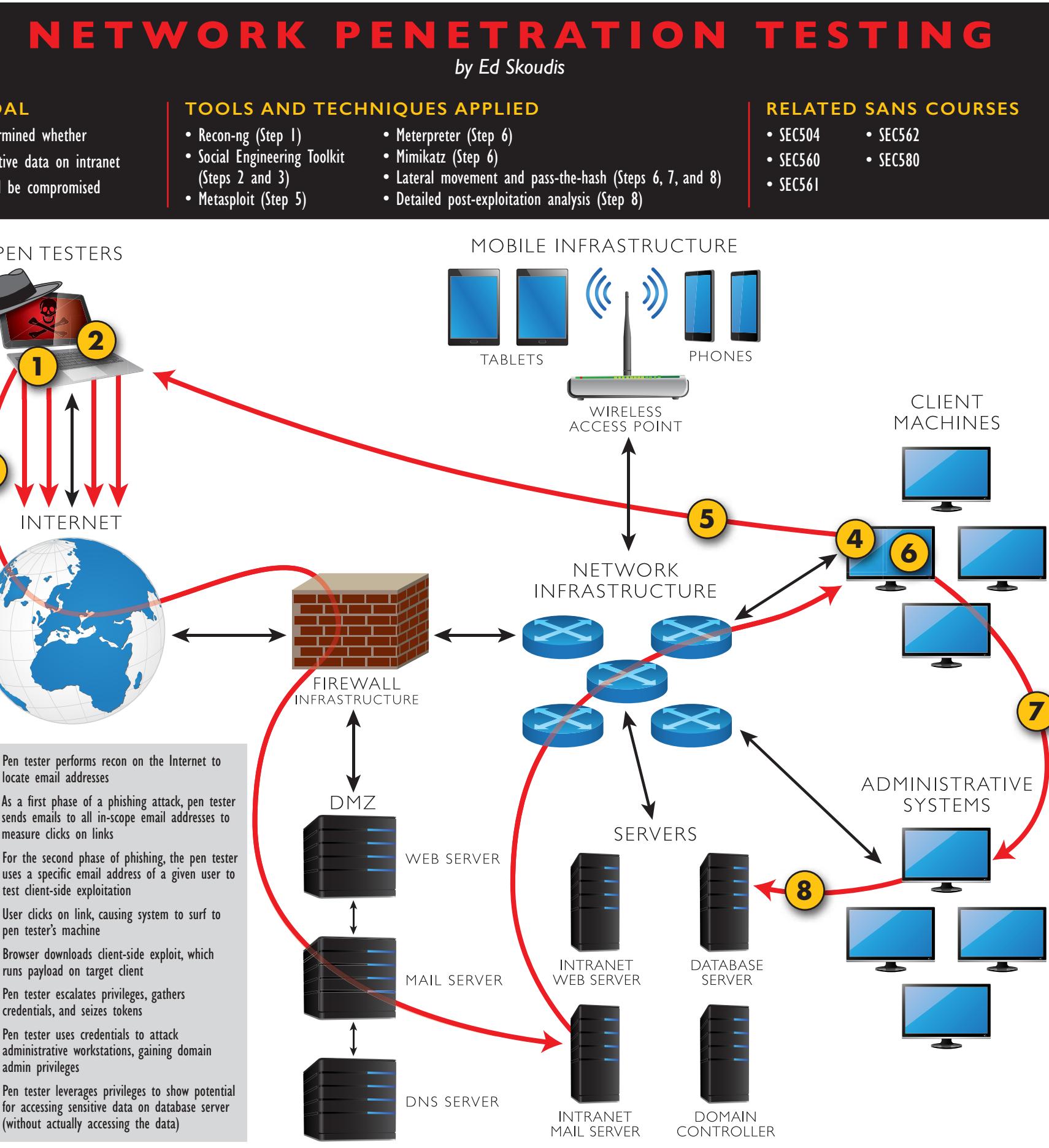
**New & Updated**  
**JANUARY 2015**

JANUARY 201

Building your skills through hands-on lab experimentation is vital in the life of a penetration tester. Aman Hardikar .M built a hugely useful mind map showing various free, publicly available distributions, challenges, and other resources for practicing your skills. The mind map is available on-line at [amanhardikar.com/mindmaps/Practice.html](http://amanhardikar.com/mindmaps/Practice.html), but feel free to use this poster version to check off the ones you've visited and beat. Thank you, Aman, for letting us include the mind map in this poster.



**Please make sure you have explicit permission before analyzing or attacking any site in the list above. Always review the site's policies to ensure that you have explicit permission for any planned activities before proceeding.**



# Treasure Island

Robert Louis Stevenson



This eBook was designed and published by Planet PDF. For more free eBooks visit our Web site at <http://www.planetpdf.com/>. To hear about our latest releases subscribe to the [Planet PDF Newsletter](#).

## TREASURE ISLAND

To  
S.L.O.,  
an American gentleman  
in accordance with whose classic taste  
the following narrative has been designed,  
it is now, in return for numerous delightful hours,  
and with the kindest wishes,  
dedicated  
by his affectionate friend, the author.

## TO THE HESITATING PURCHASER

If sailor tales to sailor tunes,  
Storm and adventure, heat and cold,  
If schooners, islands, and maroons,  
And buccaneers, and buried gold,  
And all the old romance, retold  
Exactly in the ancient way,  
Can please, as me they pleased of old,  
The wiser youngsters of today:

—So be it, and fall on! If not,  
If studious youth no longer crave,  
His ancient appetites forgot,  
Kingston, or Ballantyne the brave,

*Treasure Island*

Or Cooper of the wood and wave:  
So be it, also! And may I  
And all my pirates share the grave  
Where these and their creations lie!

## PART ONE

### The Old Buccaneer

1

## The Old Sea-dog at the Admiral Benbow

SQUIRE TRELAWNEY, Dr. Livesey, and the rest of these gentlemen having asked me to write down the whole particulars about Treasure Island, from the beginning to the end, keeping nothing back but the bearings of the island, and that only because there is still treasure not yet lifted, I take up my pen in the year of grace 17 and go back to the time when my father kept the Admiral Benbow inn and the brown old seaman with the sabre cut first took up his lodging under our roof.

I remember him as if it were yesterday, as he came plodding to the inn door, his sea-chest following behind him in a hand-barrow—a tall, strong, heavy, nut-brown man, his tarry pigtail falling over the shoulder of his soiled blue coat, his hands ragged and scarred, with black, broken nails, and the sabre cut across one cheek, a dirty, livid white. I remember him looking round the cover and whistling to himself as he did so, and then breaking out in that old sea-song that he sang so often afterwards:

‘Fifteen men on the dead man’s chest—  
Yo-ho-ho, and a bottle of rum!’

in the high, old tottering voice that seemed to have been tuned and broken at the capstan bars. Then he rapped on the door with a bit of stick like a handspike that he carried, and when my father appeared, called roughly for a glass of rum. This, when it was brought to him, he drank slowly, like a connoisseur, lingering on the taste and still looking about him at the cliffs and up at our signboard.

‘This is a handy cove,’ says he at length; ‘and a pleasant sittyated grog-shop. Much company, mate?’

My father told him no, very little company, the more was the pity.

‘Well, then,’ said he, ‘this is the berth for me. Here you, matey,’ he cried to the man who trundled the barrow; ‘bring up alongside and help up my chest. I’ll stay here a bit,’ he continued. ‘I’m a plain man; rum and bacon and eggs is what I want, and that head up there for to watch ships off. What you mought call me? You mought call me captain. Oh, I see what you’re at— there”; and he threw down three or four gold pieces on the threshold. ‘You can tell me when I’ve worked through that,’ says he, looking as fierce as a commander.

And indeed bad as his clothes were and coarsely as he spoke, he had none of the appearance of a man who sailed

before the mast, but seemed like a mate or skipper accustomed to be obeyed or to strike. The man who came with the barrow told us the mail had set him down the morning before at the Royal George, that he had inquired what inns there were along the coast, and hearing ours well spoken of, I suppose, and described as lonely, had chosen it from the others for his place of residence. And that was all we could learn of our guest.

He was a very silent man by custom. All day he hung round the cove or upon the cliffs with a brass telescope; all evening he sat in a corner of the parlour next the fire and drank rum and water very strong. Mostly he would not speak when spoken to, only look up sudden and fierce and blow through his nose like a fog-horn; and we and the people who came about our house soon learned to let him be. Every day when he came back from his stroll he would ask if any seafaring men had gone by along the road. At first we thought it was the want of company of his own kind that made him ask this question, but at last we began to see he was desirous to avoid them. When a seaman did put up at the Admiral Benbow (as now and then some did, making by the coast road for Bristol) he would look in at him through the curtained door before he entered the parlour; and he was always sure to be as silent

as a mouse when any such was present. For me, at least, there was no secret about the matter, for I was, in a way, a sharer in his alarms. He had taken me aside one day and promised me a silver fourpenny on the first of every month if I would only keep my ‘weather-eye open for a seafaring man with one leg’ and let him know the moment he appeared. Often enough when the first of the month came round and I applied to him for my wage, he would only blow through his nose at me and stare me down, but before the week was out he was sure to think better of it, bring me my four-penny piece, and repeat his orders to look out for ‘the seafaring man with one leg.’

How that personage haunted my dreams, I need scarcely tell you. On stormy nights, when the wind shook the four corners of the house and the surf roared along the cove and up the cliffs, I would see him in a thousand forms, and with a thousand diabolical expressions. Now the leg would be cut off at the knee, now at the hip; now he was a monstrous kind of a creature who had never had but the one leg, and that in the middle of his body. To see him leap and run and pursue me over hedge and ditch was the worst of nightmares. And altogether I paid pretty dear for my monthly fourpenny piece, in the shape of these abominable fancies.

But though I was so terrified by the idea of the seafaring man with one leg, I was far less afraid of the captain himself than anybody else who knew him. There were nights when he took a deal more rum and water than his head would carry; and then he would sometimes sit and sing his wicked, old, wild sea-songs, minding nobody; but sometimes he would call for glasses round and force all the trembling company to listen to his stories or bear a chorus to his singing. Often I have heard the house shaking with ‘Yo-ho-ho, and a bottle of rum,’ all the neighbours joining in for dear life, with the fear of death upon them, and each singing louder than the other to avoid remark. For in these fits he was the most overriding companion ever known; he would slap his hand on the table for silence all round; he would fly up in a passion of anger at a question, or sometimes because none was put, and so he judged the company was not following his story. Nor would he allow anyone to leave the inn till he had drunk himself sleepy and reeled off to bed.

His stories were what frightened people worst of all. Dreadful stories they were—about hanging, and walking the plank, and storms at sea, and the Dry Tortugas, and wild deeds and places on the Spanish Main. By his own

account he must have lived his life among some of the wickedest men that God ever allowed upon the sea, and the language in which he told these stories shocked our plain country people almost as much as the crimes that he described. My father was always saying the inn would be ruined, for people would soon cease coming there to be tyrannized over and put down, and sent shivering to their beds; but I really believe his presence did us good. People were frightened at the time, but on looking back they rather liked it; it was a fine excitement in a quiet country life, and there was even a party of the younger men who pretended to admire him, calling him a ‘true sea-dog’ and a ‘real old salt’ and such like names, and saying there was the sort of man that made England terrible at sea.

In one way, indeed, he bade fair to ruin us, for he kept on staying week after week, and at last month after month, so that all the money had been long exhausted, and still my father never plucked up the heart to insist on having more. If ever he mentioned it, the captain blew through his nose so loudly that you might say he roared, and stared my poor father out of the room. I have seen him wringing his hands after such a rebuff, and I am sure the annoyance and the terror he lived in must have greatly hastened his early and unhappy death.

All the time he lived with us the captain made no change whatever in his dress but to buy some stockings from a hawker. One of the cocks of his hat having fallen down, he let it hang from that day forth, though it was a great annoyance when it blew. I remember the appearance of his coat, which he patched himself upstairs in his room, and which, before the end, was nothing but patches. He never wrote or received a letter, and he never spoke with any but the neighbours, and with these, for the most part, only when drunk on rum. The great sea-chest none of us had ever seen open.

He was only once crossed, and that was towards the end, when my poor father was far gone in a decline that took him off. Dr. Livesey came late one afternoon to see the patient, took a bit of dinner from my mother, and went into the parlour to smoke a pipe until his horse should come down from the hamlet, for we had no stabling at the old Benbow. I followed him in, and I remember observing the contrast the neat, bright doctor, with his powder as white as snow and his bright, black eyes and pleasant manners, made with the coltish country folk, and above all, with that filthy, heavy, bleared scarecrow of a pirate of ours, sitting, far gone in rum, with his arms on the

table. Suddenly he—the captain, that is—began to pipe up his eternal song:

‘Fifteen men on the dead man’s chest—  
Yo-ho-ho, and a bottle of rum!  
Drink and the devil had done for the rest—  
Yo-ho-ho, and a bottle of rum!’

At first I had supposed ‘the dead man’s chest’ to be that identical big box of his upstairs in the front room, and the thought had been mingled in my nightmares with that of the one-legged seafaring man. But by this time we had all long ceased to pay any particular notice to the song; it was new, that night, to nobody but Dr. Livesey, and on him I observed it did not produce an agreeable effect, for he looked up for a moment quite angrily before he went on with his talk to old Taylor, the gardener, on a new cure for the rheumatics. In the meantime, the captain gradually brightened up at his own music, and at last flapped his hand upon the table before him in a way we all knew to mean silence. The voices stopped at once, all but Dr. Livesey’s; he went on as before speaking clear and kind and drawing briskly at his pipe between every word or two. The captain glared at him for a while, flapped his hand again, glared still harder, and at last broke out with a villainous, low oath, ‘Silence, there, between decks!’

‘Were you addressing me, sir?’ says the doctor; and when the ruffian had told him, with another oath, that this was so, ‘I have only one thing to say to you, sir,’ replies the doctor, ‘that if you keep on drinking rum, the world will soon be quit of a very dirty scoundrel!’

The old fellow’s fury was awful. He sprang to his feet, drew and opened a sailor’s clasp-knife, and balancing it open on the palm of his hand, threatened to pin the doctor to the wall.

The doctor never so much as moved. He spoke to him as before, over his shoulder and in the same tone of voice, rather high, so that all the room might hear, but perfectly calm and steady: ‘If you do not put that knife this instant in your pocket, I promise, upon my honour, you shall hang at the next assizes.’

Then followed a battle of looks between them, but the captain soon knuckled under, put up his weapon, and resumed his seat, grumbling like a beaten dog.

‘And now, sir,’ continued the doctor, ‘since I now know there’s such a fellow in my district, you may count I’ll have an eye upon you day and night. I’m not a doctor only; I’m a magistrate; and if I catch a breath of complaint against you, if it’s only for a piece of incivility

like tonight's, I'll take effectual means to have you hunted down and routed out of this. Let that suffice.'

Soon after, Dr. Livesey's horse came to the door and he rode away, but the captain held his peace that evening, and for many evenings to come.

**2**

## **Black Dog Appears and Disappears**

IT was not very long after this that there occurred the first of the mysterious events that rid us at last of the captain, though not, as you will see, of his affairs. It was a bitter cold winter, with long, hard frosts and heavy gales; and it was plain from the first that my poor father was little likely to see the spring. He sank daily, and my mother and I had all the inn upon our hands, and were kept busy enough without paying much regard to our unpleasant guest.

It was one January morning, very early—a pinching, frosty morning—the cove all grey with hoar-frost, the ripple lapping softly on the stones, the sun still low and only touching the hilltops and shining far to seaward. The captain had risen earlier than usual and set out down the beach, his cutlass swinging under the broad skirts of the old blue coat, his brass telescope under his arm, his hat tilted back upon his head. I remember his breath hanging like smoke in his wake as he strode off, and the last sound I heard of him as he turned the big rock was a loud snort

of indignation, as though his mind was still running upon Dr. Livesey.

Well, mother was upstairs with father and I was laying the breakfast-table against the captain's return when the parlour door opened and a man stepped in on whom I had never set my eyes before. He was a pale, tallowy creature, wanting two fingers of the left hand, and though he wore a cutlass, he did not look much like a fighter. I had always my eye open for seafaring men, with one leg or two, and I remember this one puzzled me. He was not sailorly, and yet he had a smack of the sea about him too.

I asked him what was for his service, and he said he would take rum; but as I was going out of the room to fetch it, he sat down upon a table and motioned me to draw near. I paused where I was, with my napkin in my hand.

‘Come here, sonny,’ says he. ‘Come nearer here.’

I took a step nearer.

‘Is this here table for my mate Bill?’ he asked with a kind of leer.

I told him I did not know his mate Bill, and this was for a person who stayed in our house whom we called the captain.

‘Well,’ said he, ‘my mate Bill would be called the captain, as like as not. He has a cut on one cheek and a mighty pleasant way with him, particularly in drink, has my mate Bill. We’ll put it, for argument like, that your captain has a cut on one cheek—and we’ll put it, if you like, that that cheek’s the right one. Ah, well! I told you. Now, is my mate Bill in this here house?’

I told him he was out walking.

‘Which way, sonny? Which way is he gone?’

And when I had pointed out the rock and told him how the captain was likely to return, and how soon, and answered a few other questions, ‘Ah,’ said he, ‘this’ll be as good as drink to my mate Bill.’

The expression of his face as he said these words was not at all pleasant, and I had my own reasons for thinking that the stranger was mistaken, even supposing he meant what he said. But it was no affair of mine, I thought; and besides, it was difficult to know what to do. The stranger kept hanging about just inside the inn door, peering round the corner like a cat waiting for a mouse. Once I stepped out myself into the road, but he immediately called me back, and as I did not obey quick enough for his fancy, a most horrible change came over his tallowy face, and he ordered me in with an oath that made me jump. As soon

as I was back again he returned to his former manner, half fawning, half sneering, patted me on the shoulder, told me I was a good boy and he had taken quite a fancy to me. ‘I have a son of my own,’ said he, ‘as like you as two blocks, and he’s all the pride of my ‘art. But the great thing for boys is discipline, sonny—discipline. Now, if you had sailed along of Bill, you wouldn’t have stood there to be spoke to twice—not you. That was never Bill’s way, nor the way of sich as sailed with him. And here, sure enough, is my mate Bill, with a spy-glass under his arm, bless his old ‘art, to be sure. You and me’ll just go back into the parlour, sonny, and get behind the door, and we’ll give Bill a little surprise—bless his ‘art, I say again.

So saying, the stranger backed along with me into the parlour and put me behind him in the corner so that we were both hidden by the open door. I was very uneasy and alarmed, as you may fancy, and it rather added to my fears to observe that the stranger was certainly frightened himself. He cleared the hilt of his cutlass and loosened the blade in the sheath; and all the time we were waiting there he kept swallowing as if he felt what we used to call a lump in the throat.

At last in strode the captain, slammed the door behind him, without looking to the right or left, and marched

straight across the room to where his breakfast awaited him.

‘Bill,’ said the stranger in a voice that I thought he had tried to make bold and big.

The captain spun round on his heel and fronted us; all the brown had gone out of his face, and even his nose was blue; he had the look of a man who sees a ghost, or the evil one, or something worse, if anything can be; and upon my word, I felt sorry to see him all in a moment turn so old and sick.

‘Come, Bill, you know me; you know an old shipmate, Bill, surely,’ said the stranger.

The captain made a sort of gasp.

‘Black Dog!’ said he.

‘And who else?’ returned the other, getting more at his ease. ‘Black Dog as ever was, come for to see his old shipmate Billy, at the Admiral Benbow inn. Ah, Bill, Bill, we have seen a sight of times, us two, since I lost them two talons,’ holding up his mutilated hand.

‘Now, look here,’ said the captain; ‘you’ve run me down; here I am; well, then, speak up; what is it?’

‘That’s you, Bill,’ returned Black Dog, ‘you’re in the right of it, Billy. I’ll have a glass of rum from this dear

child here, as I've took such a liking to; and we'll sit down, if you please, and talk square, like old shipmates.'

When I returned with the rum, they were already seated on either side of the captain's breakfast-table—Black Dog next to the door and sitting sideways so as to have one eye on his old shipmate and one, as I thought, on his retreat.

He bade me go and leave the door wide open. 'None of your keyholes for me, sonny,' he said; and I left them together and retired into the bar.

'For a long time, though I certainly did my best to listen, I could hear nothing but a low gattling; but at last the voices began to grow higher, and I could pick up a word or two, mostly oaths, from the captain.

'No, no, no, no; and an end of it!' he cried once. And again, 'If it comes to swinging, swing all, say I.'

Then all of a sudden there was a tremendous explosion of oaths and other noises—the chair and table went over in a lump, a clash of steel followed, and then a cry of pain, and the next instant I saw Black Dog in full flight, and the captain hotly pursuing, both with drawn cutlasses, and the former streaming blood from the left shoulder. Just at the door the captain aimed at the fugitive one last tremendous cut, which would certainly have split him to

the chine had it not been intercepted by our big signboard of Admiral Benbow. You may see the notch on the lower side of the frame to this day.

That blow was the last of the battle. Once out upon the road, Black Dog, in spite of his wound, showed a wonderful clean pair of heels and disappeared over the edge of the hill in half a minute. The captain, for his part, stood staring at the signboard like a bewildered man. Then he passed his hand over his eyes several times and at last turned back into the house.

'Jim,' says he, 'rum"; and as he spoke, he reeled a little, and caught himself with one hand against the wall.

'Are you hurt?' cried I.

'Rum,' he repeated. 'I must get away from here. Rum! Rum!'

I ran to fetch it, but I was quite unsteady by all that had fallen out, and I broke one glass and fouled the tap, and while I was still getting in my own way, I heard a loud fall in the parlour, and running in, beheld the captain lying full length upon the floor. At the same instant my mother, alarmed by the cries and fighting, came running downstairs to help me. Between us we raised his head. He was breathing very loud and hard, but his eyes were closed and his face a horrible colour.

‘Dear, deary me,’ cried my mother, ‘what a disgrace upon the house! And your poor father sick!’

In the meantime, we had no idea what to do to help the captain, nor any other thought but that he had got his death-hurt in the scuffle with the stranger. I got the rum, to be sure, and tried to put it down his throat, but his teeth were tightly shut and his jaws as strong as iron. It was a happy relief for us when the door opened and Doctor Livesey came in, on his visit to my father.

‘Oh, doctor,’ we cried, ‘what shall we do? Where is he wounded?’

‘Wounded? A fiddle-stick’s end!’ said the doctor. ‘No more wounded than you or I. The man has had a stroke, as I warned him. Now, Mrs. Hawkins, just you run upstairs to your husband and tell him, if possible, nothing about it. For my part, I must do my best to save this fellow’s trebly worthless life; Jim, you get me a basin.’

When I got back with the basin, the doctor had already ripped up the captain’s sleeve and exposed his great sinewy arm. It was tattooed in several places. ‘Here’s luck,’ ‘A fair wind,’ and ‘Billy Bones his fancy,’ were very neatly and clearly executed on the forearm; and up near the shoulder there was a sketch of a gallows and a

man hanging from it—done, as I thought, with great spirit.

‘Prophetic,’ said the doctor, touching this picture with his finger. ‘And now, Master Billy Bones, if that be your name, we’ll have a look at the colour of your blood. Jim,’ he said, ‘are you afraid of blood?’

‘No, sir,’ said I.

‘Well, then,’ said he, ‘you hold the basin’; and with that he took his lancet and opened a vein.

A great deal of blood was taken before the captain opened his eyes and looked mistily about him. First he recognized the doctor with an unmistakable frown; then his glance fell upon me, and he looked relieved. But suddenly his colour changed, and he tried to raise himself, crying, ‘Where’s Black Dog?’

‘There is no Black Dog here,’ said the doctor, ‘except what you have on your own back. You have been drinking rum; you have had a stroke, precisely as I told you; and I have just, very much against my own will, dragged you headforemost out of the grave. Now, Mr. Bones—’

‘That’s not my name,’ he interrupted.

‘Much I care,’ returned the doctor. ‘It’s the name of a buccaneer of my acquaintance; and I call you by it for the

sake of shortness, and what I have to say to you is this; one glass of rum won't kill you, but if you take one you'll take another and another, and I stake my wig if you don't break off short, you'll die— do you understand that?— die, and go to your own place, like the man in the Bible. Come, now, make an effort. I'll help you to your bed for once.'

Between us, with much trouble, we managed to hoist him upstairs, and laid him on his bed, where his head fell back on the pillow as if he were almost fainting.

'Now, mind you,' said the doctor, 'I clear my conscience—the name of rum for you is death.'

And with that he went off to see my father, taking me with him by the arm.

'This is nothing,' he said as soon as he had closed the door. 'I have drawn blood enough to keep him quiet awhile; he should lie for a week where he is—that is the best thing for him and you; but another stroke would settle him.'

3

## The Black Spot

ABOUT noon I stopped at the captain's door with some cooling drinks and medicines. He was lying very much as we had left him, only a little higher, and he seemed both weak and excited.

'Jim,' he said, 'you're the only one here that's worth anything, and you know I've been always good to you. Never a month but I've given you a silver fourpenny for yourself. And now you see, mate, I'm pretty low, and deserted by all; and Jim, you'll bring me one noggin of rum, now, won't you, matey?'

'The doctor—' I began.

But he broke in cursing the doctor, in a feeble voice but heartily. 'Doctors is all swabs,' he said; 'and that doctor there, why, what do he know about seafaring men? I been in places hot as pitch, and mates dropping round with Yellow Jack, and the blessed land a-heaving like the sea with earthquakes—what to the doctor know of lands like that?—and I lived on rum, I tell you. It's been meat and drink, and man and wife, to me; and if I'm not to

have my rum now I'm a poor old hulk on a lee shore, my blood'll be on you, Jim, and that doctor swab"; and he ran on again for a while with curses. 'Look, Jim, how my fingers fidgets,' he continued in the pleading tone. 'I can't keep 'em still, not I. I haven't had a drop this blessed day. That doctor's a fool, I tell you. If I don't have a drain o' rum, Jim, I'll have the horrors; I seen some on 'em already. I seen old Flint in the corner there, behind you; as plain as print, I seen him; and if I get the horrors, I'm a man that has lived rough, and I'll raise Cain. Your doctor hisself said one glass wouldn't hurt me. I'll give you a golden guinea for a noggin, Jim.'

He was growing more and more excited, and this alarmed me for my father, who was very low that day and needed quiet; besides, I was reassured by the doctor's words, now quoted to me, and rather offended by the offer of a bribe.

'I want none of your money,' said I, 'but what you owe my father. I'll get you one glass, and no more.'

When I brought it to him, he seized it greedily and drank it out.

'Aye, aye,' said he, 'that's some better, sure enough. And now, matey, did that doctor say how long I was to lie here in this old berth?'

## Treasure Island

‘A week at least,’ said I.

‘Thunder!’ he cried. ‘A week! I can’t do that; they’d have the black spot on me by then. The lubbers is going about to get the wind of me this blessed moment; lubbers as couldn’t keep what they got, and want to nail what is another’s. Is that seamanly behaviour, now, I want to know? But I’m a saving soul. I never wasted good money of mine, nor lost it neither; and I’ll trick ‘em again. I’m not afraid on ‘em. I’ll shake out another reef, matey, and daddle ‘em again.’

As he was thus speaking, he had risen from bed with great difficulty, holding to my shoulder with a grip that almost made me cry out, and moving his legs like so much dead weight. His words, spirited as they were in meaning, contrasted sadly with the weakness of the voice in which they were uttered. He paused when he had got into a sitting position on the edge.

‘That doctor’s done me,’ he murmured. ‘My ears is singing. Lay me back.’

Before I could do much to help him he had fallen back again to his former place, where he lay for a while silent.

‘Jim,’ he said at length, ‘you saw that seafaring man today?’

‘Black Dog?’ I asked.

‘Ah! Black Dog,’ says he. ‘HE’S a bad un; but there’s worse that put him on. Now, if I can’t get away nohow, and they tip me the black spot, mind you, it’s my old sea-chest they’re after; you get on a horse—you can, can’t you? Well, then, you get on a horse, and go to— well, yes, I will!—to that eternal doctor swab, and tell him to pipe all hands—magistrates and sich—and he’ll lay ‘em aboard at the Admiral Benbow—all old Flint’s crew, man and boy, all on ‘em that’s left. I was first mate, I was, old Flint’s first mate, and I’m the on’y one as knows the place. He gave it me at Savannah, when he lay a-dying, like as if I was to now, you see. But you won’t peach unless they get the black spot on me, or unless you see that Black Dog again or a seafaring man with one leg, Jim—him above all.’

‘But what is the black spot, captain?’ I asked.

‘That’s a summons, mate. I’ll tell you if they get that. But you keep your weather-eye open, Jim, and I’ll share with you equals, upon my honour.’

He wandered a little longer, his voice growing weaker; but soon after I had given him his medicine, which he took like a child, with the remark, ‘If ever a seaman wanted drugs, it’s me,’ he fell at last into a heavy, swoon-like sleep, in which I left him. What I should have done

had all gone well I do not know. Probably I should have told the whole story to the doctor, for I was in mortal fear lest the captain should repent of his confessions and make an end of me. But as things fell out, my poor father died quite suddenly that evening, which put all other matters on one side. Our natural distress, the visits of the neighbours, the arranging of the funeral, and all the work of the inn to be carried on in the meanwhile kept me so busy that I had scarcely time to think of the captain, far less to be afraid of him.

He got downstairs next morning, to be sure, and had his meals as usual, though he ate little and had more, I am afraid, than his usual supply of rum, for he helped himself out of the bar, scowling and blowing through his nose, and no one dared to cross him. On the night before the funeral he was as drunk as ever; and it was shocking, in that house of mourning, to hear him singing away at his ugly old sea-song; but weak as he was, we were all in the fear of death for him, and the doctor was suddenly taken up with a case many miles away and was never near the house after my father's death. I have said the captain was weak, and indeed he seemed rather to grow weaker than regain his strength. He clambered up and down stairs, and went from the parlour to the bar and back again, and

sometimes put his nose out of doors to smell the sea, holding on to the walls as he went for support and breathing hard and fast like a man on a steep mountain. He never particularly addressed me, and it is my belief he had as good as forgotten his confidences; but his temper was more flighty, and allowing for his bodily weakness, more violent than ever. He had an alarming way now when he was drunk of drawing his cutlass and laying it bare before him on the table. But with all that, he minded people less and seemed shut up in his own thoughts and rather wandering. Once, for instance, to our extreme wonder, he piped up to a different air, a kind of country love-song that he must have learned in his youth before he had begun to follow the sea.

So things passed until, the day after the funeral, and about three o'clock of a bitter, foggy, frosty afternoon, I was standing at the door for a moment, full of sad thoughts about my father, when I saw someone drawing slowly near along the road. He was plainly blind, for he tapped before him with a stick and wore a great green shade over his eyes and nose; and he was hunched, as if with age or weakness, and wore a huge old tattered sea-cloak with a hood that made him appear positively deformed. I never saw in my life a more dreadful-looking

figure. He stopped a little from the inn, and raising his voice in an odd sing-song, addressed the air in front of him, ‘Will any kind friend inform a poor blind man, who has lost the precious sight of his eyes in the gracious defence of his native country, England—and God bless King George!—where or in what part of this country he may now be?’

‘You are at the Admiral Benbow, Black Hill Cove, my good man,’ said I.

‘I hear a voice,’ said he, ‘a young voice. Will you give me your hand, my kind young friend, and lead me in?’

I held out my hand, and the horrible, soft-spoken, eyeless creature gripped it in a moment like a vise. I was so much startled that I struggled to withdraw, but the blind man pulled me close up to him with a single action of his arm.

‘Now, boy,’ he said, ‘take me in to the captain.’

‘Sir,’ said I, ‘upon my word I dare not.’

‘Oh,’ he sneered, ‘that’s it! Take me in straight or I’ll break your arm.’

And he gave it, as he spoke, a wrench that made me cry out.

‘Sir,’ said I, ‘it is for yourself I mean. The captain is not what he used to be. He sits with a drawn cutlass. Another gentleman—’

‘Come, now, march,’ interrupted he; and I never heard a voice so cruel, and cold, and ugly as that blind man’s. It cowed me more than the pain, and I began to obey him at once, walking straight in at the door and towards the parlour, where our sick old buccaneer was sitting, dazed with rum. The blind man clung close to me, holding me in one iron fist and leaning almost more of his weight on me than I could carry. ‘Lead me straight up to him, and when I’m in view, cry out, ‘Here’s a friend for you, Bill.’ If you don’t, I’ll do this,’ and with that he gave me a twitch that I thought would have made me faint. Between this and that, I was so utterly terrified of the blind beggar that I forgot my terror of the captain, and as I opened the parlour door, cried out the words he had ordered in a trembling voice.

The poor captain raised his eyes, and at one look the rum went out of him and left him staring sober. The expression of his face was not so much of terror as of mortal sickness. He made a movement to rise, but I do not believe he had enough force left in his body.

‘Now, Bill, sit where you are,’ said the beggar. ‘If I can’t see, I can hear a finger stirring. Business is business. Hold out your left hand. Boy, take his left hand by the wrist and bring it near to my right.’

We both obeyed him to the letter, and I saw him pass something from the hollow of the hand that held his stick into the palm of the captain’s, which closed upon it instantly.

‘And now that’s done,’ said the blind man; and at the words he suddenly left hold of me, and with incredible accuracy and nimbleness, skipped out of the parlour and into the road, where, as I still stood motionless, I could hear his stick go tap-tap-tapping into the distance.

It was some time before either I or the captain seemed to gather our senses, but at length, and about at the same moment, I released his wrist, which I was still holding, and he drew in his hand and looked sharply into the palm.

‘Ten o’clock!’ he cried. ‘Six hours. We’ll do them yet,’ and he sprang to his feet.

Even as he did so, he reeled, put his hand to his throat, stood swaying for a moment, and then, with a peculiar sound, fell from his whole height face foremost to the floor.

I ran to him at once, calling to my mother. But haste was all in vain. The captain had been struck dead by thundering apoplexy. It is a curious thing to understand, for I had certainly never liked the man, though of late I had begun to pity him, but as soon as I saw that he was dead, I burst into a flood of tears. It was the second death I had known, and the sorrow of the first was still fresh in my heart.

## The Sea-chest

I LOST no time, of course, in telling my mother all that I knew, and perhaps should have told her long before, and we saw ourselves at once in a difficult and dangerous position. Some of the man's money—if he had any—was certainly due to us, but it was not likely that our captain's shipmates, above all the two specimens seen by me, Black Dog and the blind beggar, would be inclined to give up their booty in payment of the dead man's debts. The captain's order to mount at once and ride for Doctor Livesey would have left my mother alone and unprotected, which was not to be thought of. Indeed, it seemed impossible for either of us to remain much longer in the house; the fall of coals in the kitchen grate, the very ticking of the clock, filled us with alarms. The neighbourhood, to our ears, seemed haunted by approaching footsteps; and what between the dead body of the captain on the parlour floor and the thought of that detestable blind beggar hovering near at hand and ready to return, there were moments when, as the saying goes, I

jumped in my skin for terror. Something must speedily be resolved upon, and it occurred to us at last to go forth together and seek help in the neighbouring hamlet. No sooner said than done. Bare-headed as we were, we ran out at once in the gathering evening and the frosty fog.

The hamlet lay not many hundred yards away, though out of view, on the other side of the next cove; and what greatly encouraged me, it was in an opposite direction from that whence the blind man had made his appearance and whither he had presumably returned. We were not many minutes on the road, though we sometimes stopped to lay hold of each other and hearken. But there was no unusual sound—nothing but the low wash of the ripple and the croaking of the inmates of the wood.

It was already candle-light when we reached the hamlet, and I shall never forget how much I was cheered to see the yellow shine in doors and windows; but that, as it proved, was the best of the help we were likely to get in that quarter. For—you would have thought men would have been ashamed of themselves—no soul would consent to return with us to the Admiral Benbow. The more we told of our troubles, the more—man, woman, and child—they clung to the shelter of their houses. The name of Captain Flint, though it was strange to me, was

well enough known to some there and carried a great weight of terror. Some of the men who had been to field-work on the far side of the Admiral Benbow remembered, besides, to have seen several strangers on the road, and taking them to be smugglers, to have bolted away; and one at least had seen a little lugger in what we called Kitt's Hole. For that matter, anyone who was a comrade of the captain's was enough to frighten them to death. And the short and the long of the matter was, that while we could get several who were willing enough to ride to Dr. Livesey's, which lay in another direction, not one would help us to defend the inn.

They say cowardice is infectious; but then argument is, on the other hand, a great emboldener; and so when each had said his say, my mother made them a speech. She would not, she declared, lose money that belonged to her fatherless boy; 'If none of the rest of you dare,' she said, 'Jim and I dare. Back we will go, the way we came, and small thanks to you big, hulking, chicken-hearted men. We'll have that chest open, if we die for it. And I'll thank you for that bag, Mrs. Crossley, to bring back our lawful money in.'

Of course I said I would go with my mother, and of course they all cried out at our foolhardiness, but even

then not a man would go along with us. All they would do was to give me a loaded pistol lest we were attacked, and to promise to have horses ready saddled in case we were pursued on our return, while one lad was to ride forward to the doctor's in search of armed assistance.

My heart was beating finely when we two set forth in the cold night upon this dangerous venture. A full moon was beginning to rise and peered redly through the upper edges of the fog, and this increased our haste, for it was plain, before we came forth again, that all would be as bright as day, and our departure exposed to the eyes of any watchers. We slipped along the hedges, noiseless and swift, nor did we see or hear anything to increase our terrors, till, to our relief, the door of the Admiral Benbow had closed behind us.

I slipped the bolt at once, and we stood and panted for a moment in the dark, alone in the house with the dead captain's body. Then my mother got a candle in the bar, and holding each other's hands, we advanced into the parlour. He lay as we had left him, on his back, with his eyes open and one arm stretched out.

'Draw down the blind, Jim,' whispered my mother; 'they might come and watch outside. And now,' said she when I had done so, 'we have to get the key off THAT;

## Treasure Island

and who's to touch it, I should like to know!" and she gave a kind of sob as she said the words.

I went down on my knees at once. On the floor close to his hand there was a little round of paper, blackened on the one side. I could not doubt that this was the BLACK SPOT; and taking it up, I found written on the other side, in a very good, clear hand, this short message: 'You have till ten tonight.'

'He had till ten, Mother,' said I; and just as I said it, our old clock began striking. This sudden noise startled us shockingly; but the news was good, for it was only six.

'Now, Jim,' she said, 'that key.'

I felt in his pockets, one after another. A few small coins, a thimble, and some thread and big needles, a piece of pigtail tobacco bitten away at the end, his gully with the crooked handle, a pocket compass, and a tinder box were all that they contained, and I began to despair.

'Perhaps it's round his neck,' suggested my mother.

Overcoming a strong repugnance, I tore open his shirt at the neck, and there, sure enough, hanging to a bit of tarry string, which I cut with his own gully, we found the key. At this triumph we were filled with hope and hurried upstairs without delay to the little room where he had

slept so long and where his box had stood since the day of his arrival.

It was like any other seaman's chest on the outside, the initial 'B' burned on the top of it with a hot iron, and the corners somewhat smashed and broken as by long, rough usage.

'Give me the key,' said my mother; and though the lock was very stiff, she had turned it and thrown back the lid in a twinkling.

A strong smell of tobacco and tar rose from the interior, but nothing was to be seen on the top except a suit of very good clothes, carefully brushed and folded. They had never been worn, my mother said. Under that, the miscellany began—a quadrant, a tin canikin, several sticks of tobacco, two brace of very handsome pistols, a piece of bar silver, an old Spanish watch and some other trinkets of little value and mostly of foreign make, a pair of compasses mounted with brass, and five or six curious West Indian shells. I have often wondered since why he should have carried about these shells with him in his wandering, guilty, and hunted life.

In the meantime, we had found nothing of any value but the silver and the trinkets, and neither of these were in our way. Underneath there was an old boat-cloak,

whitened with sea-salt on many a harbour-bar. My mother pulled it up with impatience, and there lay before us, the last things in the chest, a bundle tied up in oilcloth, and looking like papers, and a canvas bag that gave forth, at a touch, the jingle of gold.

'I'll show these rogues that I'm an honest woman,' said my mother. 'I'll have my dues, and not a farthing over. Hold Mrs. Crossley's bag.' And she began to count over the amount of the captain's score from the sailor's bag into the one that I was holding.

It was a long, difficult business, for the coins were of all countries and sizes—doubloons, and louis d'ors, and guineas, and pieces of eight, and I know not what besides, all shaken together at random. The guineas, too, were about the scarcest, and it was with these only that my mother knew how to make her count.

When we were about half-way through, I suddenly put my hand upon her arm, for I had heard in the silent frosty air a sound that brought my heart into my mouth—the tap-tapping of the blind man's stick upon the frozen road. It drew nearer and nearer, while we sat holding our breath. Then it struck sharp on the inn door, and then we could hear the handle being turned and the bolt rattling as the wretched being tried to enter; and then there was a

long time of silence both within and without. At last the tapping recommenced, and, to our indescribable joy and gratitude, died slowly away again until it ceased to be heard.

‘Mother,’ said I, ‘take the whole and let’s be going,’ for I was sure the bolted door must have seemed suspicious and would bring the whole hornet’s nest about our ears, though how thankful I was that I had bolted it, none could tell who had never met that terrible blind man.

But my mother, frightened as she was, would not consent to take a fraction more than was due to her and was obstinately unwilling to be content with less. It was not yet seven, she said, by a long way; she knew her rights and she would have them; and she was still arguing with me when a little low whistle sounded a good way off upon the hill. That was enough, and more than enough, for both of us.

‘I’ll take what I have,’ she said, jumping to her feet.

‘And I’ll take this to square the count,’ said I, picking up the oilskin packet.

Next moment we were both groping downstairs, leaving the candle by the empty chest; and the next we had opened the door and were in full retreat. We had not started a moment too soon. The fog was rapidly

dispersing; already the moon shone quite clear on the high ground on either side; and it was only in the exact bottom of the dell and round the tavern door that a thin veil still hung unbroken to conceal the first steps of our escape. Far less than half-way to the hamlet, very little beyond the bottom of the hill, we must come forth into the moonlight. Nor was this all, for the sound of several footsteps running came already to our ears, and as we looked back in their direction, a light tossing to and fro and still rapidly advancing showed that one of the newcomers carried a lantern.

‘My dear,’ said my mother suddenly, ‘take the money and run on. I am going to faint.’

This was certainly the end for both of us, I thought. How I cursed the cowardice of the neighbours; how I blamed my poor mother for her honesty and her greed, for her past foolhardiness and present weakness! We were just at the little bridge, by good fortune; and I helped her, tottering as she was, to the edge of the bank, where, sure enough, she gave a sigh and fell on my shoulder. I do not know how I found the strength to do it at all, and I am afraid it was roughly done, but I managed to drag her down the bank and a little way under the arch. Farther I could not move her, for the bridge was too low to let me

do more than crawl below it. So there we had to stay—my mother almost entirely exposed and both of us within earshot of the inn.

## The Last of the Blind Man

MY curiosity, in a sense, was stronger than my fear, for I could not remain where I was, but crept back to the bank again, whence, sheltering my head behind a bush of broom, I might command the road before our door. I was scarcely in position ere my enemies began to arrive, seven or eight of them, running hard, their feet beating out of time along the road and the man with the lantern some paces in front. Three men ran together, hand in hand; and I made out, even through the mist, that the middle man of this trio was the blind beggar. The next moment his voice showed me that I was right.

‘Down with the door!’ he cried.

‘Aye, aye, sir!’ answered two or three; and a rush was made upon the Admiral Benbow, the lantern-bearer following; and then I could see them pause, and hear speeches passed in a lower key, as if they were surprised to find the door open. But the pause was brief, for the blind man again issued his commands. His voice sounded

louder and higher, as if he were afire with eagerness and rage.

‘In, in, in!’ he shouted, and cursed them for their delay.

Four or five of them obeyed at once, two remaining on the road with the formidable beggar. There was a pause, then a cry of surprise, and then a voice shouting from the house, ‘Bill’s dead.’

But the blind man swore at them again for their delay.

‘Search him, some of you shirking lubbers, and the rest of you aloft and get the chest,’ he cried.

I could hear their feet rattling up our old stairs, so that the house must have shook with it. Promptly afterwards, fresh sounds of astonishment arose; the window of the captain’s room was thrown open with a slam and a jingle of broken glass, and a man leaned out into the moonlight, head and shoulders, and addressed the blind beggar on the road below him.

‘Pew,’ he cried, ‘they’ve been before us. Someone’s turned the chest out alow and aloft.’

‘Is it there?’ roared Pew.

‘The money’s there.’

The blind man cursed the money.

‘Flint’s fist, I mean,’ he cried.

‘We don’t see it here nohow,’ returned the man.

‘Here, you below there, is it on Bill?’ cried the blind man again.

At that another fellow, probably him who had remained below to search the captain’s body, came to the door of the inn. ‘Bill’s been overhauled a’ready,’ said he; ‘nothin’ left.’

‘It’s these people of the inn—it’s that boy. I wish I had put his eyes out!’ cried the blind man, Pew. ‘There were no time ago—they had the door bolted when I tried it. Scatter, lads, and find ‘em.’

‘Sure enough, they left their glim here,’ said the fellow from the window.

‘Scatter and find ‘em! Rout the house out!’ reiterated Pew, striking with his stick upon the road.

Then there followed a great to-do through all our old inn, heavy feet pounding to and fro, furniture thrown over, doors kicked in, until the very rocks re-echoed and the men came out again, one after another, on the road and declared that we were nowhere to be found. And just the same whistle that had alarmed my mother and myself over the dead captain’s money was once more clearly audible through the night, but this time twice repeated. I had thought it to be the blind man’s trumpet, so to speak, summoning his crew to the assault, but I now found that it

was a signal from the hillside towards the hamlet, and from its effect upon the buccaneers, a signal to warn them of approaching danger.

‘There’s Dirk again,’ said one. ‘Twice! We’ll have to budge, mates.’

‘Budge, you skulk!’ cried Pew. ‘Dirk was a fool and a coward from the first—you wouldn’t mind him. They must be close by; they can’t be far; you have your hands on it. Scatter and look for them, dogs! Oh, shiver my soul,’ he cried, ‘if I had eyes!’

This appeal seemed to produce some effect, for two of the fellows began to look here and there among the lumber, but half-heartedly, I thought, and with half an eye to their own danger all the time, while the rest stood irresolute on the road.

‘You have your hands on thousands, you fools, and you hang a leg! You’d be as rich as kings if you could find it, and you know it’s here, and you stand there skulking. There wasn’t one of you dared face Bill, and I did it—a blind man! And I’m to lose my chance for you! I’m to be a poor, crawling beggar, sponging for rum, when I might be rolling in a coach! If you had the pluck of a weevil in a biscuit you would catch them still.’

‘Hang it, Pew, we’ve got the doubloons!’ grumbled one.

‘They might have hid the blessed thing,’ said another. ‘Take the Georges, Pew, and don’t stand here squalling.’

Squalling was the word for it; Pew’s anger rose so high at these objections till at last, his passion completely taking the upper hand, he struck at them right and left in his blindness and his stick sounded heavily on more than one.

These, in their turn, cursed back at the blind miscreant, threatened him in horrid terms, and tried in vain to catch the stick and wrest it from his grasp.

This quarrel was the saving of us, for while it was still raging, another sound came from the top of the hill on the side of the hamlet—the tramp of horses galloping. Almost at the same time a pistol-shot, flash and report, came from the hedge side. And that was plainly the last signal of danger, for the buccaneers turned at once and ran, separating in every direction, one seaward along the cove, one slant across the hill, and so on, so that in half a minute not a sign of them remained but Pew. Him they had deserted, whether in sheer panic or out of revenge for his ill words and blows I know not; but there he remained behind, tapping up and down the road in a frenzy, and

groping and calling for his comrades. Finally he took a wrong turn and ran a few steps past me, towards the hamlet, crying, ‘Johnny, Black Dog, Dirk,’ and other names, ‘you won’t leave old Pew, mates—not old Pew!’

Just then the noise of horses topped the rise, and four or five riders came in sight in the moonlight and swept at full gallop down the slope.

At this Pew saw his error, turned with a scream, and ran straight for the ditch, into which he rolled. But he was on his feet again in a second and made another dash, now utterly bewildered, right under the nearest of the coming horses.

The rider tried to save him, but in vain. Down went Pew with a cry that rang high into the night; and the four hoofs trampled and spurned him and passed by. He fell on his side, then gently collapsed upon his face and moved no more.

I leaped to my feet and hailed the riders. They were pulling up, at any rate, horrified at the accident; and I soon saw what they were. One, tailing out behind the rest, was a lad that had gone from the hamlet to Dr. Livesey’s; the rest were revenue officers, whom he had met by the way, and with whom he had had the intelligence to return at once. Some news of the lugger in Kitt’s Hole had found

## Treasure Island

its way to Supervisor Dance and set him forth that night in our direction, and to that circumstance my mother and I owed our preservation from death.

Pew was dead, stone dead. As for my mother, when we had carried her up to the hamlet, a little cold water and salts and that soon brought her back again, and she was none the worse for her terror, though she still continued to deplore the balance of the money. In the meantime the supervisor rode on, as fast as he could, to Kitt's Hole; but his men had to dismount and grope down the dingle, leading, and sometimes supporting, their horses, and in continual fear of ambushes; so it was no great matter for surprise that when they got down to the Hole the lugger was already under way, though still close in. He hailed her. A voice replied, telling him to keep out of the moonlight or he would get some lead in him, and at the same time a bullet whistled close by his arm. Soon after, the lugger doubled the point and disappeared. Mr. Dance stood there, as he said, 'like a fish out of water,' and all he could do was to dispatch a man to B—— to warn the cutter. 'And that,' said he, 'is just about as good as nothing. They've got off clean, and there's an end. 'Only,' he added, 'I'm glad I trod on Master Pew's corns,' for by this time he had heard my story.

I went back with him to the Admiral Benbow, and you cannot imagine a house in such a state of smash; the very clock had been thrown down by these fellows in their furious hunt after my mother and myself; and though nothing had actually been taken away except the captain's money-bag and a little silver from the till, I could see at once that we were ruined. Mr. Dance could make nothing of the scene.

'They got the money, you say? Well, then, Hawkins, what in fortune were they after? More money, I suppose?'

'No, sir; not money, I think,' replied I. 'In fact, sir, I believe I have the thing in my breast pocket; and to tell you the truth, I should like to get it put in safety.'

'To be sure, boy; quite right,' said he. 'I'll take it, if you like.'

'I thought perhaps Dr. Livesey—' I began.

'Perfectly right,' he interrupted very cheerily, 'perfectly right—a gentleman and a magistrate. And, now I come to think of it, I might as well ride round there myself and report to him or squire. Master Pew's dead, when all's done; not that I regret it, but he's dead, you see, and people will make it out against an officer of his Majesty's revenue, if make it out they can. Now, I'll tell you, Hawkins, if you like, I'll take you along.'

I thanked him heartily for the offer, and we walked back to the hamlet where the horses were. By the time I had told mother of my purpose they were all in the saddle.

‘Dogger,’ said Mr. Dance, ‘you have a good horse; take up this lad behind you.’

As soon as I was mounted, holding on to Dogger’s belt, the supervisor gave the word, and the party struck out at a bouncing trot on the road to Dr. Livesey’s house.

## 6

## The Captain's Papers

WE rode hard all the way till we drew up before Dr. Livesey's door. The house was all dark to the front.

Mr. Dance told me to jump down and knock, and Dogger gave me a stirrup to descend by. The door was opened almost at once by the maid.

'Is Dr. Livesey in?' I asked.

No, she said, he had come home in the afternoon but had gone up to the hall to dine and pass the evening with the squire.

'So there we go, boys,' said Mr. Dance.

This time, as the distance was short, I did not mount, but ran with Dogger's stirrup-leather to the lodge gates and up the long, leafless, moonlit avenue to where the white line of the hall buildings looked on either hand on great old gardens. Here Mr. Dance dismounted, and taking me along with him, was admitted at a word into the house.

The servant led us down a matted passage and showed us at the end into a great library, all lined with bookcases

and busts upon the top of them, where the squire and Dr. Livesey sat, pipe in hand, on either side of a bright fire.

I had never seen the squire so near at hand. He was a tall man, over six feet high, and broad in proportion, and he had a bluff, rough-and-ready face, all roughened and reddened and lined in his long travels. His eyebrows were very black, and moved readily, and this gave him a look of some temper, not bad, you would say, but quick and high.

‘Come in, Mr. Dance,’ says he, very stately and condescending.

‘Good evening, Dance,’ says the doctor with a nod. ‘And good evening to you, friend Jim. What good wind brings you here?’

The supervisor stood up straight and stiff and told his story like a lesson; and you should have seen how the two gentlemen leaned forward and looked at each other, and forgot to smoke in their surprise and interest. When they heard how my mother went back to the inn, Dr. Livesey fairly slapped his thigh, and the squire cried ‘Bravo!’ and broke his long pipe against the grate. Long before it was done, Mr. Trelawney (that, you will remember, was the squire’s name) had got up from his seat and was striding about the room, and the doctor, as if to hear the better,

had taken off his powdered wig and sat there looking very strange indeed with his own close-cropped black poll.'

At last Mr. Dance finished the story.

'Mr. Dance,' said the squire, 'you are a very noble fellow. And as for riding down that black, atrocious miscreant, I regard it as an act of virtue, sir, like stamping on a cockroach. This lad Hawkins is a trump, I perceive. Hawkins, will you ring that bell? Mr. Dance must have some ale.'

'And so, Jim,' said the doctor, 'you have the thing that they were after, have you?'

'Here it is, sir,' said I, and gave him the oilskin packet.

The doctor looked it all over, as if his fingers were itching to open it; but instead of doing that, he put it quietly in the pocket of his coat.

'Squire,' said he, 'when Dance has had his ale he must, of course, be off on his Majesty's service; but I mean to keep Jim Hawkins here to sleep at my house, and with your permission, I propose we should have up the cold pie and let him sup.'

'As you will, Livesey,' said the squire; 'Hawkins has earned better than cold pie.'

So a big pigeon pie was brought in and put on a sidetable, and I made a hearty supper, for I was as hungry

as a hawk, while Mr. Dance was further complimented and at last dismissed.

‘And now, squire,’ said the doctor.

‘And now, Livesey,’ said the squire in the same breath.

‘One at a time, one at a time,’ laughed Dr. Livesey.  
‘You have heard of this Flint, I suppose?’

‘Heard of him!’ cried the squire. ‘Heard of him, you say! He was the bloodthirstiest buccaneer that sailed. Blackbeard was a child to Flint. The Spaniards were so prodigiously afraid of him that, I tell you, sir, I was sometimes proud he was an Englishman. I’ve seen his top-sails with these eyes, off Trinidad, and the cowardly son of a rum-puncheon that I sailed with put back—put back, sir, into Port of Spain.’

‘Well, I’ve heard of him myself, in England,’ said the doctor. ‘But the point is, had he money?’

‘Money!’ cried the squire. ‘Have you heard the story? What were these villains after but money? What do they care for but money? For what would they risk their rascal carcasses but money?’

‘That we shall soon know,’ replied the doctor. ‘But you are so confoundedly hot-headed and exclamatory that I cannot get a word in. What I want to know is this: Supposing that I have here in my pocket some clue to

where Flint buried his treasure, will that treasure amount to much?"

'Amount, sir!' cried the squire. 'It will amount to this: If we have the clue you talk about, I fit out a ship in Bristol dock, and take you and Hawkins here along, and I'll have that treasure if I search a year.'

'Very well,' said the doctor. 'Now, then, if Jim is agreeable, we'll open the packet"; and he laid it before him on the table.

The bundle was sewn together, and the doctor had to get out his instrument case and cut the stitches with his medical scissors. It contained two things—a book and a sealed paper.

'First of all we'll try the book,' observed the doctor.

The squire and I were both peering over his shoulder as he opened it, for Dr. Livesey had kindly motioned me to come round from the side-table, where I had been eating, to enjoy the sport of the search. On the first page there were only some scraps of writing, such as a man with a pen in his hand might make for idleness or practice. One was the same as the tattoo mark, 'Billy Bones his fancy"; then there was 'Mr. W. Bones, mate,' 'No more rum,' 'Off Palm Key he got itt,' and some other snatches, mostly single words and unintelligible. I could

not help wondering who it was that had ‘got itt,’ and what ‘itt’ was that he got. A knife in his back as like as not.

‘Not much instruction there,’ said Dr. Livesey as he passed on.

The next ten or twelve pages were filled with a curious series of entries. There was a date at one end of the line and at the other a sum of money, as in common account-books, but instead of explanatory writing, only a varying number of crosses between the two. On the 12th of June, 1745, for instance, a sum of seventy pounds had plainly become due to someone, and there was nothing but six crosses to explain the cause. In a few cases, to be sure, the name of a place would be added, as ‘Offe Caraccas,’ or a mere entry of latitude and longitude, as ‘62° 17' 20”, 19° 2' 40”.’

The record lasted over nearly twenty years, the amount of the separate entries growing larger as time went on, and at the end a grand total had been made out after five or six wrong additions, and these words appended, ‘Bones, his pile.’

‘I can’t make head or tail of this,’ said Dr. Livesey.

‘The thing is as clear as noonday,’ cried the squire. ‘This is the black-hearted hound’s account-book. These crosses stand for the names of ships or towns that they

sank or plundered. The sums are the scoundrel's share, and where he feared an ambiguity, you see he added something clearer. 'Offe Caraccas,' now; you see, here was some unhappy vessel boarded off that coast. God help the poor souls that manned her—coral long ago.'

'Right!' said the doctor. 'See what it is to be a traveller. Right! And the amounts increase, you see, as he rose in rank.'

There was little else in the volume but a few bearings of places noted in the blank leaves towards the end and a table for reducing French, English, and Spanish moneys to a common value.

'Thrifty man!' cried the doctor. 'He wasn't the one to be cheated.'

'And now,' said the squire, 'for the other.'

The paper had been sealed in several places with a thimble by way of seal; the very thimble, perhaps, that I had found in the captain's pocket. The doctor opened the seals with great care, and there fell out the map of an island, with latitude and longitude, soundings, names of hills and bays and inlets, and every particular that would be needed to bring a ship to a safe anchorage upon its shores. It was about nine miles long and five across, shaped, you might say, like a fat dragon standing up, and

had two fine land-locked harbours, and a hill in the centre part marked ‘The Spy-glass.’ There were several additions of a later date, but above all, three crosses of red ink—two on the north part of the island, one in the southwest—and beside this last, in the same red ink, and in a small, neat hand, very different from the captain’s tottery characters, these words: ‘Bulk of treasure here.’

Over on the back the same hand had written this further information:

Tall tree, Spy-glass shoulder, bearing a point to the N. of N.N.E.

Skeleton Island E.S.E. and by E.

Ten feet.

The bar silver is in the north cache; you can find it by the trend of the east hummock, ten fathoms south of the black crag with the face on it.

The arms are easy found, in the sand-hill, N. point of north inlet cape, bearing E. and a quarter N. J.F.

That was all; but brief as it was, and to me incomprehensible, it filled the squire and Dr. Livesey with delight.

‘Livesey,’ said the squire, ‘you will give up this wretched practice at once. Tomorrow I start for Bristol. In three weeks’ time—three weeks!—two weeks—ten

days—we'll have the best ship, sir, and the choicest crew in England. Hawkins shall come as cabin-boy. You'll make a famous cabin-boy, Hawkins. You, Livesey, are ship's doctor; I am admiral. We'll take Redruth, Joyce, and Hunter. We'll have favourable winds, a quick passage, and not the least difficulty in finding the spot, and money to eat, to roll in, to play duck and drake with ever after.'

'Trelawney,' said the doctor, 'I'll go with you; and I'll go bail for it, so will Jim, and be a credit to the undertaking. There's only one man I'm afraid of.'

'And who's that?' cried the squire. 'Name the dog, sir!'

'You,' replied the doctor; 'for you cannot hold your tongue. We are not the only men who know of this paper. These fellows who attacked the inn tonight—bold, desperate blades, for sure—and the rest who stayed aboard that lugger, and more, I dare say, not far off, are, one and all, through thick and thin, bound that they'll get that money. We must none of us go alone till we get to sea. Jim and I shall stick together in the meanwhile; you'll take Joyce and Hunter when you ride to Bristol, and from first to last, not one of us must breathe a word of what we've found.'

*Treasure Island*

‘Livesey,’ returned the squire, ‘you are always in the right of it. I’ll be as silent as the grave.’

## PART TWO

### The Sea-cook

## I Go to Bristol

IT was longer than the squire imagined ere we were ready for the sea, and none of our first plans—not even Dr. Livesey's, of keeping me beside him—could be carried out as we intended. The doctor had to go to London for a physician to take charge of his practice; the squire was hard at work at Bristol; and I lived on at the hall under the charge of old Redruth, the gamekeeper, almost a prisoner, but full of sea-dreams and the most charming anticipations of strange islands and adventures. I brooded by the hour together over the map, all the details of which I well remembered. Sitting by the fire in the housekeeper's room, I approached that island in my fancy from every possible direction; I explored every acre of its surface; I climbed a thousand times to that tall hill they call the Spy-glass, and from the top enjoyed the most wonderful and changing prospects. Sometimes the isle was thick with savages, with whom we fought, sometimes full of dangerous animals that hunted us, but in all my fancies nothing occurred to me so strange and tragic as our actual adventures.

So the weeks passed on, till one fine day there came a letter addressed to Dr. Livesey, with this addition, ‘To be opened, in the case of his absence, by Tom Redruth or young Hawkins.’ Obeying this order, we found, or rather I found—for the gamekeeper was a poor hand at reading anything but print—the following important news:

Old Anchor Inn, Bristol, March 1, 17—

Dear Livesey—As I do not know whether you are at the hall or still in London, I send this in double to both places. The ship is bought and fitted. She lies at anchor, ready for sea. You never imagined a sweeter schooner—a child might sail her—two hundred tons; name, HISPANIOLA. I got her through my old friend, Blandly, who has proved himself throughout the most surprising trump. The admirable fellow literally slaved in my interest, and so, I may say, did everyone in Bristol, as soon as they got wind of the port we sailed for—treasure, I mean.

‘Redruth,’ said I, interrupting the letter, ‘Dr. Livesey will not like that. The squire has been talking, after all.’

‘Well, who’s a better right?’ growled the gamekeeper. ‘A pretty rum go if squire ain’t to talk for Dr. Livesey, I should think.’

At that I gave up all attempts at commentary and read straight on:

Blandly himself found the HISPANIOLA, and by the most admirable management got her for the merest trifle. There is a class of men in Bristol monstrously prejudiced against Blandly. They go the length of declaring that this honest creature would do anything for money, that the HISPANIOLA belonged to him, and that he sold it me absurdly high—the most transparent calumnies. None of them dare, however, to deny the merits of the ship. Wo far there was not a hitch. The workpeople, to be sure—riggers and what not—were most annoyingly slow; but time cured that. It was the crew that troubled me. I wished a round score of men—in case of natives, buccaneers, or the odious French—and I had the worry of the deuce itself to find so much as half a dozen, till the most remarkable stroke of fortune brought me the very man that I required. I was standing on the dock, when, by the merest accident, I fell in talk with him. I found he was an old sailor, kept a public-house, knew all the seafaring men in Bristol, had lost his health ashore, and wanted a good berth as cook to get to sea again. He had hobbled down there that morning, he said, to get a smell of the salt. I was monstrously touched—so would you have been—and, out of pure pity,

I engaged him on the spot to be ship's cook. Long John Silver, he is called, and has lost a leg; but that I regarded as a recommendation, since he lost it in his country's service, under the immortal Hawke. He has no pension, Livesey. Imagine the abominable age we live in! Well, sir, I thought I had only found a cook, but it was a crew I had discovered. Between Silver and myself we got together in a few days a company of the toughest old salts imaginable—not pretty to look at, but fellows, by their faces, of the most indomitable spirit. I declare we could fight a frigate. Long John even got rid of two out of the six or seven I had already engaged. He showed me in a moment that they were just the sort of fresh-water swabs we had to fear in an adventure of importance. I am in the most magnificent health and spirits, eating like a bull, sleeping like a tree, yet I shall not enjoy a moment till I hear my old tarpaulins tramping round the capstan. Seaward, ho! Hang the treasure! It's the glory of the sea that has turned my head. So now, Livesey, come post; do not lose an hour, if you respect me. Let young Hawkins go at once to see his mother, with Redruth for a guard; and then both come full speed to Bristol. John Trelawney

Postscript—I did not tell you that Blandly, who, by the way, is to send a consort after us if we don't turn up by

the end of August, had found an admirable fellow for sailing master—a stiff man, which I regret, but in all other respects a treasure. Long John Silver unearthed a very competent man for a mate, a man named Arrow. I have a boatswain who pipes, Livesey; so things shall go man-o'-war fashion on board the good ship HISPANIOLA. I forgot to tell you that Silver is a man of substance; I know of my own knowledge that he has a banker's account, which has never been overdrawn. He leaves his wife to manage the inn; and as she is a woman of colour, a pair of old bachelors like you and I may be excused for guessing that it is the wife, quite as much as the health, that sends him back to roving. J. T.

P.P.S.—Hawkins may stay one night with his mother.  
J. T.

You can fancy the excitement into which that letter put me. I was half beside myself with glee; and if ever I despised a man, it was old Tom Redruth, who could do nothing but grumble and lament. Any of the under-gamekeepers would gladly have changed places with him; but such was not the squire's pleasure, and the squire's pleasure was like law among them all. Nobody but old Redruth would have dared so much as even to grumble.

The next morning he and I set out on foot for the Admiral Benbow, and there I found my mother in good health and spirits. The captain, who had so long been a cause of so much discomfort, was gone where the wicked cease from troubling. The squire had had everything repaired, and the public rooms and the sign repainted, and had added some furniture—above all a beautiful armchair for mother in the bar. He had found her a boy as an apprentice also so that she should not want help while I was gone.

It was on seeing that boy that I understood, for the first time, my situation. I had thought up to that moment of the adventures before me, not at all of the home that I was leaving; and now, at sight of this clumsy stranger, who was to stay here in my place beside my mother, I had my first attack of tears. I am afraid I led that boy a dog's life, for as he was new to the work, I had a hundred opportunities of setting him right and putting him down, and I was not slow to profit by them.

The night passed, and the next day, after dinner, Redruth and I were afoot again and on the road. I said good-bye to Mother and the cove where I had lived since I was born, and the dear old Admiral Benbow—since he was repainted, no longer quite so dear. One of my last

thoughts was of the captain, who had so often strode along the beach with his cocked hat, his sabre-cut cheek, and his old brass telescope. Next moment we had turned the corner and my home was out of sight.

The mail picked us up about dusk at the Royal George on the heath. I was wedged in between Redruth and a stout old gentleman, and in spite of the swift motion and the cold night air, I must have dozed a great deal from the very first, and then slept like a log up hill and down dale through stage after stage, for when I was awakened at last it was by a punch in the ribs, and I opened my eyes to find that we were standing still before a large building in a city street and that the day had already broken a long time.

‘Where are we?’ I asked.

‘Bristol,’ said Tom. ‘Get down.’

Mr. Trelawney had taken up his residence at an inn far down the docks to superintend the work upon the schooner. Thither we had now to walk, and our way, to my great delight, lay along the quays and beside the great multitude of ships of all sizes and rigs and nations. In one, sailors were singing at their work, in another there were men aloft, high over my head, hanging to threads that seemed no thicker than a spider’s. Though I had lived by the shore all my life, I seemed never to have been near the

sea till then. The smell of tar and salt was something new. I saw the most wonderful figureheads, that had all been far over the ocean. I saw, besides, many old sailors, with rings in their ears, and whiskers curled in ringlets, and tarry pigtails, and their swaggering, clumsy sea-walk; and if I had seen as many kings or archbishops I could not have been more delighted.

And I was going to sea myself, to sea in a schooner, with a piping boatswain and pig-tailed singing seamen, to sea, bound for an unknown island, and to seek for buried treasure!

While I was still in this delightful dream, we came suddenly in front of a large inn and met Squire Trelawney, all dressed out like a sea-officer, in stout blue cloth, coming out of the door with a smile on his face and a capital imitation of a sailor's walk.

'Here you are,' he cried, 'and the doctor came last night from London. Bravo! The ship's company complete!'

'Oh, sir,' cried I, 'when do we sail?'

'Sail!' says he. 'We sail tomorrow!'

## **At the Sign of the Spy-glass**

WHEN I had done breakfasting the squire gave me a note addressed to John Silver, at the sign of the Spy-glass, and told me I should easily find the place by following the line of the docks and keeping a bright lookout for a little tavern with a large brass telescope for sign. I set off, overjoyed at this opportunity to see some more of the ships and seamen, and picked my way among a great crowd of people and carts and bales, for the dock was now at its busiest, until I found the tavern in question.

It was a bright enough little place of entertainment. The sign was newly painted; the windows had neat red curtains; the floor was cleanly sanded. There was a street on each side and an open door on both, which made the large, low room pretty clear to see in, in spite of clouds of tobacco smoke.

The customers were mostly seafaring men, and they talked so loudly that I hung at the door, almost afraid to enter.

As I was waiting, a man came out of a side room, and at a glance I was sure he must be Long John. His left leg was cut off close by the hip, and under the left shoulder he carried a crutch, which he managed with wonderful dexterity, hopping about upon it like a bird. He was very tall and strong, with a face as big as a ham—plain and pale, but intelligent and smiling. Indeed, he seemed in the most cheerful spirits, whistling as he moved about among the tables, with a merry word or a slap on the shoulder for the more favoured of his guests.

Now, to tell you the truth, from the very first mention of Long John in Squire Trelawney's letter I had taken a fear in my mind that he might prove to be the very one-legged sailor whom I had watched for so long at the old Benbow. But one look at the man before me was enough. I had seen the captain, and Black Dog, and the blind man, Pew, and I thought I knew what a buccaneer was like—a very different creature, according to me, from this clean and pleasant-tempered landlord.

I plucked up courage at once, crossed the threshold, and walked right up to the man where he stood, propped on his crutch, talking to a customer.

‘Mr. Silver, sir?’ I asked, holding out the note.

## Treasure Island

‘Yes, my lad,’ said he; ‘such is my name, to be sure. And who may you be?’ And then as he saw the squire’s letter, he seemed to me to give something almost like a start.

‘Oh!’ said he, quite loud, and offering his hand. ‘I see. You are our new cabin-boy; pleased I am to see you.’

And he took my hand in his large firm grasp.

Just then one of the customers at the far side rose suddenly and made for the door. It was close by him, and he was out in the street in a moment. But his hurry had attracted my notice, and I recognized him at glance. It was the tallow-faced man, wanting two fingers, who had come first to the Admiral Benbow.

‘Oh,’ I cried, ‘stop him! It’s Black Dog!’

‘I don’t care two coppers who he is,’ cried Silver. ‘But he hasn’t paid his score. Harry, run and catch him.’

One of the others who was nearest the door leaped up and started in pursuit.

‘If he were Admiral Hawke he shall pay his score,’ cried Silver; and then, relinquishing my hand, ‘Who did you say he was?’ he asked. ‘Black what?’

‘Dog, sir,’ said I. Has Mr. Trelawney not told you of the buccaneers? He was one of them.’

‘So?’ cried Silver. ‘In my house! Ben, run and help Harry. One of those swabs, was he? Was that you drinking with him, Morgan? Step up here.’

The man whom he called Morgan—an old, grey-haired, mahogany-faced sailor—came forward pretty sheepishly, rolling his quid.

‘Now, Morgan,’ said Long John very sternly, ‘you never clapped your eyes on that Black—Black Dog before, did you, now?’

‘Not I, sir,’ said Morgan with a salute.

‘You didn’t know his name, did you?’

‘No, sir.’

‘By the powers, Tom Morgan, it’s as good for you!’ exclaimed the landlord. ‘If you had been mixed up with the like of that, you would never have put another foot in my house, you may lay to that. And what was he saying to you?’

‘I don’t rightly know, sir,’ answered Morgan.

‘Do you call that a head on your shoulders, or a blessed dead-eye?’ cried Long John. ‘Don’t rightly know, don’t you! Perhaps you don’t happen to rightly know who you was speaking to, perhaps? Come, now, what was he jawing—v’yages, cap’ns, ships? Pipe up! What was it?’

‘We was a-talkin’ of keel-hauling,’ answered Morgan.

‘Keel-hauling, was you? And a mighty suitable thing, too, and you may lay to that. Get back to your place for a lubber, Tom.’

And then, as Morgan rolled back to his seat, Silver added to me in a confidential whisper that was very flattering, as I thought, ‘He’s quite an honest man, Tom Morgan, on’y stupid. And now,’ he ran on again, aloud, ‘let’s see—Black Dog? No, I don’t know the name, not I. Yet I kind of think I’ve—yes, I’ve seen the swab. He used to come here with a blind beggar, he used.’

‘That he did, you may be sure,’ said I. ‘I knew that blind man too. His name was Pew.’

‘It was!’ cried Silver, now quite excited. ‘Pew! That were his name for certain. Ah, he looked a shark, he did! If we run down this Black Dog, now, there’ll be news for Cap’n Trelawney! Ben’s a good runner; few seamen run better than Ben. He should run him down, hand over hand, by the powers! He talked o’ keel- hauling, did he? I’LL keel-haul him!’

All the time he was jerking out these phrases he was stumping up and down the tavern on his crutch, slapping tables with his hand, and giving such a show of excitement as would have convinced an Old Bailey judge or a Bow Street runner. My suspicions had been

thoroughly reawakened on finding Black Dog at the Spy-glass, and I watched the cook narrowly. But he was too deep, and too ready, and too clever for me, and by the time the two men had come back out of breath and confessed that they had lost the track in a crowd, and been scolded like thieves, I would have gone bail for the innocence of Long John Silver.

‘See here, now, Hawkins,’ said he, ‘here’s a blessed hard thing on a man like me, now, ain’t it? There’s Cap’n Trelawney—what’s he to think? Here I have this confounded son of a Dutchman sitting in my own house drinking of my own rum! Here you comes and tells me of it plain; and here I let him give us all the slip before my blessed deadlights! Now, Hawkins, you do me justice with the cap’n. You’re a lad, you are, but you’re as smart as paint. I see that when you first come in. Now, here it is: What could I do, with this old timber I hobble on? When I was an A B master mariner I’d have come up alongside of him, hand over hand, and broached him to in a brace of old shakes, I would; but now—‘

And then, all of a sudden, he stopped, and his jaw dropped as though he had remembered something.

‘The score!’ he burst out. ‘Three goes o’ rum! Why, shiver my timbers, if I hadn’t forgotten my score!’

And falling on a bench, he laughed until the tears ran down his cheeks. I could not help joining, and we laughed together, peal after peal, until the tavern rang again.

‘Why, what a precious old sea-calf I am!’ he said at last, wiping his cheeks. ‘You and me should get on well, Hawkins, for I’ll take my davy I should be rated ship’s boy. But come now, stand by to go about. This won’t do. Dooty is dooty, messmates. I’ll put on my old cockerel hat, and step along of you to Cap’n Trelawney, and report this here affair. For mind you, it’s serious, young Hawkins; and neither you nor me’s come out of it with what I should make so bold as to call credit. Nor you neither, says you; not smart— none of the pair of us smart. But dash my buttons! That was a good un about my score.’

And he began to laugh again, and that so heartily, that though I did not see the joke as he did, I was again obliged to join him in his mirth.

On our little walk along the quays, he made himself the most interesting companion, telling me about the different ships that we passed by, their rig, tonnage, and nationality, explaining the work that was going forward—how one was discharging, another taking in cargo, and a third making ready for sea—and every now and then

telling me some little anecdote of ships or seamen or repeating a nautical phrase till I had learned it perfectly. I began to see that here was one of the best of possible shipmates.

When we got to the inn, the squire and Dr. Livesey were seated together, finishing a quart of ale with a toast in it, before they should go aboard the schooner on a visit of inspection.

Long John told the story from first to last, with a great deal of spirit and the most perfect truth. ‘That was how it were, now, weren’t it, Hawkins?’ he would say, now and again, and I could always bear him entirely out.

The two gentlemen regretted that Black Dog had got away, but we all agreed there was nothing to be done, and after he had been complimented, Long John took up his crutch and departed.

‘All hands aboard by four this afternoon,’ shouted the squire after him.

‘Aye, aye, sir,’ cried the cook, in the passage.

‘Well, squire,’ said Dr. Livesey, ‘I don’t put much faith in your discoveries, as a general thing; but I will say this, John Silver suits me.’

‘The man’s a perfect trump,’ declared the squire.

‘And now,’ added the doctor, ‘Jim may come on board with us, may he not?’

‘To be sure he may,’ says squire. ‘Take your hat, Hawkins, and we’ll see the ship.’

## Powder and Arms

THE HISPANIOLA lay some way out, and we went under the figureheads and round the sterns of many other ships, and their cables sometimes grated underneath our keel, and sometimes swung above us. At last, however, we got alongside, and were met and saluted as we stepped aboard by the mate, Mr. Arrow, a brown old sailor with earrings in his ears and a squint. He and the squire were very thick and friendly, but I soon observed that things were not the same between Mr. Trelawney and the captain.

This last was a sharp-looking man who seemed angry with everything on board and was soon to tell us why, for we had hardly got down into the cabin when a sailor followed us.

‘Captain Smollett, sir, axing to speak with you,’ said he.

‘I am always at the captain’s orders. Show him in,’ said the squire.

The captain, who was close behind his messenger, entered at once and shut the door behind him.

‘Well, Captain Smollett, what have you to say? All well, I hope; all shipshape and seaworthy?’

‘Well, sir,’ said the captain, ‘better speak plain, I believe, even at the risk of offence. I don’t like this cruise; I don’t like the men; and I don’t like my officer. That’s short and sweet.’

‘Perhaps, sir, you don’t like the ship?’ inquired the squire, very angry, as I could see.

‘I can’t speak as to that, sir, not having seen her tried,’ said the captain. ‘She seems a clever craft; more I can’t say.’

‘Possibly, sir, you may not like your employer, either?’ says the squire.

But here Dr. Livesey cut in.

‘Stay a bit,’ said he, ‘stay a bit. No use of such questions as that but to produce ill feeling. The captain has said too much or he has said too little, and I’m bound to say that I require an explanation of his words. You don’t, you say, like this cruise. Now, why?’

‘I was engaged, sir, on what we call sealed orders, to sail this ship for that gentleman where he should bid me,’ said the captain. ‘So far so good. But now I find that

every man before the mast knows more than I do. I don't call that fair, now, do you?"

'No,' said Dr. Livesey, 'I don't.'

'Next,' said the captain, 'I learn we are going after treasure—hear it from my own hands, mind you. Now, treasure is ticklish work; I don't like treasure voyages on any account, and I don't like them, above all, when they are secret and when (begging your pardon, Mr. Trelawney) the secret has been told to the parrot.'

'Silver's parrot?' asked the squire.

'It's a way of speaking,' said the captain. 'Blabbed, I mean. It's my belief neither of you gentlemen know what you are about, but I'll tell you my way of it— life or death, and a close run.'

'That is all clear, and, I dare say, true enough,' replied Dr. Livesey. 'We take the risk, but we are not so ignorant as you believe us. Next, you say you don't like the crew. Are they not good seamen?'

'I don't like them, sir,' returned Captain Smollett. 'And I think I should have had the choosing of my own hands, if you go to that.'

'Perhaps you should,' replied the doctor. 'My friend should, perhaps, have taken you along with him; but the

slight, if there be one, was unintentional. And you don't like Mr. Arrow?"

"I don't, sir. I believe he's a good seaman, but he's too free with the crew to be a good officer. A mate should keep himself to himself—shouldn't drink with the men before the mast!"

"Do you mean he drinks?" cried the squire.

"No, sir," replied the captain, "only that he's too familiar."

"Well, now, and the short and long of it, captain?" asked the doctor. "Tell us what you want."

"Well, gentlemen, are you determined to go on this cruise?"

"Like iron," answered the squire.

"Very good," said the captain. "Then, as you've heard me very patiently, saying things that I could not prove, hear me a few words more. They are putting the powder and the arms in the fore hold. Now, you have a good place under the cabin; why not put them there?— first point. Then, you are bringing four of your own people with you, and they tell me some of them are to be berthed forward. Why not give them the berths here beside the cabin?— second point."

"Any more?" asked Mr. Trelawney.

‘One more,’ said the captain. ‘There’s been too much blabbing already.’

‘Far too much,’ agreed the doctor.

‘I’ll tell you what I’ve heard myself,’ continued Captain Smollett: ‘that you have a map of an island, that there’s crosses on the map to show where treasure is, and that the island lies—’ And then he named the latitude and longitude exactly.

‘I never told that,’ cried the squire, ‘to a soul!’

‘The hands know it, sir,’ returned the captain.

‘Livesey, that must have been you or Hawkins,’ cried the squire.

‘It doesn’t much matter who it was,’ replied the doctor. And I could see that neither he nor the captain paid much regard to Mr. Trelawney’s protestations. Neither did I, to be sure, he was so loose a talker; yet in this case I believe he was really right and that nobody had told the situation of the island.

‘Well, gentlemen,’ continued the captain, ‘I don’t know who has this map; but I make it a point, it shall be kept secret even from me and Mr. Arrow. Otherwise I would ask you to let me resign.’

‘I see,’ said the doctor. ‘You wish us to keep this matter dark and to make a garrison of the stern part of the

## Treasure Island

ship, manned with my friend's own people, and provided with all the arms and powder on board. In other words, you fear a mutiny.'

'Sir,' said Captain Smollett, 'with no intention to take offence, I deny your right to put words into my mouth. No captain, sir, would be justified in going to sea at all if he had ground enough to say that. As for Mr. Arrow, I believe him thoroughly honest; some of the men are the same; all may be for what I know. But I am responsible for the ship's safety and the life of every man Jack aboard of her. I see things going, as I think, not quite right. And I ask you to take certain precautions or let me resign my berth. And that's all.'

'Captain Smollett,' began the doctor with a smile, 'did ever you hear the fable of the mountain and the mouse? You'll excuse me, I dare say, but you remind me of that fable. When you came in here, I'll stake my wig, you meant more than this.'

'Doctor,' said the captain, 'you are smart. When I came in here I meant to get discharged. I had no thought that Mr. Trelawney would hear a word.'

'No more I would,' cried the squire. 'Had Livesey not been here I should have seen you to the deuce. As it is, I

have heard you. I will do as you desire, but I think the worse of you.'

'That's as you please, sir,' said the captain. 'You'll find I do my duty.'

And with that he took his leave.

'Trelawney,' said the doctor, 'contrary to all my notions, I believed you have managed to get two honest men on board with you—that man and John Silver.'

'Silver, if you like,' cried the squire; 'but as for that intolerable humbug, I declare I think his conduct unmanly, unsailorly, and downright un-English.'

'Well,' says the doctor, 'we shall see.'

When we came on deck, the men had begun already to take out the arms and powder, yo-ho-ing at their work, while the captain and Mr. Arrow stood by superintending.

The new arrangement was quite to my liking. The whole schooner had been overhauled; six berths had been made astern out of what had been the after-part of the main hold; and this set of cabins was only joined to the galley and forecastle by a sparred passage on the port side. It had been originally meant that the captain, Mr. Arrow, Hunter, Joyce, the doctor, and the squire were to occupy these six berths. Now Redruth and I were to get two of them and Mr. Arrow and the captain were to sleep

on deck in the companion, which had been enlarged on each side till you might almost have called it a round-house. Very low it was still, of course; but there was room to swing two hammocks, and even the mate seemed pleased with the arrangement. Even he, perhaps, had been doubtful as to the crew, but that is only guess, for as you shall hear, we had not long the benefit of his opinion.

We were all hard at work, changing the powder and the berths, when the last man or two, and Long John along with them, came off in a shore-boat.

The cook came up the side like a monkey for cleverness, and as soon as he saw what was doing, ‘So ho, mates!’ says he. ‘What’s this?’

‘We’re a-changing of the powder, Jack,’ answers one.

‘Why, by the powers,’ cried Long John, ‘if we do, we’ll miss the morning tide!’

‘My orders!’ said the captain shortly. ‘You may go below, my man. Hands will want supper.’

‘Aye, aye, sir,’ answered the cook, and touching his forelock, he disappeared at once in the direction of his galley.

‘That’s a good man, captain,’ said the doctor.

‘Very likely, sir,’ replied Captain Smollett. ‘Easy with that, men—easy,’ he ran on, to the fellows who were

shifting the powder; and then suddenly observing me examining the swivel we carried amidships, a long brass nine, ‘Here you, ship’s boy,’ he cried, ‘out o’ that! Off with you to the cook and get some work.’

And then as I was hurrying off I heard him say, quite loudly, to the doctor, ‘I’ll have no favourites on my ship.’

I assure you I was quite of the squire’s way of thinking, and hated the captain deeply.

# 10

## The Voyage

ALL that night we were in a great bustle getting things stowed in their place, and boatfuls of the squire's friends, Mr. Blandly and the like, coming off to wish him a good voyage and a safe return. We never had a night at the Admiral Benbow when I had half the work; and I was dog-tired when, a little before dawn, the boatswain sounded his pipe and the crew began to man the capstan-bars. I might have been twice as weary, yet I would not have left the deck, all was so new and interesting to me—the brief commands, the shrill note of the whistle, the men bustling to their places in the glimmer of the ship's lanterns.

‘Now, Barbecue, tip us a stave,’ cried one voice.

‘The old one,’ cried another.

‘Aye, aye, mates,’ said Long John, who was standing by, with his crutch under his arm, and at once broke out in the air and words I knew so well:

‘Fifteen men on the dead man’s chest—‘

And then the whole crew bore chorus:—

‘Yo-ho-ho, and a bottle of rum!’

And at the third ‘Ho!’ drove the bars before them with a will.

Even at that exciting moment it carried me back to the old Admiral Benbow in a second, and I seemed to hear the voice of the captain piping in the chorus. But soon the anchor was short up; soon it was hanging dripping at the bows; soon the sails began to draw, and the land and shipping to flit by on either side; and before I could lie down to snatch an hour of slumber the HISPANIOLA had begun her voyage to the Isle of Treasure.

I am not going to relate that voyage in detail. It was fairly prosperous. The ship proved to be a good ship, the crew were capable seamen, and the captain thoroughly understood his business. But before we came the length of Treasure Island, two or three things had happened which require to be known.

Mr. Arrow, first of all, turned out even worse than the captain had feared. He had no command among the men, and people did what they pleased with him. But that was by no means the worst of it, for after a day or two at sea he began to appear on deck with hazy eye, red cheeks, stuttering tongue, and other marks of drunkenness. Time after time he was ordered below in disgrace. Sometimes

he fell and cut himself; sometimes he lay all day long in his little bunk at one side of the companion; sometimes for a day or two he would be almost sober and attend to his work at least passably.

In the meantime, we could never make out where he got the drink. That was the ship's mystery. Watch him as we pleased, we could do nothing to solve it; and when we asked him to his face, he would only laugh if he were drunk, and if he were sober deny solemnly that he ever tasted anything but water.

He was not only useless as an officer and a bad influence amongst the men, but it was plain that at this rate he must soon kill himself outright, so nobody was much surprised, nor very sorry, when one dark night, with a head sea, he disappeared entirely and was seen no more.

'Overboard!' said the captain. 'Well, gentlemen, that saves the trouble of putting him in irons.'

But there we were, without a mate; and it was necessary, of course, to advance one of the men. The boatswain, Job Anderson, was the likeliest man aboard, and though he kept his old title, he served in a way as mate. Mr. Trelawney had followed the sea, and his knowledge made him very useful, for he often took a watch himself in easy weather. And the coxswain, Israel

Hands, was a careful, wily, old, experienced seaman who could be trusted at a pinch with almost anything.

He was a great confidant of Long John Silver, and so the mention of his name leads me on to speak of our ship's cook, Barbecue, as the men called him.

Aboard ship he carried his crutch by a lanyard round his neck, to have both hands as free as possible. It was something to see him wedge the foot of the crutch against a bulkhead, and propped against it, yielding to every movement of the ship, get on with his cooking like someone safe ashore. Still more strange was it to see him in the heaviest of weather cross the deck. He had a line or two rigged up to help him across the widest spaces—Long John's earrings, they were called; and he would hand himself from one place to another, now using the crutch, now trailing it alongside by the lanyard, as quickly as another man could walk. Yet some of the men who had sailed with him before expressed their pity to see him so reduced.

'He's no common man, Barbecue,' said the coxswain to me. 'He had good schooling in his young days and can speak like a book when so minded; and brave—a lion's nothing alongside of Long John! I seen him grapple four and knock their heads together—him unarmed.'

All the crew respected and even obeyed him. He had a way of talking to each and doing everybody some particular service. To me he was unweariedly kind, and always glad to see me in the galley, which he kept as clean as a new pin, the dishes hanging up burnished and his parrot in a cage in one corner.

‘Come away, Hawkins,’ he would say; ‘come and have a yarn with John. Nobody more welcome than yourself, my son. Sit you down and hear the news. Here’s Cap’n Flint—I calls my parrot Cap’n Flint, after the famous buccaneer—here’s Cap’n Flint predicting success to our v’yage. Wasn’t you, cap’n?’

And the parrot would say, with great rapidity, ‘Pieces of eight! Pieces of eight! Pieces of eight!’ till you wondered that it was not out of breath, or till John threw his handkerchief over the cage.

‘Now, that bird,’ he would say, ‘is, maybe, two hundred years old, Hawkins—they live forever mostly; and if anybody’s seen more wickedness, it must be the devil himself. She’s sailed with England, the great Cap’n England, the pirate. She’s been at Madagascar, and at Malabar, and Surinam, and Providence, and Portobello. She was at the fishing up of the wrecked plate ships. It’s there she learned ‘Pieces of eight,’ and little wonder; three

hundred and fifty thousand of ‘em, Hawkins! She was at the boarding of the viceroy of the Indies out of Goa, she was; and to look at her you would think she was a babby. But you smelt powder— didn’t you, cap’n?’

‘Stand by to go about,’ the parrot would scream.

‘Ah, she’s a handsome craft, she is,’ the cook would say, and give her sugar from his pocket, and then the bird would peck at the bars and swear straight on, passing belief for wickedness. ‘There,’ John would add, ‘you can’t touch pitch and not be mucked, lad. Here’s this poor old innocent bird o’ mine swearing blue fire, and none the wiser, you may lay to that. She would swear the same, in a manner of speaking, before chaplain.’ And John would touch his forelock with a solemn way he had that made me think he was the best of men.

In the meantime, the squire and Captain Smollett were still on pretty distant terms with one another. The squire made no bones about the matter; he despised the captain. The captain, on his part, never spoke but when he was spoken to, and then sharp and short and dry, and not a word wasted. He owned, when driven into a corner, that he seemed to have been wrong about the crew, that some of them were as brisk as he wanted to see and all had behaved fairly well. As for the ship, he had taken a

downright fancy to her. ‘She’ll lie a point nearer the wind than a man has a right to expect of his own married wife, sir. But,’ he would add, ‘all I say is, we’re not home again, and I don’t like the cruise.’

The squire, at this, would turn away and march up and down the deck, chin in air.

‘A trifle more of that man,’ he would say, ‘and I shall explode.’

We had some heavy weather, which only proved the qualities of the HISPANIOLA. Every man on board seemed well content, and they must have been hard to please if they had been otherwise, for it is my belief there was never a ship’s company so spoiled since Noah put to sea. Double grog was going on the least excuse; there was duff on odd days, as, for instance, if the squire heard it was any man’s birthday, and always a barrel of apples standing broached in the waist for anyone to help himself that had a fancy.

‘Never knew good come of it yet,’ the captain said to Dr. Livesey. ‘Spoil forecastle hands, make devils. That’s my belief.’

But good did come of the apple barrel, as you shall hear, for if it had not been for that, we should have had no

note of warning and might all have perished by the hand of treachery.

This was how it came about.

We had run up the trades to get the wind of the island we were after—I am not allowed to be more plain—and now we were running down for it with a bright lookout day and night. It was about the last day of our outward voyage by the largest computation; some time that night, or at latest before noon of the morrow, we should sight the Treasure Island. We were heading S.S.W. and had a steady breeze abeam and a quiet sea. The HISPANIOLA rolled steadily, dipping her bowsprit now and then with a whiff of spray. All was drawing alow and aloft; everyone was in the bravest spirits because we were now so near an end of the first part of our adventure.

Now, just after sundown, when all my work was over and I was on my way to my berth, it occurred to me that I should like an apple. I ran on deck. The watch was all forward looking out for the island. The man at the helm was watching the luff of the sail and whistling away gently to himself, and that was the only sound excepting the swish of the sea against the bows and around the sides of the ship.

## *Treasure Island*

In I got bodily into the apple barrel, and found there was scarce an apple left; but sitting down there in the dark, what with the sound of the waters and the rocking movement of the ship, I had either fallen asleep or was on the point of doing so when a heavy man sat down with rather a clash close by. The barrel shook as he leaned his shoulders against it, and I was just about to jump up when the man began to speak. It was Silver's voice, and before I had heard a dozen words, I would not have shown myself for all the world, but lay there, trembling and listening, in the extreme of fear and curiosity, for from these dozen words I understood that the lives of all the honest men aboard depended upon me alone.

## 11

## What I Heard in the Apple Barrel

‘NO, not I,’ said Silver. ‘Flint was cap’n; I was quartermaster, along of my timber leg. The same broadside I lost my leg, old Pew lost his deadlights. It was a master surgeon, him that amputated me—out of college and all—Latin by the bucket, and what not; but he was hanged like a dog, and sun-dried like the rest, at Corso Castle. That was Roberts’ men, that was, and comed of changing names to their ships—ROYAL FORTUNE and so on. Now, what a ship was christened, so let her stay, I says. So it was with the CASSANDRA, as brought us all safe home from Malabar, after England took the viceroy of the Indies; so it was with the old WALRUS, Flint’s old ship, as I’ve seen amuck with the red blood and fit to sink with gold.’

‘Ah!’ cried another voice, that of the youngest hand on board, and evidently full of admiration. ‘He was the flower of the flock, was Flint!’

‘Davis was a man too, by all accounts,’ said Silver. ‘I never sailed along of him; first with England, then with

Flint, that's my story; and now here on my own account, in a manner of speaking. I laid by nine hundred safe, from England, and two thousand after Flint. That ain't bad for a man before the mast—all safe in bank. ‘Tain’t earning now, it’s saving does it, you may lay to that. Where’s all England’s men now? I dunno. Where’s Flint’s? Why, most on ‘em aboard here, and glad to get the duff—been begging before that, some on ‘em. Old Pew, as had lost his sight, and might have thought shame, spends twelve hundred pound in a year, like a lord in Parliament. Where is he now? Well, he’s dead now and under hatches; but for two year before that, shiver my timbers, the man was starving! He begged, and he stole, and he cut throats, and starved at that, by the powers!’

‘Well, it ain’t much use, after all,’ said the young seaman.

“Tain’t much use for fools, you may lay to it—that, nor nothing,’ cried Silver. ‘But now, you look here: you’re young, you are, but you’re as smart as paint. I see that when I set my eyes on you, and I’ll talk to you like a man.’

You may imagine how I felt when I heard this abominable old rogue addressing another in the very same words of flattery as he had used to myself. I think, if I had

been able, that I would have killed him through the barrel. Meantime, he ran on, little supposing he was overheard.

‘Here it is about gentlemen of fortune. They lives rough, and they risk swinging, but they eat and drink like fighting-cocks, and when a cruise is done, why, it’s hundreds of pounds instead of hundreds of farthings in their pockets. Now, the most goes for rum and a good fling, and to sea again in their shirts. But that’s not the course I lay. I puts it all away, some here, some there, and none too much anywhere, by reason of suspicion. I’m fifty, mark you; once back from this cruise, I set up gentleman in earnest. Time enough too, says you. Ah, but I’ve lived easy in the meantime, never denied myself o’ nothing heart desires, and slep’ soft and ate dainty all my days but when at sea. And how did I begin? Before the mast, like you!’

‘Well,’ said the other, ‘but all the other money’s gone now, ain’t it? You daren’t show face in Bristol after this.’

‘Why, where might you suppose it was?’ asked Silver derisively.

‘At Bristol, in banks and places,’ answered his companion.

‘It were,’ said the cook; ‘it were when we weighed anchor. But my old missis has it all by now. And the Spy-

glass is sold, lease and goodwill and rigging; and the old girl's off to meet me. I would tell you where, for I trust you, but it'd make jealousy among the mates.'

'And can you trust your missis?' asked the other.

'Gentlemen of fortune,' returned the cook, 'usually trusts little among themselves, and right they are, you may lay to it. But I have a way with me, I have. When a mate brings a slip on his cable—one as knows me, I mean—it won't be in the same world with old John. There was some that was feared of Pew, and some that was feared of Flint; but Flint his own self was feared of me. Feared he was, and proud. They was the roughest crew afloat, was Flint's; the devil himself would have been feared to go to sea with them. Well now, I tell you, I'm not a boasting man, and you seen yourself how easy I keep company, but when I was quartermaster, LAMBS wasn't the word for Flint's old buccaneers. Ah, you may be sure of yourself in old John's ship.'

'Well, I tell you now,' replied the lad, 'I didn't half a quarter like the job till I had this talk with you, John; but there's my hand on it now.'

'And a brave lad you were, and smart too,' answered Silver, shaking hands so heartily that all the barrel shook,

‘and a finer figurehead for a gentleman of fortune I never clapped my eyes on.’

By this time I had begun to understand the meaning of their terms. By a ‘gentleman of fortune’ they plainly meant neither more nor less than a common pirate, and the little scene that I had overheard was the last act in the corruption of one of the honest hands—perhaps of the last one left aboard. But on this point I was soon to be relieved, for Silver giving a little whistle, a third man strolled up and sat down by the party.

‘Dick’s square,’ said Silver.

‘Oh, I know’d Dick was square,’ returned the voice of the coxswain, Israel Hands. ‘He’s no fool, is Dick.’ And he turned his quid and spat. ‘But look here,’ he went on, ‘here’s what I want to know, Barbecue: how long are we a-going to stand off and on like a blessed bumboat? I’ve had a’most enough o’ Cap’n Smollett; he’s hazed me long enough, by thunder! I want to go into that cabin, I do. I want their pickles and wines, and that.’

‘Israel,’ said Silver, ‘your head ain’t much account, nor ever was. But you’re able to hear, I reckon; leastways, your ears is big enough. Now, here’s what I say: you’ll berth forward, and you’ll live hard, and you’ll speak soft,

and you'll keep sober till I give the word; and you may lay to that, my son.'

'Well, I don't say no, do I?' growled the coxswain.  
'What I say is, when? That's what I say.'

'When! By the powers!' cried Silver. 'Well now, if you want to know, I'll tell you when. The last moment I can manage, and that's when. Here's a first-rate seaman, Cap'n Smollett, sails the blessed ship for us. Here's this squire and doctor with a map and such—I don't know where it is, do I? No more do you, says you. Well then, I mean this squire and doctor shall find the stuff, and help us to get it aboard, by the powers. Then we'll see. If I was sure of you all, sons of double Dutchmen, I'd have Cap'n Smollett navigate us half-way back again before I struck.'

'Why, we're all seamen aboard here, I should think,' said the lad Dick.

'We're all forecastle hands, you mean,' snapped Silver. 'We can steer a course, but who's to set one? That's what all you gentlemen split on, first and last. If I had my way, I'd have Cap'n Smollett work us back into the trades at least; then we'd have no blessed miscalculations and a spoonful of water a day. But I know the sort you are. I'll finish with 'em at the island, as soon's the blunt's on board, and a pity it is. But you're

never happy till you're drunk. Split my sides, I've a sick heart to sail with the likes of you!'

'Easy all, Long John,' cried Israel. 'Who's a-crossin' of you?'

'Why, how many tall ships, think ye, now, have I seen laid aboard? And how many brisk lads drying in the sun at Execution Dock?' cried Silver. 'And all for this same hurry and hurry and hurry. You hear me? I seen a thing or two at sea, I have. If you would on'y lay your course, and a p'int to windward, you would ride in carriages, you would. But not you! I know you. You'll have your mouthful of rum tomorrow, and go hang.'

'Everybody knowed you was a kind of a chapling, John; but there's others as could hand and steer as well as you,' said Israel. 'They liked a bit o' fun, they did. They wasn't so high and dry, nohow, but took their fling, like jolly companions every one.'

'So?' says Silver. 'Well, and where are they now? Pew was that sort, and he died a beggar-man. Flint was, and he died of rum at Savannah. Ah, they was a sweet crew, they was! On'y, where are they?'

'But,' asked Dick, 'when we do lay 'em athwart, what are we to do with 'em, anyhow?'

‘There’s the man for me!’ cried the cook admiringly. ‘That’s what I call business. Well, what would you think? Put ‘em ashore like maroons? That would have been England’s way. Or cut ‘em down like that much pork? That would have been Flint’s, or Billy Bones’s.’

‘Billy was the man for that,’ said Israel. ‘Dead men don’t bite,’ says he. Well, he’s dead now hisself; he knows the long and short on it now; and if ever a rough hand come to port, it was Billy.’

‘Right you are,’ said Silver; ‘rough and ready. But mark you here, I’m an easy man—I’m quite the gentleman, says you; but this time it’s serious. Dooty is dooty, mates. I give my vote—death. When I’m in Parlyment and riding in my coach, I don’t want none of these sea-lawyers in the cabin a-coming home, unlooked for, like the devil at prayers. Wait is what I say; but when the time comes, why, let her rip!’

‘John,’ cries the coxswain, ‘you’re a man!’

‘You’ll say so, Israel when you see,’ said Silver. ‘Only one thing I claim—I claim Trelawney. I’ll wring his calf’s head off his body with these hands, Dick!’ he added, breaking off. ‘You just jump up, like a sweet lad, and get me an apple, to wet my pipe like.’

You may fancy the terror I was in! I should have leaped out and run for it if I had found the strength, but my limbs and heart alike misgave me. I heard Dick begin to rise, and then someone seemingly stopped him, and the voice of Hands exclaimed, ‘Oh, stow that! Don’t you get sucking of that bilge, John. Let’s have a go of the rum.’

‘Dick,’ said Silver, ‘I trust you. I’ve a gauge on the keg, mind. There’s the key; you fill a pannikin and bring it up.’

Terrified as I was, I could not help thinking to myself that this must have been how Mr. Arrow got the strong waters that destroyed him.

Dick was gone but a little while, and during his absence Israel spoke straight on in the cook’s ear. It was but a word or two that I could catch, and yet I gathered some important news, for besides other scraps that tended to the same purpose, this whole clause was audible: ‘Not another man of them’ll jine.’ Hence there were still faithful men on board.

When Dick returned, one after another of the trio took the pannikin and drank—one ‘To luck,’ another with a ‘Here’s to old Flint,’ and Silver himself saying, in a kind of song, ‘Here’s to ourselves, and hold your luff, plenty of prizes and plenty of duff.’

*Treasure Island*

Just then a sort of brightness fell upon me in the barrel, and looking up, I found the moon had risen and was silverying the mizzen-top and shining white on the luff of the fore-sail; and almost at the same time the voice of the lookout shouted, ‘Land ho!’

# 12

## Council of War

THERE was a great rush of feet across the deck. I could hear people tumbling up from the cabin and the forecastle, and slipping in an instant outside my barrel, I dived behind the fore-sail, made a double towards the stern, and came out upon the open deck in time to join Hunter and Dr. Livesey in the rush for the weather bow.

There all hands were already congregated. A belt of fog had lifted almost simultaneously with the appearance of the moon. Away to the south-west of us we saw two low hills, about a couple of miles apart, and rising behind one of them a third and higher hill, whose peak was still buried in the fog. All three seemed sharp and conical in figure.

So much I saw, almost in a dream, for I had not yet recovered from my horrid fear of a minute or two before. And then I heard the voice of Captain Smollett issuing orders. The HISPANIOLA was laid a couple of points nearer the wind and now sailed a course that would just clear the island on the east.

## Treasure Island

‘And now, men,’ said the captain, when all was sheeted home, ‘has any one of you ever seen that land ahead?’

‘I have, sir,’ said Silver. ‘I’ve watered there with a trader I was cook in.’

‘The anchorage is on the south, behind an islet, I fancy?’ asked the captain.

‘Yes, sir; Skeleton Island they calls it. It were a main place for pirates once, and a hand we had on board knowed all their names for it. That hill to the nor’ard they calls the Fore-mast Hill; there are three hills in a row running south’ard—fore, main, and mizzen, sir. But the main—that’s the big un, with the cloud on it—they usually calls the Spy-glass, by reason of a lookout they kept when they was in the anchorage cleaning, for it’s there they cleaned their ships, sir, asking your pardon.’

‘I have a chart here,’ says Captain Smollett. ‘See if that’s the place.’

Long John’s eyes burned in his head as he took the chart, but by the fresh look of the paper I knew he was doomed to disappointment. This was not the map we found in Billy Bones’s chest, but an accurate copy, complete in all things—names and heights and soundings—with the single exception of the red crosses

and the written notes. Sharp as must have been his annoyance, Silver had the strength of mind to hide it.

‘Yes, sir,’ said he, ‘this is the spot, to be sure, and very prettily drawed out. Who might have done that, I wonder? The pirates were too ignorant, I reckon. Aye, here it is: ‘Capt. Kidd’s Anchorage’—just the name my shipmate called it. There’s a strong current runs along the south, and then away nor’ard up the west coast. Right you was, sir,’ says he, ‘to haul your wind and keep the weather of the island. Leastways, if such was your intention as to enter and careen, and there ain’t no better place for that in these waters.’

‘Thank you, my man,’ says Captain Smollett. ‘I’ll ask you later on to give us a help. You may go.’

I was surprised at the coolness with which John avowed his knowledge of the island, and I own I was half-frightened when I saw him drawing nearer to myself. He did not know, to be sure, that I had overheard his council from the apple barrel, and yet I had by this time taken such a horror of his cruelty, duplicity, and power that I could scarce conceal a shudder when he laid his hand upon my arm.

‘Ah,’ says he, ‘this here is a sweet spot, this island—a sweet spot for a lad to get ashore on. You’ll bathe, and

you'll climb trees, and you'll hunt goats, you will; and you'll get aloft on them hills like a goat yourself. Why, it makes me young again. I was going to forget my timber leg, I was. It's a pleasant thing to be young and have ten toes, and you may lay to that. When you want to go a bit of exploring, you just ask old John, and he'll put up a snack for you to take along.'

And clapping me in the friendliest way upon the shoulder, he hobbled off forward and went below.

Captain Smollett, the squire, and Dr. Livesey were talking together on the quarter-deck, and anxious as I was to tell them my story, I durst not interrupt them openly. While I was still casting about in my thoughts to find some probable excuse, Dr. Livesey called me to his side. He had left his pipe below, and being a slave to tobacco, had meant that I should fetch it; but as soon as I was near enough to speak and not to be overheard, I broke immediately, 'Doctor, let me speak. Get the captain and squire down to the cabin, and then make some pretence to send for me. I have terrible news.'

The doctor changed countenance a little, but next moment he was master of himself.

'Thank you, Jim,' said he quite loudly, 'that was all I wanted to know,' as if he had asked me a question.

And with that he turned on his heel and rejoined the other two. They spoke together for a little, and though none of them started, or raised his voice, or so much as whistled, it was plain enough that Dr. Livesey had communicated my request, for the next thing that I heard was the captain giving an order to Job Anderson, and all hands were piped on deck.

‘My lads,’ said Captain Smollett, ‘I’ve a word to say to you. This land that we have sighted is the place we have been sailing for. Mr. Trelawney, being a very open-handed gentleman, as we all know, has just asked me a word or two, and as I was able to tell him that every man on board had done his duty, alow and aloft, as I never ask to see it done better, why, he and I and the doctor are going below to the cabin to drink YOUR health and luck, and you’ll have grog served out for you to drink OUR health and luck. I’ll tell you what I think of this: I think it handsome. And if you think as I do, you’ll give a good sea-cheer for the gentleman that does it.’

The cheer followed—that was a matter of course; but it rang out so full and hearty that I confess I could hardly believe these same men were plotting for our blood.

‘One more cheer for Cap’n Smollett,’ cried Long John when the first had subsided.

And this also was given with a will.

On the top of that the three gentlemen went below, and not long after, word was sent forward that Jim Hawkins was wanted in the cabin.

I found them all three seated round the table, a bottle of Spanish wine and some raisins before them, and the doctor smoking away, with his wig on his lap, and that, I knew, was a sign that he was agitated. The stern window was open, for it was a warm night, and you could see the moon shining behind on the ship's wake.

'Now, Hawkins,' said the squire, 'you have something to say. Speak up.'

I did as I was bid, and as short as I could make it, told the whole details of Silver's conversation. Nobody interrupted me till I was done, nor did any one of the three of them make so much as a movement, but they kept their eyes upon my face from first to last.

'Jim,' said Dr. Livesey, 'take a seat.'

And they made me sit down at table beside them, poured me out a glass of wine, filled my hands with raisins, and all three, one after the other, and each with a bow, drank my good health, and their service to me, for my luck and courage.

‘Now, captain,’ said the squire, ‘you were right, and I was wrong. I own myself an ass, and I await your orders.’

‘No more an ass than I, sir,’ returned the captain. ‘I never heard of a crew that meant to mutiny but what showed signs before, for any man that had an eye in his head to see the mischief and take steps according. But this crew,’ he added, ‘beats me.’

‘Captain,’ said the doctor, ‘with your permission, that’s Silver. A very remarkable man.’

‘He’d look remarkably well from a yard-arm, sir,’ returned the captain. ‘But this is talk; this don’t lead to anything. I see three or four points, and with Mr. Trelawney’s permission, I’ll name them.’

‘You, sir, are the captain. It is for you to speak,’ says Mr. Trelawney grandly.

‘First point,’ began Mr. Smollett. ‘We must go on, because we can’t turn back. If I gave the word to go about, they would rise at once. Second point, we have time before us—at least until this treasure’s found. Third point, there are faithful hands. Now, sir, it’s got to come to blows sooner or later, and what I propose is to take time by the forelock, as the saying is, and come to blows some fine day when they least expect it. We can count, I take it, on your own home servants, Mr. Trelawney?’

‘As upon myself,’ declared the squire.

‘Three,’ reckoned the captain; ‘ourselves make seven, counting Hawkins here. Now, about the honest hands?’

‘Most likely Trelawney’s own men,’ said the doctor; ‘those he had picked up for himself before he lit on Silver.’

‘Nay,’ replied the squire. ‘Hands was one of mine.’

‘I did think I could have trusted Hands,’ added the captain.

‘And to think that they’re all Englishmen!’ broke out the squire. ‘Sir, I could find it in my heart to blow the ship up.’

‘Well, gentlemen,’ said the captain, ‘the best that I can say is not much. We must lay to, if you please, and keep a bright lookout. It’s trying on a man, I know. It would be pleasanter to come to blows. But there’s no help for it till we know our men. Lay to, and whistle for a wind, that’s my view.’

‘Jim here,’ said the doctor, ‘can help us more than anyone. The men are not shy with him, and Jim is a noticing lad.’

‘Hawkins, I put prodigious faith in you,’ added the squire.

I began to feel pretty desperate at this, for I felt altogether helpless; and yet, by an odd train of circumstances, it was indeed through me that safety came. In the meantime, talk as we pleased, there were only seven out of the twenty-six on whom we knew we could rely; and out of these seven one was a boy, so that the grown men on our side were six to their nineteen.

## **PART THREE**

### **My Shore Adventure**

## 13

### How My Shore Adventure Began

THE appearance of the island when I came on deck next morning was altogether changed. Although the breeze had now utterly ceased, we had made a great deal of way during the night and were now lying becalmed about half a mile to the south-east of the low eastern coast. Grey-coloured woods covered a large part of the surface. This even tint was indeed broken up by streaks of yellow sand-break in the lower lands, and by many tall trees of the pine family, out-topping the others—some singly, some in clumps; but the general colouring was uniform and sad. The hills ran up clear above the vegetation in spires of naked rock. All were strangely shaped, and the Spy-glass, which was by three or four hundred feet the tallest on the island, was likewise the strangest in configuration, running up sheer from almost every side and then suddenly cut off at the top like a pedestal to put a statue on.

The HISPANIOLA was rolling scuppers under in the ocean swell. The booms were tearing at the blocks, the rudder was banging to and fro, and the whole ship

creaking, groaning, and jumping like a manufactory. I had to cling tight to the backstay, and the world turned giddily before my eyes, for though I was a good enough sailor when there was way on, this standing still and being rolled about like a bottle was a thing I never learned to stand without a qualm or so, above all in the morning, on an empty stomach.

Perhaps it was this—perhaps it was the look of the island, with its grey, melancholy woods, and wild stone spires, and the surf that we could both see and hear foaming and thundering on the steep beach—at least, although the sun shone bright and hot, and the shore birds were fishing and crying all around us, and you would have thought anyone would have been glad to get to land after being so long at sea, my heart sank, as the saying is, into my boots; and from the first look onward, I hated the very thought of Treasure Island.

We had a dreary morning's work before us, for there was no sign of any wind, and the boats had to be got out and manned, and the ship warped three or four miles round the corner of the island and up the narrow passage to the haven behind Skeleton Island. I volunteered for one of the boats, where I had, of course, no business. The heat was sweltering, and the men grumbled fiercely over their

work. Anderson was in command of my boat, and instead of keeping the crew in order, he grumbled as loud as the worst.

‘Well,’ he said with an oath, ‘it’s not forever.’

I thought this was a very bad sign, for up to that day the men had gone briskly and willingly about their business; but the very sight of the island had relaxed the cords of discipline.

All the way in, Long John stood by the steersman and conned the ship. He knew the passage like the palm of his hand, and though the man in the chains got everywhere more water than was down in the chart, John never hesitated once.

‘There’s a strong scour with the ebb,’ he said, ‘and this here passage has been dug out, in a manner of speaking, with a spade.’

We brought up just where the anchor was in the chart, about a third of a mile from each shore, the mainland on one side and Skeleton Island on the other. The bottom was clean sand. The plunge of our anchor sent up clouds of birds wheeling and crying over the woods, but in less than a minute they were down again and all was once more silent.

## Treasure Island

The place was entirely land-locked, buried in woods, the trees coming right down to high-water mark, the shores mostly flat, and the hilltops standing round at a distance in a sort of amphitheatre, one here, one there. Two little rivers, or rather two swamps, emptied out into this pond, as you might call it; and the foliage round that part of the shore had a kind of poisonous brightness. From the ship we could see nothing of the house or stockade, for they were quite buried among trees; and if it had not been for the chart on the companion, we might have been the first that had ever anchored there since the island arose out of the seas.

There was not a breath of air moving, nor a sound but that of the surf booming half a mile away along the beaches and against the rocks outside. A peculiar stagnant smell hung over the anchorage—a smell of sodden leaves and rotting tree trunks. I observed the doctor sniffing and sniffing, like someone tasting a bad egg.

‘I don’t know about treasure,’ he said, ‘but I’ll stake my wig there’s fever here.’

If the conduct of the men had been alarming in the boat, it became truly threatening when they had come aboard. They lay about the deck growling together in talk. The slightest order was received with a black look and

grudgingly and carelessly obeyed. Even the honest hands must have caught the infection, for there was not one man aboard to mend another. Mutiny, it was plain, hung over us like a thunder-cloud.

And it was not only we of the cabin party who perceived the danger. Long John was hard at work going from group to group, spending himself in good advice, and as for example no man could have shown a better. He fairly outstripped himself in willingness and civility; he was all smiles to everyone. If an order were given, John would be on his crutch in an instant, with the cheeriest ‘Aye, aye, sir!’ in the world; and when there was nothing else to do, he kept up one song after another, as if to conceal the discontent of the rest.

Of all the gloomy features of that gloomy afternoon, this obvious anxiety on the part of Long John appeared the worst.

We held a council in the cabin.

‘Sir,’ said the captain, ‘if I risk another order, the whole ship’ll come about our ears by the run. You see, sir, here it is. I get a rough answer, do I not? Well, if I speak back, pikes will be going in two shakes; if I don’t, Silver will see there’s something under that, and the game’s up. Now, we’ve only one man to rely on.’

‘And who is that?’ asked the squire.

‘Silver, sir,’ returned the captain; ‘he’s as anxious as you and I to smother things up. This is a tiff; he’d soon talk ‘em out of it if he had the chance, and what I propose to do is to give him the chance. Let’s allow the men an afternoon ashore. If they all go, why we’ll fight the ship. If they none of them go, well then, we hold the cabin, and God defend the right. If some go, you mark my words, sir, Silver’ll bring ‘em aboard again as mild as lambs.’

It was so decided; loaded pistols were served out to all the sure men; Hunter, Joyce, and Redruth were taken into our confidence and received the news with less surprise and a better spirit than we had looked for, and then the captain went on deck and addressed the crew.

‘My lads,’ said he, ‘we’ve had a hot day and are all tired and out of sorts. A turn ashore’ll hurt nobody—the boats are still in the water; you can take the gigs, and as many as please may go ashore for the afternoon. I’ll fire a gun half an hour before sundown.’

I believe the silly fellows must have thought they would break their shins over treasure as soon as they were landed, for they all came out of their sulks in a moment and gave a cheer that started the echo in a far-away hill

and sent the birds once more flying and squalling round the anchorage.

The captain was too bright to be in the way. He whipped out of sight in a moment, leaving Silver to arrange the party, and I fancy it was as well he did so. Had he been on deck, he could no longer so much as have pretended not to understand the situation. It was as plain as day. Silver was the captain, and a mighty rebellious crew he had of it. The honest hands—and I was soon to see it proved that there were such on board—must have been very stupid fellows. Or rather, I suppose the truth was this, that all hands were disaffected by the example of the ringleaders—only some more, some less; and a few, being good fellows in the main, could neither be led nor driven any further. It is one thing to be idle and skulk and quite another to take a ship and murder a number of innocent men.

At last, however, the party was made up. Six fellows were to stay on board, and the remaining thirteen, including Silver, began to embark.

Then it was that there came into my head the first of the mad notions that contributed so much to save our lives. If six men were left by Silver, it was plain our party could not take and fight the ship; and since only six were

left, it was equally plain that the cabin party had no present need of my assistance. It occurred to me at once to go ashore. In a jiffy I had slipped over the side and curled up in the fore-sheets of the nearest boat, and almost at the same moment she shoved off.

No one took notice of me, only the bow oar saying, ‘Is that you, Jim? Keep your head down.’ But Silver, from the other boat, looked sharply over and called out to know if that were me; and from that moment I began to regret what I had done.

The crews raced for the beach, but the boat I was in, having some start and being at once the lighter and the better manned, shot far ahead of her consort, and the bow had struck among the shore-side trees and I had caught a branch and swung myself out and plunged into the nearest thicket while Silver and the rest were still a hundred yards behind.

‘Jim, Jim!’ I heard him shouting.

But you may suppose I paid no heed; jumping, ducking, and breaking through, I ran straight before my nose till I could run no longer.

## The First Blow

I WAS so pleased at having given the slip to Long John that I began to enjoy myself and look around me with some interest on the strange land that I was in.

I had crossed a marshy tract full of willows, bulrushes, and odd, outlandish, swampy trees; and I had now come out upon the skirts of an open piece of undulating, sandy country, about a mile long, dotted with a few pines and a great number of contorted trees, not unlike the oak in growth, but pale in the foliage, like willows. On the far side of the open stood one of the hills, with two quaint, craggy peaks shining vividly in the sun.

I now felt for the first time the joy of exploration. The isle was uninhabited; my shipmates I had left behind, and nothing lived in front of me but dumb brutes and fowls. I turned hither and thither among the trees. Here and there were flowering plants, unknown to me; here and there I saw snakes, and one raised his head from a ledge of rock and hissed at me with a noise not unlike the spinning of a

top. Little did I suppose that he was a deadly enemy and that the noise was the famous rattle.

Then I came to a long thicket of these oaklike trees—live, or evergreen, oaks, I heard afterwards they should be called—which grew low along the sand like brambles, the boughs curiously twisted, the foliage compact, like thatch. The thicket stretched down from the top of one of the sandy knolls, spreading and growing taller as it went, until it reached the margin of the broad, reedy fen, through which the nearest of the little rivers soaked its way into the anchorage. The marsh was steaming in the strong sun, and the outline of the Spy-glass trembled through the haze.

All at once there began to go a sort of bustle among the bulrushes; a wild duck flew up with a quack, another followed, and soon over the whole surface of the marsh a great cloud of birds hung screaming and circling in the air. I judged at once that some of my shipmates must be drawing near along the borders of the fen. Nor was I deceived, for soon I heard the very distant and low tones of a human voice, which, as I continued to give ear, grew steadily louder and nearer.

This put me in a great fear, and I crawled under cover of the nearest live-oak and squatted there, hearkening, as silent as a mouse.

Another voice answered, and then the first voice, which I now recognized to be Silver's, once more took up the story and ran on for a long while in a stream, only now and again interrupted by the other. By the sound they must have been talking earnestly, and almost fiercely; but no distinct word came to my hearing.

At last the speakers seemed to have paused and perhaps to have sat down, for not only did they cease to draw any nearer, but the birds themselves began to grow more quiet and to settle again to their places in the swamp.

And now I began to feel that I was neglecting my business, that since I had been so foolhardy as to come ashore with these desperadoes, the least I could do was to overhear them at their councils, and that my plain and obvious duty was to draw as close as I could manage, under the favourable ambush of the crouching trees.

I could tell the direction of the speakers pretty exactly, not only by the sound of their voices but by the behaviour of the few birds that still hung in alarm above the heads of the intruders.

Crawling on all fours, I made steadily but slowly towards them, till at last, raising my head to an aperture among the leaves, I could see clear down into a little green dell beside the marsh, and closely set about with trees, where Long John Silver and another of the crew stood face to face in conversation.

The sun beat full upon them. Silver had thrown his hat beside him on the ground, and his great, smooth, blond face, all shining with heat, was lifted to the other man's in a kind of appeal.

'Mate,' he was saying, 'it's because I thinks gold dust of you—gold dust, and you may lay to that! If I hadn't took to you like pitch, do you think I'd have been here a-warning of you? All's up—you can't make nor mend; it's to save your neck that I'm a-speaking, and if one of the wild uns knew it, where'd I be, Tom— now, tell me, where'd I be?'

'Silver,' said the other man—and I observed he was not only red in the face, but spoke as hoarse as a crow, and his voice shook too, like a taut rope—'Silver,' says he, 'you're old, and you're honest, or has the name for it; and you've money too, which lots of poor sailors hasn't; and you're brave, or I'm mistook. And will you tell me you'll let yourself be led away with that kind of a mess of

swabs? Not you! As sure as God sees me, I'd sooner lose my hand. If I turn agin my dooty—‘

And then all of a sudden he was interrupted by a noise. I had found one of the honest hands—well, here, at that same moment, came news of another. Far away out in the marsh there arose, all of a sudden, a sound like the cry of anger, then another on the back of it; and then one horrid, long-drawn scream. The rocks of the Spy-glass re-echoed it a score of times; the whole troop of marsh-birds rose again, darkening heaven, with a simultaneous whirr; and long after that death yell was still ringing in my brain, silence had re-established its empire, and only the rustle of the redescending birds and the boom of the distant surges disturbed the languor of the afternoon.

Tom had leaped at the sound, like a horse at the spur, but Silver had not winked an eye. He stood where he was, resting lightly on his crutch, watching his companion like a snake about to spring.

‘John!’ said the sailor, stretching out his hand.

‘Hands off!’ cried Silver, leaping back a yard, as it seemed to me, with the speed and security of a trained gymnast.

‘Hands off, if you like, John Silver,’ said the other. ‘It’s a black conscience that can make you feared of me. But in heaven’s name, tell me, what was that?’

‘That?’ returned Silver, smiling away, but warier than ever, his eye a mere pin-point in his big face, but gleaming like a crumb of glass. ‘That?’ Oh, I reckon that’ll be Alan.’

And at this point Tom flashed out like a hero.

‘Alan!’ he cried. ‘Then rest his soul for a true seaman! And as for you, John Silver, long you’ve been a mate of mine, but you’re mate of mine no more. If I die like a dog, I’ll die in my dooty. You’ve killed Alan, have you? Kill me too, if you can. But I defies you.’

And with that, this brave fellow turned his back directly on the cook and set off walking for the beach. But he was not destined to go far. With a cry John seized the branch of a tree, whipped the crutch out of his armpit, and sent that uncouth missile hurtling through the air. It struck poor Tom, point foremost, and with stunning violence, right between the shoulders in the middle of his back. His hands flew up, he gave a sort of gasp, and fell.

Whether he were injured much or little, none could ever tell. Like enough, to judge from the sound, his back was broken on the spot. But he had no time given him to

recover. Silver, agile as a monkey even without leg or crutch, was on the top of him next moment and had twice buried his knife up to the hilt in that defenceless body. From my place of ambush, I could hear him pant aloud as he struck the blows.

I do not know what it rightly is to faint, but I do know that for the next little while the whole world swam away from before me in a whirling mist; Silver and the birds, and the tall Spy-glass hilltop, going round and round and topsy-turvy before my eyes, and all manner of bells ringing and distant voices shouting in my ear.

When I came again to myself the monster had pulled himself together, his crutch under his arm, his hat upon his head. Just before him Tom lay motionless upon the sward; but the murderer minded him not a whit, cleansing his blood-stained knife the while upon a wisp of grass. Everything else was unchanged, the sun still shining mercilessly on the steaming marsh and the tall pinnacle of the mountain, and I could scarce persuade myself that murder had been actually done and a human life cruelly cut short a moment since before my eyes.

But now John put his hand into his pocket, brought out a whistle, and blew upon it several modulated blasts that rang far across the heated air. I could not tell, of course,

## *Treasure Island*

the meaning of the signal, but it instantly awoke my fears. More men would be coming. I might be discovered. They had already slain two of the honest people; after Tom and Alan, might not I come next?

Instantly I began to extricate myself and crawl back again, with what speed and silence I could manage, to the more open portion of the wood. As I did so, I could hear hails coming and going between the old buccaneer and his comrades, and this sound of danger lent me wings. As soon as I was clear of the thicket, I ran as I never ran before, scarce minding the direction of my flight, so long as it led me from the murderers; and as I ran, fear grew and grew upon me until it turned into a kind of frenzy.

Indeed, could anyone be more entirely lost than I? When the gun fired, how should I dare to go down to the boats among those fiends, still smoking from their crime? Would not the first of them who saw me wring my neck like a snipe's? Would not my absence itself be an evidence to them of my alarm, and therefore of my fatal knowledge? It was all over, I thought. Good-bye to the HISPANIOLA; good-bye to the squire, the doctor, and the captain! There was nothing left for me but death by starvation or death by the hands of the mutineers.

All this while, as I say, I was still running, and without taking any notice, I had drawn near to the foot of the little hill with the two peaks and had got into a part of the island where the live-oaks grew more widely apart and seemed more like forest trees in their bearing and dimensions. Mingled with these were a few scattered pines, some fifty, some nearer seventy, feet high. The air too smelt more freshly than down beside the marsh.

And here a fresh alarm brought me to a standstill with a thumping heart.

## The Man of the Island

FROM the side of the hill, which was here steep and stony, a spout of gravel was dislodged and fell rattling and bounding through the trees. My eyes turned instinctively in that direction, and I saw a figure leap with great rapidity behind the trunk of a pine. What it was, whether bear or man or monkey, I could in no wise tell. It seemed dark and shaggy; more I knew not. But the terror of this new apparition brought me to a stand.

I was now, it seemed, cut off upon both sides; behind me the murderers, before me this lurking nondescript. And immediately I began to prefer the dangers that I knew to those I knew not. Silver himself appeared less terrible in contrast with this creature of the woods, and I turned on my heel, and looking sharply behind me over my shoulder, began to retrace my steps in the direction of the boats.

Instantly the figure reappeared, and making a wide circuit, began to head me off. I was tired, at any rate; but had I been as fresh as when I rose, I could see it was in

vain for me to contend in speed with such an adversary. From trunk to trunk the creature flitted like a deer, running manlike on two legs, but unlike any man that I had ever seen, stooping almost double as it ran. Yet a man it was, I could no longer be in doubt about that.

I began to recall what I had heard of cannibals. I was within an ace of calling for help. But the mere fact that he was a man, however wild, had somewhat reassured me, and my fear of Silver began to revive in proportion. I stood still, therefore, and cast about for some method of escape; and as I was so thinking, the recollection of my pistol flashed into my mind. As soon as I remembered I was not defenceless, courage glowed again in my heart and I set my face resolutely for this man of the island and walked briskly towards him.

He was concealed by this time behind another tree trunk; but he must have been watching me closely, for as soon as I began to move in his direction he reappeared and took a step to meet me. Then he hesitated, drew back, came forward again, and at last, to my wonder and confusion, threw himself on his knees and held out his clasped hands in supplication.

At that I once more stopped.

‘Who are you?’ I asked.

‘Ben Gunn,’ he answered, and his voice sounded hoarse and awkward, like a rusty lock. ‘I’m poor Ben Gunn, I am; and I haven’t spoke with a Christian these three years.’

I could now see that he was a white man like myself and that his features were even pleasing. His skin, wherever it was exposed, was burnt by the sun; even his lips were black, and his fair eyes looked quite startling in so dark a face. Of all the beggar-men that I had seen or fancied, he was the chief for raggedness. He was clothed with tatters of old ship’s canvas and old sea-cloth, and this extraordinary patchwork was all held together by a system of the most various and incongruous fastenings, brass buttons, bits of stick, and loops of tarry gaskin. About his waist he wore an old brass-buckled leather belt, which was the one thing solid in his whole accoutrement.

‘Three years!’ I cried. ‘Were you shipwrecked?’

‘Nay, mate,’ said he; ‘marooned.’

I had heard the word, and I knew it stood for a horrible kind of punishment common enough among the buccaneers, in which the offender is put ashore with a little powder and shot and left behind on some desolate and distant island.

‘Marooned three years agone,’ he continued, ‘and lived on goats since then, and berries, and oysters. Wherever a man is, says I, a man can do for himself. But, mate, my heart is sore for Christian diet. You mightn’t happen to have a piece of cheese about you, now? No? Well, many’s the long night I’ve dreamed of cheese—toasted, mostly—and woke up again, and here I were.’

‘If ever I can get aboard again,’ said I, ‘you shall have cheese by the stone.’

All this time he had been feeling the stuff of my jacket, smoothing my hands, looking at my boots, and generally, in the intervals of his speech, showing a childish pleasure in the presence of a fellow creature. But at my last words he perked up into a kind of startled slyness.

‘If ever you can get aboard again, says you?’ he repeated. ‘Why, now, who’s to hinder you?’

‘Not you, I know,’ was my reply.

‘And right you was,’ he cried. ‘Now you—what do you call yourself, mate?’

‘Jim,’ I told him.

‘Jim, Jim,’ says he, quite pleased apparently. ‘Well, now, Jim, I’ve lived that rough as you’d be ashamed to hear of. Now, for instance, you wouldn’t think I had had a pious mother—to look at me?’ he asked.

‘Why, no, not in particular,’ I answered.

‘Ah, well,’ said he, ‘but I had—remarkable pious. And I was a civil, pious boy, and could rattle off my catechism that fast, as you couldn’t tell one word from another. And here’s what it come to, Jim, and it begun with chuck-farthen on the blessed grave-stones! That’s what it begun with, but it went further’n that; and so my mother told me, and predicked the whole, she did, the pious woman! But it were Providence that put me here. I’ve thought it all out in this here lonely island, and I’m back on piety. You don’t catch me tasting rum so much, but just a thimbleful for luck, of course, the first chance I have. I’m bound I’ll be good, and I see the way to. And, Jim’—looking all round him and lowering his voice to a whisper—‘I’m rich.’

I now felt sure that the poor fellow had gone crazy in his solitude, and I suppose I must have shown the feeling in my face, for he repeated the statement hotly: ‘Rich! Rich! I says. And I’ll tell you what: I’ll make a man of you, Jim. Ah, Jim, you’ll bless your stars, you will, you was the first that found me!’

And at this there came suddenly a lowering shadow over his face, and he tightened his grasp upon my hand and raised a forefinger threateningly before my eyes.

‘Now, Jim, you tell me true: that ain’t Flint’s ship?’ he asked.

At this I had a happy inspiration. I began to believe that I had found an ally, and I answered him at once.

‘It’s not Flint’s ship, and Flint is dead; but I’ll tell you true, as you ask me—there are some of Flint’s hands aboard; worse luck for the rest of us.’

‘Not a man—with one—leg?’ he gasped.

‘Silver?’ I asked.

‘Ah, Silver!’ says he. ‘That were his name.’

‘He’s the cook, and the ringleader too.’

He was still holding me by the wrist, and at that he give it quite a wring.

‘If you was sent by Long John,’ he said, ‘I’m as good as pork, and I know it. But where was you, do you suppose?’

I had made my mind up in a moment, and by way of answer told him the whole story of our voyage and the predicament in which we found ourselves. He heard me with the keenest interest, and when I had done he patted me on the head.

‘You’re a good lad, Jim,’ he said; ‘and you’re all in a clove hitch, ain’t you? Well, you just put your trust in Ben Gunn—Ben Gunn’s the man to do it. Would you think it

likely, now, that your squire would prove a liberal-minded one in case of help—him being in a clove hitch, as you remark?’

I told him the squire was the most liberal of men.

‘Aye, but you see,’ returned Ben Gunn, ‘I didn’t mean giving me a gate to keep, and a suit of livery clothes, and such; that’s not my mark, Jim. What I mean is, would he be likely to come down to the toon of, say one thousand pounds out of money that’s as good as a man’s own already?’

‘I am sure he would,’ said I. ‘As it was, all hands were to share.’

‘AND a passage home?’ he added with a look of great shrewdness.

‘Why,’ I cried, ‘the squire’s a gentleman. And besides, if we got rid of the others, we should want you to help work the vessel home.’

‘Ah,’ said he, ‘so you would.’ And he seemed very much relieved.

‘Now, I’ll tell you what,’ he went on. ‘So much I’ll tell you, and no more. I were in Flint’s ship when he buried the treasure; he and six along—six strong seamen. They was ashore nigh on a week, and us standing off and on in the old WALRUS. One fine day up went the signal, and

here come Flint by himself in a little boat, and his head done up in a blue scarf. The sun was getting up, and mortal white he looked about the cutwater. But, there he was, you mind, and the six all dead—dead and buried. How he done it, not a man aboard us could make out. It was battle, murder, and sudden death, leastways—him against six. Billy Bones was the mate; Long John, he was quartermaster; and they asked him where the treasure was. ‘Ah,’ says he, ‘you can go ashore, if you like, and stay,’ he says; ‘but as for the ship, she’ll beat up for more, by thunder!’ That’s what he said.

‘Well, I was in another ship three years back, and we sighted this island. ‘Boys,’ said I, ‘here’s Flint’s treasure; let’s land and find it.’ The cap’n was displeased at that, but my messmates were all of a mind and landed. Twelve days they looked for it, and every day they had the worse word for me, until one fine morning all hands went aboard. ‘As for you, Benjamin Gunn,’ says they, ‘here’s a musket,’ they says, ‘and a spade, and pick-axe. You can stay here and find Flint’s money for yourself,’ they says.

‘Well, Jim, three years have I been here, and not a bite of Christian diet from that day to this. But now, you look here; look at me. Do I look like a man before the mast? No, says you. Nor I weren’t, neither, I says.’

And with that he winked and pinched me hard.

‘Just you mention them words to your squire, Jim,’ he went on. ‘Nor he weren’t, neither—that’s the words. Three years he were the man of this island, light and dark, fair and rain; and sometimes he would maybe think upon a prayer (says you), and sometimes he would maybe think of his old mother, so be as she’s alive (you’ll say); but the most part of Gunn’s time (this is what you’ll say)—the most part of his time was took up with another matter. And then you’ll give him a nip, like I do.’

And he pinched me again in the most confidential manner.

‘Then,’ he continued, ‘then you’ll up, and you’ll say this: Gunn is a good man (you’ll say), and he puts a precious sight more confidence—a precious sight, mind that—in a gen’leman born than in these gen’leman of fortune, having been one hisself.’

‘Well,’ I said, ‘I don’t understand one word that you’ve been saying. But that’s neither here nor there; for how am I to get on board?’

‘Ah,’ said he, ‘that’s the hitch, for sure. Well, there’s my boat, that I made with my two hands. I keep her under the white rock. If the worst come to the worst, we might try that after dark. Hi!’ he broke out. ‘What’s that?’

For just then, although the sun had still an hour or two to run, all the echoes of the island awoke and bellowed to the thunder of a cannon.

‘They have begun to fight!’ I cried. ‘Follow me.’

And I began to run towards the anchorage, my terrors all forgotten, while close at my side the marooned man in his goatskins trotted easily and lightly.

‘Left, left,’ says he; ‘keep to your left hand, mate Jim! Under the trees with you! Theer’s where I killed my first goat. They don’t come down here now; they’re all mastheaded on them mountings for the fear of Benjamin Gunn. Ah! And there’s the ceteemory’— cemetery, he must have meant. ‘You see the mounds? I come here and prayed, nows and thens, when I thought maybe a Sunday would be about doo. It weren’t quite a chapel, but it seemed more solemn like; and then, says you, Ben Gunn was short-handed—no chapling, nor so much as a Bible and a flag, you says.’

So he kept talking as I ran, neither expecting nor receiving any answer.

The cannon-shot was followed after a considerable interval by a volley of small arms.

*Treasure Island*

Another pause, and then, not a quarter of a mile in front of me, I beheld the Union Jack flutter in the air above a wood.

## PART FOUR

### The Stockade

## 16

### **Narrative Continued by the Doctor: How the Ship Was Abandoned**

IT was about half past one—three bells in the sea phrase—that the two boats went ashore from the HISPANIOLA. The captain, the squire, and I were talking matters over in the cabin. Had there been a breath of wind, we should have fallen on the six mutineers who were left aboard with us, slipped our cable, and away to sea. But the wind was wanting; and to complete our helplessness, down came Hunter with the news that Jim Hawkins had slipped into a boat and was gone ashore with the rest.

It never occurred to us to doubt Jim Hawkins, but we were alarmed for his safety. With the men in the temper they were in, it seemed an even chance if we should see the lad again. We ran on deck. The pitch was bubbling in the seams; the nasty stench of the place turned me sick; if ever a man smelt fever and dysentery, it was in that abominable anchorage. The six scoundrels were sitting grumbling under a sail in the forecastle; ashore we could see the gigs made fast and a man sitting in each, hard by

where the river runs in. One of them was whistling ‘Lillibullero.’

Waiting was a strain, and it was decided that Hunter and I should go ashore with the jolly-boat in quest of information.

The gigs had leaned to their right, but Hunter and I pulled straight in, in the direction of the stockade upon the chart. The two who were left guarding their boats seemed in a bustle at our appearance; ‘Lillibullero’ stopped off, and I could see the pair discussing what they ought to do. Had they gone and told Silver, all might have turned out differently; but they had their orders, I suppose, and decided to sit quietly where they were and hark back again to ‘Lillibullero.’

There was a slight bend in the coast, and I steered so as to put it between us; even before we landed we had thus lost sight of the gigs. I jumped out and came as near running as I durst, with a big silk handkerchief under my hat for coolness’ sake and a brace of pistols ready primed for safety.

I had not gone a hundred yards when I reached the stockade.

This was how it was: a spring of clear water rose almost at the top of a knoll. Well, on the knoll, and

enclosing the spring, they had clapped a stout log-house fit to hold two score of people on a pinch and loopholed for musketry on either side. All round this they had cleared a wide space, and then the thing was completed by a palisade six feet high, without door or opening, too strong to pull down without time and labour and too open to shelter the besiegers. The people in the log-house had them in every way; they stood quiet in shelter and shot the others like partridges. All they wanted was a good watch and food; for, short of a complete surprise, they might have held the place against a regiment.

What particularly took my fancy was the spring. For though we had a good enough place of it in the cabin of the HISPANIOLA, with plenty of arms and ammunition, and things to eat, and excellent wines, there had been one thing overlooked—we had no water. I was thinking this over when there came ringing over the island the cry of a man at the point of death. I was not new to violent death—I have served his Royal Highness the Duke of Cumberland, and got a wound myself at Fontenoy—but I know my pulse went dot and carry one. ‘Jim Hawkins is gone,’ was my first thought.

It is something to have been an old soldier, but more still to have been a doctor. There is no time to dilly-dally

in our work. And so now I made up my mind instantly, and with no time lost returned to the shore and jumped on board the jolly-boat.

By good fortune Hunter pulled a good oar. We made the water fly, and the boat was soon alongside and I aboard the schooner.

I found them all shaken, as was natural. The squire was sitting down, as white as a sheet, thinking of the harm he had led us to, the good soul! And one of the six forecastle hands was little better.

‘There’s a man,’ says Captain Smollett, nodding towards him, ‘new to this work. He came nigh-hand fainting, doctor, when he heard the cry. Another touch of the rudder and that man would join us.’

I told my plan to the captain, and between us we settled on the details of its accomplishment.

We put old Redruth in the gallery between the cabin and the forecastle, with three or four loaded muskets and a mattress for protection. Hunter brought the boat round under the stern-port, and Joyce and I set to work loading her with powder tins, muskets, bags of biscuits, kegs of pork, a cask of cognac, and my invaluable medicine chest.

In the meantime, the squire and the captain stayed on deck, and the latter hailed the coxswain, who was the principal man aboard.

‘Mr. Hands,’ he said, ‘here are two of us with a brace of pistols each. If any one of you six make a signal of any description, that man’s dead.’

They were a good deal taken aback, and after a little consultation one and all tumbled down the fore companion, thinking no doubt to take us on the rear. But when they saw Redruth waiting for them in the sparred galley, they went about ship at once, and a head popped out again on deck.

‘Down, dog!’ cries the captain.

And the head popped back again; and we heard no more, for the time, of these six very faint-hearted seamen.

By this time, tumbling things in as they came, we had the jolly-boat loaded as much as we dared. Joyce and I got out through the stern-port, and we made for shore again as fast as oars could take us.

This second trip fairly aroused the watchers along shore. ‘Lillibullero’ was dropped again; and just before we lost sight of them behind the little point, one of them whipped ashore and disappeared. I had half a mind to change my plan and destroy their boats, but I feared that

Silver and the others might be close at hand, and all might very well be lost by trying for too much.

We had soon touched land in the same place as before and set to provision the block house. All three made the first journey, heavily laden, and tossed our stores over the palisade. Then, leaving Joyce to guard them—one man, to be sure, but with half a dozen muskets—Hunter and I returned to the jolly-boat and loaded ourselves once more. So we proceeded without pausing to take breath, till the whole cargo was bestowed, when the two servants took up their position in the block house, and I, with all my power, sculled back to the HISPANIOLA.

That we should have risked a second boat load seems more daring than it really was. They had the advantage of numbers, of course, but we had the advantage of arms. Not one of the men ashore had a musket, and before they could get within range for pistol shooting, we flattered ourselves we should be able to give a good account of a half-dozen at least.

The squire was waiting for me at the stern window, all his faintness gone from him. He caught the painter and made it fast, and we fell to loading the boat for our very lives. Pork, powder, and biscuit was the cargo, with only a musket and a cutlass apiece for the squire and me and

Redruth and the captain. The rest of the arms and powder we dropped overboard in two fathoms and a half of water, so that we could see the bright steel shining far below us in the sun, on the clean, sandy bottom.

By this time the tide was beginning to ebb, and the ship was swinging round to her anchor. Voices were heard faintly hallooing in the direction of the two gigs; and though this reassured us for Joyce and Hunter, who were well to the eastward, it warned our party to be off.

Redruth retreated from his place in the gallery and dropped into the boat, which we then brought round to the ship's counter, to be handier for Captain Smollett.

'Now, men,' said he, 'do you hear me?'

There was no answer from the forecastle.

'It's to you, Abraham Gray—it's to you I am speaking.'

Still no reply.

'Gray,' resumed Mr. Smollett, a little louder, 'I am leaving this ship, and I order you to follow your captain. I know you are a good man at bottom, and I dare say not one of the lot of you's as bad as he makes out. I have my watch here in my hand; I give you thirty seconds to join me in.'

There was a pause.

‘Come, my fine fellow,’ continued the captain; ‘don’t hang so long in stays. I’m risking my life and the lives of these good gentlemen every second.’

There was a sudden scuffle, a sound of blows, and out burst Abraham Gray with a knife cut on the side of the cheek, and came running to the captain like a dog to the whistle.

‘I’m with you, sir,’ said he.

And the next moment he and the captain had dropped aboard of us, and we had shoved off and given way.

We were clear out of the ship, but not yet ashore in our stockade.

## **Narrative Continued by the Doctor: The Jolly-boat's Last Trip**

THIS fifth trip was quite different from any of the others. In the first place, the little gallipot of a boat that we were in was gravely overloaded. Five grown men, and three of them—Trelawney, Redruth, and the captain—over six feet high, was already more than she was meant to carry. Add to that the powder, pork, and bread-bags. The gunwale was lipping astern. Several times we shipped a little water, and my breeches and the tails of my coat were all soaking wet before we had gone a hundred yards.

The captain made us trim the boat, and we got her to lie a little more evenly. All the same, we were afraid to breathe.

In the second place, the ebb was now making—a strong rippling current running westward through the basin, and then south'ard and seaward down the straits by which we had entered in the morning. Even the ripples were a danger to our overloaded craft, but the worst of it

was that we were swept out of our true course and away from our proper landing-place behind the point. If we let the current have its way we should come ashore beside the gigs, where the pirates might appear at any moment.

‘I cannot keep her head for the stockade, sir,’ said I to the captain. I was steering, while he and Redruth, two fresh men, were at the oars. ‘The tide keeps washing her down. Could you pull a little stronger?’

‘Not without swamping the boat,’ said he. ‘You must bear up, sir, if you please—bear up until you see you’re gaining.’

I tried and found by experiment that the tide kept sweeping us westward until I had laid her head due east, or just about right angles to the way we ought to go.

‘We’ll never get ashore at this rate,’ said I.

‘If it’s the only course that we can lie, sir, we must even lie it,’ returned the captain. ‘We must keep upstream. You see, sir,’ he went on, ‘if once we dropped to leeward of the landing-place, it’s hard to say where we should get ashore, besides the chance of being boarded by the gigs; whereas, the way we go the current must slacken, and then we can dodge back along the shore.’

## Treasure Island

‘The current’s less a’ready, sir,’ said the man Gray, who was sitting in the fore-sheets; ‘you can ease her off a bit.’

‘Thank you, my man,’ said I, quite as if nothing had happened, for we had all quietly made up our minds to treat him like one of ourselves.

Suddenly the captain spoke up again, and I thought his voice was a little changed.

‘The gun!’ said he.

‘I have thought of that,’ said I, for I made sure he was thinking of a bombardment of the fort. ‘They could never get the gun ashore, and if they did, they could never haul it through the woods.’

‘Look astern, doctor,’ replied the captain.

We had entirely forgotten the long nine; and there, to our horror, were the five rogues busy about her, getting off her jacket, as they called the stout tarpaulin cover under which she sailed. Not only that, but it flashed into my mind at the same moment that the round-shot and the powder for the gun had been left behind, and a stroke with an axe would put it all into the possession of the evil ones abroad.

‘Israel was Flint’s gunner,’ said Gray hoarsely.

At any risk, we put the boat's head direct for the landing-place. By this time we had got so far out of the run of the current that we kept steerage way even at our necessarily gentle rate of rowing, and I could keep her steady for the goal. But the worst of it was that with the course I now held we turned our broadside instead of our stern to the HISPANIOLA and offered a target like a barn door.

I could hear as well as see that brandy-faced rascal Israel Hands plumping down a round-shot on the deck.

‘Who’s the best shot?’ asked the captain.

‘Mr. Trelawney, out and away,’ said I.

‘Mr. Trelawney, will you please pick me off one of these men, sir? Hands, if possible,’ said the captain.

Trelawney was as cool as steel. He looked to the priming of his gun.

‘Now,’ cried the captain, ‘easy with that gun, sir, or you’ll swamp the boat. All hands stand by to trim her when he aims.’

The squire raised his gun, the rowing ceased, and we leaned over to the other side to keep the balance, and all was so nicely contrived that we did not ship a drop.

They had the gun, by this time, slewed round upon the swivel, and Hands, who was at the muzzle with the

rammer, was in consequence the most exposed. However, we had no luck, for just as Trelawney fired, down he stooped, the ball whistled over him, and it was one of the other four who fell.

The cry he gave was echoed not only by his companions on board but by a great number of voices from the shore, and looking in that direction I saw the other pirates trooping out from among the trees and tumbling into their places in the boats.

‘Here come the gigs, sir,’ said I.

‘Give way, then,’ cried the captain. ‘We mustn’t mind if we swamp her now. If we can’t get ashore, all’s up.’

‘Only one of the gigs is being manned, sir,’ I added; ‘the crew of the other most likely going round by shore to cut us off.’

‘They’ll have a hot run, sir,’ returned the captain. ‘Jack ashore, you know. It’s not them I mind; it’s the round-shot. Carpet bowls! My lady’s maid couldn’t miss. Tell us, squire, when you see the match, and we’ll hold water.’

In the meanwhile we had been making headway at a good pace for a boat so overloaded, and we had shipped but little water in the process. We were now close in; thirty or forty strokes and we should beach her, for the ebb had already disclosed a narrow belt of sand below the

clustering trees. The gig was no longer to be feared; the little point had already concealed it from our eyes. The ebb-tide, which had so cruelly delayed us, was now making reparation and delaying our assailants. The one source of danger was the gun.

‘If I durst,’ said the captain, ‘I’d stop and pick off another man.’

But it was plain that they meant nothing should delay their shot. They had never so much as looked at their fallen comrade, though he was not dead, and I could see him trying to crawl away.

‘Ready!’ cried the squire.

‘Hold!’ cried the captain, quick as an echo.

And he and Redruth backed with a great heave that sent her stern bodily under water. The report fell in at the same instant of time. This was the first that Jim heard, the sound of the squire’s shot not having reached him. Where the ball passed, not one of us precisely knew, but I fancy it must have been over our heads and that the wind of it may have contributed to our disaster.

At any rate, the boat sank by the stern, quite gently, in three feet of water, leaving the captain and myself, facing each other, on our feet. The other three took complete headers, and came up again drenched and bubbling.

So far there was no great harm. No lives were lost, and we could wade ashore in safety. But there were all our stores at the bottom, and to make things worse, only two guns out of five remained in a state for service. Mine I had snatched from my knees and held over my head, by a sort of instinct. As for the captain, he had carried his over his shoulder by a bandoleer, and like a wise man, lock uppermost. The other three had gone down with the boat.

To add to our concern, we heard voices already drawing near us in the woods along shore, and we had not only the danger of being cut off from the stockade in our half-crippled state but the fear before us whether, if Hunter and Joyce were attacked by half a dozen, they would have the sense and conduct to stand firm. Hunter was steady, that we knew; Joyce was a doubtful case—a pleasant, polite man for a valet and to brush one's clothes, but not entirely fitted for a man of war.

With all this in our minds, we waded ashore as fast as we could, leaving behind us the poor jolly-boat and a good half of all our powder and provisions.

## 18

### Narrative Continued by the Doctor: End of the First Day's Fighting

WE made our best speed across the strip of wood that now divided us from the stockade, and at every step we took the voices of the buccaneers rang nearer. Soon we could hear their footfalls as they ran and the cracking of the branches as they breasted across a bit of thicket.

I began to see we should have a brush for it in earnest and looked to my priming.

'Captain,' said I, 'Trelawney is the dead shot. Give him your gun; his own is useless.'

They exchanged guns, and Trelawney, silent and cool as he had been since the beginning of the bustle, hung a moment on his heel to see that all was fit for service. At the same time, observing Gray to be unarmed, I handed him my cutlass. It did all our hearts good to see him spit in his hand, knit his brows, and make the blade sing through the air. It was plain from every line of his body that our new hand was worth his salt.

Forty paces farther we came to the edge of the wood and saw the stockade in front of us. We struck the enclosure about the middle of the south side, and almost at the same time, seven mutineers—Job Anderson, the boatswain, at their head—appeared in full cry at the southwestern corner.

They paused as if taken aback, and before they recovered, not only the squire and I, but Hunter and Joyce from the block house, had time to fire. The four shots came in rather a scattering volley, but they did the business: one of the enemy actually fell, and the rest, without hesitation, turned and plunged into the trees.

After reloading, we walked down the outside of the palisade to see to the fallen enemy. He was stone dead—shot through the heart.

We began to rejoice over our good success when just at that moment a pistol cracked in the bush, a ball whistled close past my ear, and poor Tom Redruth stumbled and fell his length on the ground. Both the squire and I returned the shot, but as we had nothing to aim at, it is probable we only wasted powder. Then we reloaded and turned our attention to poor Tom.

The captain and Gray were already examining him, and I saw with half an eye that all was over.

I believe the readiness of our return volley had scattered the mutineers once more, for we were suffered without further molestation to get the poor old gamekeeper hoisted over the stockade and carried, groaning and bleeding, into the log-house.

Poor old fellow, he had not uttered one word of surprise, complaint, fear, or even acquiescence from the very beginning of our troubles till now, when we had laid him down in the log-house to die. He had lain like a Trojan behind his mattress in the gallery; he had followed every order silently, doggedly, and well; he was the oldest of our party by a score of years; and now, sullen, old, serviceable servant, it was he that was to die.

The squire dropped down beside him on his knees and kissed his hand, crying like a child.

‘Be I going, doctor?’ he asked.

‘Tom, my man,’ said I, ‘you’re going home.’

‘I wish I had had a lick at them with the gun first,’ he replied.

‘Tom,’ said the squire, ‘say you forgive me, won’t you?’

‘Would that be respectful like, from me to you, squire?’ was the answer. ‘Howsoever, so be it, amen!’

After a little while of silence, he said he thought somebody might read a prayer. ‘It’s the custom, sir,’ he added apologetically. And not long after, without another word, he passed away.

In the meantime the captain, whom I had observed to be wonderfully swollen about the chest and pockets, had turned out a great many various stores—the British colours, a Bible, a coil of stoutish rope, pen, ink, the log-book, and pounds of tobacco. He had found a longish fir-tree lying felled and trimmed in the enclosure, and with the help of Hunter he had set it up at the corner of the log-house where the trunks crossed and made an angle. Then, climbing on the roof, he had with his own hand bent and run up the colours.

This seemed mightily to relieve him. He re-entered the log-house and set about counting up the stores as if nothing else existed. But he had an eye on Tom’s passage for all that, and as soon as all was over, came forward with another flag and reverently spread it on the body.

‘Don’t you take on, sir,’ he said, shaking the squire’s hand. ‘All’s well with him; no fear for a hand that’s been shot down in his duty to captain and owner. It mayn’t be good divinity, but it’s a fact.’

Then he pulled me aside.

‘Dr. Livesey,’ he said, ‘in how many weeks do you and squire expect the consort?’

I told him it was a question not of weeks but of months, that if we were not back by the end of August Blandly was to send to find us, but neither sooner nor later. ‘You can calculate for yourself,’ I said.

‘Why, yes,’ returned the captain, scratching his head; ‘and making a large allowance, sir, for all the gifts of Providence, I should say we were pretty close hauled.’

‘How do you mean?’ I asked.

‘It’s a pity, sir, we lost that second load. That’s what I mean,’ replied the captain. ‘As for powder and shot, we’ll do. But the rations are short, very short— so short, Dr. Livesey, that we’re perhaps as well without that extra mouth.’

And he pointed to the dead body under the flag.

Just then, with a roar and a whistle, a round-shot passed high above the roof of the log-house and plumped far beyond us in the wood.

‘Oho!’ said the captain. ‘Blaze away! You’ve little enough powder already, my lads.’

At the second trial, the aim was better, and the ball descended inside the stockade, scattering a cloud of sand but doing no further damage.

‘Captain,’ said the squire, ‘the house is quite invisible from the ship. It must be the flag they are aiming at. Would it not be wiser to take it in?’

‘Strike my colours!’ cried the captain. ‘No, sir, not I’; and as soon as he had said the words, I think we all agreed with him. For it was not only a piece of stout, seamanly, good feeling; it was good policy besides and showed our enemies that we despised their cannonade.

All through the evening they kept thundering away. Ball after ball flew over or fell short or kicked up the sand in the enclosure, but they had to fire so high that the shot fell dead and buried itself in the soft sand. We had no ricochet to fear, and though one popped in through the roof of the log-house and out again through the floor, we soon got used to that sort of horse-play and minded it no more than cricket.

‘There is one good thing about all this,’ observed the captain; ‘the wood in front of us is likely clear. The ebb has made a good while; our stores should be uncovered. Volunteers to go and bring in pork.

Gray and hunter were the first to come forward. Well armed, they stole out of the stockade, but it proved a useless mission. The mutineers were bolder than we fancied or they put more trust in Israel’s gunnery. For

four or five of them were busy carrying off our stores and wading out with them to one of the gigs that lay close by, pulling an oar or so to hold her steady against the current. Silver was in the stern-sheets in command; and every man of them was now provided with a musket from some secret magazine of their own.

The captain sat down to his log, and here is the beginning of the entry:

Alexander Smollett, master; David Livesey, ship's doctor; Abraham Gray, carpenter's mate; John Trelawney, owner; John Hunter and Richard Joyce, owner's servants, landsmen—being all that is left faithful of the ship's company—with stores for ten days at short rations, came ashore this day and flew British colours on the log-house in Treasure Island. Thomas Redruth, owner's servant, landsman, shot by the mutineers; James Hawkins, cabin-boy—

And at the same time, I was wondering over poor Jim Hawkins' fate.

A hail on the land side.

'Somebody hailing us,' said Hunter, who was on guard.

'Doctor! Squire! Captain! Hullo, Hunter, is that you?' came the cries.

*Treasure Island*

And I ran to the door in time to see Jim Hawkins, safe and sound, come climbing over the stockade.

## Narrative Resumed by Jim Hawkins: The Garrison in the Stockade

AS soon as Ben Gunn saw the colours he came to a halt, stopped me by the arm, and sat down.

‘Now,’ said he, ‘there’s your friends, sure enough.’

‘Far more likely it’s the mutineers,’ I answered.

‘That!’ he cried. ‘Why, in a place like this, where nobody puts in but gen’lemen of fortune, Silver would fly the Jolly Roger, you don’t make no doubt of that. No, that’s your friends. There’s been blows too, and I reckon your friends has had the best of it; and here they are ashore in the old stockade, as was made years and years ago by Flint. Ah, he was the man to have a headpiece, was Flint! Barring rum, his match were never seen. He were afraid of none, not he; on’y Silver—Silver was that genteel.’

‘Well,’ said I, ‘that may be so, and so be it; all the more reason that I should hurry on and join my friends.’

‘Nay, mate,’ returned Ben, ‘not you. You’re a good boy, or I’m mistook; but you’re on’y a boy, all told. Now,

Ben Gunn is fly. Rum wouldn't bring me there, where you're going—not rum wouldn't, till I see your born gen'leman and gets it on his word of honour. And you won't forget my words; 'A precious sight (that's what you'll say), a precious sight more confidence'— and then nips him.

And he pinched me the third time with the same air of cleverness.

'And when Ben Gunn is wanted, you know where to find him, Jim. Just wheer you found him today. And him that comes is to have a white thing in his hand, and he's to come alone. Oh! And you'll say this: 'Ben Gunn,' says you, 'has reasons of his own.'

'Well,' said I, 'I believe I understand. You have something to propose, and you wish to see the squire or the doctor, and you're to be found where I found you. Is that all?'

'And when? says you,' he added. 'Why, from about noon observation to about six bells.'

'Good,' said I, 'and now may I go?'

'You won't forget?' he inquired anxiously. 'Precious sight, and reasons of his own, says you. Reasons of his own; that's the mainstay; as between man and man. Well, then'—still holding me—'I reckon you can go, Jim. And,

Jim, if you was to see Silver, you wouldn't go for to sell Ben Gunn? Wild horses wouldn't draw it from you? No, says you. And if them pirates camp ashore, Jim, what would you say but there'd be widders in the morning?"

Here he was interrupted by a loud report, and a cannonball came tearing through the trees and pitched in the sand not a hundred yards from where we two were talking. The next moment each of us had taken to his heels in a different direction.

For a good hour to come frequent reports shook the island, and balls kept crashing through the woods. I moved from hiding-place to hiding-place, always pursued, or so it seemed to me, by these terrifying missiles. But towards the end of the bombardment, though still I durst not venture in the direction of the stockade, where the balls fell oftenest, I had begun, in a manner, to pluck up my heart again, and after a long detour to the east, crept down among the shore-side trees.

The sun had just set, the sea breeze was rustling and tumbling in the woods and ruffling the grey surface of the anchorage; the tide, too, was far out, and great tracts of sand lay uncovered; the air, after the heat of the day, chilled me through my jacket.

The HISPANIOLA still lay where she had anchored; but, sure enough, there was the Jolly Roger—the black flag of piracy —flying from her peak. Even as I looked, there came another red flash and another report that sent the echoes clattering, and one more round-shot whistled through the air. It was the last of the cannonade.

I lay for some time watching the bustle which succeeded the attack. Men were demolishing something with axes on the beach near the stockade—the poor jolly-boat, I afterwards discovered. Away, near the mouth of the river, a great fire was glowing among the trees, and between that point and the ship one of the gigs kept coming and going, the men, whom I had seen so gloomy, shouting at the oars like children. But there was a sound in their voices which suggested rum.

At length I thought I might return towards the stockade. I was pretty far down on the low, sandy spit that encloses the anchorage to the east, and is joined at half-water to Skeleton Island; and now, as I rose to my feet, I saw, some distance further down the spit and rising from among low bushes, an isolated rock, pretty high, and peculiarly white in colour. It occurred to me that this might be the white rock of which Ben Gunn had spoken

and that some day or other a boat might be wanted and I should know where to look for one.

Then I skirted among the woods until I had regained the rear, or shoreward side, of the stockade, and was soon warmly welcomed by the faithful party.

I had soon told my story and began to look about me. The log-house was made of unsquared trunks of pine—roof, walls, and floor. The latter stood in several places as much as a foot or a foot and a half above the surface of the sand. There was a porch at the door, and under this porch the little spring welled up into an artificial basin of a rather odd kind—no other than a great ship's kettle of iron, with the bottom knocked out, and sunk ‘to her bearings,’ as the captain said, among the sand.

Little had been left besides the framework of the house, but in one corner there was a stone slab laid down by way of hearth and an old rusty iron basket to contain the fire.

The slopes of the knoll and all the inside of the stockade had been cleared of timber to build the house, and we could see by the stumps what a fine and lofty grove had been destroyed. Most of the soil had been washed away or buried in drift after the removal of the trees; only where the streamlet ran down from the kettle a

thick bed of moss and some ferns and little creeping bushes were still green among the sand. Very close around the stockade—too close for defence, they said—the wood still flourished high and dense, all of fir on the land side, but towards the sea with a large admixture of live-oaks.

The cold evening breeze, of which I have spoken, whistled through every chink of the rude building and sprinkled the floor with a continual rain of fine sand. There was sand in our eyes, sand in our teeth, sand in our suppers, sand dancing in the spring at the bottom of the kettle, for all the world like porridge beginning to boil. Our chimney was a square hole in the roof; it was but a little part of the smoke that found its way out, and the rest eddied about the house and kept us coughing and piping the eye.

Add to this that Gray, the new man, had his face tied up in a bandage for a cut he had got in breaking away from the mutineers and that poor old Tom Redruth, still unburied, lay along the wall, stiff and stark, under the Union Jack.

If we had been allowed to sit idle, we should all have fallen in the blues, but Captain Smollett was never the man for that. All hands were called up before him, and he

divided us into watches. The doctor and Gray and I for one; the squire, Hunter, and Joyce upon the other. Tired though we all were, two were sent out for firewood; two more were set to dig a grave for Redruth; the doctor was named cook; I was put sentry at the door; and the captain himself went from one to another, keeping up our spirits and lending a hand wherever it was wanted.

From time to time the doctor came to the door for a little air and to rest his eyes, which were almost smoked out of his head, and whenever he did so, he had a word for me.

‘That man Smollett,’ he said once, ‘is a better man than I am. And when I say that it means a deal, Jim.’

Another time he came and was silent for a while. Then he put his head on one side, and looked at me.

‘Is this Ben Gunn a man?’ he asked.

‘I do not know, sir,’ said I. ‘I am not very sure whether he’s sane.’

‘If there’s any doubt about the matter, he is,’ returned the doctor. ‘A man who has been three years biting his nails on a desert island, Jim, can’t expect to appear as sane as you or me. It doesn’t lie in human nature. Was it cheese you said he had a fancy for?’

‘Yes, sir, cheese,’ I answered.

‘Well, Jim,’ says he, ‘just see the good that comes of being dainty in your food. You’ve seen my snuff-box, haven’t you? And you never saw me take snuff, the reason being that in my snuff-box I carry a piece of Parmesan cheese—a cheese made in Italy, very nutritious. Well, that’s for Ben Gunn!’

Before supper was eaten we buried old Tom in the sand and stood round him for a while bare-headed in the breeze. A good deal of firewood had been got in, but not enough for the captain’s fancy, and he shook his head over it and told us we ‘must get back to this tomorrow rather livelier.’ Then, when we had eaten our pork and each had a good stiff glass of brandy grog, the three chiefs got together in a corner to discuss our prospects.

It appears they were at their wits’ end what to do, the stores being so low that we must have been starved into surrender long before help came. But our best hope, it was decided, was to kill off the buccaneers until they either hauled down their flag or ran away with the HISPANIOLA. From nineteen they were already reduced to fifteen, two others were wounded, and one at least—the man shot beside the gun—severely wounded, if he were not dead. Every time we had a crack at them, we were to take it, saving our own lives, with the extremest

care. And besides that, we had two able allies—rum and the climate.

As for the first, though we were about half a mile away, we could hear them roaring and singing late into the night; and as for the second, the doctor staked his wig that, camped where they were in the marsh and unprovided with remedies, the half of them would be on their backs before a week.

‘So,’ he added, ‘if we are not all shot down first they’ll be glad to be packing in the schooner. It’s always a ship, and they can get to buccaneering again, I suppose.’

‘First ship that ever I lost,’ said Captain Smollett.

I was dead tired, as you may fancy; and when I got to sleep, which was not till after a great deal of tossing, I slept like a log of wood.

The rest had long been up and had already breakfasted and increased the pile of firewood by about half as much again when I was wakened by a bustle and the sound of voices.

‘Flag of truce!’ I heard someone say; and then, immediately after, with a cry of surprise, ‘Silver himself!’

And at that, up I jumped, and rubbing my eyes, ran to a loophole in the wall.

## 20

### Silver's Embassy

SURE enough, there were two men just outside the stockade, one of them waving a white cloth, the other, no less a person than Silver himself, standing placidly by.

It was still quite early, and the coldest morning that I think I ever was abroad in—a chill that pierced into the marrow. The sky was bright and cloudless overhead, and the tops of the trees shone rosily in the sun. But where Silver stood with his lieutenant, all was still in shadow, and they waded knee-deep in a low white vapour that had crawled during the night out of the morass. The chill and the vapour taken together told a poor tale of the island. It was plainly a damp, feverish, unhealthy spot.

'Keep indoors, men,' said the captain. 'Ten to one this is a trick.'

Then he hailed the buccaneer.

'Who goes? Stand, or we fire.'

'Flag of truce,' cried Silver.

The captain was in the porch, keeping himself carefully out of the way of a treacherous shot, should any

be intended. He turned and spoke to us, ‘Doctor’s watch on the lookout. Dr. Livesey take the north side, if you please; Jim, the east; Gray, west. The watch below, all hands to load muskets. Lively, men, and careful.’

And then he turned again to the mutineers.

‘And what do you want with your flag of truce?’ he cried.

This time it was the other man who replied.

‘Cap’n Silver, sir, to come on board and make terms,’ he shouted.

‘Cap’n Silver! Don’t know him. Who’s he?’ cried the captain. And we could hear him adding to himself, ‘Cap’n, is it? My heart, and here’s promotion!’

Long John answered for himself. ‘Me, sir. These poor lads have chosen me cap’n, after your desertion, sir’— laying a particular emphasis upon the word ‘desertion.’ ‘We’re willing to submit, if we can come to terms, and no bones about it. All I ask is your word, Cap’n Smollett, to let me safe and sound out of this here stockade, and one minute to get out o’ shot before a gun is fired.’

‘My man,’ said Captain Smollett, ‘I have not the slightest desire to talk to you. If you wish to talk to me, you can come, that’s all. If there’s any treachery, it’ll be on your side, and the Lord help you.’

## Treasure Island

‘That’s enough, cap’n,’ shouted Long John cheerily. ‘A word from you’s enough. I know a gentleman, and you may lay to that.’

We could see the man who carried the flag of truce attempting to hold Silver back. Nor was that wonderful, seeing how cavalier had been the captain’s answer. But Silver laughed at him aloud and slapped him on the back as if the idea of alarm had been absurd. Then he advanced to the stockade, threw over his crutch, got a leg up, and with great vigour and skill succeeded in surmounting the fence and dropping safely to the other side.

I will confess that I was far too much taken up with what was going on to be of the slightest use as sentry; indeed, I had already deserted my eastern loophole and crept up behind the captain, who had now seated himself on the threshold, with his elbows on his knees, his head in his hands, and his eyes fixed on the water as it bubbled out of the old iron kettle in the sand. He was whistling ‘Come, Lasses and Lads.’

Silver had terrible hard work getting up the knoll. What with the steepness of the incline, the thick tree stumps, and the soft sand, he and his crutch were as helpless as a ship in stays. But he stuck to it like a man in silence, and at last arrived before the captain, whom he

saluted in the handsomest style. He was tricked out in his best; an immense blue coat, thick with brass buttons, hung as low as to his knees, and a fine laced hat was set on the back of his head.

‘Here you are, my man,’ said the captain, raising his head. ‘You had better sit down.’

‘You ain’t a-going to let me inside, cap’n?’ complained Long John. ‘It’s a main cold morning, to be sure, sir, to sit outside upon the sand.’

‘Why, Silver,’ said the captain, ‘if you had pleased to be an honest man, you might have been sitting in your galley. It’s your own doing. You’re either my ship’s cook—and then you were treated handsome—or Cap’n Silver, a common mutineer and pirate, and then you can go hang!’

‘Well, well, cap’n,’ returned the sea-cook, sitting down as he was bidden on the sand, ‘you’ll have to give me a hand up again, that’s all. A sweet pretty place you have of it here. Ah, there’s Jim! The top of the morning to you, Jim. Doctor, here’s my service. Why, there you all are together like a happy family, in a manner of speaking.’

‘If you have anything to say, my man, better say it,’ said the captain.

‘Right you were, Cap’n Smollett,’ replied Silver. ‘Dooty is dooty, to be sure. Well now, you look here, that was a good lay of yours last night. I don’t deny it was a good lay. Some of you pretty handy with a handspike-end. And I’ll not deny neither but what some of my people was shook—maybe all was shook; maybe I was shook myself; maybe that’s why I’m here for terms. But you mark me, cap’n, it won’t do twice, by thunder! We’ll have to do sentry-go and ease off a point or so on the rum. Maybe you think we were all a sheet in the wind’s eye. But I’ll tell you I was sober; I was on’y dog tired; and if I’d awoke a second sooner, I’d ‘a caught you at the act, I would. He wasn’t dead when I got round to him, not he.’

‘Well?’ says Captain Smollett as cool as can be.

All that Silver said was a riddle to him, but you would never have guessed it from his tone. As for me, I began to have an inkling. Ben Gunn’s last words came back to my mind. I began to suppose that he had paid the buccaneers a visit while they all lay drunk together round their fire, and I reckoned up with glee that we had only fourteen enemies to deal with.

‘Well, here it is,’ said Silver. ‘We want that treasure, and we’ll have it—that’s our point! You would just as

soon save your lives, I reckon; and that's yours. You have a chart, haven't you?"

"That's as may be," replied the captain.

"Oh, well, you have, I know that," returned Long John. "You needn't be so husky with a man; there ain't a particle of service in that, and you may lay to it. What I mean is, we want your chart. Now, I never meant you no harm, myself."

"That won't do with me, my man," interrupted the captain. "We know exactly what you meant to do, and we don't care, for now, you see, you can't do it."

And the captain looked at him calmly and proceeded to fill a pipe.

"If Abe Gray—" Silver broke out.

"Avast there!" cried Mr. Smollett. "Gray told me nothing, and I asked him nothing; and what's more, I would see you and him and this whole island blown clean out of the water into blazes first. So there's my mind for you, my man, on that."

This little whiff of temper seemed to cool Silver down. He had been growing nettled before, but now he pulled himself together.

"Like enough," said he. "I would set no limits to what gentlemen might consider shipshape, or might not, as the

case were. And seein' as how you are about to take a pipe, cap'n, I'll make so free as do likewise.'

And he filled a pipe and lighted it; and the two men sat silently smoking for quite a while, now looking each other in the face, now stopping their tobacco, now leaning forward to spit. It was as good as the play to see them.

'Now,' resumed Silver, 'here it is. You give us the chart to get the treasure by, and drop shooting poor seamen and stoving of their heads in while asleep. You do that, and we'll offer you a choice. Either you come aboard along of us, once the treasure shipped, and then I'll give you my affy-davy, upon my word of honour, to clap you somewhere safe ashore. Or if that ain't to your fancy, some of my hands being rough and having old scores on account of hazing, then you can stay here, you can. We'll divide stores with you, man for man; and I'll give my affy-davy, as before to speak the first ship I sight, and send 'em here to pick you up. Now, you'll own that's talking. Handsomer you couldn't look to get, now you. And I hope'—raising his voice—'that all hands in this here block house will overhaul my words, for what is spoke to one is spoke to all.'

Captain Smollett rose from his seat and knocked out the ashes of his pipe in the palm of his left hand.

‘Is that all?’ he asked.

‘Every last word, by thunder!’ answered John. ‘Refuse that, and you’ve seen the last of me but musket-balls.’

‘Very good,’ said the captain. ‘Now you’ll hear me. If you’ll come up one by one, unarmed, I’ll engage to clap you all in irons and take you home to a fair trial in England. If you won’t, my name is Alexander Smollett, I’ve flown my sovereign’s colours, and I’ll see you all to Davy Jones. You can’t find the treasure. You can’t sail the ship—there’s not a man among you fit to sail the ship. You can’t fight us— Gray, there, got away from five of you. Your ship’s in irons, Master Silver; you’re on a lee shore, and so you’ll find. I stand here and tell you so; and they’re the last good words you’ll get from me, for in the name of heaven, I’ll put a bullet in your back when next I meet you. Tramp, my lad. Bundle out of this, please, hand over hand, and double quick.’

Silver’s face was a picture; his eyes started in his head with wrath. He shook the fire out of his pipe.

‘Give me a hand up!’ he cried.

‘Not I,’ returned the captain.

‘Who’ll give me a hand up?’ he roared.

Not a man among us moved. Growling the foulest imprecations, he crawled along the sand till he got hold of

the porch and could hoist himself again upon his crutch. Then he spat into the spring.

‘There!’ he cried. ‘That’s what I think of ye. Before an hour’s out, I’ll stove in your old block house like a rum puncheon. Laugh, by thunder, laugh! Before an hour’s out, ye’ll laugh upon the other side. Them that die’ll be the lucky ones.’

And with a dreadful oath he stumbled off, ploughed down the sand, was helped across the stockade, after four or five failures, by the man with the flag of truce, and disappeared in an instant afterwards among the trees.

## 21

### The Attack

AS soon as Silver disappeared, the captain, who had been closely watching him, turned towards the interior of the house and found not a man of us at his post but Gray. It was the first time we had ever seen him angry.

‘Quarters!’ he roared. And then, as we all slunk back to our places, ‘Gray,’ he said, ‘I’ll put your name in the log; you’ve stood by your duty like a seaman. Mr. Trelawney, I’m surprised at you, sir. Doctor, I thought you had worn the king’s coat! If that was how you served at Fontenoy, sir, you’d have been better in your berth.’

The doctor’s watch were all back at their loopholes, the rest were busy loading the spare muskets, and everyone with a red face, you may be certain, and a flea in his ear, as the saying is.

The captain looked on for a while in silence. Then he spoke.

‘My lads,’ said he, ‘I’ve given Silver a broadside. I pitched it in red-hot on purpose; and before the hour’s out, as he said, we shall be boarded. We’re outnumbered,

I needn't tell you that, but we fight in shelter; and a minute ago I should have said we fought with discipline. I've no manner of doubt that we can drub them, if you choose.'

Then he went the rounds and saw, as he said, that all was clear.

On the two short sides of the house, east and west, there were only two loopholes; on the south side where the porch was, two again; and on the north side, five. There was a round score of muskets for the seven of us; the firewood had been built into four piles—tables, you might say—one about the middle of each side, and on each of these tables some ammunition and four loaded muskets were laid ready to the hand of the defenders. In the middle, the cutlasses lay ranged.

'Toss out the fire,' said the captain; 'the chill is past, and we mustn't have smoke in our eyes.'

The iron fire-basket was carried bodily out by Mr. Trelawney, and the embers smothered among sand.

'Hawkins hasn't had his breakfast. Hawkins, help yourself, and back to your post to eat it,' continued Captain Smollett. 'Lively, now, my lad; you'll want it before you've done. Hunter, serve out a round of brandy to all hands.'

And while this was going on, the captain completed, in his own mind, the plan of the defence.

'Doctor, you will take the door,' he resumed. 'See, and don't expose yourself; keep within, and fire through the porch. Hunter, take the east side, there. Joyce, you stand by the west, my man. Mr. Trelawney, you are the best shot—you and Gray will take this long north side, with the five loopholes; it's there the danger is. If they can get up to it and fire in upon us through our own ports, things would begin to look dirty. Hawkins, neither you nor I are much account at the shooting; we'll stand by to load and bear a hand.'

As the captain had said, the chill was past. As soon as the sun had climbed above our girdle of trees, it fell with all its force upon the clearing and drank up the vapours at a draught. Soon the sane was baking and the resin melting in the logs of the block house. Jackets and coats were flung aside, shirts thrown open at the neck and rolled up to the shoulders; and we stood there, each at his post, in a fever of heat and anxiety.

An hour passed away.

'Hang them!' said the captain. 'This is as dull as the doldrums. Gray, whistle for a wind.'

And just at that moment came the first news of the attack.

'If you please, sir,' said Joyce, 'if I see anyone, am I to fire?'

'I told you so!' cried the captain.

'Thank you, sir,' returned Joyce with the same quiet civility.

Nothing followed for a time, but the remark had set us all on the alert, straining ears and eyes—the musketeers with their pieces balanced in their hands, the captain out in the middle of the block house with his mouth very tight and a frown on his face.

So some seconds passed, till suddenly Joyce whipped up his musket and fired. The report had scarcely died away ere it was repeated and repeated from without in a scattering volley, shot behind shot, like a string of geese, from every side of the enclosure. Several bullets struck the log-house, but not one entered; and as the smoke cleared away and vanished, the stockade and the woods around it looked as quiet and empty as before. Not a bough waved, not the gleam of a musket-barrel betrayed the presence of our foes.

'Did you hit your man?' asked the captain.

'No, sir,' replied Joyce. 'I believe not, sir.'

‘Next best thing to tell the truth,’ muttered Captain Smollett. ‘Load his gun, Hawkins. How many should say there were on your side, doctor?’

‘I know precisely,’ said Dr. Livesey. ‘Three shots were fired on this side. I saw the three flashes—two close together—one farther to the west.’

‘Three!’ repeated the captain. ‘And how many on yours, Mr. Trelawney?’

But this was not so easily answered. There had come many from the north—seven by the squire’s computation, eight or nine according to Gray. From the east and west only a single shot had been fired. It was plain, therefore, that the attack would be developed from the north and that on the other three sides we were only to be annoyed by a show of hostilities. But Captain Smollett made no change in his arrangements. If the mutineers succeeded in crossing the stockade, he argued, they would take possession of any unprotected loophole and shoot us down like rats in our own stronghold.

Nor had we much time left to us for thought. Suddenly, with a loud huzza, a little cloud of pirates leaped from the woods on the north side and ran straight on the stockade. At the same moment, the fire was once more opened from

## *Treasure Island*

the woods, and a rifle ball sang through the doorway and knocked the doctor's musket into bits.

The boarders swarmed over the fence like monkeys. Squire and Gray fired again and yet again; three men fell, one forwards into the enclosure, two back on the outside. But of these, one was evidently more frightened than hurt, for he was on his feet again in a crack and instantly disappeared among the trees.

Two had bit the dust, one had fled, four had made good their footing inside our defences, while from the shelter of the woods seven or eight men, each evidently supplied with several muskets, kept up a hot though useless fire on the log-house.

The four who had boarded made straight before them for the building, shouting as they ran, and the men among the trees shouted back to encourage them. Several shots were fired, but such was the hurry of the marksmen that not one appears to have taken effect. In a moment, the four pirates had swarmed up the mound and were upon us.

The head of Job Anderson, the boatswain, appeared at the middle loophole.

'At 'em, all hands—all hands!' he roared in a voice of thunder.

At the same moment, another pirate grasped Hunter's musket by the muzzle, wrenched it from his hands, plucked it through the loophole, and with one stunning blow, laid the poor fellow senseless on the floor. Meanwhile a third, running unharmed all around the house, appeared suddenly in the doorway and fell with his cutlass on the doctor.

Our position was utterly reversed. A moment since we were firing, under cover, at an exposed enemy; now it was we who lay uncovered and could not return a blow.

The log-house was full of smoke, to which we owed our comparative safety. Cries and confusion, the flashes and reports of pistol-shots, and one loud groan rang in my ears.

'Out, lads, out, and fight 'em in the open! Cutlasses!' cried the captain.

I snatched a cutlass from the pile, and someone, at the same time snatching another, gave me a cut across the knuckles which I hardly felt. I dashed out of the door into the clear sunlight. Someone was close behind, I knew not whom. Right in front, the doctor was pursuing his assailant down the hill, and just as my eyes fell upon him, beat down his guard and sent him sprawling on his back with a great slash across the face.

‘Round the house, lads! Round the house!’ cried the captain; and even in the hurly-burly, I perceived a change in his voice.

Mechanically, I obeyed, turned eastwards, and with my cutlass raised, ran round the corner of the house. Next moment I was face to face with Anderson. He roared aloud, and his hanger went up above his head, flashing in the sunlight. I had not time to be afraid, but as the blow still hung impending, leaped in a trice upon one side, and missing my foot in the soft sand, rolled headlong down the slope.

When I had first sallied from the door, the other mutineers had been already swarming up the palisade to make an end of us. One man, in a red night-cap, with his cutlass in his mouth, had even got upon the top and thrown a leg across. Well, so short had been the interval that when I found my feet again all was in the same posture, the fellow with the red night-cap still half-way over, another still just showing his head above the top of the stockade. And yet, in this breath of time, the fight was over and the victory was ours.

Gray, following close behind me, had cut down the big boatswain ere he had time to recover from his last blow. Another had been shot at a loophole in the very act of

firing into the house and now lay in agony, the pistol still smoking in his hand. A third, as I had seen, the doctor had disposed of at a blow. Of the four who had scaled the palisade, one only remained unaccounted for, and he, having left his cutlass on the field, was now clambering out again with the fear of death upon him.

‘Fire—fire from the house!’ cried the doctor. ‘And you, lads, back into cover.’

But his words were unheeded, no shot was fired, and the last boarder made good his escape and disappeared with the rest into the wood. In three seconds nothing remained of the attacking party but the five who had fallen, four on the inside and one on the outside of the palisade.

The doctor and Gray and I ran full speed for shelter. The survivors would soon be back where they had left their muskets, and at any moment the fire might recommence.

The house was by this time somewhat cleared of smoke, and we saw at a glance the price we had paid for victory. Hunter lay beside his loophole, stunned; Joyce by his, shot through the head, never to move again; while right in the centre, the squire was supporting the captain, one as pale as the other.

‘The captain’s wounded,’ said Mr. Trelawney.

‘Have they run?’ asked Mr. Smollett.

‘All that could, you may be bound,’ returned the doctor; ‘but there’s five of them will never run again.’

‘Five!’ cried the captain. ‘Come, that’s better. Five against three leaves us four to nine. That’s better odds than we had at starting. We were seven to nineteen then, or thought we were, and that’s as bad to bear.’\*

\*The mutineers were soon only eight in number, for the man shot by Mr. Trelawney on board the schooner died that same evening of his wound. But this was, of course, not known till after by the faithful party.

## PART FIVE

### My Sea Adventure

## How My Sea Adventure Began

THERE was no return of the mutineers—not so much as another shot out of the woods. They had ‘got their rations for that day,’ as the captain put it, and we had the place to ourselves and a quiet time to overhaul the wounded and get dinner. Squire and I cooked outside in spite of the danger, and even outside we could hardly tell what we were at, for horror of the loud groans that reached us from the doctor’s patients.

Out of the eight men who had fallen in the action, only three still breathed—that one of the pirates who had been shot at the loophole, Hunter, and Captain Smollett; and of these, the first two were as good as dead; the mutineer indeed died under the doctor’s knife, and Hunter, do what we could, never recovered consciousness in this world. He lingered all day, breathing loudly like the old buccaneer at home in his apoplectic fit, but the bones of his chest had been crushed by the blow and his skull fractured in falling, and some time in the following night, without sign or sound, he went to his Maker.

As for the captain, his wounds were grievous indeed, but not dangerous. No organ was fatally injured. Anderson's ball—for it was Job that shot him first—had broken his shoulder-blade and touched the lung, not badly; the second had only torn and displaced some muscles in the calf. He was sure to recover, the doctor said, but in the meantime, and for weeks to come, he must not walk nor move his arm, nor so much as speak when he could help it.

My own accidental cut across the knuckles was a flea-bite. Doctor Livesey patched it up with plaster and pulled my ears for me into the bargain.

After dinner the squire and the doctor sat by the captain's side awhile in consultation; and when they had talked to their hearts' content, it being then a little past noon, the doctor took up his hat and pistols, girt on a cutlass, put the chart in his pocket, and with a musket over his shoulder crossed the palisade on the north side and set off briskly through the trees.

Gray and I were sitting together at the far end of the block house, to be out of earshot of our officers consulting; and Gray took his pipe out of his mouth and fairly forgot to put it back again, so thunder-struck he was at this occurrence.

‘Why, in the name of Davy Jones,’ said he, ‘is Dr. Livesey mad?’

‘Why no,’ says I. ‘He’s about the last of this crew for that, I take it.’

‘Well, shipmate,’ said Gray, ‘mad he may not be; but if HE’S not, you mark my words, I am.’

‘I take it,’ replied I, ‘the doctor has his idea; and if I am right, he’s going now to see Ben Gunn.’

I was right, as appeared later; but in the meantime, the house being stifling hot and the little patch of sand inside the palisade ablaze with midday sun, I began to get another thought into my head, which was not by any means so right. What I began to do was to envy the doctor walking in the cool shadow of the woods with the birds about him and the pleasant smell of the pines, while I sat grilling, with my clothes stuck to the hot resin, and so much blood about me and so many poor dead bodies lying all around that I took a disgust of the place that was almost as strong as fear.

All the time I was washing out the block house, and then washing up the things from dinner, this disgust and envy kept growing stronger and stronger, till at last, being near a bread-bag, and no one then observing me, I took

the first step towards my escapade and filled both pockets of my coat with biscuit.

I was a fool, if you like, and certainly I was going to do a foolish, over-bold act; but I was determined to do it with all the precautions in my power. These biscuits, should anything befall me, would keep me, at least, from starving till far on in the next day.

The next thing I laid hold of was a brace of pistols, and as I already had a powder-horn and bullets, I felt myself well supplied with arms.

As for the scheme I had in my head, it was not a bad one in itself. I was to go down the sandy spit that divides the anchorage on the east from the open sea, find the white rock I had observed last evening, and ascertain whether it was there or not that Ben Gunn had hidden his boat, a thing quite worth doing, as I still believe. But as I was certain I should not be allowed to leave the enclosure, my only plan was to take French leave and slip out when nobody was watching, and that was so bad a way of doing it as made the thing itself wrong. But I was only a boy, and I had made my mind up.

Well, as things at last fell out, I found an admirable opportunity. The squire and Gray were busy helping the captain with his bandages, the coast was clear, I made a

bolt for it over the stockade and into the thickest of the trees, and before my absence was observed I was out of cry of my companions.

This was my second folly, far worse than the first, as I left but two sound men to guard the house; but like the first, it was a help towards saving all of us.

I took my way straight for the east coast of the island, for I was determined to go down the sea side of the spit to avoid all chance of observation from the anchorage. It was already late in the afternoon, although still warm and sunny. As I continued to thread the tall woods, I could hear from far before me not only the continuous thunder of the surf, but a certain tossing of foliage and grinding of boughs which showed me the sea breeze had set in higher than usual. Soon cool draughts of air began to reach me, and a few steps farther I came forth into the open borders of the grove, and saw the sea lying blue and sunny to the horizon and the surf tumbling and tossing its foam along the beach.

I have never seen the sea quiet round Treasure Island. The sun might blaze overhead, the air be without a breath, the surface smooth and blue, but still these great rollers would be running along all the external coast, thundering and thundering by day and night; and I scarce believe

there is one spot in the island where a man would be out of earshot of their noise.

I walked along beside the surf with great enjoyment, till, thinking I was now got far enough to the south, I took the cover of some thick bushes and crept warily up to the ridge of the spit.

Behind me was the sea, in front the anchorage. The sea breeze, as though it had the sooner blown itself out by its unusual violence, was already at an end; it had been succeeded by light, variable airs from the south and south-east, carrying great banks of fog; and the anchorage, under lee of Skeleton Island, lay still and leaden as when first we entered it. The HISPANIOLA, in that unbroken mirror, was exactly portrayed from the truck to the waterline, the Jolly Roger hanging from her peak.

Alongside lay one of the gigs, Silver in the stern-sheets—him I could always recognize—while a couple of men were leaning over the stern bulwarks, one of them with a red cap—the very rogue that I had seen some hours before stride-legs upon the palisade. Apparently they were talking and laughing, though at that distance—upwards of a mile—I could, of course, hear no word of what was said. All at once there began the most horrid, unearthly screaming, which at first startled me badly, though I had

## *Treasure Island*

soon remembered the voice of Captain Flint and even thought I could make out the bird by her bright plumage as she sat perched upon her master's wrist.

Soon after, the jolly-boat shoved off and pulled for shore, and the man with the red cap and his comrade went below by the cabin companion.

Just about the same time, the sun had gone down behind the Spy-glass, and as the fog was collecting rapidly, it began to grow dark in earnest. I saw I must lose no time if I were to find the boat that evening.

The white rock, visible enough above the brush, was still some eighth of a mile further down the spit, and it took me a goodish while to get up with it, crawling, often on all fours, among the scrub. Night had almost come when I laid my hand on its rough sides. Right below it there was an exceedingly small hollow of green turf, hidden by banks and a thick underwood about knee-deep, that grew there very plentifully; and in the centre of the dell, sure enough, a little tent of goat-skins, like what the gipsies carry about with them in England.

I dropped into the hollow, lifted the side of the tent, and there was Ben Gunn's boat—home-made if ever anything was home-made; a rude, lop-sided framework of tough wood, and stretched upon that a covering of goat-

skin, with the hair inside. The thing was extremely small, even for me, and I can hardly imagine that it could have floated with a full-sized man. There was one thwart set as low as possible, a kind of stretcher in the bows, and a double paddle for propulsion.

I had not then seen a coracle, such as the ancient Britons made, but I have seen one since, and I can give you no fairer idea of Ben Gunn's boat than by saying it was like the first and the worst coracle ever made by man. But the great advantage of the coracle it certainly possessed, for it was exceedingly light and portable.

Well, now that I had found the boat, you would have thought I had had enough of truancy for once, but in the meantime I had taken another notion and become so obstinately fond of it that I would have carried it out, I believe, in the teeth of Captain Smollett himself. This was to slip out under cover of the night, cut the HISPANIOLA adrift, and let her go ashore where she fancied. I had quite made up my mind that the mutineers, after their repulse of the morning, had nothing nearer their hearts than to up anchor and away to sea; this, I thought, it would be a fine thing to prevent, and now that I had seen how they left their watchmen unprovided with a boat, I thought it might be done with little risk.

Down I sat to wait for darkness, and made a hearty meal of biscuit. It was a night out of ten thousand for my purpose. The fog had now buried all heaven. As the last rays of daylight dwindled and disappeared, absolute blackness settled down on Treasure Island. And when, at last, I shouldered the coracle and groped my way stumblingly out of the hollow where I had supped, there were but two points visible on the whole anchorage.

One was the great fire on shore, by which the defeated pirates lay carousing in the swamp. The other, a mere blur of light upon the darkness, indicated the position of the anchored ship. She had swung round to the ebb—her bow was now towards me—the only lights on board were in the cabin, and what I saw was merely a reflection on the fog of the strong rays that flowed from the stern window.

The ebb had already run some time, and I had to wade through a long belt of swampy sand, where I sank several times above the ankle, before I came to the edge of the retreating water, and wading a little way in, with some strength and dexterity, set my coracle, keel downwards, on the surface.

## The Ebb-tide Runs

THE coracle—as I had ample reason to know before I was done with her—was a very safe boat for a person of my height and weight, both buoyant and clever in a sea-way; but she was the most cross-grained, lop-sided craft to manage. Do as you pleased, she always made more leeway than anything else, and turning round and round was the manoeuvre she was best at. Even Ben Gunn himself has admitted that she was ‘queer to handle till you knew her way.’

Certainly I did not know her way. She turned in every direction but the one I was bound to go; the most part of the time we were broadside on, and I am very sure I never should have made the ship at all but for the tide. By good fortune, paddle as I pleased, the tide was still sweeping me down; and there lay the HISPANIOLA right in the fairway, hardly to be missed.

First she loomed before me like a blot of something yet blacker than darkness, then her spars and hull began to take shape, and the next moment, as it seemed (for, the

farther I went, the brisker grew the current of the ebb), I was alongside of her hawser and had laid hold.

The hawser was as taut as a bowstring, and the current so strong she pulled upon her anchor. All round the hull, in the blackness, the rippling current bubbled and chattered like a little mountain stream. One cut with my sea-gully and the HISPANIOLA would go humming down the tide.

So far so good, but it next occurred to my recollection that a taut hawser, suddenly cut, is a thing as dangerous as a kicking horse. Ten to one, if I were so foolhardy as to cut the HISPANIOLA from her anchor, I and the coracle would be knocked clean out of the water.

This brought me to a full stop, and if fortune had not again particularly favoured me, I should have had to abandon my design. But the light airs which had begun blowing from the south-east and south had hauled round after nightfall into the south-west. Just while I was meditating, a puff came, caught the HISPANIOLA, and forced her up into the current; and to my great joy, I felt the hawser slacken in my grasp, and the hand by which I held it dip for a second under water.

With that I made my mind up, took out my gully, opened it with my teeth, and cut one strand after another,

till the vessel swung only by two. Then I lay quiet, waiting to sever these last when the strain should be once more lightened by a breath of wind.

All this time I had heard the sound of loud voices from the cabin, but to say truth, my mind had been so entirely taken up with other thoughts that I had scarcely given ear. Now, however, when I had nothing else to do, I began to pay more heed.

One I recognized for the coxswain's, Israel Hands, that had been Flint's gunner in former days. The other was, of course, my friend of the red night-cap. Both men were plainly the worse of drink, and they were still drinking, for even while I was listening, one of them, with a drunken cry, opened the stern window and threw out something, which I divined to be an empty bottle. But they were not only tipsy; it was plain that they were furiously angry. Oaths flew like hailstones, and every now and then there came forth such an explosion as I thought was sure to end in blows. But each time the quarrel passed off and the voices grumbled lower for a while, until the next crisis came and in its turn passed away without result.

On shore, I could see the glow of the great camp-fire burning warmly through the shore-side trees. Someone

was singing, a dull, old, droning sailor's song, with a droop and a quaver at the end of every verse, and seemingly no end to it at all but the patience of the singer. I had heard it on the voyage more than once and remembered these words:

'But one man of her crew alive,  
What put to sea with seventy-five.'

And I thought it was a ditty rather too dolefully appropriate for a company that had met such cruel losses in the morning. But, indeed, from what I saw, all these buccaneers were as callous as the sea they sailed on.

At last the breeze came; the schooner sidled and drew nearer in the dark; I felt the hawser slacken once more, and with a good, tough effort, cut the last fibres through.

The breeze had but little action on the coracle, and I was almost instantly swept against the bows of the HISPANIOLA. At the same time, the schooner began to turn upon her heel, spinning slowly, end for end, across the current.

I wrought like a fiend, for I expected every moment to be swamped; and since I found I could not push the coracle directly off, I now shoved straight astern. At length I was clear of my dangerous neighbour, and just as I gave the last impulsion, my hands came across a light

cord that was trailing overboard across the stern bulwarks. Instantly I grasped it.

Why I should have done so I can hardly say. It was at first mere instinct, but once I had it in my hands and found it fast, curiosity began to get the upper hand, and I determined I should have one look through the cabin window.

I pulled in hand over hand on the cord, and when I judged myself near enough, rose at infinite risk to about half my height and thus commanded the roof and a slice of the interior of the cabin.

By this time the schooner and her little consort were gliding pretty swiftly through the water; indeed, we had already fetched up level with the camp-fire. The ship was talking, as sailors say, loudly, treading the innumerable ripples with an incessant weltering splash; and until I got my eye above the window-sill I could not comprehend why the watchmen had taken no alarm. One glance, however, was sufficient; and it was only one glance that I durst take from that unsteady skiff. It showed me Hands and his companion locked together in deadly wrestle, each with a hand upon the other's throat.

I dropped upon the thwart again, none too soon, for I was near overboard. I could see nothing for the moment

but these two furious, encrimsoned faces swaying together under the smoky lamp, and I shut my eyes to let them grow once more familiar with the darkness.

The endless ballad had come to an end at last, and the whole diminished company about the camp-fire had broken into the chorus I had heard so often:

‘Fifteen men on the dead man’s chest—  
Yo-ho-ho, and a bottle of rum!  
Drink and the devil had done for the rest—  
Yo-ho-ho, and a bottle of rum!’

I was just thinking how busy drink and the devil were at that very moment in the cabin of the *HISPA NIOLA*, when I was surprised by a sudden lurch of the coracle. At the same moment, she yawed sharply and seemed to change her course. The speed in the meantime had strangely increased.

I opened my eyes at once. All round me were little ripples, combing over with a sharp, bristling sound and slightly phosphorescent. The *HISPA NIOLA* herself, a few yards in whose wake I was still being whirled along, seemed to stagger in her course, and I saw her spars toss a little against the blackness of the night; nay, as I looked longer, I made sure she also was wheeling to the southward.

I glanced over my shoulder, and my heart jumped against my ribs. There, right behind me, was the glow of the camp-fire. The current had turned at right angles, sweeping round along with it the tall schooner and the little dancing coracle; ever quickening, ever bubbling higher, ever muttering louder, it went spinning through the narrows for the open sea.

Suddenly the schooner in front of me gave a violent yaw, turning, perhaps, through twenty degrees; and almost at the same moment one shout followed another from on board; I could hear feet pounding on the companion ladder and I knew that the two drunkards had at last been interrupted in their quarrel and awakened to a sense of their disaster.

I lay down flat in the bottom of that wretched skiff and devoutly recommended my spirit to its Maker. At the end of the straits, I made sure we must fall into some bar of raging breakers, where all my troubles would be ended speedily; and though I could, perhaps, bear to die, I could not bear to look upon my fate as it approached.

So I must have lain for hours, continually beaten to and fro upon the billows, now and again wetted with flying sprays, and never ceasing to expect death at the next plunge. Gradually weariness grew upon me; a numbness,

an occasional stupor, fell upon my mind even in the midst of my terrors, until sleep at last supervened and in my sea-tossed coracle I lay and dreamed of home and the old Admiral Benbow.

## The Cruise of the Coracle

IT was broad day when I awoke and found myself tossing at the south-west end of Treasure Island. The sun was up but was still hid from me behind the great bulk of the Spy-glass, which on this side descended almost to the sea in formidable cliffs.

Haulbowline Head and Mizzen-mast Hill were at my elbow, the hill bare and dark, the head bound with cliffs forty or fifty feet high and fringed with great masses of fallen rock. I was scarce a quarter of a mile to seaward, and it was my first thought to paddle in and land.

That notion was soon given over. Among the fallen rocks the breakers spouted and bellowed; loud reverberations, heavy sprays flying and falling, succeeded one another from second to second; and I saw myself, if I ventured nearer, dashed to death upon the rough shore or spending my strength in vain to scale the beetling crags.

Nor was that all, for crawling together on flat tables of rock or letting themselves drop into the sea with loud reports I beheld huge slimy monsters—soft snails, as it

## Treasure Island

were, of incredible bigness—two or three score of them together, making the rocks to echo with their barkings.

I have understood since that they were sea lions, and entirely harmless. But the look of them, added to the difficulty of the shore and the high running of the surf, was more than enough to disgust me of that landing-place. I felt willing rather to starve at sea than to confront such perils.

In the meantime I had a better chance, as I supposed, before me. North of Haulbowline Head, the land runs in a long way, leaving at low tide a long stretch of yellow sand. To the north of that, again, there comes another cape—Cape of the Woods, as it was marked upon the chart—buried in tall green pines, which descended to the margin of the sea.

I remembered what Silver had said about the current that sets northward along the whole west coast of Treasure Island, and seeing from my position that I was already under its influence, I preferred to leave Haulbowline Head behind me and reserve my strength for an attempt to land upon the kindlier-looking Cape of the Woods.

There was a great, smooth swell upon the sea. The wind blowing steady and gentle from the south, there was

no contrariety between that and the current, and the billows rose and fell unbroken.

Had it been otherwise, I must long ago have perished; but as it was, it is surprising how easily and securely my little and light boat could ride. Often, as I still lay at the bottom and kept no more than an eye above the gunwale, I would see a big blue summit heaving close above me; yet the coracle would but bounce a little, dance as if on springs, and subside on the other side into the trough as lightly as a bird.

I began after a little to grow very bold and sat up to try my skill at paddling. But even a small change in the disposition of the weight will produce violent changes in the behaviour of a coracle. And I had hardly moved before the boat, giving up at once her gentle dancing movement, ran straight down a slope of water so steep that it made me giddy, and struck her nose, with a spout of spray, deep into the side of the next wave.

I was drenched and terrified, and fell instantly back into my old position, whereupon the coracle seemed to find her head again and led me as softly as before among the billows. It was plain she was not to be interfered with, and at that rate, since I could in no way influence her course, what hope had I left of reaching land?

I began to be horribly frightened, but I kept my head, for all that. First, moving with all care, I gradually baled out the coracle with my sea-cap; then, getting my eye once more above the gunwale, I set myself to study how it was she managed to slip so quietly through the rollers.

I found each wave, instead of the big, smooth glossy mountain it looks from shore or from a vessel's deck, was for all the world like any range of hills on dry land, full of peaks and smooth places and valleys. The coracle, left to herself, turning from side to side, threaded, so to speak, her way through these lower parts and avoided the steep slopes and higher, toppling summits of the wave.

'Well, now,' thought I to myself, 'it is plain I must lie where I am and not disturb the balance; but it is plain also that I can put the paddle over the side and from time to time, in smooth places, give her a shove or two towards land.' No sooner thought upon than done. There I lay on my elbows in the most trying attitude, and every now and again gave a weak stroke or two to turn her head to shore.

It was very tiring and slow work, yet I did visibly gain ground; and as we drew near the Cape of the Woods, though I saw I must infallibly miss that point, I had still made some hundred yards of easting. I was, indeed, close in. I could see the cool green tree-tops swaying together

in the breeze, and I felt sure I should make the next promontory without fail.

It was high time, for I now began to be tortured with thirst. The glow of the sun from above, its thousandfold reflection from the waves, the sea-water that fell and dried upon me, caking my very lips with salt, combined to make my throat burn and my brain ache. The sight of the trees so near at hand had almost made me sick with longing, but the current had soon carried me past the point, and as the next reach of sea opened out, I beheld a sight that changed the nature of my thoughts.

Right in front of me, not half a mile away, I beheld the HISPANIOLA under sail. I made sure, of course, that I should be taken; but I was so distressed for want of water that I scarce knew whether to be glad or sorry at the thought, and long before I had come to a conclusion, surprise had taken entire possession of my mind and I could do nothing but stare and wonder.

The HISPANIOLA was under her main-sail and two jibs, and the beautiful white canvas shone in the sun like snow or silver. When I first sighted her, all her sails were drawing; she was lying a course about north-west, and I presumed the men on board were going round the island on their way back to the anchorage. Presently she began

to fetch more and more to the westward, so that I thought they had sighted me and were going about in chase. At last, however, she fell right into the wind's eye, was taken dead aback, and stood there awhile helpless, with her sails shivering.

'Clumsy fellows,' said I; 'they must still be drunk as owls.' And I thought how Captain Smollett would have set them skipping.

Meanwhile the schooner gradually fell off and filled again upon another tack, sailed swiftly for a minute or so, and brought up once more dead in the wind's eye. Again and again was this repeated. To and fro, up and down, north, south, east, and west, the HISPANIOLA sailed by swoops and dashes, and at each repetition ended as she had begun, with idly flapping canvas. It became plain to me that nobody was steering. And if so, where were the men? Either they were dead drunk or had deserted her, I thought, and perhaps if I could get on board I might return the vessel to her captain.

The current was bearing coracle and schooner southward at an equal rate. As for the latter's sailing, it was so wild and intermittent, and she hung each time so long in irons, that she certainly gained nothing, if she did not even lose. If only I dared to sit up and paddle, I made

sure that I could overhaul her. The scheme had an air of adventure that inspired me, and the thought of the water breaker beside the fore companion doubled my growing courage.

Up I got, was welcomed almost instantly by another cloud of spray, but this time stuck to my purpose and set myself, with all my strength and caution, to paddle after the unsteered HISPANIOLA. Once I shipped a sea so heavy that I had to stop and bail, with my heart fluttering like a bird, but gradually I got into the way of the thing and guided my coracle among the waves, with only now and then a blow upon her bows and a dash of foam in my face.

I was now gaining rapidly on the schooner; I could see the brass glisten on the tiller as it banged about, and still no soul appeared upon her decks. I could not choose but suppose she was deserted. If not, the men were lying drunk below, where I might batten them down, perhaps, and do what I chose with the ship.

For some time she had been doing the worse thing possible for me—standing still. She headed nearly due south, yawning, of course, all the time. Each time she fell off, her sails partly filled, and these brought her in a moment right to the wind again. I have said this was the

worst thing possible for me, for helpless as she looked in this situation, with the canvas cracking like cannon and the blocks trundling and banging on the deck, she still continued to run away from me, not only with the speed of the current, but by the whole amount of her leeway, which was naturally great.

But now, at last, I had my chance. The breeze fell for some seconds, very low, and the current gradually turning her, the *HISPANIOLA* revolved slowly round her centre and at last presented me her stern, with the cabin window still gaping open and the lamp over the table still burning on into the day. The main-sail hung drooped like a banner. She was stock-still but for the current.

For the last little while I had even lost, but now redoubling my efforts, I began once more to overhaul the chase.

I was not a hundred yards from her when the wind came again in a clap; she filled on the port tack and was off again, stooping and skimming like a swallow.

My first impulse was one of despair, but my second was towards joy. Round she came, till she was broadside on to me—round still till she had covered a half and then two thirds and then three quarters of the distance that separated us. I could see the waves boiling white under

her forefoot. Immensely tall she looked to me from my low station in the coracle.

And then, of a sudden, I began to comprehend. I had scarce time to think—scarce time to act and save myself. I was on the summit of one swell when the schooner came stooping over the next. The bowsprit was over my head. I sprang to my feet and leaped, stamping the coracle under water. With one hand I caught the jib-boom, while my foot was lodged between the stay and the brace; and as I still clung there panting, a dull blow told me that the schooner had charged down upon and struck the coracle and that I was left without retreat on the HISPANIOLA.

## I Strike the Jolly Roger

I HAD scarce gained a position on the bowsprit when the flying jib flapped and filled upon the other tack, with a report like a gun. The schooner trembled to her keel under the reverse, but next moment, the other sails still drawing, the jib flapped back again and hung idle.

This had nearly tossed me off into the sea; and now I lost no time, crawled back along the bowsprit, and tumbled head foremost on the deck.

I was on the lee side of the forecastle, and the main-sail, which was still drawing, concealed from me a certain portion of the after-deck. Not a soul was to be seen. The planks, which had not been swabbed since the mutiny, bore the print of many feet, and an empty bottle, broken by the neck, tumbled to and fro like a live thing in the scuppers.

Suddenly the HISPANIOLA came right into the wind. The jibs behind me cracked aloud, the rudder slammed to, the whole ship gave a sickening heave and shudder, and at the same moment the main-boom swung inboard, the

sheet groaning in the blocks, and showed me the lee after-deck.

There were the two watchmen, sure enough: red-cap on his back, as stiff as a handspike, with his arms stretched out like those of a crucifix and his teeth showing through his open lips; Israel Hands propped against the bulwarks, his chin on his chest, his hands lying open before him on the deck, his face as white, under its tan, as a tallow candle.

For a while the ship kept bucking and sidling like a vicious horse, the sails filling, now on one tack, now on another, and the boom swinging to and fro till the mast groaned aloud under the strain. Now and again too there would come a cloud of light sprays over the bulwark and a heavy blow of the ship's bows against the swell; so much heavier weather was made of it by this great rigged ship than by my home-made, lop-sided coracle, now gone to the bottom of the sea.

At every jump of the schooner, red-cap slipped to and fro, but—what was ghastly to behold—neither his attitude nor his fixed teeth-disclosing grin was anyway disturbed by this rough usage. At every jump too, Hands appeared still more to sink into himself and settle down upon the deck, his feet sliding ever the farther out, and the whole

body canting towards the stern, so that his face became, little by little, hid from me; and at last I could see nothing beyond his ear and the frayed ringlet of one whisker.

At the same time, I observed, around both of them, splashes of dark blood upon the planks and began to feel sure that they had killed each other in their drunken wrath.

While I was thus looking and wondering, in a calm moment, when the ship was still, Israel Hands turned partly round and with a low moan writhed himself back to the position in which I had seen him first. The moan, which told of pain and deadly weakness, and the way in which his jaw hung open went right to my heart. But when I remembered the talk I had overheard from the apple barrel, all pity left me.

I walked aft until I reached the main-mast.

‘Come aboard, Mr. Hands,’ I said ironically.

He rolled his eyes round heavily, but he was too far gone to express surprise. All he could do was to utter one word, ‘Brandy.’

It occurred to me there was no time to lose, and dodging the boom as it once more lurched across the deck, I slipped aft and down the companion stairs into the cabin.

It was such a scene of confusion as you can hardly fancy. All the lockfast places had been broken open in quest of the chart. The floor was thick with mud where ruffians had sat down to drink or consult after wading in the marshes round their camp. The bulkheads, all painted in clear white and beaded round with gilt, bore a pattern of dirty hands. Dozens of empty bottles clinked together in corners to the rolling of the ship. One of the doctor's medical books lay open on the table, half of the leaves gutted out, I suppose, for pipelights. In the midst of all this the lamp still cast a smoky glow, obscure and brown as umber.

I went into the cellar; all the barrels were gone, and of the bottles a most surprising number had been drunk out and thrown away. Certainly, since the mutiny began, not a man of them could ever have been sober.

Foraging about, I found a bottle with some brandy left, for Hands; and for myself I routed out some biscuit, some pickled fruits, a great bunch of raisins, and a piece of cheese. With these I came on deck, put down my own stock behind the rudder head and well out of the coxswain's reach, went forward to the water-breaker, and had a good deep drink of water, and then, and not till then, gave Hands the brandy.

## Treasure Island

He must have drunk a gill before he took the bottle from his mouth.

‘Aye,’ said he, ‘by thunder, but I wanted some o’ that!’

I had sat down already in my own corner and begun to eat.

‘Much hurt?’ I asked him.

He grunted, or rather, I might say, he barked.

‘If that doctor was aboard,’ he said, ‘I’d be right enough in a couple of turns, but I don’t have no manner of luck, you see, and that’s what’s the matter with me. As for that swab, he’s good and dead, he is,’ he added, indicating the man with the red cap. ‘He warn’t no seaman anyhow. And where mought you have come from?’

‘Well,’ said I, ‘I’ve come aboard to take possession of this ship, Mr. Hands; and you’ll please regard me as your captain until further notice.’

He looked at me sourly enough but said nothing. Some of the colour had come back into his cheeks, though he still looked very sick and still continued to slip out and settle down as the ship banged about.

‘By the by,’ I continued, ‘I can’t have these colours, Mr. Hands; and by your leave, I’ll strike ‘em. Better none than these.’

And again dodging the boom, I ran to the colour lines, handed down their cursed black flag, and chucked it overboard.

‘God save the king!’ said I, waving my cap. ‘And there’s an end to Captain Silver!’

He watched me keenly and slyly, his chin all the while on his breast.

‘I reckon,’ he said at last, ‘I reckon, Cap’n Hawkins, you’ll kind of want to get ashore now. S’pose we talks.’

‘Why, yes,’ says I, ‘with all my heart, Mr. Hands. Say on.’ And I went back to my meal with a good appetite.

‘This man,’ he began, nodding feebly at the corpse ‘— O’Brien were his name, a rank Irisher—this man and me got the canvas on her, meaning for to sail her back. Well, HE’S dead now, he is—as dead as bilge; and who’s to sail this ship, I don’t see. Without I gives you a hint, you ain’t that man, as far’s I can tell. Now, look here, you gives me food and drink and a old scarf or ankecher to tie my wound up, you do, and I’ll tell you how to tail her, and that’s about square all round, I take it.’

‘I’ll tell you one thing,’ says I: ‘I’m not going back to Captain Kidd’s anchorage. I mean to get into North Inlet and beach her quietly there.’

‘To be sure you did,’ he cried. ‘Why, I ain’t sich an infernal lubber after all. I can see, can’t I? I’ve tried my fling, I have, and I’ve lost, and it’s you has the wind of me. North Inlet? Why, I haven’t no ch’ice, not I! I’d help you sail her up to Execution Dock, by thunder! So I would.’

Well, as it seemed to me, there was some sense in this. We struck our bargain on the spot. In three minutes I had the **HISPANIOLA** sailing easily before the wind along the coast of Treasure Island, with good hopes of turning the northern point ere noon and beating down again as far as North Inlet before high water, when we might beach her safely and wait till the subsiding tide permitted us to land.

Then I lashed the tiller and went below to my own chest, where I got a soft silk handkerchief of my mother’s. With this, and with my aid, Hands bound up the great bleeding stab he had received in the thigh, and after he had eaten a little and had a swallow or two more of the brandy, he began to pick up visibly, sat straighter up, spoke louder and clearer, and looked in every way another man.

The breeze served us admirably. We skimmed before it like a bird, the coast of the island flashing by and the view

changing every minute. Soon we were past the high lands and bowling beside low, sandy country, sparsely dotted with dwarf pines, and soon we were beyond that again and had turned the corner of the rocky hill that ends the island on the north.

I was greatly elated with my new command, and pleased with the bright, sunshiny weather and these different prospects of the coast. I had now plenty of water and good things to eat, and my conscience, which had smitten me hard for my desertion, was quieted by the great conquest I had made. I should, I think, have had nothing left me to desire but for the eyes of the coxswain as they followed me derisively about the deck and the odd smile that appeared continually on his face. It was a smile that had in it something both of pain and weakness—a haggard old man's smile; but there was, besides that, a grain of derision, a shadow of treachery, in his expression as he craftily watched, and watched, and watched me at my work.

## **Israel Hands**

THE wind, serving us to a desire, now hauled into the west. We could run so much the easier from the north-east corner of the island to the mouth of the North Inlet. Only, as we had no power to anchor and dared not beach her till the tide had flowed a good deal farther, time hung on our hands. The coxswain told me how to lay the ship to; after a good many trials I succeeded, and we both sat in silence over another meal.

‘Cap’n,’ said he at length with that same uncomfortable smile, ‘here’s my old shipmate, O’Brien; s’pose you was to heave him overboard. I ain’t partic’lar as a rule, and I don’t take no blame for settling his hash, but I don’t reckon him ornamental now, do you?’

‘I’m not strong enough, and I don’t like the job; and there he lies, for me,’ said I.

‘This here’s an unlucky ship, this HISPANIOLA, Jim,’ he went on, blinking. ‘There’s a power of men been killed in this HISPANIOLA—a sight o’ poor seamen dead and gone since you and me took ship to Bristol. I never seen

sich dirty luck, not I. There was this here O'Brien now—he's dead, ain't he? Well now, I'm no scholar, and you're a lad as can read and figure, and to put it straight, do you take it as a dead man is dead for good, or do he come alive again?"

'You can kill the body, Mr. Hands, but not the spirit; you must know that already,' I replied. 'O'Brien there is in another world, and may be watching us.'

'Ah!' says he. 'Well, that's unfort'nate—appears as if killing parties was a waste of time. Howsomever, sperrits don't reckon for much, by what I've seen. I'll chance it with the sperrits, Jim. And now, you've spoke up free, and I'll take it kind if you'd step down into that there cabin and get me a—well, a—shiver my timbers! I can't hit the name on 't; well, you get me a bottle of wine, Jim—this here brandy's too strong for my head.'

Now, the coxswain's hesitation seemed to be unnatural, and as for the notion of his preferring wine to brandy, I entirely disbelieved it. The whole story was a pretext. He wanted me to leave the deck—so much was plain; but with what purpose I could in no way imagine. His eyes never met mine; they kept wandering to and fro, up and down, now with a look to the sky, now with a flitting glance upon the dead O'Brien. All the time he

kept smiling and putting his tongue out in the most guilty, embarrassed manner, so that a child could have told that he was bent on some deception. I was prompt with my answer, however, for I saw where my advantage lay and that with a fellow so densely stupid I could easily conceal my suspicions to the end.

‘Some wine?’ I said. ‘Far better. Will you have white or red?’

‘Well, I reckon it’s about the blessed same to me, shipmate,’ he replied; ‘so it’s strong, and plenty of it, what’s the odds?’

‘All right,’ I answered. ‘I’ll bring you port, Mr. Hands. But I’ll have to dig for it.’

With that I scuttled down the companion with all the noise I could, slipped off my shoes, ran quietly along the sparr'd gallery, mounted the forecastle ladder, and popped my head out of the fore companion. I knew he would not expect to see me there, yet I took every precaution possible, and certainly the worst of my suspicions proved too true.

He had risen from his position to his hands and knees, and though his leg obviously hurt him pretty sharply when he moved—for I could hear him stifle a groan—yet it was at a good, rattling rate that he trailed himself across

the deck. In half a minute he had reached the port scuppers and picked, out of a coil of rope, a long knife, or rather a short dirk, discoloured to the hilt with blood. He looked upon it for a moment, thrusting forth his under jaw, tried the point upon his hand, and then, hastily concealing it in the bosom of his jacket, trundled back again into his old place against the bulwark.

This was all that I required to know. Israel could move about, he was now armed, and if he had been at so much trouble to get rid of me, it was plain that I was meant to be the victim. What he would do afterwards—whether he would try to crawl right across the island from North Inlet to the camp among the swamps or whether he would fire Long Tom, trusting that his own comrades might come first to help him—was, of course, more than I could say.

Yet I felt sure that I could trust him in one point, since in that our interests jumped together, and that was in the disposition of the schooner. We both desired to have her stranded safe enough, in a sheltered place, and so that, when the time came, she could be got off again with as little labour and danger as might be; and until that was done I considered that my life would certainly be spared.

While I was thus turning the business over in my mind, I had not been idle with my body. I had stolen back to the

cabin, slipped once more into my shoes, and laid my hand at random on a bottle of wine, and now, with this for an excuse, I made my reappearance on the deck.

Hands lay as I had left him, all fallen together in a bundle and with his eyelids lowered as though he were too weak to bear the light. He looked up, however, at my coming, knocked the neck off the bottle like a man who had done the same thing often, and took a good swig, with his favourite toast of ‘Here’s luck!’ Then he lay quiet for a little, and then, pulling out a stick of tobacco, begged me to cut him a quid.

‘Cut me a junk o’ that,’ says he, ‘for I haven’t no knife and hardly strength enough, so be as I had. Ah, Jim, Jim, I reckon I’ve missed stays! Cut me a quid, as’ll likely be the last, lad, for I’m for my long home, and no mistake.’

‘Well,’ said I, ‘I’ll cut you some tobacco, but if I was you and thought myself so badly, I would go to my prayers like a Christian man.’

‘Why?’ said he. ‘Now, you tell me why.’

‘Why?’ I cried. ‘You were asking me just now about the dead. You’ve broken your trust; you’ve lived in sin and lies and blood; there’s a man you killed lying at your feet this moment, and you ask me why! For God’s mercy, Mr. Hands, that’s why.’

I spoke with a little heat, thinking of the bloody dirk he had hidden in his pocket and designed, in his ill thoughts, to end me with. He, for his part, took a great draught of the wine and spoke with the most unusual solemnity.

'For thirty years,' he said, 'I've sailed the seas and seen good and bad, better and worse, fair weather and foul, provisions running out, knives going, and what not. Well, now I tell you, I never seen good come o' goodness yet. Him as strikes first is my fancy; dead men don't bite; them's my views—amen, so be it. And now, you look here,' he added, suddenly changing his tone, 'we've had about enough of this foolery. The tide's made good enough by now. You just take my orders, Cap'n Hawkins, and we'll sail slap in and be done with it.'

All told, we had scarce two miles to run; but the navigation was delicate, the entrance to this northern anchorage was not only narrow and shoal, but lay east and west, so that the schooner must be nicely handled to be got in. I think I was a good, prompt subaltern, and I am very sure that Hands was an excellent pilot, for we went about and about and dodged in, shaving the banks, with a certainty and a neatness that were a pleasure to behold.

Scarcely had we passed the heads before the land closed around us. The shores of North Inlet were as

thickly wooded as those of the southern anchorage, but the space was longer and narrower and more like, what in truth it was, the estuary of a river. Right before us, at the southern end, we saw the wreck of a ship in the last stages of dilapidation. It had been a great vessel of three masts but had lain so long exposed to the injuries of the weather that it was hung about with great webs of dripping seaweed, and on the deck of it shore bushes had taken root and now flourished thick with flowers. It was a sad sight, but it showed us that the anchorage was calm.

‘Now,’ said Hands, ‘look there; there’s a pet bit for to beach a ship in. Fine flat sand, never a cat’s paw, trees all around of it, and flowers a-blowing like a garding on that old ship.’

‘And once beached,’ I inquired, ‘how shall we get her off again?’

‘Why, so,’ he replied: ‘you take a line ashore there on the other side at low water, take a turn about one of them big pines; bring it back, take a turn around the capstan, and lie to for the tide. Come high water, all hands take a pull upon the line, and off she comes as sweet as natur’. And now, boy, you stand by. We’re near the bit now, and she’s too much way on her. Starboard a little—so—steady—starboard—larboard a little—steady—steady!’

So he issued his commands, which I breathlessly obeyed, till, all of a sudden, he cried, ‘Now, my hearty, luff!’ And I put the helm hard up, and the HISPANIOLA swung round rapidly and ran stem on for the low, wooded shore.

The excitement of these last manoeuvres had somewhat interfered with the watch I had kept hitherto, sharply enough, upon the coxswain. Even then I was still so much interested, waiting for the ship to touch, that I had quite forgot the peril that hung over my head and stood craning over the starboard bulwarks and watching the ripples spreading wide before the bows. I might have fallen without a struggle for my life had not a sudden disquietude seized upon me and made me turn my head. Perhaps I had heard a creak or seen his shadow moving with the tail of my eye; perhaps it was an instinct like a cat’s; but, sure enough, when I looked round, there was Hands, already half-way towards me, with the dirk in his right hand.

We must both have cried out aloud when our eyes met, but while mine was the shrill cry of terror, his was a roar of fury like a charging bully’s. At the same instant, he threw himself forward and I leapt sideways towards the bows. As I did so, I let go of the tiller, which sprang sharp

## *Treasure Island*

to leeward, and I think this saved my life, for it struck Hands across the chest and stopped him, for the moment, dead.

Before he could recover, I was safe out of the corner where he had me trapped, with all the deck to dodge about. Just forward of the main-mast I stopped, drew a pistol from my pocket, took a cool aim, though he had already turned and was once more coming directly after me, and drew the trigger. The hammer fell, but there followed neither flash nor sound; the priming was useless with sea-water. I cursed myself for my neglect. Why had not I, long before, reprimed and reloaded my only weapons? Then I should not have been as now, a mere fleeing sheep before this butcher.

Wounded as he was, it was wonderful how fast he could move, his grizzled hair tumbling over his face, and his face itself as red as a red ensign with his haste and fury. I had no time to try my other pistol, nor indeed much inclination, for I was sure it would be useless. One thing I saw plainly: I must not simply retreat before him, or he would speedily hold me boxed into the bows, as a moment since he had so nearly boxed me in the stern. Once so caught, and nine or ten inches of the blood-stained dirk would be my last experience on this side of

eternity. I placed my palms against the main-mast, which was of a goodish bigness, and waited, every nerve upon the stretch.

Seeing that I meant to dodge, he also paused; and a moment or two passed in feints on his part and corresponding movements upon mine. It was such a game as I had often played at home about the rocks of Black Hill Cove, but never before, you may be sure, with such a wildly beating heart as now. Still, as I say, it was a boy's game, and I thought I could hold my own at it against an elderly seaman with a wounded thigh. Indeed my courage had begun to rise so high that I allowed myself a few darting thoughts on what would be the end of the affair, and while I saw certainly that I could spin it out for long, I saw no hope of any ultimate escape.

Well, while things stood thus, suddenly the HISPANIOLA struck, staggered, ground for an instant in the sand, and then, swift as a blow, canted over to the port side till the deck stood at an angle of forty-five degrees and about a puncheon of water splashed into the scupper holes and lay, in a pool, between the deck and bulwark.

We were both of us capsized in a second, and both of us rolled, almost together, into the scuppers, the dead red-cap, with his arms still spread out, tumbling stiffly after

us. So near were we, indeed, that my head came against the coxswain's foot with a crack that made my teeth rattle. Blow and all, I was the first afoot again, for Hands had got involved with the dead body. The sudden canting of the ship had made the deck no place for running on; I had to find some new way of escape, and that upon the instant, for my foe was almost touching me. Quick as thought, I sprang into the mizzen shrouds, rattled up hand over hand, and did not draw a breath till I was seated on the cross-trees.

I had been saved by being prompt; the dirk had struck not half a foot below me as I pursued my upward flight; and there stood Israel Hands with his mouth open and his face upturned to mine, a perfect statue of surprise and disappointment.

Now that I had a moment to myself, I lost no time in changing the priming of my pistol, and then, having one ready for service, and to make assurance doubly sure, I proceeded to draw the load of the other and recharge it afresh from the beginning.

My new employment struck Hands all of a heap; he began to see the dice going against him, and after an obvious hesitation, he also hauled himself heavily into the shrouds, and with the dirk in his teeth, began slowly and

painfully to mount. It cost him no end of time and groans to haul his wounded leg behind him, and I had quietly finished my arrangements before he was much more than a third of the way up. Then, with a pistol in either hand, I addressed him.

‘One more step, Mr. Hands,’ said I, ‘and I’ll blow your brains out! Dead men don’t bite, you know,’ I added with a chuckle.

He stopped instantly. I could see by the working of his face that he was trying to think, and the process was so slow and laborious that, in my new-found security, I laughed aloud. At last, with a swallow or two, he spoke, his face still wearing the same expression of extreme perplexity. In order to speak he had to take the dagger from his mouth, but in all else he remained unmoved.

‘Jim,’ says he, ‘I reckon we’re fouled, you and me, and we’ll have to sign articles. I’d have had you but for that there lurch, but I don’t have no luck, not I; and I reckon I’ll have to strike, which comes hard, you see, for a master mariner to a ship’s younker like you, Jim.’

I was drinking in his words and smiling away, as conceited as a cock upon a wall, when, all in a breath, back went his right hand over his shoulder. Something sang like an arrow through the air; I felt a blow and then a

sharp pang, and there I was pinned by the shoulder to the mast. In the horrid pain and surprise of the moment—I scarce can say it was by my own volition, and I am sure it was without a conscious aim— both my pistols went off, and both escaped out of my hands. They did not fall alone; with a choked cry, the coxswain loosed his grasp upon the shrouds and plunged head first into the water.

## "Pieces of Eight"

OWING to the cant of the vessel, the masts hung far out over the water, and from my perch on the cross-trees I had nothing below me but the surface of the bay. Hands, who was not so far up, was in consequence nearer to the ship and fell between me and the bulwarks. He rose once to the surface in a lather of foam and blood and then sank again for good. As the water settled, I could see him lying huddled together on the clean, bright sand in the shadow of the vessel's sides. A fish or two whipped past his body. Sometimes, by the quivering of the water, he appeared to move a little, as if he were trying to rise. But he was dead enough, for all that, being both shot and drowned, and was food for fish in the very place where he had designed my slaughter.

I was no sooner certain of this than I began to feel sick, faint, and terrified. The hot blood was running over my back and chest. The dirk, where it had pinned my shoulder to the mast, seemed to burn like a hot iron; yet it was not so much these real sufferings that distressed me,

for these, it seemed to me, I could bear without a murmur; it was the horror I had upon my mind of falling from the cross-trees into that still green water, beside the body of the coxswain.

I clung with both hands till my nails ached, and I shut my eyes as if to cover up the peril. Gradually my mind came back again, my pulses quieted down to a more natural time, and I was once more in possession of myself.

It was my first thought to pluck forth the dirk, but either it stuck too hard or my nerve failed me, and I desisted with a violent shudder. Oddly enough, that very shudder did the business. The knife, in fact, had come the nearest in the world to missing me altogether; it held me by a mere pinch of skin, and this the shudder tore away. The blood ran down the faster, to be sure, but I was my own master again and only tacked to the mast by my coat and shirt.

These last I broke through with a sudden jerk, and then regained the deck by the starboard shrouds. For nothing in the world would I have again ventured, shaken as I was, upon the overhanging port shrouds from which Israel had so lately fallen.

I went below and did what I could for my wound; it pained me a good deal and still bled freely, but it was neither deep nor dangerous, nor did it greatly gall me when I used my arm. Then I looked around me, and as the ship was now, in a sense, my own, I began to think of clearing it from its last passenger—the dead man, O'Brien.

He had pitched, as I have said, against the bulwarks, where he lay like some horrible, ungainly sort of puppet, life-size, indeed, but how different from life's colour or life's comeliness! In that position I could easily have my way with him, and as the habit of tragical adventures had worn off almost all my terror for the dead, I took him by the waist as if he had been a sack of bran and with one good heave, tumbled him overboard. He went in with a sounding plunge; the red cap came off and remained floating on the surface; and as soon as the splash subsided, I could see him and Israel lying side by side, both wavering with the tremulous movement of the water. O'Brien, though still quite a young man, was very bald. There he lay, with that bald head across the knees of the man who had killed him and the quick fishes steering to and fro over both.

I was now alone upon the ship; the tide had just turned. The sun was within so few degrees of setting that already the shadow of the pines upon the western shore began to reach right across the anchorage and fall in patterns on the deck. The evening breeze had sprung up, and though it was well warded off by the hill with the two peaks upon the east, the cordage had begun to sing a little softly to itself and the idle sails to rattle to and fro.

I began to see a danger to the ship. The jibs I speedily doused and brought tumbling to the deck, but the main-sail was a harder matter. Of course, when the schooner canted over, the boom had swung out-board, and the cap of it and a foot or two of sail hung even under water. I thought this made it still more dangerous; yet the strain was so heavy that I half feared to meddle. At last I got my knife and cut the halyards. The peak dropped instantly, a great belly of loose canvas floated broad upon the water, and since, pull as I liked, I could not budge the downhall, that was the extent of what I could accomplish. For the rest, the **HISPANIOLA** must trust to luck, like myself.

By this time the whole anchorage had fallen into shadow—the last rays, I remember, falling through a glade of the wood and shining bright as jewels on the flowery mantle of the wreck. It began to be chill; the tide

was rapidly fleeting seaward, the schooner settling more and more on her beam-ends.

I scrambled forward and looked over. It seemed shallow enough, and holding the cut hawser in both hands for a last security, I let myself drop softly overboard. The water scarcely reached my waist; the sand was firm and covered with ripple marks, and I waded ashore in great spirits, leaving the HISPANIOLA on her side, with her main-sail trailing wide upon the surface of the bay. About the same time, the sun went fairly down and the breeze whistled low in the dusk among the tossing pines.

At least, and at last, I was off the sea, nor had I returned thence empty-handed. There lay the schooner, clear at last from buccaneers and ready for our own men to board and get to sea again. I had nothing nearer my fancy than to get home to the stockade and boast of my achievements. Possibly I might be blamed a bit for my truancy, but the recapture of the HISPANIOLA was a clenching answer, and I hoped that even Captain Smollett would confess I had not lost my time.

So thinking, and in famous spirits, I began to set my face homeward for the block house and my companions. I remembered that the most easterly of the rivers which drain into Captain Kidd's anchorage ran from the two-

peaked hill upon my left, and I bent my course in that direction that I might pass the stream while it was small. The wood was pretty open, and keeping along the lower spurs, I had soon turned the corner of that hill, and not long after waded to the mid-calf across the watercourse.

This brought me near to where I had encountered Ben Gunn, the maroon; and I walked more circumspectly, keeping an eye on every side. The dusk had come nigh hand completely, and as I opened out the cleft between the two peaks, I became aware of a wavering glow against the sky, where, as I judged, the man of the island was cooking his supper before a roaring fire. And yet I wondered, in my heart, that he should show himself so careless. For if I could see this radiance, might it not reach the eyes of Silver himself where he camped upon the shore among the marshes?

Gradually the night fell blacker; it was all I could do to guide myself even roughly towards my destination; the double hill behind me and the Spy-glass on my right hand loomed faint and fainter; the stars were few and pale; and in the low ground where I wandered I kept tripping among bushes and rolling into sandy pits.

Suddenly a kind of brightness fell about me. I looked up; a pale glimmer of moonbeams had alighted on the

summit of the Spy-glass, and soon after I saw something broad and silvery moving low down behind the trees, and knew the moon had risen.

With this to help me, I passed rapidly over what remained to me of my journey, and sometimes walking, sometimes running, impatiently drew near to the stockade. Yet, as I began to thread the grove that lies before it, I was not so thoughtless but that I slacked my pace and went a trifle warily. It would have been a poor end of my adventures to get shot down by my own party in mistake.

The moon was climbing higher and higher, its light began to fall here and there in masses through the more open districts of the wood, and right in front of me a glow of a different colour appeared among the trees. It was red and hot, and now and again it was a little darkened—as it were, the embers of a bonfire smouldering.

For the life of me I could not think what it might be.

At last I came right down upon the borders of the clearing. The western end was already steeped in moon-shine; the rest, and the block house itself, still lay in a black shadow chequered with long silvery streaks of light. On the other side of the house an immense fire had burned itself into clear embers and shed a steady, red

## Treasure Island

reverberation, contrasted strongly with the mellow paleness of the moon. There was not a soul stirring nor a sound beside the noises of the breeze.

I stopped, with much wonder in my heart, and perhaps a little terror also. It had not been our way to build great fires; we were, indeed, by the captain's orders, somewhat niggardly of firewood, and I began to fear that something had gone wrong while I was absent.

I stole round by the eastern end, keeping close in shadow, and at a convenient place, where the darkness was thickest, crossed the palisade.

To make assurance surer, I got upon my hands and knees and crawled, without a sound, towards the corner of the house. As I drew nearer, my heart was suddenly and greatly lightened. It is not a pleasant noise in itself, and I have often complained of it at other times, but just then it was like music to hear my friends snoring together so loud and peaceful in their sleep. The sea-cry of the watch, that beautiful 'All's well,' never fell more reassuringly on my ear.

In the meantime, there was no doubt of one thing; they kept an infamous bad watch. If it had been Silver and his lads that were now creeping in on them, not a soul would have seen daybreak. That was what it was, thought I, to

have the captain wounded; and again I blamed myself sharply for leaving them in that danger with so few to mount guard.

By this time I had got to the door and stood up. All was dark within, so that I could distinguish nothing by the eye. As for sounds, there was the steady drone of the snorers and a small occasional noise, a flickering or pecking that I could in no way account for.

With my arms before me I walked steadily in. I should lie down in my own place (I thought with a silent chuckle) and enjoy their faces when they found me in the morning.

My foot struck something yielding—it was a sleeper's leg; and he turned and groaned, but without awaking.

And then, all of a sudden, a shrill voice broke forth out of the darkness:

'Pieces of eight! Pieces of eight! Pieces of eight!  
Pieces of eight! Pieces of eight! and so forth, without pause or change, like the clacking of a tiny mill.

Silver's green parrot, Captain Flint! It was she whom I had heard pecking at a piece of bark; it was she, keeping better watch than any human being, who thus announced my arrival with her wearisome refrain.

I had no time left me to recover. At the sharp, clipping tone of the parrot, the sleepers awoke and sprang up; and with a mighty oath, the voice of Silver cried, ‘Who goes?’

I turned to run, struck violently against one person, recoiled, and ran full into the arms of a second, who for his part closed upon and held me tight.

‘Bring a torch, Dick,’ said Silver when my capture was thus assured.

And one of the men left the log-house and presently returned with a lighted brand.

## PART SIX

### Captain Silver

28

#### In the Enemy's Camp

THE red glare of the torch, lighting up the interior of the block house, showed me the worst of my apprehensions realized. The pirates were in possession of the house and stores: there was the cask of cognac, there were the pork and bread, as before, and what tenfold increased my horror, not a sign of any prisoner. I could only judge that all had perished, and my heart smote me sorely that I had not been there to perish with them.

There were six of the buccaneers, all told; not another man was left alive. Five of them were on their feet, flushed and swollen, suddenly called out of the first sleep of drunkenness. The sixth had only risen upon his elbow; he was deadly pale, and the blood-stained bandage round his head told that he had recently been wounded, and still more recently dressed. I remembered the man who had

been shot and had run back among the woods in the great attack, and doubted not that this was he.

The parrot sat, preening her plumage, on Long John's shoulder. He himself, I thought, looked somewhat paler and more stern than I was used to. He still wore the fine broadcloth suit in which he had fulfilled his mission, but it was bitterly the worse for wear, daubed with clay and torn with the sharp briars of the wood.

'So,' said he, 'here's Jim Hawkins, shiver my timbers! Dropped in, like, eh? Well, come, I take that friendly.'

And thereupon he sat down across the brandy cask and began to fill a pipe.

'Give me a loan of the link, Dick,' said he; and then, when he had a good light, 'That'll do, lad,' he added; 'stick the glim in the wood heap; and you, gentlemen, bring yourselves to! You needn't stand up for Mr. Hawkins; HE'LL excuse you, you may lay to that. And so, Jim'—stopping the tobacco—'here you were, and quite a pleasant surprise for poor old John. I see you were smart when first I set my eyes on you, but this here gets away from me clean, it do.'

To all this, as may be well supposed, I made no answer. They had set me with my back against the wall, and I stood there, looking Silver in the face, pluckily

enough, I hope, to all outward appearance, but with black despair in my heart.

Silver took a whiff or two of his pipe with great composure and then ran on again.

‘Now, you see, Jim, so be as you ARE here,’ says he, ‘I’ll give you a piece of my mind. I’ve always liked you, I have, for a lad of spirit, and the picter of my own self when I was young and handsome. I always wanted you to jine and take your share, and die a gentleman, and now, my cock, you’ve got to. Cap’n Smollett’s a fine seaman, as I’ll own up to any day, but stiff on discipline. ‘Dooty is dooty,’ says he, and right he is. Just you keep clear of the cap’n. The doctor himself is gone dead again you—‘ungrateful scamp’ was what he said; and the short and the long of the whole story is about here: you can’t go back to your own lot, for they won’t have you; and without you start a third ship’s company all by yourself, which might be lonely, you’ll have to jine with Cap’n Silver.’

So far so good. My friends, then, were still alive, and though I partly believed the truth of Silver’s statement, that the cabin party were incensed at me for my desertion, I was more relieved than distressed by what I heard.

‘I don’t say nothing as to your being in our hands,’ continued Silver, ‘though there you are, and you may lay to it. I’m all for argyment; I never seen good come out o’ threatening. If you like the service, well, you’ll jine; and if you don’t, Jim, why, you’re free to answer no—free and welcome, shipmate; and if fairer can be said by mortal seaman, shiver my sides!’

‘Am I to answer, then?’ I asked with a very tremulous voice. Through all this sneering talk, I was made to feel the threat of death that overhung me, and my cheeks burned and my heart beat painfully in my breast.

‘Lad,’ said Silver, ‘no one’s a-pressing of you. Take your bearings. None of us won’t hurry you, mate; time goes so pleasant in your company, you see.’

‘Well,’ says I, growing a bit bolder, ‘if I’m to choose, I declare I have a right to know what’s what, and why you’re here, and where my friends are.’

‘Wot’s wot?’ repeated one of the buccaneers in a deep growl. ‘Ah, he’d be a lucky one as knowed that!’

‘You’ll perhaps batten down your hatches till you’re spoke to, my friend,’ cried Silver truculently to this speaker. And then, in his first gracious tones, he replied to me, ‘Yesterday morning, Mr. Hawkins,’ said he, ‘in the dog-watch, down came Doctor Livesey with a flag of

truce. Says he, ‘Cap’n Silver, you’re sold out. Ship’s gone.’ Well, maybe we’d been taking a glass, and a song to help it round. I won’t say no. Leastways, none of us had looked out. We looked out, and by thunder, the old ship was gone! I never seen a pack o’ fools look fishier; and you may lay to that, if I tells you that looked the fishiest. ‘Well,’ says the doctor, ‘let’s bargain.’ We bargained, him and I, and here we are: stores, brandy, block house, the firewood you was thoughtful enough to cut, and in a manner of speaking, the whole blessed boat, from cross-trees to kelson. As for them, they’ve tramped; I don’t know where’s they are.’

He drew again quietly at his pipe.

‘And lest you should take it into that head of yours,’ he went on, ‘that you was included in the treaty, here’s the last word that was said: ‘How many are you,’ says I, ‘to leave?’ ‘Four,’ says he; ‘four, and one of us wounded. As for that boy, I don’t know where he is, confound him,’ says he, ‘nor I don’t much care. We’re about sick of him.’ These was his words.

‘Is that all?’ I asked.

‘Well, it’s all that you’re to hear, my son,’ returned Silver.

‘And now I am to choose?’

‘And now you are to choose, and you may lay to that,’ said Silver.

‘Well,’ said I, ‘I am not such a fool but I know pretty well what I have to look for. Let the worst come to the worst, it’s little I care. I’ve seen too many die since I fell in with you. But there’s a thing or two I have to tell you,’ I said, and by this time I was quite excited; ‘and the first is this: here you are, in a bad way—ship lost, treasure lost, men lost, your whole business gone to wreck; and if you want to know who did it—it was I! I was in the apple barrel the night we sighted land, and I heard you, John, and you, Dick Johnson, and Hands, who is now at the bottom of the sea, and told every word you said before the hour was out. And as for the schooner, it was I who cut her cable, and it was I that killed the men you had aboard of her, and it was I who brought her where you’ll never see her more, not one of you. The laugh’s on my side; I’ve had the top of this business from the first; I no more fear you than I fear a fly. Kill me, if you please, or spare me. But one thing I’ll say, and no more; if you spare me, bygones are bygones, and when you fellows are in court for piracy, I’ll save you all I can. It is for you to choose. Kill another and do yourselves no good, or spare me and keep a witness to save you from the gallows.’

I stopped, for, I tell you, I was out of breath, and to my wonder, not a man of them moved, but all sat staring at me like as many sheep. And while they were still staring, I broke out again, ‘And now, Mr. Silver,’ I said, ‘I believe you’re the best man here, and if things go to the worst, I’ll take it kind of you to let the doctor know the way I took it.’

‘I’ll bear it in mind,’ said Silver with an accent so curious that I could not, for the life of me, decide whether he were laughing at my request or had been favourably affected by my courage.

‘I’ll put one to that,’ cried the old mahogany-faced seaman—Morgan by name—whom I had seen in Long John’s public-house upon the quays of Bristol. ‘It was him that knowed Black Dog.’

‘Well, and see here,’ added the sea-cook. ‘I’ll put another again to that, by thunder! For it was this same boy that faked the chart from Billy Bones. First and last, we’ve split upon Jim Hawkins!’

‘Then here goes!’ said Morgan with an oath.

And he sprang up, drawing his knife as if he had been twenty.

‘Avast, there!’ cried Silver. ‘Who are you, Tom Morgan? Maybe you thought you was cap’n here,

perhaps. By the powers, but I'll teach you better! Cross me, and you'll go where many a good man's gone before you, first and last, these thirty year back—some to the yard-arm, shiver my timbers, and some by the board, and all to feed the fishes. There's never a man looked me between the eyes and seen a good day a'terwards, Tom Morgan, you may lay to that.'

Morgan paused, but a hoarse murmur rose from the others.

'Tom's right,' said one.

'I stood hazing long enough from one,' added another. 'I'll be hanged if I'll be hazed by you, John Silver.'

'Did any of you gentlemen want to have it out with ME?' roared Silver, bending far forward from his position on the keg, with his pipe still glowing in his right hand. 'Put a name on what you're at; you ain't dumb, I reckon. Him that wants shall get it. Have I lived this many years, and a son of a rum puncheon cock his hat athwart my hawse at the latter end of it? You know the way; you're all gentlemen o' fortune, by your account. Well, I'm ready. Take a cutlass, him that dares, and I'll see the colour of his inside, crutch and all, before that pipe's empty.'

Not a man stirred; not a man answered.

‘That’s your sort, is it?’ he added, returning his pipe to his mouth. ‘Well, you’re a gay lot to look at, anyway. Not much worth to fight, you ain’t. P’raps you can understand King George’s English. I’m cap’n here by ‘lection. I’m cap’n here because I’m the best man by a long sea-mile. You won’t fight, as gentlemen o’ fortune should; then, by thunder, you’ll obey, and you may lay to it! I like that boy, now; I never seen a better boy than that. He’s more a man than any pair of rats of you in this here house, and what I say is this: let me see him that’ll lay a hand on him—that’s what I say, and you may lay to it.’

There was a long pause after this. I stood straight up against the wall, my heart still going like a sledge-hammer, but with a ray of hope now shining in my bosom. Silver leant back against the wall, his arms crossed, his pipe in the corner of his mouth, as calm as though he had been in church; yet his eye kept wandering furtively, and he kept the tail of it on his unruly followers. They, on their part, drew gradually together towards the far end of the block house, and the low hiss of their whispering sounded in my ear continuously, like a stream. One after another, they would look up, and the red light of the torch would fall for a second on their nervous faces;

## *Treasure Island*

but it was not towards me, it was towards Silver that they turned their eyes.

‘You seem to have a lot to say,’ remarked Silver, spitting far into the air. ‘Pipe up and let me hear it, or lay to.’

‘Ax your pardon, sir,’ returned one of the men; ‘you’re pretty free with some of the rules; maybe you’ll kindly keep an eye upon the rest. This crew’s dissatisfied; this crew don’t vally bullying a marlin-spike; this crew has its rights like other crews, I’ll make so free as that; and by your own rules, I take it we can talk together. I ax your pardon, sir, acknowledging you for to be captaining at this present; but I claim my right, and steps outside for a council.’

And with an elaborate sea-salute, this fellow, a long, ill-looking, yellow-eyed man of five and thirty, stepped coolly towards the door and disappeared out of the house. One after another the rest followed his example, each making a salute as he passed, each adding some apology. ‘According to rules,’ said one. ‘Forecastle council,’ said Morgan. And so with one remark or another all marched out and left Silver and me alone with the torch.

The sea-cook instantly removed his pipe.

‘Now, look you here, Jim Hawkins,’ he said in a steady whisper that was no more than audible, ‘you’re within half a plank of death, and what’s a long sight worse, of torture. They’re going to throw me off. But, you mark, I stand by you through thick and thin. I didn’t mean to; no, not till you spoke up. I was about desperate to lose that much blunt, and be hanged into the bargain. But I see you was the right sort. I says to myself, you stand by Hawkins, John, and Hawkins’ll stand by you. You’re his last card, and by the living thunder, John, he’s yours! Back to back, says I. You save your witness, and he’ll save your neck!’

I began dimly to understand.

‘You mean all’s lost?’ I asked.

‘Aye, by gum, I do!’ he answered. ‘Ship gone, neck gone —that’s the size of it. Once I looked into that bay, Jim Hawkins, and seen no schooner—well, I’m tough, but I gave out. As for that lot and their council, mark me, they’re outright fools and cowards. I’ll save your life—if so be as I can—from them. But, see here, Jim—tit for tat—you save Long John from swinging.’

I was bewildered; it seemed a thing so hopeless he was asking—he, the old buccaneer, the ringleader throughout.

‘What I can do, that I’ll do,’ I said.

‘It’s a bargain!’ cried Long John. ‘You speak up plucky, and by thunder, I’ve a chance!’

He hobbled to the torch, where it stood propped among the firewood, and took a fresh light to his pipe.

‘Understand me, Jim,’ he said, returning. ‘I’ve a head on my shoulders, I have. I’m on squire’s side now. I know you’ve got that ship safe somewhere. How you done it, I don’t know, but safe it is. I guess Hands and O’Brien turned soft. I never much believed in either of THEM. Now you mark me. I ask no questions, nor I won’t let others. I know when a game’s up, I do; and I know a lad that’s staunch. Ah, you that’s young—you and me might have done a power of good together!’

He drew some cognac from the cask into a tin cannikin.

‘Will you taste, messmate?’ he asked; and when I had refused: ‘Well, I’ll take a drain myself, Jim,’ said he. ‘I need a caulk, for there’s trouble on hand. And talking o’ trouble, why did that doctor give me the chart, Jim?’

My face expressed a wonder so unaffected that he saw the needlessness of further questions.

‘Ah, well, he did, though,’ said he. ‘And there’s something under that, no doubt—something, surely, under that, Jim—bad or good.’

And he took another swallow of the brandy, shaking his great fair head like a man who looks forward to the worst.

## **The Black Spot Again**

THE council of buccaneers had lasted some time, when one of them re-entered the house, and with a repetition of the same salute, which had in my eyes an ironical air, begged for a moment's loan of the torch. Silver briefly agreed, and this emissary retired again, leaving us together in the dark.

'There's a breeze coming, Jim,' said Silver, who had by this time adopted quite a friendly and familiar tone.

I turned to the loophole nearest me and looked out. The embers of the great fire had so far burned themselves out and now glowed so low and duskily that I understood why these conspirators desired a torch. About half-way down the slope to the stockade, they were collected in a group; one held the light, another was on his knees in their midst, and I saw the blade of an open knife shine in his hand with varying colours in the moon and torchlight. The rest were all somewhat stooping, as though watching the manoeuvres of this last. I could just make out that he had a book as well as a knife in his hand, and was still

wondering how anything so incongruous had come in their possession when the kneeling figure rose once more to his feet and the whole party began to move together towards the house.

‘Here they come,’ said I; and I returned to my former position, for it seemed beneath my dignity that they should find me watching them.

‘Well, let ‘em come, lad—let ‘em come,’ said Silver cheerily. ‘I’ve still a shot in my locker.’

The door opened, and the five men, standing huddled together just inside, pushed one of their number forward. In any other circumstances it would have been comical to see his slow advance, hesitating as he set down each foot, but holding his closed right hand in front of him.

‘Step up, lad,’ cried Silver. ‘I won’t eat you. Hand it over, lubber. I know the rules, I do; I won’t hurt a depytation.’

Thus encouraged, the buccaneer stepped forth more briskly, and having passed something to Silver, from hand to hand, slipped yet more smartly back again to his companions.

The sea-cook looked at what had been given him.

‘The black spot! I thought so,’ he observed. ‘Where might you have got the paper? Why, hillo! Look here,

now; this ain't lucky! You've gone and cut this out of a Bible. What fool's cut a Bible?"

'Ah, there!' said Morgan. 'There! Wot did I say? No good'll come o' that, I said.'

'Well, you've about fixed it now, among you,' continued Silver. 'You'll all swing now, I reckon. What soft-headed lubber had a Bible?"

'It was Dick,' said one.

'Dick, was it? Then Dick can get to prayers,' said Silver. 'He's seen his slice of luck, has Dick, and you may lay to that.'

But here the long man with the yellow eyes struck in.

'Belay that talk, John Silver,' he said. 'This crew has tipped you the black spot in full council, as in dooty bound; just you turn it over, as in dooty bound, and see what's wrote there. Then you can talk.'

'Thanky, George,' replied the sea-cook. 'You always was brisk for business, and has the rules by heart, George, as I'm pleased to see. Well, what is it, anyway? Ah! 'Deposed'—that's it, is it? Very pretty wrote, to be sure; like print, I swear. Your hand o' write, George? Why, you was gettin' quite a leadin' man in this here crew. You'll be cap'n next, I shouldn't wonder. Just oblige me with that torch again, will you? This pipe don't draw.'

‘Come, now,’ said George, ‘you don’t fool this crew no more. You’re a funny man, by your account; but you’re over now, and you’ll maybe step down off that barrel and help vote.’

‘I thought you said you knowed the rules,’ returned Silver contemptuously. ‘Leastways, if you don’t, I do; and I wait here—and I’m still your cap’n, mind—till you outs with your grievances and I reply; in the meantime, your black spot ain’t worth a biscuit. After that, we’ll see.’

‘Oh,’ replied George, ‘you don’t be under no kind of apprehension; WE’RE all square, we are. First, you’ve made a hash of this cruise—you’ll be a bold man to say no to that. Second, you let the enemy out o’ this here trap for nothing. Why did they want out? I dunno, but it’s pretty plain they wanted it. Third, you wouldn’t let us go at them upon the march. Oh, we see through you, John Silver; you want to play booty, that’s what’s wrong with you. And then, fourth, there’s this here boy.’

‘Is that all?’ asked Silver quietly.

‘Enough, too,’ retorted George. ‘We’ll all swing and sun-dry for your bungling.’

‘Well now, look here, I’ll answer these four p’ints; one after another I’ll answer ‘em. I made a hash o’ this cruise, did I? Well now, you all know what I wanted, and you all

know if that had been done that we'd 'a been aboard the HISPANIOLA this night as ever was, every man of us alive, and fit, and full of good plum-duff, and the treasure in the hold of her, by thunder! Well, who crossed me? Who forced my hand, as was the lawful cap'n? Who tipped me the black spot the day we landed and began this dance? Ah, it's a fine dance—I'm with you there—and looks mighty like a hornpipe in a rope's end at Execution Dock by London town, it does. But who done it? Why, it was Anderson, and Hands, and you, George Merry! And you're the last above board of that same meddling crew; and you have the Davy Jones's insolence to up and stand for cap'n over me—you, that sank the lot of us! By the powers! But this tops the stiffest yarn to nothing.'

Silver paused, and I could see by the faces of George and his late comrades that these words had not been said in vain.

'That's for number one,' cried the accused, wiping the sweat from his brow, for he had been talking with a vehemence that shook the house. 'Why, I give you my word, I'm sick to speak to you. You've neither sense nor memory, and I leave it to fancy where your mothers was that let you come to sea. Sea! Gentlemen o' fortune! I reckon tailors is your trade.'

‘Go on, John,’ said Morgan. ‘Speak up to the others.’

‘Ah, the others!’ returned John. ‘They’re a nice lot, ain’t they? You say this cruise is bungled. Ah! By gum, if you could understand how bad it’s bungled, you would see! We’re that near the gibbet that my neck’s stiff with thinking on it. You’ve seen ‘em, maybe, hanged in chains, birds about ‘em, seamen p’inting ‘em out as they go down with the tide. ‘Who’s that?’ says one. ‘That! Why, that’s John Silver. I knowed him well,’ says another. And you can hear the chains a-jangle as you go about and reach for the other buoy. Now, that’s about where we are, every mother’s son of us, thanks to him, and Hands, and Anderson, and other ruination fools of you. And if you want to know about number four, and that boy, why, shiver my timbers, isn’t he a hostage? Are we a-going to waste a hostage? No, not us; he might be our last chance, and I shouldn’t wonder. Kill that boy? Not me, mates! And number three? Ah, well, there’s a deal to say to number three. Maybe you don’t count it nothing to have a real college doctor to see you every day—you, John, with your head broke—or you, George Merry, that had the ague shakes upon you not six hours agone, and has your eyes the colour of lemon peel to this same moment on the clock? And maybe, perhaps, you didn’t know there was a

consort coming either? But there is, and not so long till then; and we'll see who'll be glad to have a hostage when it comes to that. And as for number two, and why I made a bargain—well, you came crawling on your knees to me to make it—on your knees you came, you was that downhearted—and you'd have starved too if I hadn't—but that's a trifle! You look there—that's why!’

And he cast down upon the floor a paper that I instantly recognized—none other than the chart on yellow paper, with the three red crosses, that I had found in the oilcloth at the bottom of the captain’s chest. Why the doctor had given it to him was more than I could fancy.

But if it were inexplicable to me, the appearance of the chart was incredible to the surviving mutineers. They leaped upon it like cats upon a mouse. It went from hand to hand, one tearing it from another; and by the oaths and the cries and the childish laughter with which they accompanied their examination, you would have thought, not only they were fingering the very gold, but were at sea with it, besides, in safety.

‘Yes,’ said one, ‘that’s Flint, sure enough. J. F., and a score below, with a clove hitch to it; so he done ever.’

‘Mighty pretty,’ said George. ‘But how are we to get away with it, and us no ship.’

Silver suddenly sprang up, and supporting himself with a hand against the wall: ‘Now I give you warning, George,’ he cried. ‘One more word of your sauce, and I’ll call you down and fight you. How? Why, how do I know? You had ought to tell me that—you and the rest, that lost me my schooner, with your interference, burn you! But not you, you can’t; you hain’t got the invention of a cockroach. But civil you can speak, and shall, George Merry, you may lay to that.’

‘That’s fair enow,’ said the old man Morgan.

‘Fair! I reckon so,’ said the sea-cook. ‘You lost the ship; I found the treasure. Who’s the better man at that? And now I resign, by thunder! Elect whom you please to be your cap’n now; I’m done with it.’

‘Silver!’ they cried. ‘Barbecue forever! Barbecue for cap’n!’

‘So that’s the toon, is it?’ cried the cook. ‘George, I reckon you’ll have to wait another turn, friend; and lucky for you as I’m not a revengeful man. But that was never my way. And now, shipmates, this black spot? ‘Tain’t much good now, is it? Dick’s crossed his luck and spoiled his Bible, and that’s about all.’

## *Treasure Island*

‘It’ll do to kiss the book on still, won’t it?’ growled Dick, who was evidently uneasy at the curse he had brought upon himself.

‘A Bible with a bit cut out!’ returned Silver derisively.  
‘Not it. It don’t bind no more’n a ballad-book.’

‘Don’t it, though?’ cried Dick with a sort of joy. ‘Well, I reckon that’s worth having too.’

‘Here, Jim—here’s a cur’osity for you,’ said Silver, and he tossed me the paper.

It was around about the size of a crown piece. One side was blank, for it had been the last leaf; the other contained a verse or two of Revelation—these words among the rest, which struck sharply home upon my mind: ‘Without are dogs and murderers.’ The printed side had been blackened with wood ash, which already began to come off and soil my fingers; on the blank side had been written with the same material the one word ‘Deposed.’ I have that curiosity beside me at this moment, but not a trace of writing now remains beyond a single scratch, such as a man might make with his thumb-nail.

That was the end of the night’s business. Soon after, with a drink all round, we lay down to sleep, and the outside of Silver’s vengeance was to put George Merry up

for sentinel and threaten him with death if he should prove unfaithful.

It was long ere I could close an eye, and heaven knows I had matter enough for thought in the man whom I had slain that afternoon, in my own most perilous position, and above all, in the remarkable game that I saw Silver now engaged upon—keeping the mutineers together with one hand and grasping with the other after every means, possible and impossible, to make his peace and save his miserable life. He himself slept peacefully and snored aloud, yet my heart was sore for him, wicked as he was, to think on the dark perils that environed and the shameful gibbet that awaited him.

**30**

## **On Parole**

I WAS wakened—indeed, we were all wakened, for I could see even the sentinel shake himself together from where he had fallen against the door-post—by a clear, hearty voice hailing us from the margin of the wood:

‘Block house, ahoy!’ it cried. ‘Here’s the doctor.’

And the doctor it was. Although I was glad to hear the sound, yet my gladness was not without admixture. I remembered with confusion my insubordinate and stealthy conduct, and when I saw where it had brought me—among what companions and surrounded by what dangers—I felt ashamed to look him in the face.

He must have risen in the dark, for the day had hardly come; and when I ran to a loophole and looked out, I saw him standing, like Silver once before, up to the mid-leg in creeping vapour.

‘You, doctor! Top o’ the morning to you, sir!’ cried Silver, broad awake and beaming with good nature in a moment. ‘Bright and early, to be sure; and it’s the early bird, as the saying goes, that gets the rations. George,

shake up your timbers, son, and help Dr. Livesey over the ship's side. All a-doin' well, your patients was—all well and merry.'

So he pattered on, standing on the hilltop with his crutch under his elbow and one hand upon the side of the log-house —quite the old John in voice, manner, and expression.

'We've quite a surprise for you too, sir,' he continued. 'We've a little stranger here—he! he! A noo boarder and lodger, sir, and looking fit and taut as a fiddle; slep' like a supercargo, he did, right alongside of John—stem to stem we was, all night.'

Dr. Livesey was by this time across the stockade and pretty near the cook, and I could hear the alteration in his voice as he said, 'Not Jim?'

'The very same Jim as ever was,' says Silver.

The doctor stopped outright, although he did not speak, and it was some seconds before he seemed able to move on.

'Well, well,' he said at last, 'duty first and pleasure afterwards, as you might have said yourself, Silver. Let us overhaul these patients of yours.'

A moment afterwards he had entered the block house and with one grim nod to me proceeded with his work

among the sick. He seemed under no apprehension, though he must have known that his life, among these treacherous demons, depended on a hair; and he rattled on to his patients as if he were paying an ordinary professional visit in a quiet English family. His manner, I suppose, reacted on the men, for they behaved to him as if nothing had occurred, as if he were still ship's doctor and they still faithful hands before the mast.

'You're doing well, my friend,' he said to the fellow with the bandaged head, 'and if ever any person had a close shave, it was you; your head must be as hard as iron. Well, George, how goes it? You're a pretty colour, certainly; why, your liver, man, is upside down. Did you take that medicine? Did he take that medicine, men?'

'Aye, aye, sir, he took it, sure enough,' returned Morgan.

'Because, you see, since I am mutineers' doctor, or prison doctor as I prefer to call it,' says Doctor Livesey in his pleasantest way, 'I make it a point of honour not to lose a man for King George (God bless him!) and the gallows.'

The rogues looked at each other but swallowed the home-thrust in silence.

'Dick don't feel well, sir,' said one.

‘Don’t he?’ replied the doctor. ‘Well, step up here, Dick, and let me see your tongue. No, I should be surprised if he did! The man’s tongue is fit to frighten the French. Another fever.’

‘Ah, there,’ said Morgan, ‘that comed of sp’iling Bibles.’

‘That comes—as you call it—of being arrant asses,’ retorted the doctor, ‘and not having sense enough to know honest air from poison, and the dry land from a vile, pestiferous slough. I think it most probable— though of course it’s only an opinion—that you’ll all have the deuce to pay before you get that malaria out of your systems. Camp in a bog, would you? Silver, I’m surprised at you. You’re less of a fool than many, take you all round; but you don’t appear to me to have the rudiments of a notion of the rules of health.

‘Well,’ he added after he had dosed them round and they had taken his prescriptions, with really laughable humility, more like charity schoolchildren than blood-guilty mutineers and pirates—‘well, that’s done for today. And now I should wish to have a talk with that boy, please.’

And he nodded his head in my direction carelessly.

George Merry was at the door, spitting and spluttering over some bad-tasted medicine; but at the first word of the doctor's proposal he swung round with a deep flush and cried 'No!' and swore.

Silver struck the barrel with his open hand.

'Si-lence!' he roared and looked about him positively like a lion. 'Doctor,' he went on in his usual tones, 'I was a-thinking of that, knowing as how you had a fancy for the boy. We're all humbly grateful for your kindness, and as you see, puts faith in you and takes the drugs down like that much grog. And I take it I've found a way as'll suit all. Hawkins, will you give me your word of honour as a young gentleman—for a young gentleman you are, although poor born—your word of honour not to slip your cable?'

I readily gave the pledge required.

'Then, doctor,' said Silver, 'you just step outside o' that stockade, and once you're there I'll bring the boy down on the inside, and I reckon you can yarn through the spars. Good day to you, sir, and all our dooties to the squire and Cap'n Smollett.'

The explosion of disapproval, which nothing but Silver's black looks had restrained, broke out immediately the doctor had left the house. Silver was roundly accused

of playing double—of trying to make a separate peace for himself, of sacrificing the interests of his accomplices and victims, and, in one word, of the identical, exact thing that he was doing. It seemed to me so obvious, in this case, that I could not imagine how he was to turn their anger. But he was twice the man the rest were, and his last night's victory had given him a huge preponderance on their minds. He called them all the fools and dolts you can imagine, said it was necessary I should talk to the doctor, fluttered the chart in their faces, asked them if they could afford to break the treaty the very day they were bound a-treasure-hunting.

'No, by thunder!' he cried. 'It's us must break the treaty when the time comes; and till then I'll gammon that doctor, if I have to ile his boots with brandy.'

And then he bade them get the fire lit, and stalked out upon his crutch, with his hand on my shoulder, leaving them in a disarray, and silenced by his volubility rather than convinced.

'Slow, lad, slow,' he said. 'They might round upon us in a twinkle of an eye if we was seen to hurry.'

Very deliberately, then, did we advance across the sand to where the doctor awaited us on the other side of

the stockade, and as soon as we were within easy speaking distance Silver stopped.

‘You’ll make a note of this here also, doctor,’ says he, ‘and the boy’ll tell you how I saved his life, and were deposed for it too, and you may lay to that. Doctor, when a man’s steering as near the wind as me—playing chuck-farthing with the last breath in his body, like—you wouldn’t think it too much, mayhap, to give him one good word? You’ll please bear in mind it’s not my life only now—it’s that boy’s into the bargain; and you’ll speak me fair, doctor, and give me a bit o’ hope to go on, for the sake of mercy.’

Silver was a changed man once he was out there and had his back to his friends and the block house; his cheeks seemed to have fallen in, his voice trembled; never was a soul more dead in earnest.

‘Why, John, you’re not afraid?’ asked Dr. Livesey.

‘Doctor, I’m no coward; no, not I—not SO much!’ and he snapped his fingers. ‘If I was I wouldn’t say it. But I’ll own up fairly, I’ve the shakes upon me for the gallows. You’re a good man and a true; I never seen a better man! And you’ll not forget what I done good, not any more than you’ll forget the bad, I know. And I step aside—see

here—and leave you and Jim alone. And you'll put that down for me too, for it's a long stretch, is that!&#x2019;

So saying, he stepped back a little way, till he was out of earshot, and there sat down upon a tree-stump and began to whistle, spinning round now and again upon his seat so as to command a sight, sometimes of me and the doctor and sometimes of his unruly ruffians as they went to and fro in the sand between the fire—which they were busy rekindling—and the house, from which they brought forth pork and bread to make the breakfast.

‘So, Jim,’ said the doctor sadly, ‘here you are. As you have brewed, so shall you drink, my boy. Heaven knows, I cannot find it in my heart to blame you, but this much I will say, be it kind or unkind: when Captain Smollett was well, you dared not have gone off; and when he was ill and couldn’t help it, by George, it was downright cowardly!’

I will own that I here began to weep. ‘Doctor,’ I said, ‘you might spare me. I have blamed myself enough; my life’s forfeit anyway, and I should have been dead by now if Silver hadn’t stood for me; and doctor, believe this, I can die—and I dare say I deserve it—but what I fear is torture. If they come to torture me—‘

‘Jim,’ the doctor interrupted, and his voice was quite changed, ‘Jim, I can’t have this. Whip over, and we’ll run for it.’

‘Doctor,’ said I, ‘I passed my word.’

‘I know, I know,’ he cried. ‘We can’t help that, Jim, now. I’ll take it on my shoulders, holus bolus, blame and shame, my boy; but stay here, I cannot let you. Jump! One jump, and you’re out, and we’ll run for it like antelopes.’

‘No,’ I replied; ‘you know right well you wouldn’t do the thing yourself—neither you nor squire nor captain; and no more will I. Silver trusted me; I passed my word, and back I go. But, doctor, you did not let me finish. If they come to torture me, I might let slip a word of where the ship is, for I got the ship, part by luck and part by risking, and she lies in North Inlet, on the southern beach, and just below high water. At half tide she must be high and dry.’

‘The ship!’ exclaimed the doctor.

Rapidly I described to him my adventures, and he heard me out in silence.

‘There is a kind of fate in this,’ he observed when I had done. ‘Every step, it’s you that saves our lives; and do you suppose by any chance that we are going to let you lose yours? That would be a poor return, my boy. You

found out the plot; you found Ben Gunn—the best deed that ever you did, or will do, though you live to ninety. Oh, by Jupiter, and talking of Ben Gunn! Why, this is the mischief in person. Silver!' he cried. 'Silver! I'll give you a piece of advice,' he continued as the cook drew near again; 'don't you be in any great hurry after that treasure.'

'Why, sir, I do my possible, which that ain't,' said Silver. 'I can only, asking your pardon, save my life and the boy's by seeking for that treasure; and you may lay to that.'

'Well, Silver,' replied the doctor, 'if that is so, I'll go one step further: look out for squalls when you find it.'

'Sir,' said Silver, 'as between man and man, that's too much and too little. What you're after, why you left the block house, why you given me that there chart, I don't know, now, do I? And yet I done your bidding with my eyes shut and never a word of hope! But no, this here's too much. If you won't tell me what you mean plain out, just say so and I'll leave the helm.'

'No,' said the doctor musingly; 'I've no right to say more; it's not my secret, you see, Silver, or, I give you my word, I'd tell it you. But I'll go as far with you as I dare go, and a step beyond, for I'll have my wig sorted by the captain or I'm mistaken! And first, I'll give you a bit of

## *Treasure Island*

hope; Silver, if we both get alive out of this wolf-trap, I'll do my best to save you, short of perjury.'

Silver's face was radiant. 'You couldn't say more, I'm sure, sir, not if you was my mother,' he cried.

'Well, that's my first concession,' added the doctor. 'My second is a piece of advice: keep the boy close beside you, and when you need help, halloo. I'm off to seek it for you, and that itself will show you if I speak at random. Good-bye, Jim.'

And Dr. Livesey shook hands with me through the stockade, nodded to Silver, and set off at a brisk pace into the wood.

## The Treasure-hunt—Flint's Pointer

'JIM,' said Silver when we were alone, 'if I saved your life, you saved mine; and I'll not forget it. I seen the doctor waving you to run for it—with the tail of my eye, I did; and I seen you say no, as plain as hearing. Jim, that's one to you. This is the first glint of hope I had since the attack failed, and I owe it you. And now, Jim, we're to go in for this here treasure-hunting, with sealed orders too, and I don't like it; and you and me must stick close, back to back like, and we'll save our necks in spite o' fate and fortune.'

Just then a man hailed us from the fire that breakfast was ready, and we were soon seated here and there about the sand over biscuit and fried junk. They had lit a fire fit to roast an ox, and it was now grown so hot that they could only approach it from the windward, and even there not without precaution. In the same wasteful spirit, they had cooked, I suppose, three times more than we could eat; and one of them, with an empty laugh, threw what was left into the fire, which blazed and roared again over

this unusual fuel. I never in my life saw men so careless of the morrow; hand to mouth is the only word that can describe their way of doing; and what with wasted food and sleeping sentries, though they were bold enough for a brush and be done with it, I could see their entire unfitness for anything like a prolonged campaign.

Even Silver, eating away, with Captain Flint upon his shoulder, had not a word of blame for their recklessness. And this the more surprised me, for I thought he had never shown himself so cunning as he did then.

‘Aye, mates,’ said he, ‘it’s lucky you have Barbecue to think for you with this here head. I got what I wanted, I did. Sure enough, they have the ship. Where they have it, I don’t know yet; but once we hit the treasure, we’ll have to jump about and find out. And then, mates, us that has the boats, I reckon, has the upper hand.’

Thus he kept running on, with his mouth full of the hot bacon; thus he restored their hope and confidence, and, I more than suspect, repaired his own at the same time.

‘As for hostage,’ he continued, ‘that’s his last talk, I guess, with them he loves so dear. I’ve got my piece o’ news, and thanky to him for that; but it’s over and done. I’ll take him in a line when we go treasure-hunting, for we’ll keep him like so much gold, in case of accidents,

you mark, and in the meantime. Once we got the ship and treasure both and off to sea like jolly companions, why then we'll talk Mr. Hawkins over, we will, and we'll give him his share, to be sure, for all his kindness.'

It was no wonder the men were in a good humour now. For my part, I was horribly cast down. Should the scheme he had now sketched prove feasible, Silver, already doubly a traitor, would not hesitate to adopt it. He had still a foot in either camp, and there was no doubt he would prefer wealth and freedom with the pirates to a bare escape from hanging, which was the best he had to hope on our side.

Nay, and even if things so fell out that he was forced to keep his faith with Dr. Livesey, even then what danger lay before us! What a moment that would be when the suspicions of his followers turned to certainty and he and I should have to fight for dear life—he a cripple and I a boy—against five strong and active seamen!

Add to this double apprehension the mystery that still hung over the behaviour of my friends, their unexplained desertion of the stockade, their inexplicable cession of the chart, or harder still to understand, the doctor's last warning to Silver, 'Look out for squalls when you find it,' and you will readily believe how little taste I found in my

breakfast and with how uneasy a heart I set forth behind my captors on the quest for treasure.

We made a curious figure, had anyone been there to see us—all in soiled sailor clothes and all but me armed to the teeth. Silver had two guns slung about him—one before and one behind—besides the great cutlass at his waist and a pistol in each pocket of his square-tailed coat. To complete his strange appearance, Captain Flint sat perched upon his shoulder and gabbling odds and ends of purposeless sea-talk. I had a line about my waist and followed obediently after the sea-cook, who held the loose end of the rope, now in his free hand, now between his powerful teeth. For all the world, I was led like a dancing bear.

The other men were variously burthened, some carrying picks and shovels—for that had been the very first necessary they brought ashore from the HISPANIOLA— others laden with pork, bread, and brandy for the midday meal. All the stores, I observed, came from our stock, and I could see the truth of Silver's words the night before. Had he not struck a bargain with the doctor, he and his mutineers, deserted by the ship, must have been driven to subsist on clear water and the proceeds of their hunting. Water would have been little to

their taste; a sailor is not usually a good shot; and besides all that, when they were so short of eatables, it was not likely they would be very flush of powder.

Well, thus equipped, we all set out—even the fellow with the broken head, who should certainly have kept in shadow—and straggled, one after another, to the beach, where the two gigs awaited us. Even these bore trace of the drunken folly of the pirates, one in a broken thwart, and both in their muddy and unbailed condition. Both were to be carried along with us for the sake of safety; and so, with our numbers divided between them, we set forth upon the bosom of the anchorage.

As we pulled over, there was some discussion on the chart. The red cross was, of course, far too large to be a guide; and the terms of the note on the back, as you will hear, admitted of some ambiguity. They ran, the reader may remember, thus:

Tall tree, Spy-glass shoulder, bearing a point to  
the N. of N.N.E.  
Skeleton Island E.S.E. and by E.  
Ten feet.

A tall tree was thus the principal mark. Now, right before us the anchorage was bounded by a plateau from two to three hundred feet high, adjoining on the north the

sloping southern shoulder of the Spy-glass and rising again towards the south into the rough, cliffy eminence called the Mizzen-mast Hill. The top of the plateau was dotted thickly with pine-trees of varying height. Every here and there, one of a different species rose forty or fifty feet clear above its neighbours, and which of these was the particular ‘tall tree’ of Captain Flint could only be decided on the spot, and by the readings of the compass.

Yet, although that was the case, every man on board the boats had picked a favourite of his own ere we were half-way over, Long John alone shrugging his shoulders and bidding them wait till they were there.

We pulled easily, by Silver’s directions, not to weary the hands prematurely, and after quite a long passage, landed at the mouth of the second river—that which runs down a woody cleft of the Spy-glass. Thence, bending to our left, we began to ascend the slope towards the plateau.

At the first outset, heavy, miry ground and a matted, marish vegetation greatly delayed our progress; but by little and little the hill began to steepen and become stony under foot, and the wood to change its character and to grow in a more open order. It was, indeed, a most pleasant portion of the island that we were now approaching. A heavy-scented broom and many flowering shrubs had

almost taken the place of grass. Thickets of green nutmeg-trees were dotted here and there with the red columns and the broad shadow of the pines; and the first mingled their spice with the aroma of the others. The air, besides, was fresh and stirring, and this, under the sheer sunbeams, was a wonderful refreshment to our senses.

The party spread itself abroad, in a fan shape, shouting and leaping to and fro. About the centre, and a good way behind the rest, Silver and I followed—I tethered by my rope, he ploughing, with deep pants, among the sliding gravel. From time to time, indeed, I had to lend him a hand, or he must have missed his footing and fallen backward down the hill.

We had thus proceeded for about half a mile and were approaching the brow of the plateau when the man upon the farthest left began to cry aloud, as if in terror. Shout after shout came from him, and the others began to run in his direction.

‘He can’t ‘a found the treasure,’ said old Morgan, hurrying past us from the right, ‘for that’s clean a-top.’

Indeed, as we found when we also reached the spot, it was something very different. At the foot of a pretty big pine and involved in a green creeper, which had even partly lifted some of the smaller bones, a human skeleton

lay, with a few shreds of clothing, on the ground. I believe a chill struck for a moment to every heart.

'He was a seaman,' said George Merry, who, bolder than the rest, had gone up close and was examining the rags of clothing. 'Leastways, this is good sea-cloth.'

'Aye, aye,' said Silver; 'like enough; you wouldn't look to find a bishop here, I reckon. But what sort of a way is that for bones to lie? 'Tain't in natur'.'

Indeed, on a second glance, it seemed impossible to fancy that the body was in a natural position. But for some disarray (the work, perhaps, of the birds that had fed upon him or of the slow-growing creeper that had gradually enveloped his remains) the man lay perfectly straight—his feet pointing in one direction, his hands, raised above his head like a diver's, pointing directly in the opposite.

'I've taken a notion into my old numbskull,' observed Silver. 'Here's the compass; there's the tip-top p'int o' Skeleton Island, stickin' out like a tooth. Just take a bearing, will you, along the line of them bones.'

It was done. The body pointed straight in the direction of the island, and the compass read duly E.S.E. and by E.

'I thought so,' cried the cook; 'this here is a p'inter. Right up there is our line for the Pole Star and the jolly

dollars. But, by thunder! If it don't make me cold inside to think of Flint. This is one of HIS jokes, and no mistake. Him and these six was alone here; he killed 'em, every man; and this one he hauled here and laid down by compass, shiver my timbers! They're long bones, and the hair's been yellow. Aye, that would be Allardyce. You mind Allardyce, Tom Morgan?"

'Aye, aye,' returned Morgan; 'I mind him; he owed me money, he did, and took my knife ashore with him.'

'Speaking of knives,' said another, 'why don't we find his'n lying round? Flint warn't the man to pick a seaman's pocket; and the birds, I guess, would leave it be.'

'By the powers, and that's true!' cried Silver.

'There ain't a thing left here,' said Merry, still feeling round among the bones; 'not a copper doit nor a baccy box. It don't look nat'ral to me.'

'No, by gum, it don't,' agreed Silver; 'not nat'ral, nor not nice, says you. Great guns! Messmates, but if Flint was living, this would be a hot spot for you and me. Six they were, and six are we; and bones is what they are now.'

‘I saw him dead with these here deadlights,’ said Morgan. ‘Billy took me in. There he laid, with penny-pieces on his eyes.’

‘Dead—aye, sure enough he’s dead and gone below,’ said the fellow with the bandage; ‘but if ever sperrit walked, it would be Flint’s. Dear heart, but he died bad, did Flint!’

‘Aye, that he did,’ observed another; ‘now he raged, and now he hollered for the rum, and now he sang. ‘Fifteen Men’ were his only song, mates; and I tell you true, I never rightly liked to hear it since. It was main hot, and the windy was open, and I hear that old song comin’ out as clear as clear—and the death-haul on the man already.’

‘Come, come,’ said Silver; ‘stow this talk. He’s dead, and he don’t walk, that I know; leastways, he won’t walk by day, and you may lay to that. Care killed a cat. Fetch ahead for the doubloons.’

We started, certainly; but in spite of the hot sun and the staring daylight, the pirates no longer ran separate and shouting through the wood, but kept side by side and spoke with bated breath. The terror of the dead buccaneer had fallen on their spirits.

## The Treasure-hunt—The Voice Among the Trees

PARTLY from the damping influence of this alarm, partly to rest Silver and the sick folk, the whole party sat down as soon as they had gained the brow of the ascent.

The plateau being somewhat tilted towards the west, this spot on which we had paused commanded a wide prospect on either hand. Before us, over the tree-tops, we beheld the Cape of the Woods fringed with surf; behind, we not only looked down upon the anchorage and Skeleton Island, but saw—clear across the spit and the eastern lowlands—a great field of open sea upon the east. Sheer above us rose the Spy-glass, here dotted with single pines, there black with precipices. There was no sound but that of the distant breakers, mounting from all round, and the chirp of countless insects in the brush. Not a man, not a sail, upon the sea; the very largeness of the view increased the sense of solitude.

Silver, as he sat, took certain bearings with his compass.

## Treasure Island

‘There are three ‘tall trees’’ said he, ‘about in the right line from Skeleton Island. ‘Spy-glass shoulder,’ I take it, means that lower p’int there. It’s child’s play to find the stuff now. I’ve half a mind to dine first.’

‘I don’t feel sharp,’ growled Morgan. ‘Thinkin’ o’ Flint—I think it were—as done me.’

‘Ah, well, my son, you praise your stars he’s dead,’ said Silver.

‘He were an ugly devil,’ cried a third pirate with a shudder; ‘that blue in the face too!’

‘That was how the rum took him,’ added Merry. ‘Blue! Well, I reckon he was blue. That’s a true word.’

Ever since they had found the skeleton and got upon this train of thought, they had spoken lower and lower, and they had almost got to whispering by now, so that the sound of their talk hardly interrupted the silence of the wood. All of a sudden, out of the middle of the trees in front of us, a thin, high, trembling voice struck up the well-known air and words:

‘Fifteen men on the dead man’s chest—  
Yo-ho-ho, and a bottle of rum!’

I never have seen men more dreadfully affected than the pirates. The colour went from their six faces like

enchantment; some leaped to their feet, some clawed hold of others; Morgan grovelled on the ground.

‘It’s Flint, by ——!’ cried Merry.

The song had stopped as suddenly as it began—broken off, you would have said, in the middle of a note, as though someone had laid his hand upon the singer’s mouth. Coming through the clear, sunny atmosphere among the green tree-tops, I thought it had sounded airily and sweetly; and the effect on my companions was the stranger.

‘Come,’ said Silver, struggling with his ashen lips to get the word out; ‘this won’t do. Stand by to go about. This is a rum start, and I can’t name the voice, but it’s someone skylarking—someone that’s flesh and blood, and you may lay to that.’

His courage had come back as he spoke, and some of the colour to his face along with it. Already the others had begun to lend an ear to this encouragement and were coming a little to themselves, when the same voice broke out again—not this time singing, but in a faint distant hail that echoed yet fainter among the clefts of the Spy-glass.

‘Darby M’Graw,’ it wailed—for that is the word that best describes the sound—‘Darby M’Graw! Darby M’Graw!’ again and again and again; and then rising a

little higher, and with an oath that I leave out: ‘Fetch aft the rum, Darby!’

The buccaneers remained rooted to the ground, their eyes starting from their heads. Long after the voice had died away they still stared in silence, dreadfully, before them.

‘That fixes it!’ gasped one. ‘Let’s go.’

‘They was his last words,’ moaned Morgan, ‘his last words above board.’

Dick had his Bible out and was praying volubly. He had been well brought up, had Dick, before he came to sea and fell among bad companions.

Still Silver was unconquered. I could hear his teeth rattle in his head, but he had not yet surrendered.

‘Nobody in this here island ever heard of Darby,’ he muttered; ‘not one but us that’s here.’ And then, making a great effort: ‘Shipmates,’ he cried, ‘I’m here to get that stuff, and I’ll not be beat by man or devil. I never was feared of Flint in his life, and, by the powers, I’ll face him dead. There’s seven hundred thousand pound not a quarter of a mile from here. When did ever a gentleman o’ fortune show his stern to that much dollars for a boozy old seaman with a blue mug—and him dead too?’

But there was no sign of reawakening courage in his followers, rather, indeed, of growing terror at the irreverence of his words.

‘Belay there, John!’ said Merry. ‘Don’t you cross a sperrit.’

And the rest were all too terrified to reply. They would have run away severally had they dared; but fear kept them together, and kept them close by John, as if his daring helped them. He, on his part, had pretty well fought his weakness down.

‘Sperrit? Well, maybe,’ he said. ‘But there’s one thing not clear to me. There was an echo. Now, no man ever seen a sperrit with a shadow; well then, what’s he doing with an echo to him, I should like to know? That ain’t in natur’, surely?’

This argument seemed weak enough to me. But you can never tell what will affect the superstitious, and to my wonder, George Merry was greatly relieved.

‘Well, that’s so,’ he said. ‘You’ve a head upon your shoulders, John, and no mistake. ‘Bout ship, mates! This here crew is on a wrong tack, I do believe. And come to think on it, it was like Flint’s voice, I grant you, but not just so clear-away like it, after all. It was liker somebody else’s voice now—it was liker—‘

‘By the powers, Ben Gunn!’ roared Silver.

‘Aye, and so it were,’ cried Morgan, springing on his knees. ‘Ben Gunn it were!’

‘It don’t make much odds, do it, now?’ asked Dick. ‘Ben Gunn’s not here in the body any more’n Flint.’

But the older hands greeted this remark with scorn.

‘Why, nobody minds Ben Gunn,’ cried Merry; ‘dead or alive, nobody minds him.’

It was extraordinary how their spirits had returned and how the natural colour had revived in their faces. Soon they were chatting together, with intervals of listening; and not long after, hearing no further sound, they shouldered the tools and set forth again, Merry walking first with Silver’s compass to keep them on the right line with Skeleton Island. He had said the truth: dead or alive, nobody minded Ben Gunn.

Dick alone still held his Bible, and looked around him as he went, with fearful glances; but he found no sympathy, and Silver even joked him on his precautions.

‘I told you,’ said he—‘I told you you had sp’iled your Bible. If it ain’t no good to swear by, what do you suppose a sperrit would give for it? Not that!’ and he snapped his big fingers, halting a moment on his crutch.

But Dick was not to be comforted; indeed, it was soon plain to me that the lad was falling sick; hastened by heat, exhaustion, and the shock of his alarm, the fever, predicted by Dr. Livesey, was evidently growing swiftly higher.

It was fine open walking here, upon the summit; our way lay a little downhill, for, as I have said, the plateau tilted towards the west. The pines, great and small, grew wide apart; and even between the clumps of nutmeg and azalea, wide open spaces baked in the hot sunshine. Striking, as we did, pretty near north-west across the island, we drew, on the one hand, ever nearer under the shoulders of the Spy-glass, and on the other, looked ever wider over that western bay where I had once tossed and trembled in the oracle.

The first of the tall trees was reached, and by the bearings proved the wrong one. So with the second. The third rose nearly two hundred feet into the air above a clump of underwood—a giant of a vegetable, with a red column as big as a cottage, and a wide shadow around in which a company could have manoeuvred. It was conspicuous far to sea both on the east and west and might have been entered as a sailing mark upon the chart.

But it was not its size that now impressed my companions; it was the knowledge that seven hundred thousand pounds in gold lay somewhere buried below its spreading shadow. The thought of the money, as they drew nearer, swallowed up their previous terrors. Their eyes burned in their heads; their feet grew speedier and lighter; their whole soul was found up in that fortune, that whole lifetime of extravagance and pleasure, that lay waiting there for each of them.

Silver hobbled, grunting, on his crutch; his nostrils stood out and quivered; he cursed like a madman when the flies settled on his hot and shiny countenance; he plucked furiously at the line that held me to him and from time to time turned his eyes upon me with a deadly look. Certainly he took no pains to hide his thoughts, and certainly I read them like print. In the immediate nearness of the gold, all else had been forgotten: his promise and the doctor's warning were both things of the past, and I could not doubt that he hoped to seize upon the treasure, find and board the HISPANIOLA under cover of night, cut every honest throat about that island, and sail away as he had at first intended, laden with crimes and riches.

Shaken as I was with these alarms, it was hard for me to keep up with the rapid pace of the treasure-hunters.

Now and again I stumbled, and it was then that Silver plucked so roughly at the rope and launched at me his murderous glances. Dick, who had dropped behind us and now brought up the rear, was babbling to himself both prayers and curses as his fever kept rising. This also added to my wretchedness, and to crown all, I was haunted by the thought of the tragedy that had once been acted on that plateau, when that ungodly buccaneer with the blue face —he who died at Savannah, singing and shouting for drink— had there, with his own hand, cut down his six accomplices. This grove that was now so peaceful must then have rung with cries, I thought; and even with the thought I could believe I heard it ringing still.

We were now at the margin of the thicket.

‘Huzza, mates, all together!’ shouted Merry; and the foremost broke into a run.

And suddenly, not ten yards further, we beheld them stop. A low cry arose. Silver doubled his pace, digging away with the foot of his crutch like one possessed; and next moment he and I had come also to a dead halt.

Before us was a great excavation, not very recent, for the sides had fallen in and grass had sprouted on the bottom. In this were the shaft of a pick broken in two and

the boards of several packing-cases strewn around. On one of these boards I saw, branded with a hot iron, the name WALRUS—the name of Flint's ship.

All was clear to probation. The CACHE had been found and rifled; the seven hundred thousand pounds were gone!

## The Fall of a Chieftain

THERE never was such an overturn in this world. Each of these six men was as though he had been struck. But with Silver the blow passed almost instantly. Every thought of his soul had been set full-stretch, like a racer, on that money; well, he was brought up, in a single second, dead; and he kept his head, found his temper, and changed his plan before the others had had time to realize the disappointment.

'Jim,' he whispered, 'take that, and stand by for trouble.'

And he passed me a double-barrelled pistol.

At the same time, he began quietly moving northward, and in a few steps had put the hollow between us two and the other five. Then he looked at me and nodded, as much as to say, 'Here is a narrow corner,' as, indeed, I thought it was. His looks were not quite friendly, and I was so revolted at these constant changes that I could not forbear whispering, 'So you've changed sides again.'

There was no time left for him to answer in. The buccaneers, with oaths and cries, began to leap, one after another, into the pit and to dig with their fingers, throwing the boards aside as they did so. Morgan found a piece of gold. He held it up with a perfect spout of oaths. It was a two-guinea piece, and it went from hand to hand among them for a quarter of a minute.

‘Two guineas!’ roared Merry, shaking it at Silver. ‘That’s your seven hundred thousand pounds, is it? You’re the man for bargains, ain’t you? You’re him that never bungled nothing, you wooden-headed lubber!’

‘Dig away, boys,’ said Silver with the coolest insolence; ‘you’ll find some pig-nuts and I shouldn’t wonder.’

‘Pig-nuts!’ repeated Merry, in a scream. ‘Mates, do you hear that? I tell you now, that man there knew it all along. Look in the face of him and you’ll see it wrote there.’

‘Ah, Merry,’ remarked Silver, ‘standing for cap’n again? You’re a pushing lad, to be sure.’

But this time everyone was entirely in Merry’s favour. They began to scramble out of the excavation, darting furious glances behind them. One thing I observed, which

looked well for us: they all got out upon the opposite side from Silver.

Well, there we stood, two on one side, five on the other, the pit between us, and nobody screwed up high enough to offer the first blow. Silver never moved; he watched them, very upright on his crutch, and looked as cool as ever I saw him. He was brave, and no mistake.

At last Merry seemed to think a speech might help matters.

‘Mates,’ says he, ‘there’s two of them alone there; one’s the old cripple that brought us all here and blundered us down to this; the other’s that cub that I mean to have the heart of. Now, mates—‘

He was raising his arm and his voice, and plainly meant to lead a charge. But just then—crack! crack! crack!— three musket-shots flashed out of the thicket. Merry tumbled head foremost into the excavation; the man with the bandage spun round like a teetotum and fell all his length upon his side, where he lay dead, but still twitching; and the other three turned and ran for it with all their might.

Before you could wink, Long John had fired two barrels of a pistol into the struggling Merry, and as the

## Treasure Island

man rolled up his eyes at him in the last agony, ‘George,’ said he, ‘I reckon I settled you.’

At the same moment, the doctor, Gray, and Ben Gunn joined us, with smoking muskets, from among the nutmeg-trees.

‘Forward!’ cried the doctor. ‘Double quick, my lads. We must head ‘em off the boats.’

And we set off at a great pace, sometimes plunging through the bushes to the chest.

I tell you, but Silver was anxious to keep up with us. The work that man went through, leaping on his crutch till the muscles of his chest were fit to burst, was work no sound man ever equalled; and so thinks the doctor. As it was, he was already thirty yards behind us and on the verge of strangling when we reached the brow of the slope.

‘Doctor,’ he hailed, ‘see there! No hurry!’

Sure enough there was no hurry. In a more open part of the plateau, we could see the three survivors still running in the same direction as they had started, right for Mizzen-mast Hill. We were already between them and the boats; and so we four sat down to breathe, while Long John, mopping his face, came slowly up with us.

‘Thank ye kindly, doctor,’ says he. ‘You came in in about the nick, I guess, for me and Hawkins. And so it’s you, Ben Gunn!’ he added. ‘Well, you’re a nice one, to be sure.’

‘I’m Ben Gunn, I am,’ replied the maroon, wriggling like an eel in his embarrassment. ‘And,’ he added, after a long pause, ‘how do, Mr. Silver? Pretty well, I thank ye, says you.’

‘Ben, Ben,’ murmured Silver, ‘to think as you’ve done me!’

The doctor sent back Gray for one of the pick-axes deserted, in their flight, by the mutineers, and then as we proceeded leisurely downhill to where the boats were lying, related in a few words what had taken place. It was a story that profoundly interested Silver; and Ben Gunn, the half-idiot maroon, was the hero from beginning to end.

Ben, in his long, lonely wanderings about the island, had found the skeleton—it was he that had rifled it; he had found the treasure; he had dug it up (it was the haft of his pick-axe that lay broken in the excavation); he had carried it on his back, in many weary journeys, from the foot of the tall pine to a cave he had on the two-pointed hill at the north-east angle of the island, and there it had

laid stored in safety since two months before the arrival of the HISPANIOLA.

When the doctor had wormed this secret from him on the afternoon of the attack, and when next morning he saw the anchorage deserted, he had gone to Silver, given him the chart, which was now useless—given him the stores, for Ben Gunn's cave was well supplied with goats' meat salted by himself—given anything and everything to get a chance of moving in safety from the stockade to the two-pointed hill, there to be clear of malaria and keep a guard upon the money.

'As for you, Jim,' he said, 'it went against my heart, but I did what I thought best for those who had stood by their duty; and if you were not one of these, whose fault was it?'

That morning, finding that I was to be involved in the horrid disappointment he had prepared for the mutineers, he had run all the way to the cave, and leaving the squire to guard the captain, had taken Gray and the maroon and started, making the diagonal across the island to be at hand beside the pine. Soon, however, he saw that our party had the start of him; and Ben Gunn, being fleet of foot, had been dispatched in front to do his best alone. Then it had occurred to him to work upon the

superstitions of his former shipmates, and he was so far successful that Gray and the doctor had come up and were already ambushed before the arrival of the treasure-hunters.

‘Ah,’ said Silver, ‘it were fortunate for me that I had Hawkins here. You would have let old John be cut to bits, and never given it a thought, doctor.’

‘Not a thought,’ replied Dr. Livesey cheerily.

And by this time we had reached the gigs. The doctor, with the pick-axe, demolished one of them, and then we all got aboard the other and set out to go round by sea for North Inlet.

This was a run of eight or nine miles. Silver, though he was almost killed already with fatigue, was set to an oar, like the rest of us, and we were soon skimming swiftly over a smooth sea. Soon we passed out of the straits and doubled the south-east corner of the island, round which, four days ago, we had towed the HISPANIOLA.

As we passed the two-pointed hill, we could see the black mouth of Ben Gunn’s cave and a figure standing by it, leaning on a musket. It was the squire, and we waved a handkerchief and gave him three cheers, in which the voice of Silver joined as heartily as any.

Three miles farther, just inside the mouth of North Inlet, what should we meet but the HISPANIOLA, cruising by herself? The last flood had lifted her, and had there been much wind or a strong tide current, as in the southern anchorage, we should never have found her more, or found her stranded beyond help. As it was, there was little amiss beyond the wreck of the main-sail. Another anchor was got ready and dropped in a fathom and a half of water. We all pulled round again to Rum Cove, the nearest point for Ben Gunn's treasure-house; and then Gray, single-handed, returned with the gig to the HISPANIOLA, where he was to pass the night on guard.

A gentle slope ran up from the beach to the entrance of the cave. At the top, the squire met us. To me he was cordial and kind, saying nothing of my escapade either in the way of blame or praise. At Silver's polite salute he somewhat flushed.

'John Silver,' he said, 'you're a prodigious villain and imposter—a monstrous imposter, sir. I am told I am not to prosecute you. Well, then, I will not. But the dead men, sir, hang about your neck like mill-stones.'

'Thank you kindly, sir,' replied Long John, again saluting.

‘I dare you to thank me!’ cried the squire. ‘It is a gross dereliction of my duty. Stand back.’

And thereupon we all entered the cave. It was a large, airy place, with a little spring and a pool of clear water, overhung with ferns. The floor was sand. Before a big fire lay Captain Smollett; and in a far corner, only duskily flickered over by the blaze, I beheld great heaps of coin and quadrilaterals built of bars of gold. That was Flint’s treasure that we had come so far to seek and that had cost already the lives of seventeen men from the HISPANIOLA. How many it had cost in the amassing, what blood and sorrow, what good ships scuttled on the deep, what brave men walking the plank blindfold, what shot of cannon, what shame and lies and cruelty, perhaps no man alive could tell. Yet there were still three upon that island—Silver, and old Morgan, and Ben Gunn—who had each taken his share in these crimes, as each had hoped in vain to share in the reward.

‘Come in, Jim,’ said the captain. ‘You’re a good boy in your line, Jim, but I don’t think you and me’ll go to sea again. You’re too much of the born favourite for me. Is that you, John Silver? What brings you here, man?’

‘Come back to my dooty, sir,’ returned Silver.

‘Ah!’ said the captain, and that was all he said.

What a supper I had of it that night, with all my friends around me; and what a meal it was, with Ben Gunn's salted goat and some delicacies and a bottle of old wine from the HISPANIOLA. Never, I am sure, were people gayer or happier. And there was Silver, sitting back almost out of the firelight, but eating heartily, prompt to spring forward when anything was wanted, even joining quietly in our laughter—the same bland, polite, obsequious seaman of the voyage out.

## 34 And Last

THE next morning we fell early to work, for the transportation of this great mass of gold near a mile by land to the beach, and thence three miles by boat to the HISPANIOLA, was a considerable task for so small a number of workmen. The three fellows still abroad upon the island did not greatly trouble us; a single sentry on the shoulder of the hill was sufficient to ensure us against any sudden onslaught, and we thought, besides, they had had more than enough of fighting.

Therefore the work was pushed on briskly. Gray and Ben Gunn came and went with the boat, while the rest during their absences piled treasure on the beach. Two of the bars, slung in a rope's end, made a good load for a grown man—one that he was glad to walk slowly with. For my part, as I was not much use at carrying, I was kept busy all day in the cave packing the minted money into bread-bags.

It was a strange collection, like Billy Bones's hoard for the diversity of coinage, but so much larger and so much more varied that I think I never had more pleasure than in

sorting them. English, French, Spanish, Portuguese, Georges, and Louises, doubloons and double guineas and moidores and sequins, the pictures of all the kings of Europe for the last hundred years, strange Oriental pieces stamped with what looked like wisps of string or bits of spider's web, round pieces and square pieces, and pieces bored through the middle, as if to wear them round your neck—nearly every variety of money in the world must, I think, have found a place in that collection; and for number, I am sure they were like autumn leaves, so that my back ached with stooping and my fingers with sorting them out.

Day after day this work went on; by every evening a fortune had been stowed aboard, but there was another fortune waiting for the morrow; and all this time we heard nothing of the three surviving mutineers.

At last—I think it was on the third night—the doctor and I were strolling on the shoulder of the hill where it overlooks the lowlands of the isle, when, from out the thick darkness below, the wind brought us a noise between shrieking and singing. It was only a snatch that reached our ears, followed by the former silence.

‘Heaven forgive them,’ said the doctor; “tis the mutineers!”

‘All drunk, sir,’ struck in the voice of Silver from behind us.

Silver, I should say, was allowed his entire liberty, and in spite of daily rebuffs, seemed to regard himself once more as quite a privileged and friendly dependent. Indeed, it was remarkable how well he bore these slights and with what unwearying politeness he kept on trying to ingratiate himself with all. Yet, I think, none treated him better than a dog, unless it was Ben Gunn, who was still terribly afraid of his old quartermaster, or myself, who had really something to thank him for; although for that matter, I suppose, I had reason to think even worse of him than anybody else, for I had seen him meditating a fresh treachery upon the plateau. Accordingly, it was pretty gruffly that the doctor answered him.

‘Drunk or raving,’ said he.

‘Right you were, sir,’ replied Silver; ‘and precious little odds which, to you and me.’

‘I suppose you would hardly ask me to call you a humane man,’ returned the doctor with a sneer, ‘and so my feelings may surprise you, Master Silver. But if I were sure they were raving—as I am morally certain one, at least, of them is down with fever—I should leave this

camp, and at whatever risk to my own carcass, take them the assistance of my skill.'

'Ask your pardon, sir, you would be very wrong,' quoth Silver. 'You would lose your precious life, and you may lay to that. I'm on your side now, hand and glove; and I shouldn't wish for to see the party weakened, let alone yourself, seeing as I know what I owes you. But these men down there, they couldn't keep their word—no, not supposing they wished to; and what's more, they couldn't believe as you could.'

'No,' said the doctor. 'You're the man to keep your word, we know that.'

Well, that was about the last news we had of the three pirates. Only once we heard a gunshot a great way off and supposed them to be hunting. A council was held, and it was decided that we must desert them on the island —to the huge glee, I must say, of Ben Gunn, and with the strong approval of Gray. We left a good stock of powder and shot, the bulk of the salt goat, a few medicines, and some other necessaries, tools, clothing, a spare sail, a fathom or two of rope, and by the particular desire of the doctor, a handsome present of tobacco.

That was about our last doing on the island. Before that, we had got the treasure stowed and had shipped

enough water and the remainder of the goat meat in case of any distress; and at last, one fine morning, we weighed anchor, which was about all that we could manage, and stood out of North Inlet, the same colours flying that the captain had flown and fought under at the palisade.

The three fellows must have been watching us closer than we thought for, as we soon had proved. For coming through the narrows, we had to lie very near the southern point, and there we saw all three of them kneeling together on a spit of sand, with their arms raised in supplication. It went to all our hearts, I think, to leave them in that wretched state; but we could not risk another mutiny; and to take them home for the gibbet would have been a cruel sort of kindness. The doctor hailed them and told them of the stores we had left, and where they were to find them. But they continued to call us by name and appeal to us, for God's sake, to be merciful and not leave them to die in such a place.

At last, seeing the ship still bore on her course and was now swiftly drawing out of earshot, one of them—I know not which it was—leapt to his feet with a hoarse cry, whipped his musket to his shoulder, and sent a shot whistling over Silver's head and through the main-sail.

## Treasure Island

After that, we kept under cover of the bulwarks, and when next I looked out they had disappeared from the spit, and the spit itself had almost melted out of sight in the growing distance. That was, at least, the end of that; and before noon, to my inexpressible joy, the highest rock of Treasure Island had sunk into the blue round of sea.

We were so short of men that everyone on board had to bear a hand—only the captain lying on a mattress in the stern and giving his orders, for though greatly recovered he was still in want of quiet. We laid her head for the nearest port in Spanish America, for we could not risk the voyage home without fresh hands; and as it was, what with baffling winds and a couple of fresh gales, we were all worn out before we reached it.

It was just at sundown when we cast anchor in a most beautiful land-locked gulf, and were immediately surrounded by shore boats full of Negroes and Mexican Indians and half-bloods selling fruits and vegetables and offering to dive for bits of money. The sight of so many good-humoured faces (especially the blacks), the taste of the tropical fruits, and above all the lights that began to shine in the town made a most charming contrast to our dark and bloody sojourn on the island; and the doctor and the squire, taking me along with them, went ashore to

pass the early part of the night. Here they met the captain of an English man-of-war, fell in talk with him, went on board his ship, and, in short, had so agreeable a time that day was breaking when we came alongside the HISPANIOLA.

Ben Gunn was on deck alone, and as soon as we came on board he began, with wonderful contortions, to make us a confession. Silver was gone. The maroon had connived at his escape in a shore boat some hours ago, and he now assured us he had only done so to preserve our lives, which would certainly have been forfeit if ‘that man with the one leg had stayed aboard.’ But this was not all. The sea-cook had not gone empty-handed. He had cut through a bulkhead unobserved and had removed one of the sacks of coin, worth perhaps three or four hundred guineas, to help him on his further wanderings.

I think we were all pleased to be so cheaply quit of him.

Well, to make a long story short, we got a few hands on board, made a good cruise home, and the HISPANIOLA reached Bristol just as Mr. Blandly was beginning to think of fitting out her consort. Five men only of those who had sailed returned with her. ‘Drink and the devil had done for the rest,’ with a vengeance,

although, to be sure, we were not quite in so bad a case as that other ship they sang about:

With one man of her crew alive,  
What put to sea with seventy-five.

All of us had an ample share of the treasure and used it wisely or foolishly, according to our natures. Captain Smollett is now retired from the sea. Gray not only saved his money, but being suddenly smit with the desire to rise, also studied his profession, and he is now mate and part owner of a fine full-rigged ship, married besides, and the father of a family. As for Ben Gunn, he got a thousand pounds, which he spent or lost in three weeks, or to be more exact, in nineteen days, for he was back begging on the twentieth. Then he was given a lodge to keep, exactly as he had feared upon the island; and he still lives, a great favourite, though something of a butt, with the country boys, and a notable singer in church on Sundays and saints' days.

Of Silver we have heard no more. That formidable seafaring man with one leg has at last gone clean out of my life; but I dare say he met his old Negress, and perhaps still lives in comfort with her and Captain Flint. It is to be hoped so, I suppose, for his chances of comfort in another world are very small.

The bar silver and the arms still lie, for all that I know, where Flint buried them; and certainly they shall lie there for me. Oxen and wain-ropes would not bring me back again to that accursed island; and the worst dreams that ever I have are when I hear the surf booming about its coasts or start upright in bed with the sharp voice of Captain Flint still ringing in my ears: ‘Pieces of eight! Pieces of eight!’

In only a couple of decades, computer networks have evolved from being a complex technology accessible to only the most tech-savvy of users to being part of most people's everyday lives. Computer networks can be found in almost every business, school, and home. The use of networks is available to anyone with a computer and a network connection, but installation and upkeep of all but the smallest of networks still require a considerable degree of know-how. This chapter starts you on the path toward acquiring the skills to manage a large corporate network or simply configure a home network with a wireless router.

This chapter begins by discussing the computer and its role in a network to give you a foundation for the topics in this book. Next, you examine the components of a network and the fundamentals of communication between computers. Many new terms are introduced and defined, and the varied types of networks and network servers you might encounter are described. Finally, some specialized network types are introduced.

---

## An Overview of Computer Concepts

At the heart of a computer network is the computer. Networks were created to facilitate communication between computing devices, which ultimately facilitates communication between people. So to better understand computer networks, how they work, and how to support them, you must have a solid understanding of computer operations. In fact, most of the devices you encounter when working with a network involve a computer. The most obvious are network servers and workstations that run operating systems, such as Windows, Linux, UNIX, and Mac OS X. Not as obvious are devices such as routers and switches, which move network data from computer to computer and network to network. These complex devices are also computers, although they're specialized computers for performing specific tasks. The next sections discuss the basic functions of a computer and its associated components, along with computer hardware, the boot procedure, and the basic functions of an operating system.

### Basic Functions of a Computer

A computer's functions and features can be broken down into the three basic tasks all computers perform: input, processing, and output. Information is input to a computer from a device such as a keyboard or from a storage device such as a hard drive; the central processing unit (CPU) processes the information, and then output is usually created. The following example illustrates the process:

- *Input*—A user running a word-processing program types the letter A on the keyboard, which results in sending a code representing the letter A to the computer.
- *Processing*—The computer's CPU determines what letter was typed by looking up the keyboard code in a table.
- *Output*—The CPU sends instructions to the graphics cards to display the letter A, which is then sent to the computer monitor.

Some components of today's computers are designed to perform only one of these three functions; others are designed to perform two or all three functions. For example, a standard keyboard and mouse perform input functions, and storage devices, such as hard drives, perform



both input (when files are read from the drive) and output (when files are written to the drive). Network cards can perform all three functions. A network card is an output device when data is sent from the computer to the network and an input device when data comes from the network to the computer. In addition, many network cards have rudimentary processors that perform actions on incoming and outgoing data to help supplement the computer's main CPU.

**Input Components** Before a computer can do any processing, it requires input, commonly from user-controlled devices, such as keyboards and mice, but includes devices such as microphones, Web cameras, and scanners. External interfaces, such as serial, FireWire, and USB ports, can also be used to get input from peripheral devices.

Input is also generated by storage devices, such as hard disks and CDs/DVDs that store computer programs and data files containing computer instructions and data. For example, a spreadsheet program, such as Microsoft Excel, might contain instructions for the CPU to calculate formulas for adding the values of two columns of data and a spreadsheet file called MyBudget.xls containing the numbers and formulas the spreadsheet program should use. Both the program (Microsoft Excel) and the data file (MyBudget.xls) are used as input to the CPU, which then processes the program instructions and data.

Of course, a spreadsheet program is normally started only when a user double-clicks the spreadsheet program icon or the icon representing the spreadsheet data file. These actions are instigated by user input. Sometimes, however, your computer seems to start performing actions without user input. For example, you might have noticed that your hard drive sometimes shows activity without any obvious action from you to initiate it. However, inputs to a computer can include timers that cause programs to run periodically and data arriving from network cards, for example, that cause a program or process to run. So although it sometimes seems as though your computer has a mind of its own, computers don't actually do anything without first getting input to jolt them into action.

**Processing Components** A computer's main processing component is the CPU, which executes instructions from computer programs, such as word-processing programs and Web browsers. It also runs the instructions composing the operating system (OS), which provides a user interface and the environment in which applications run. Aside from the CPU, modern computers usually include ancillary processors associated with input/output (I/O) devices, such as graphics cards. These processors are often referred to as onboard processors. The processor on a graphics card, called a graphics processing unit (GPU), takes a high-level graphics instruction, such as "draw a circle," and performs the calculations needed to draw the circle on the display device. With an onboard GPU, the main CPU doesn't have to handle many of the complex calculations current graphical applications require, thereby improving overall system performance. Other devices, such as network interface cards and disk controller cards, might also include onboard processors.

CPUs now are often composed of two or more processors, called **cores**, in one package. A **multicore CPU** is like a person with two brains. With only one brain, you could add four numbers together, but you would probably do it in three sequential summing operations: Add the first number to the second number, take the first sum and add it to the third number, and add that sum to the fourth number to arrive at the final sum. If you had two brains, you'd still need three summing operations, but two could be done simultaneously:

The first brain adds the first two numbers while the second brain is adding the third and fourth numbers; then the second brain gives its results to the first brain, and the first brain sums the results of the first two summing operations. So multicore CPUs enable computers to carry out multiple instructions simultaneously, which results in better overall performance when running demanding applications.

**Output Components** Output components include monitors and printers, but they also include storage devices, network cards, and speakers, to name a few. The external interfaces mentioned previously as input components can be used as output components, too. For example, a disk drive connected to a USB port allows reading files from the disk (input) and writing files to the disk (output).

## Storage Components

Storage components are a major part of a computer's configuration. Generally speaking, the more storage a computer has, the better the performance is. As you saw in the previous section, most storage components are both input and output devices, allowing data to be saved (output) and then accessed again later (input). When most people think of storage, they think of disk drives, CD/DVD drives, and USB flash drives. However, there are two main categories of storage: short-term storage and long-term storage.

**RAM: Short-Term Storage** Short-term storage is the random access memory (RAM) on a computer. RAM is short-term storage because when power to the computer is turned off, RAM's contents are gone, just as though you erased a whiteboard. When power is restored, RAM has no data stored until the CPU begins to write data to it.

The amount of RAM, or memory, in a computer is crucial to the computer's capability to operate efficiently. RAM is also referred to as "working storage." Everything the CPU is currently processing must be available in RAM, including program instructions and the data the current application requires. So to run a spreadsheet program, there must be enough RAM to load both the spreadsheet program and the data in the spreadsheet. If there's not enough available memory, the spreadsheet program won't run, or the computer will use the disk drive to supplement RAM temporarily.

Neither option is desirable. The reason temporary use of the disk drive isn't optimal is because RAM is thousands of times faster than the fastest disk drives. The time required to access data in RAM is measured in nanoseconds (billions of a second), but access to data on a disk drive is measured in milliseconds (thousandths of a second). So if the disk drive must be used to supplement RAM while running an application, that application, and indeed the entire computer, slows down precipitously.

On current computers, the amount of RAM installed is usually 1 GB or more. More is generally better, but the amount of RAM that a system can use effectively depends on the OS installed. The 32-bit version of an OS can usually access a maximum of 4 GB of RAM, whereas the 64-bit version can access many thousands of gigabytes. The amount of RAM you actually need depends on how you use your computer. If you usually have only one or two typical business applications open at once, 1 GB or even less is probably enough.

However, if you run complex graphics applications or games or have several applications open simultaneously, you'll likely benefit from having more RAM.



**Long-Term Storage** Long-term storage maintains its data even when there's no power. Examples include hard disks, CDs/DVDs, and USB flash drives as well as other types of removable media. Long-term storage is used to store document and multimedia files as well as the files that make up applications and the OS. The amount of storage a computer needs depends on the type and quantity of files to be stored. In general, office documents, such as word-processing files, spreadsheets, and presentations, require comparatively little space. Multimedia files—pictures, music files, and videos—require much more space. Long-term storage is plentiful and extremely inexpensive. Hard drive specifications are in units of tens or hundreds of gigabytes, with terabyte (1000 GB) drives quite commonplace now. More details about hard disks are discussed later in “Personal Computer Hardware.”

**Data Is Stored in Bits** Whether storage is long term or short term, data on a computer is stored and processed as binary digits (“bits,” for short). A bit holds a 1 or 0 value, which make representing bits with electrical pulses easy. For example, a pulse of 5 volts of electricity can represent a 1 bit, and a pulse of 0 volts (or absence of a pulse) can represent a 0 bit. Bits can also be stored as pulses of light, as with fiber-optic cable: A 1 bit is represented by the presence of light and a 0 bit as the absence of light.

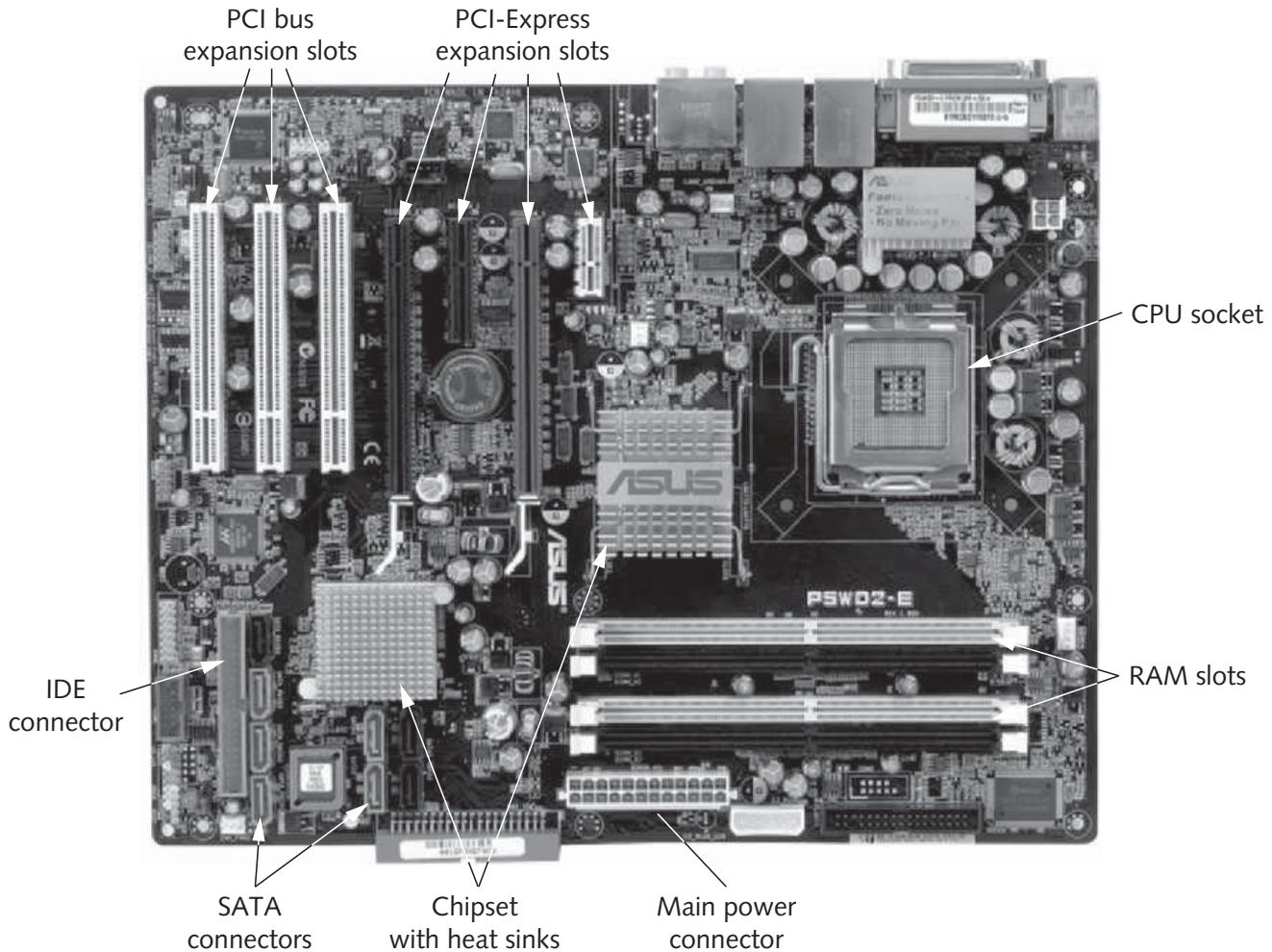
Data in a computer, such as the letters in a word-processing document or the music you hear when you play an MP3 music file, is represented by collections of 8 bits, called a byte. You can look at each byte as a printable character in a document. A single byte from an MP3 file plays about 1/17 thousandth of a second of music. To put it another way, one second of MP3 music takes more than 17,000 bytes.

## Personal Computer Hardware

Most people are familiar with personal computer (PC) hardware. Other types of computers, such as minicomputers and mainframes, are usually locked away in a heavily air-conditioned room and privy only to the eyes of IT staff. Besides, the basic hardware used to build a PC or a mainframe differs only in the details. This section describes four major PC components housed in a computer case:

- Motherboard
- Hard drive
- RAM
- BIOS/CMOS

**The Motherboard and Its Components** The motherboard is the nerve center of a computer, much like the spinal cord is the nerve center of the human body. It's a network of wires and controlling circuits that connects all computer components, including the CPU, RAM, disk drives, and I/O devices, such as network interface cards. Some key components of a motherboard are labeled in Figure 1-1 and explained in Table 1-1.



**Figure 1-1** A PC motherboard

Courtesy of Course Technology/Cengage Learning

**Table 1-1** Key components of a motherboard

Component	Description
CPU socket	The CPU is installed in this socket.
PCI bus expansion slots	Used to add functionality to a PC by adding expansion cards that have a Peripheral Component Interconnect (PCI) connector.
PCI-Express expansion slots	PCI-Express supersedes PCI and supports faster data transfer speeds. The larger slots are suitable for high-performance expansion cards, such as graphics cards and disk controllers. The smaller slots are best suited to sound cards and network interface cards.
RAM slots	Slots for installing RAM on the motherboard.
Chipset with heat sinks	The chipset consists of two chips referred to as the Northbridge and the Southbridge. These chips control data transfers between memory, expansion slots, I/O devices, and the CPU. The heat sink sits on top of the chipset to prevent it from overheating.
SATA connectors	Used for connecting hard drives and CD/DVD drives that use the Serial AT Attachment (SATA) specification.

(continues)

**Table 1-1 Key components of a motherboard (continued)**

Component	Description
IDE connector	Used for connecting Integrated Drive Electronics (IDE) hard drives and CD/DVD-ROM drives. Most systems now use SATA for hard drives and IDE for CD/DVD drives.
Main power connector	This connector is where the motherboard receives power from the system power supply.

All data that goes into or comes out of a computer goes through the motherboard because all storage and I/O devices are connected to the motherboard, as is the CPU, which processes data going in and coming out of a computer.

**Computer Bus Fundamentals** Table 1-1 mentions PCI bus expansion slots as a component of a motherboard. So what is a bus? A **bus** is a collection of wires carrying data from one place to another on the computer. There are many bus designs and formats, each designed for a particular purpose. Although bus types come and go, it's safe to say that replacements for an older bus design will almost certainly be faster than their predecessor.

In a computer, there are buses between the CPU and RAM, between the CPU and disk drives, and between the CPU and expansion slots, among others. For the purposes of this book, you're most interested in the bus connecting expansion slots to the motherboard because you usually connect a network interface card (NIC) into one of these slots. NIC installation and expansion slot bus types are discussed in Chapters 2 and 7. What you need to know now is that not all motherboards come with all types of expansion slots, and the faster and busier your computer is, the faster its bus type needs to be.

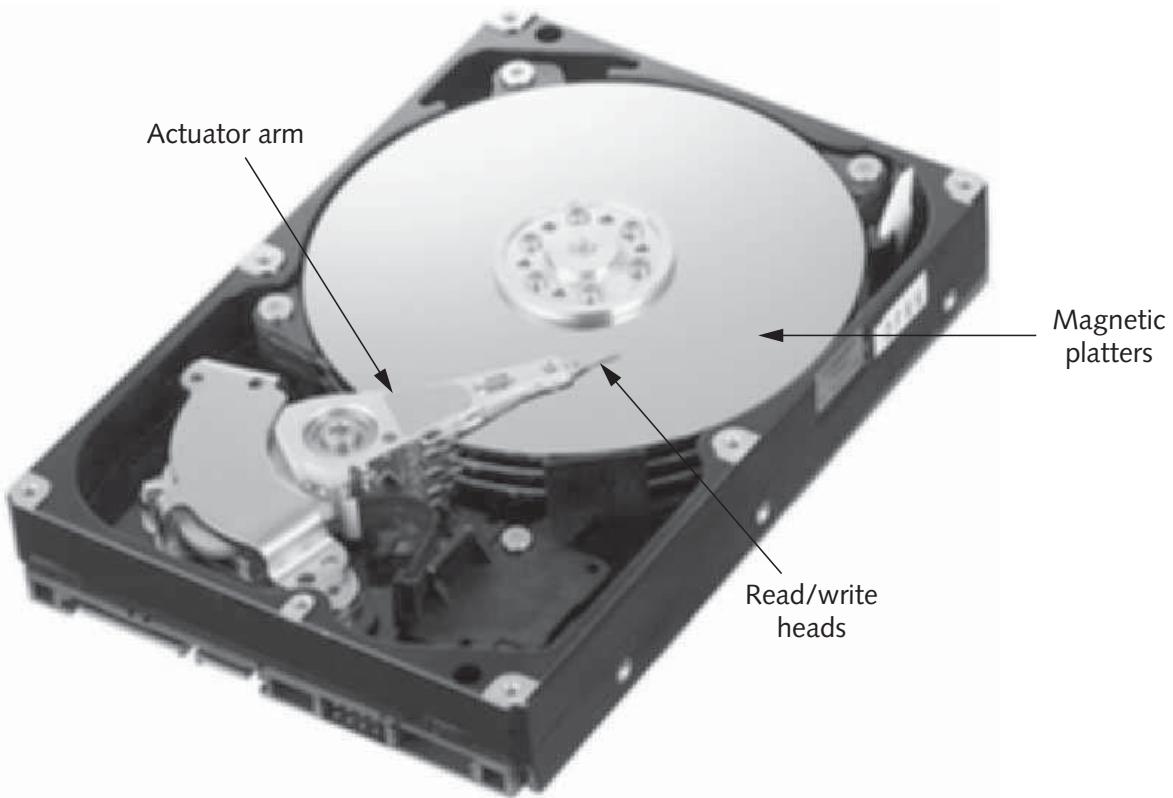
**Hard Drive Fundamentals** The hard drive is the primary long-term storage component on your computer. Hard drives consist of magnetic disks, called platters, that store data in the form of magnetic pulses. These magnetic pulses are maintained even when power is turned off. Each pulse represents a single bit of data.

The platters spin at extremely fast speeds, with some of the fastest disks having rotational speeds of 15,000 revolutions per minute (rpm). A read/write head is attached to an actuator arm that moves across the spinning platters in response to commands from the computer to read or write a file (see Figure 1-2). Generally, the faster the rotational speed, the better the hard drive performance is. When a file is requested to be written or read, its location is determined, and then the read/write heads are moved over the corresponding spot on the platter. After the platter spins to the file's starting location, the read/write heads are activated to read or write the data. The average amount of time platters take to spin into position is called the rotational delay or latency. The amount of time required to move read/write heads to the correct place is referred to as the seek time, and the time it takes to read or write data is called the transfer time. The average amount of time between the request to read or write data and the time the action is completed is referred to as the access time.



The terms used to measure hard drive performance aren't universal among manufacturers, but the terms used in the preceding paragraph represent most specifications.

**NOTE**



**Figure 1-2** Inside a hard drive

Courtesy of © 2010 Western Digital Technologies, Inc.

Hard disks store the documents you use with your computer as well as the applications that open these documents. In addition, the hard disk stores the OS your computer loads when it boots. As mentioned, the hard disk acts as an input device when files are read. When the computer boots, the OS files are read from the disk, and instructions in these files are processed by the CPU. However, the files don't go directly from the hard disk to the CPU; first, they're transferred to short-term storage (RAM).

**RAM Fundamentals** RAM, the main short-term storage component on your computer, consists of capacitors to store data and transistors to control access to data. Capacitors require power to maintain the bits they store. Because RAM requires continuous power to store data, it's referred to as "volatile memory."

RAM has no moving parts, so as mentioned, accessing data in RAM is much faster than accessing data on a hard drive—there's no seek time or rotational delay. Because RAM is so much faster than a hard drive, any information the CPU processes should be in RAM. If data the CPU requires is located on the hard drive, it's loaded into RAM first, which takes considerable time. Therefore, the more RAM your system has, the more likely it is that all the data running programs need can be stored in RAM, making the system perform much faster.

**BIOS/CMOS Fundamentals** A key component of every computer is its basic input/output system (BIOS), which is a set of instructions located in a chip on the motherboard. A main function of the BIOS is to tell the CPU to perform certain tasks when power is first applied to the computer, including initializing motherboard hardware, performing a power-on self test (POST), and beginning the boot procedure.



Because of the complexity of motherboards, configuring some of their hardware components and tuning performance parameters are often necessary. When a computer begins to boot, the BIOS program offers the user an opportunity to run the Setup utility to perform this configuration. The configuration data the user enters is stored in complementary metal oxide semiconductor (CMOS) memory. It holds information such as on which devices the CPU should look for an OS to boot, the status of hardware devices, and even a system password, if needed. CMOS is a type of low-power memory that requires only a small battery to maintain its data. It's also referred to as nonvolatile memory because it doesn't require power from the computer's main power supply.

## Computer Boot Procedure

The following six steps are necessary to take a computer from a powered-off state to running a current OS, such as Windows or Linux:

1. Power is applied to the motherboard.
2. The CPU starts.
3. The CPU carries out the BIOS startup routines, including the POST.
4. Boot devices, as specified in the BIOS configuration, are searched for an OS.
5. The OS is loaded into RAM.
6. OS services are started.

These steps apply to almost every type of computer, including very small computing devices, such as cell phones and iPods. Probably the biggest difference between computers is what occurs in the last step. OS services are programs that are part of the OS rather than applications a user starts. The particular services an OS starts can vary greatly, depending on which OS is loaded and how it's configured. The number and type of services started on a system are what, at least in part, account for the time it takes a system to boot completely. Examples of common OS services include the user interface, the file system, and, of course, networking services.



The projects in this book involving a Windows client OS use Windows 7 Enterprise Edition. Other editions of Windows 7 can be used, except Windows 7 Home Edition. Windows Vista can also be used, with some small changes to step-by-step instructions. Windows XP can be used in most cases but might require additional changes.



### Hands-On Project 1-1: Examining a Computer's Boot Procedure

**Time Required:** 10 minutes

**Objective:** Examine the computer boot procedure and BIOS setup utility.

**Required Tools/Equipment:** Your classroom computer and access to the BIOS Setup utility

**Description:** In this project, you examine the computer boot procedure from beginning to end, using a Windows computer. You also examine the BIOS Setup utility and view the configuration that specifies which devices the BIOS should search for an OS. Because the BIOS is different for different computers, your instructor might have to assist with the specific keystrokes you enter to run the BIOS Setup utility and view the boot order menu. This project uses a

virtual machine and the BIOS Setup utility in VMware Workstation 6.x. If you aren't using virtual machines for the projects in this book, the BIOS on most computers is similar.



Your computer must be turned off before you begin this project. Read the first step carefully before turning on the computer, as you need to act quickly to enter the BIOS Setup utility.

1. Turn on your computer. Watch the screen carefully for a message telling you what key to press to activate the BIOS Setup utility. On many systems, this key is F1, F2, or Delete. If you don't press the key in time, the OS boots normally. If this happens, shut down the computer and try again.
2. When you have entered the BIOS Setup utility, your screen should look similar to Figure 1-3. Before continuing, write down the steps of the boot procedure that have taken place to this point:

---

---

---

**PhoenixBIOS Setup Utility**

Main   Advanced   Security   Boot   Exit

<b>System Time:</b>	[11:08:57]	<b>Item Specific Help</b>
<b>System Date:</b>	[04/17/2010]	
<b>Legacy Diskette A:</b>	[1.44/1.25 MB 3½"]	<Tab>, <Shift-Tab>, or <Enter> selects field.
<b>Legacy Diskette B:</b>	[Disabled]	
▶ Primary Master	[None]	
▶ Primary Slave	[None]	
▶ Secondary Master	[VMware Virtual IDE]	
▶ Secondary Slave	[None]	
▶ Keyboard Features		
<b>System Memory:</b>	640 KB	
<b>Extended Memory:</b>	1047552 KB	
<b>Boot-time Diagnostic Screen:</b>	[Disabled]	

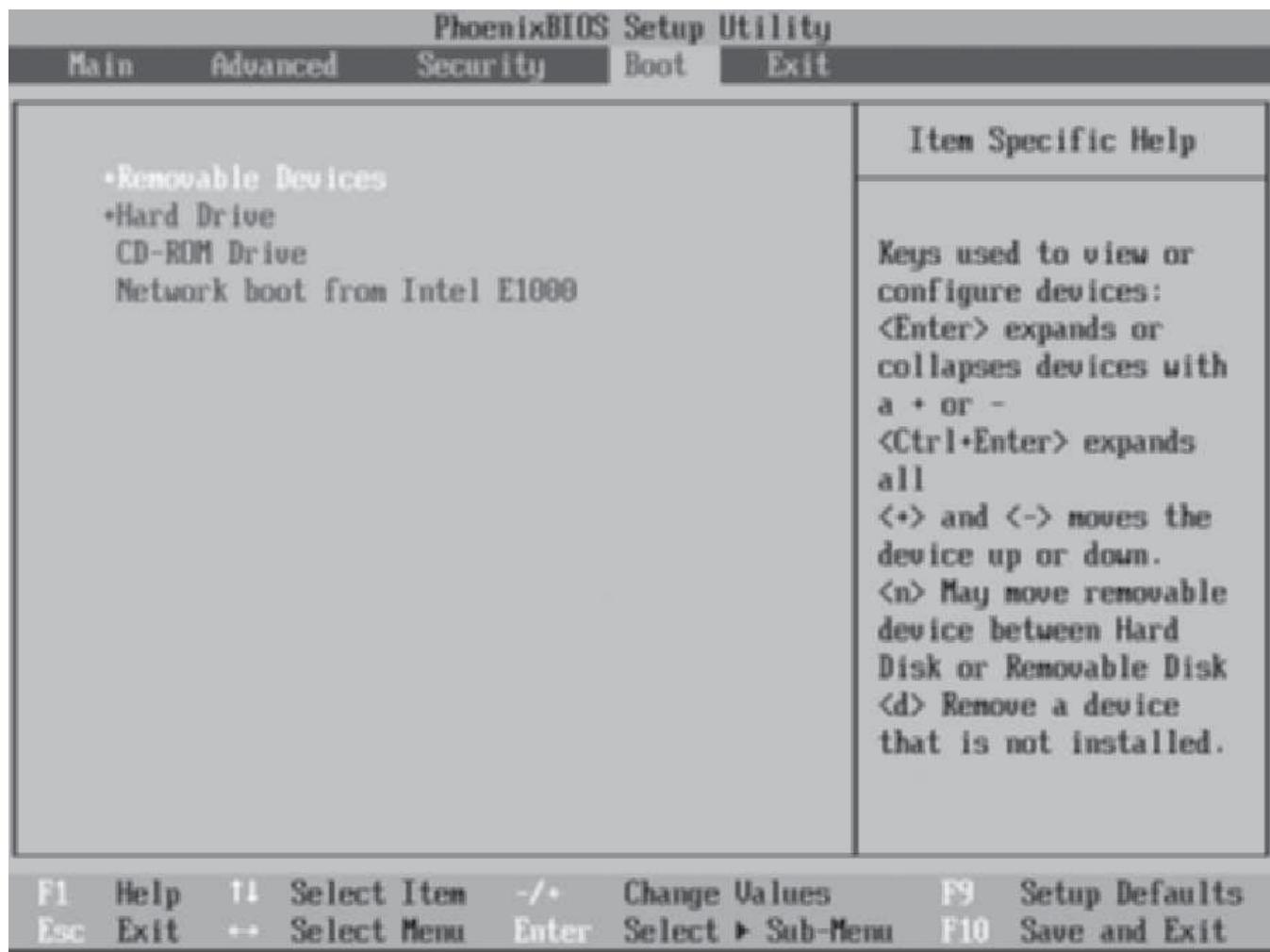
**F1 Help   F11 Select Item   -/+ Change Values   F9 Setup Defaults**  
**Esc Exit   -- Select Menu   Enter Select ▶ Sub-Menu   F10 Save and Exit**

**Figure 1-3** The BIOS Setup utility

Courtesy of Course Technology/Cengage Learning



3. Navigate the BIOS Setup utility until you find the boot order menu (see Figure 1-4). From this menu, you can change the order in which the BIOS looks for boot devices, or you can exclude a device from the boot order. The BIOS boots from the first device in which it finds an OS. You might need to change the boot order if, for example, you have an OS installed on the hard drive but want to boot from an installation CD/DVD to install a new OS. In this case, you move the CD/DVD device to the first entry in the boot order.



**Figure 1-4** The BIOS boot order menu

Courtesy of Course Technology/Cengage Learning

4. For now, you can leave the boot order as it is. To quit the Setup utility, press the correct key (usually specified at the bottom of the screen). In Figure 1-4, you press Esc to exit without saving changes or F10 to save the changes before exiting. In either case, when you exit, the computer restarts. Press the key for exiting without saving changes.
5. Write the final steps of the boot procedure that occurred as Windows started:

---

---

---

6. Shut down the computer for the next project.

## How the Operating System and Hardware Work Together

A computer's OS provides a number of critical services, including a user interface, memory management, a file system, multitasking, and the interface to hardware devices. Without an OS, each application would have to provide these services, and if a user wanted to run multiple applications at once (multitasking), the applications would have to run cooperatively. In short, without an OS, computing would still be in the proverbial Stone Age. The following sections describe these services briefly, and Chapter 8 discusses OS components in more detail.

**User Interface** The user interface enables people to interact with computers. With graphical user interfaces (GUIs), users can point and click their way around the computer to run applications, access network services, manage hard drives and files, and configure the working environment to their liking. In short, users provide input, and the OS, along with the CPU, processes that input, whether it's mouse clicks or keystrokes, and generates output. Without a user interface, computers could process only information that has been programmed into memory or storage. If something went wrong, there would be no way to indicate the problem to a person, making a computer without a user interface of little value except when it has a narrowly defined task, such as running a piece of machinery.

**Memory Management** Computers are now equipped with memory measured in hundreds of megabytes or gigabytes, whereas in the early 1990s, the typical amount of memory was about 1 megabyte. Each application requires a certain amount of memory in which to run. When the OS loads an application, memory must be allocated for the application to run in, and when the application exits, the memory it was using must be marked as available. The OS handles these memory management tasks. Without a central memory manager, an application could use any memory in the system, and it might be memory already being used by a running application or the OS itself. If this happens, the system can crash or perform erratically. Today's OSs usually detect an application's attempt to access another process's memory and force the offending application to terminate.

**File System** The file system is used to organize space on storage devices, such as disk drives and flash drives, for the purpose of storing and locating files. Contemporary file systems typically have the following objectives:

- Provide a convenient interface for users and applications to open and save files.
- Provide an efficient method to organize space on a drive.
- Provide a hierarchical filing method to store files.
- Provide an indexing system for fast retrieval of files.
- Provide secure access to files by authorized users.

When a user double-clicks a file to open it, the user interface calls the file system with a request to open the file. The file type determines exactly how the file is opened. If the file is an application, the application is loaded into memory and run by the CPU. If the file is a document, the application associated with the document type is loaded into memory and opened by the application. For example, if you double-click the Budget.xls file, the Excel



application is loaded into memory and then opens the Budget.xls document file. If a user creates a new file or changes an existing file and wants to save it, the application calls the file system to store the new or changed file on the disk. Most users of an OS interact with the file system by using Windows Explorer or a similar file manager program on another OS, but as a future computer or network professional, you need to have a deeper understanding of how a file system works so that you can make informed choices when you need to install a file system or troubleshoot file system-related problems. You can find more discussion on this topic in Chapter 8.

**Multitasking** Quite simply, **multitasking** is an operating system's capability to run more than one application or process at a time. Multitasking is what allows you to listen to a music file while browsing the Web, for example. Computer hardware can't do that by itself. The OS is designed to look for applications that have some kind of work to do (such as load a new Web page or continue playing the current music file) and then schedule CPU time so that the work gets done. For example, if you're browsing the Web and reading the current page loaded in your Web browser, the computer isn't really doing any work.

However, if you click a link on the Web page, you're telling the Web browser you want to load a new page. The OS responds by telling the CPU to start executing the part of the Web browser application responsible for loading a new Web page. You might wonder how can you play a music file at the same time the CPU is loading a new Web page. There are two possible answers: The computer contains more than one CPU or a multicore CPU and can literally do two things at once (in this case, load a Web page and play a music file), or the OS instructs the CPU to switch between the two tasks rapidly, giving the illusion that they're happening simultaneously. Because CPUs can execute hundreds of millions of instructions per second, this illusion isn't difficult to carry off.

**Interface to Hardware Devices** When an application needs to communicate with computer hardware, as when writing information to the display device or sending data to the network, it calls on the OS, which then calls on a device driver. A **device driver** is software that provides the interface between the OS and computer hardware. The reason the application can't simply read or write data directly to hardware is that other applications might also need to communicate with the same device at the same time. If this were allowed to happen, it would be akin to two or more people on different extensions of the same land line trying to dial a different number. Nobody's phone call would go through, or one person might call an unintended destination. The OS queues up each request and sends it to the device driver when it's not busy. This procedure ensures that every application's request is taken care of in a nice orderly fashion.

Every device performing an input or output function requires a device driver. When an input device has data ready for processing, or when an output device is ready to accept data, the device must signal the OS. Most devices use a signal called an interrupt to let the OS know it has data ready to be read or is ready for more data to be written. Computers spend a considerable amount of time servicing interrupts on a busy computer. For example, when the mouse is moved or a key on the keyboard is pressed, an interrupt is generated so that the OS knows the mouse pointer must be redrawn onscreen or a character must be written to

the screen. On a networked computer, an interrupt is generated by the NIC when a packet arrives.

Every time an interrupt occurs, the OS must stop what it's doing to service the interrupt. It takes many instructions for an OS to stop what it's doing, service the interrupt, and then resume what it was doing before the interrupt occurred. Because computers can execute millions of instructions per second, users don't usually notice the interruption. If enough interrupts occur simultaneously and for a prolonged period, however, a system can become noticeably sluggish or even seem to freeze. Malfunctioning hardware and network errors that generate excessive packets are two of the many possible causes of this problem. Remember this idea about excessive interrupts caused by the NIC; it's an important point later when you learn about network protocols in Chapter 5.

Networking is, of course, the focus of this book, but your grasp of the fundamentals of computer components and operations will facilitate your understanding of networking components and operations.

---

## The Fundamentals of Network Communication

A computer **network** consists of two or more computers connected by some kind of transmission medium, such as a cable or air waves. After they're connected, correctly configured computers can communicate with one another. The primary motivation for networking was the need for people to share resources, such as printers and hard drives, and information such as word-processing files and to communicate by using applications such as e-mail. These motivations remain, especially for businesses, but another motivating factor for networking for both businesses and homes is to get "online"—to access the Internet. The Internet, with its wealth of information, disinformation, fun, and games, has had a tremendous impact on how and why networks are used today. Indeed, many of the networking technologies used now that you learn about in this book were developed as a result of the Internet explosion.

You might know how to use a network already; in particular, you probably know how to use programs that access the Internet, such as Web browsers and e-mail programs. To understand *how* networks work, however, you need to learn about the underlying technologies and processes that are put into action when you open a Web browser or an e-mail program. A good place to start is with the components that make a stand-alone computer a networked computer.

### Network Components

Imagine a computer with no networking components—no networking hardware, no networking software. It's hard to imagine in this age of seemingly everything and everybody being connected. However, not too long ago, when you bought a computer, its main purpose was to run applications such as word-processing and spreadsheet programs, not Web browsers and e-mail. In fact, the computer had neither the necessary hardware nor software to run these programs. These computers were called **stand-alone computers**. If you wanted to network such a computer, you had to add the necessary components:

# **Hardware Reference Guide**

## **HP Compaq 8000 Elite Small Form Factor Business PC**

© Copyright 2009 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Microsoft, Windows, and Windows Vista are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

This document contains proprietary information that is protected by copyright. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard Company.

**Hardware Reference Guide**

HP Compaq 8000 Elite Small Form Factor Business PC

First Edition (November 2009)

Document Part Number: 588912-001

## About This Book

This guide provides basic information for upgrading this computer model.

 **WARNING!** Text set off in this manner indicates that failure to follow directions could result in bodily harm or loss of life.

 **CAUTION:** Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

 **NOTE:** Text set off in this manner provides important supplemental information.

---



---

# Table of contents

## 1 Product Features

Standard Configuration Features .....	1
Front Panel Components .....	2
Media Card Reader Components .....	3
Rear Panel Components .....	4
Keyboard .....	5
Using the Windows Logo Key .....	5
Serial Number Location .....	7

## 2 Hardware Upgrades

Serviceability Features .....	8
Warnings and Cautions .....	8
Unlocking the Smart Cover Lock .....	9
Smart Cover FailSafe Key .....	9
Using the Smart Cover FailSafe Key to Remove the Smart Cover Lock .....	9
Removing the Computer Access Panel .....	11
Replacing the Computer Access Panel .....	12
Removing the Front Bezel .....	13
Replacing Bezel Blanks .....	14
Replacing the Front Bezel .....	15
Using the Small Form Factor Computer in a Tower Orientation .....	16
Installing Additional Memory .....	17
DIMMs .....	17
DDR3-SDRAM DIMMs .....	17
Populating DIMM Sockets .....	18
Installing DIMMs .....	19
Removing or Installing an Expansion Card .....	22
Drive Positions .....	28
Installing and Removing Drives .....	29
System Board Drive Connections .....	30
Removing an External 5.25-inch Drive .....	31
Installing an Optical Drive into the 5.25-inch Drive Bay .....	33
Removing an External 3.5-inch Drive .....	36
Installing a Drive into the 3.5-inch External Drive Bay .....	38

Removing and Replacing the Primary 3.5-inch Internal SATA Hard Drive .....	39
Removing and Replacing a Removable 3.5-inch SATA Hard Drive .....	42
<b>Appendix A Specifications</b>	
<b>Appendix B Battery Replacement</b>	
<b>Appendix C External Security Devices</b>	
Installing a Security Lock .....	52
HP/Kensington MicroSaver Security Cable Lock .....	52
Padlock .....	53
HP Business PC Security Lock .....	53
Front Bezel Security .....	55
<b>Appendix D Electrostatic Discharge</b>	
Preventing Electrostatic Damage .....	57
Grounding Methods .....	57
<b>Appendix E Computer Operating Guidelines, Routine Care and Shipping Preparation</b>	
Computer Operating Guidelines and Routine Care .....	58
Optical Drive Precautions .....	59
Operation .....	59
Cleaning .....	59
Safety .....	59
Shipping Preparation .....	59
<b>Index .....</b>	<b>60</b>

---

# 1 Product Features

## Standard Configuration Features

The HP Compaq Small Form Factor features may vary depending on the model. For a complete listing of the hardware and software installed in the computer, run the diagnostic utility (included on some computer models only).

 **NOTE:** The Small Form Factor computer can also be used in a tower orientation. For more information, see [Using the Small Form Factor Computer in a Tower Orientation on page 16](#) in this guide.

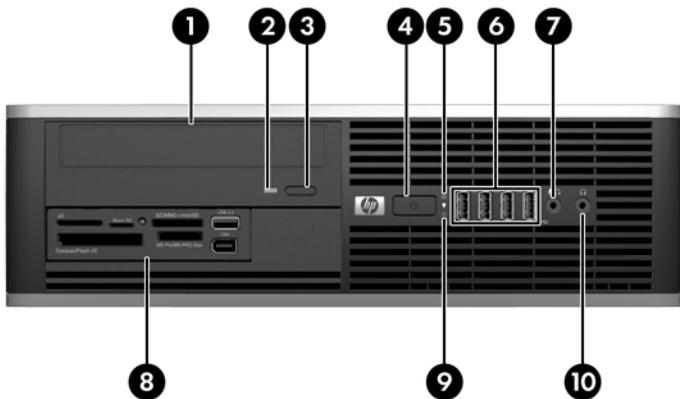
**Figure 1-1** Small Form Factor Configuration



# Front Panel Components

Drive configuration may vary by model. Some models have a bezel blank covering one or more drive bays.

**Figure 1-2** Front Panel Components



**Table 1-1** Front Panel Components

1	5.25-inch Optical Drive	6	USB (Universal Serial Bus) Ports
2	Optical Drive Activity Light	7	Microphone/Headphone Connector
3	Optical Drive Eject Button	8	3.5-inch Media Card Reader (optional)
4	Dual-State Power Button	9	Hard Drive Activity Light
5	Power On Light	10	Headphone Connector

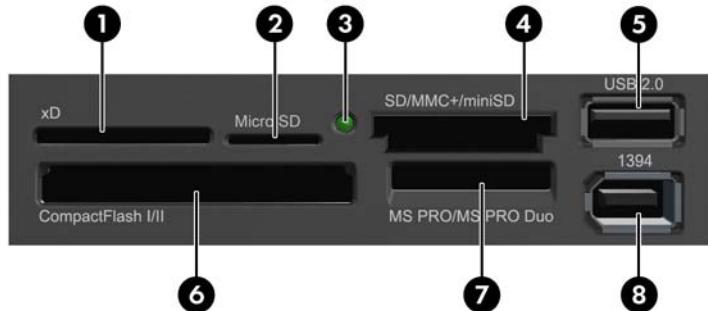
**NOTE:** When a device is plugged into the Microphone/Headphone Connector, a dialog box will pop up asking if you want to use the connector for a microphone line Line-In device or a headphone. You can reconfigure the connector at any time by double-clicking the Realtek HD Audio Manager icon in the Windows taskbar.

**NOTE:** The Power On Light is normally green when the power is on. If it is flashing red, there is a problem with the computer and it is displaying a diagnostic code.

# Media Card Reader Components

The media card reader is an optional device available on some models only. Refer to the following illustration and table to identify the media card reader components.

**Figure 1-3** Media Card Reader Components



**Table 1-2** Media Card Reader Components

No.	Slot	Media			
1	<b>xD</b>	• xD-Picture Card (xD)			
2	<b>MicroSD</b>	• MicroSD (T-Flash)	• MicroSDHC		
3	<b>Media Card Reader Activity Light</b>				
4	<b>SD/MMC+/miniSD</b>	• Secure Digital (SD) • Secure Digital High Capacity (SDHC) • MiniSD	• MiniSDHC • MultiMediaCard (MMC) • Reduced Size MultiMediaCard (RS MMC)	• MultiMediaCard 4.0 (MMC Plus) • Reduced Size MultiMediaCard 4.0 (MMC Mobile) • MMC Micro (adapter required)	
5	<b>USB</b>	• USB (Universal Serial Bus) Port			
6	<b>CompactFlash I/II</b>	• CompactFlash Card Type 1	• CompactFlash Card Type 2	• MicroDrive	
7	<b>MS PRO/MS PRO DUO</b>	• Memory Stick (MS) • MagicGate Memory Stick (MG) • MagicGate Memory Duo	• Memory Stick Select • Memory Stick Duo (MS Duo) • Memory Stick PRO (MS PRO)	• Memory Stick PRO Duo (MS PRO Duo) • Memory Stick PRO-HG Duo • Memory Stick Micro (M2) (adapter required)	
8	<b>1394</b>	• 1394 Port (available on select models only)			

# Rear Panel Components

Figure 1-4 Rear Panel Components

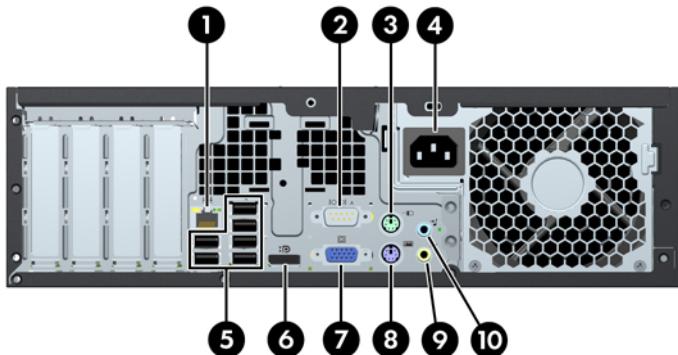


Table 1-3 Rear Panel Components

1	RJ-45 Network Connector	6	DisplayPort Monitor Connector
2	IOIOIA Serial Connector	7	VGA Monitor Connector
3	PS/2 Mouse Connector (green)	8	PS/2 Keyboard Connector (purple)
4	Power Cord Connector	9	Line-Out Connector for powered audio devices (green)
5	Universal Serial Bus (USB)	10	Line-In Audio Connector (blue)

**NOTE:** Arrangement and number of connectors may vary by model.

An optional second serial port and an optional parallel port are available from HP.

When a device is plugged into the blue Line-In Audio Connector, a dialog box will pop up asking if you want to use the connector for a line-in device or a microphone. You can reconfigure the connector at any time by double-clicking the Realtek HD Audio Manager icon in the Windows taskbar.

The monitor connectors on the system board are inactive when a graphics card is installed in the computer.

If a graphics card is installed into the PCI or PCI Express x1 slot, the connectors on the graphics card and the system board may be used at the same time. Some settings may need to be changed in Computer Setup to use both connectors.

# Keyboard

**Figure 1-5** Keyboard Components



**Table 1-4** Keyboard Components

1	Function Keys	Perform special functions depending on the software application being used.
2	Editing Keys	Includes the following: Insert, Home, Page Up, Delete, End, and Page Down.
3	Status Lights	Indicate the status of the computer and keyboard settings (Num Lock, Caps Lock, and Scroll Lock).
4	Numeric Keys	Work like a calculator keypad.
5	Arrow Keys	Used to navigate through a document or Web site. These keys allow you to move left, right, up, and down, using the keyboard instead of the mouse.
6	Ctrl Keys	Used in combination with another key; their effect depends on the application software you are using.
7	Application Key <sup>1</sup>	Used (like the right mouse button) to open pop-up menus in a Microsoft Office application. May perform other functions in other software applications.
8	Windows Logo Keys <sup>1</sup>	Used to open the Start menu in Microsoft Windows. Used in combination with other keys to perform other functions.
9	Alt Keys	Used in combination with another key; their effect depends on the application software you are using.

<sup>1</sup> Keys available in select geographic regions.

## Using the Windows Logo Key

Use the Windows Logo key in combination with other keys to perform certain functions available in the Windows operating system. Refer to [Keyboard on page 5](#) to identify the Windows Logo key.

**Table 1-5** Windows Logo Key Functions

The following Windows Logo Key functions are available in Microsoft Windows XP, Microsoft Windows Vista, and Microsoft Windows 7.

**Table 1-5 Windows Logo Key Functions (continued)**

Windows Logo Key	Displays or hides the Start menu
Windows Logo Key + d	Displays the Desktop
Windows Logo Key + m	Minimizes all open applications
Shift + Windows Logo Key + m	Undoes Minimize All
Windows Logo Key + e	Launches My Computer
Windows Logo Key + f	Launches Find Document
Windows Logo Key + Ctrl + f	Launches Find Computer
Windows Logo Key + F1	Launches Windows Help
Windows Logo Key + l	Locks the computer if you are connected to a network domain, or allows you to switch users if you are not connected to a network domain
Windows Logo Key + r	Launches the Run dialog box
Windows Logo Key + u	Launches the Utility Manager
Windows Logo Key + Tab	Windows XP - Cycles through the Taskbar buttons  Windows Vista and Windows 7 - Cycles through programs on the Taskbar using the Windows Flip 3-D

In addition to the Windows Logo Key functions described above, the following functions are also available in Microsoft Windows Vista and Windows 7.

Ctrl + Windows Logo Key + Tab	Use the arrow keys to cycle through programs on the Taskbar by using Windows Flip 3-D
Windows Logo Key + Spacebar	Brings all gadgets to the front and select Windows Sidebar
Windows Logo Key + g	Cycles through Sidebar gadgets
Windows Logo Key + t	Cycles through programs on the taskbar
Windows Logo Key + u	Launches Ease of Access Center
Windows Logo Key + any number key	Launches the Quick Launch shortcut that is in the position that corresponds to the number (for example, Windows Logo Key + 1 launches the first shortcut in the Quick Launch menu)

In addition to the Windows Logo Key functions described above, the following functions are also available in Microsoft Windows 7.

Windows Logo Key + Ctrl + b	Switches to the program that displayed a message in the notification area
Windows Logo Key + p	Choose a presentation display mode
Windows Logo Key + up arrow	Maximizes the window
Windows Logo Key + left arrow	Snaps the window to the left side of the screen
Windows Logo Key + right arrow	Snaps the window to the right side of the screen
Windows Logo Key + down arrow	Minimizes the window
Windows Logo Key + Shift + up arrow	Stretches the window to the top and bottom of the screen
Windows Logo Key + Shift + left arrow or right arrow	Moves a window from one monitor to another

**Table 1-5 Windows Logo Key Functions (continued)**

Windows Logo Key + + (on numpad)	Zooms in
Windows Logo Key + - (on numpad)	Zooms out

## Serial Number Location

Each computer has a unique serial number and product ID number in the location shown below. Keep these numbers available for use when contacting customer service for assistance.

**Figure 1-6** Serial Number and Product ID Location



---

## 2 Hardware Upgrades

### Serviceability Features

The computer includes features that make it easy to upgrade and service. No tools are needed for most of the installation procedures described in this chapter.

### Warnings and Cautions

Before performing upgrades be sure to carefully read all of the applicable instructions, cautions, and warnings in this guide.

**⚠ WARNING!** To reduce the risk of personal injury from electrical shock, hot surfaces, or fire:

Disconnect the power cord from the wall outlet and allow the internal system components to cool before touching.

Do not plug telecommunications or telephone connectors into the network interface controller (NIC) receptacles.

Do not disable the power cord grounding plug. The grounding plug is an important safety feature.

Plug the power cord in a grounded (earthed) outlet that is easily accessible at all times.

To reduce the risk of serious injury, read the *Safety & Comfort Guide*. It describes proper workstation, setup, posture, and health and work habits for computer users, and provides important electrical and mechanical safety information. This guide is located on the Web at <http://www.hp.com/ergo>.

**WARNING!** Energized and moving parts inside.

Disconnect power to the equipment before removing the enclosure.

Replace and secure the enclosure before re-energizing the equipment.

**⚠ CAUTION:** Static electricity can damage the electrical components of the computer or optional equipment. Before beginning these procedures, ensure that you are discharged of static electricity by briefly touching a grounded metal object. See Appendix D, [Electrostatic Discharge on page 57](#) for more information.

When the computer is plugged into an AC power source, voltage is always applied to the system board. You must disconnect the power cord from the power source before opening the computer to prevent damage to internal components.

---

# Unlocking the Smart Cover Lock



**NOTE:** The Smart Cover Lock is an optional feature included on some models only.

The Smart Cover Lock is a software-controllable cover lock, controlled by the setup password. This lock prevents unauthorized access to the internal components. The computer ships with the Smart Cover Lock in the unlocked position. For more information about locking the Smart Cover Lock, refer to the *Desktop Management Guide*.

## Smart Cover FailSafe Key

If you enable the Smart Cover Lock and cannot enter your password to disable the lock, you will need a Smart Cover FailSafe Key to open the computer cover. You will need the key to access the internal computer components in any of the following circumstances:

- Power outage
- Startup failure
- PC component (for example, processor or power supply) failure
- Forgotten password



**NOTE:** The Smart Cover FailSafe Key is a specialized tool available from HP. Be prepared; order this key before you need it.

To obtain a FailSafe Key:

- Contact an authorized HP reseller or service provider. Order PN 166527-001 for the wrench-style key or PN 166527-002 for the screwdriver bit key.
- Refer to the HP Web site (<http://www.hp.com>) for ordering information.
- Call the appropriate number listed in the warranty or in the *Support Telephone Numbers* guide.

## Using the Smart Cover FailSafe Key to Remove the Smart Cover Lock

To open the access panel with the Smart Cover Lock engaged:

1. Remove/disengage any security devices that prohibit opening the computer.
2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
3. Turn off the computer properly through the operating system, then turn off any external devices.
4. Disconnect the power cord from the power outlet and disconnect any external devices.

△ **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.
5. If the computer is on a stand, remove the computer from the stand.

6. Use the Smart Cover FailSafe Key to remove the tamper-proof screw that secures the Smart Cover Lock to the chassis.

**Figure 2-1** Removing the Smart Cover Lock Screw



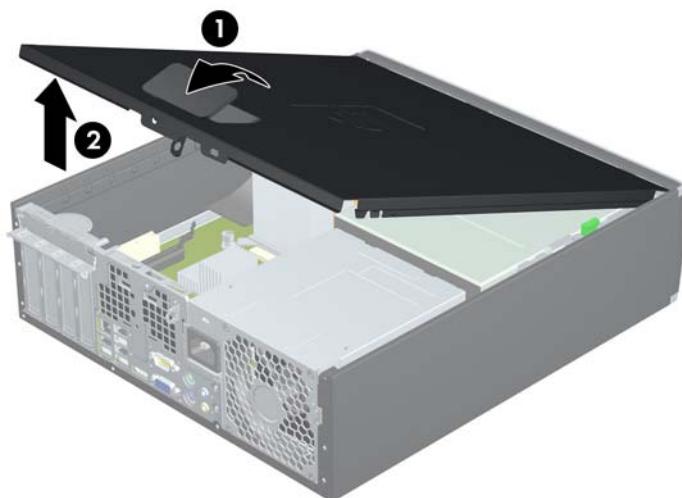
You can now remove the access panel. See [Removing the Computer Access Panel on page 11](#).

To reattach the Smart Cover Lock, secure the lock in place with the tamper-proof screw.

## Removing the Computer Access Panel

1. Remove/disengage any security devices that prohibit opening the computer.
  2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
  3. Turn off the computer properly through the operating system, then turn off any external devices.
  4. Disconnect the power cord from the power outlet and disconnect any external devices.
- △ **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.
5. If the computer is on a stand, remove the computer from the stand.
  6. Lift up on the access panel handle (1) then lift the access panel off the computer (2).

**Figure 2-2** Removing the Access Panel



## Replacing the Computer Access Panel

Slide the lip on the front end of the access panel under the lip on the front of the chassis (1) then press the back end of the access panel onto the unit so that it locks into place (2).

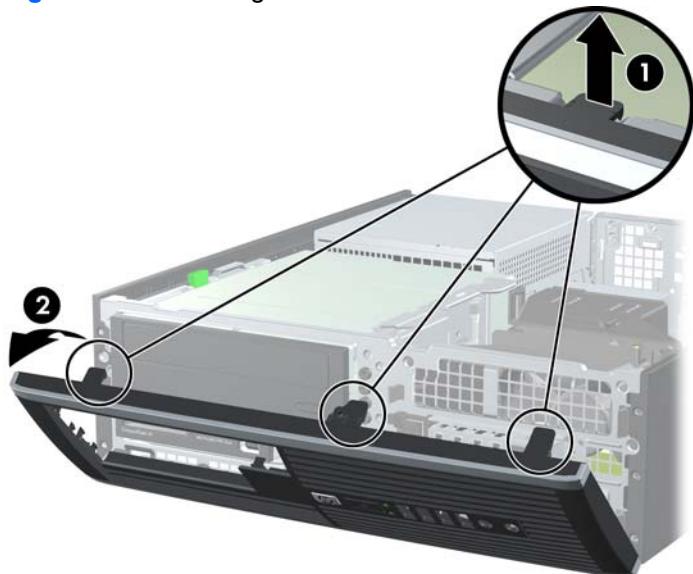
**Figure 2-3** Replacing the Access Panel



## Removing the Front Bezel

1. Remove/disengage any security devices that prohibit opening the computer.
  2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
  3. Turn off the computer properly through the operating system, then turn off any external devices.
  4. Disconnect the power cord from the power outlet and disconnect any external devices.
- △ **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.
5. Remove the access panel.
  6. Lift up the three tabs on the side of the bezel (1), then rotate the bezel off the chassis (2).

**Figure 2-4** Removing the Front Bezel

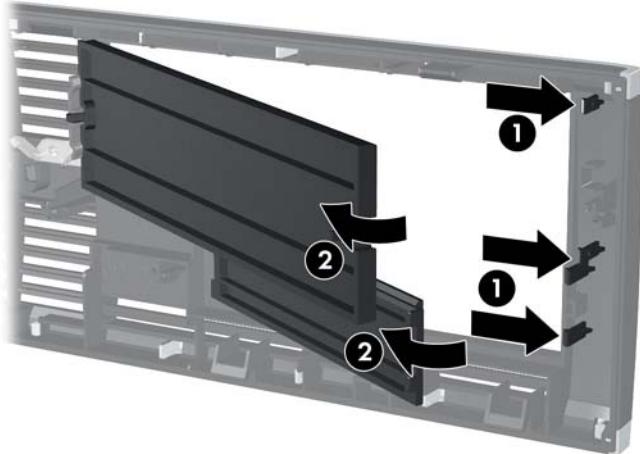


## Removing Bezel Blanks

On some models, there are bezel blanks covering the 3.5-inch and 5.25-inch external drive bays that need to be removed before installing a drive. To remove a bezel blank:

1. Remove the access panel and front bezel.
2. To remove a bezel blank, push the two retaining tabs that hold the bezel blank in place towards the outer right edge of the bezel (1) and slide the bezel blank back and to the right to remove it (2).

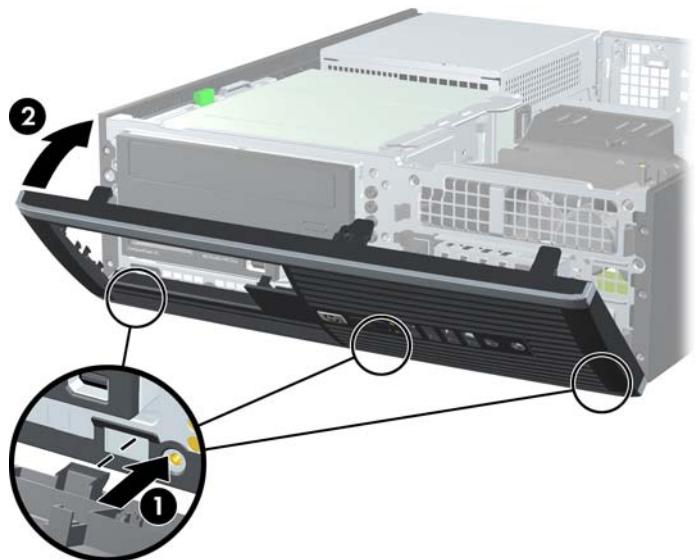
**Figure 2-5** Removing a Bezel Blank



## Replacing the Front Bezel

Insert the three hooks on the bottom side of the bezel into the rectangular holes on the chassis (1) then rotate the top side of the bezel onto the chassis (2) and snap it into place.

**Figure 2-6** Replacing the Front Bezel



## Using the Small Form Factor Computer in a Tower Orientation

The Small Form Factor computer can be used in a tower orientation with an optional tower stand that can be purchased from HP.

1. Remove/disengage any security devices that prohibit opening the computer.
2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
3. Turn off the computer properly through the operating system, then turn off any external devices.
4. Disconnect the power cord from the power outlet and disconnect any external devices.

△ **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.

5. Orient the computer so that its right side is facing down and place the computer in the optional stand.

**Figure 2-7** Changing from Desktop to Tower Orientation



☒ **NOTE:** To stabilize the computer in a tower orientation, HP recommends the use of the optional tower stand.

6. Reconnect the power cord and any external devices, then turn on the computer.

☒ **NOTE:** Ensure at least 10.2 centimeters (4 inches) of space on all sides of the computer remains clear and free of obstructions.

# Installing Additional Memory

The computer comes with double data rate 3 synchronous dynamic random access memory (DDR3-SDRAM) dual inline memory modules (DIMMs).

## DIMMs

The memory sockets on the system board can be populated with up to four industry-standard DIMMs. These memory sockets are populated with at least one preinstalled DIMM. To achieve the maximum memory support, you can populate the system board with up to 16-GB of memory configured in a high-performing dual channel mode.

## DDR3-SDRAM DIMMs

For proper system operation, the DDR3-SDRAM DIMMs must be:

- industry-standard 240-pin
- unbuffered non-ECC PC3-8500 DDR3-1066 MHz-compliant or PC3-10600 DDR3-1333 MHz-compliant
- 1.5 volt DDR3-SDRAM DIMMs

The DDR3-SDRAM DIMMs must also:

- support CAS latency 7 DDR3 1066 MHz (7-7-7 timing) and CAS latency 9 DDR3 1333 MHz (9-9-9 timing)
- contain the mandatory JEDEC SPD information

In addition, the computer supports:

- 512-Mbit, 1-Gbit, and 2-Gbit non-ECC memory technologies
- single-sided and double-sided DIMMs
- DIMMs constructed with x8 and x16 DDR devices; DIMMs constructed with x4 SDRAM are not supported

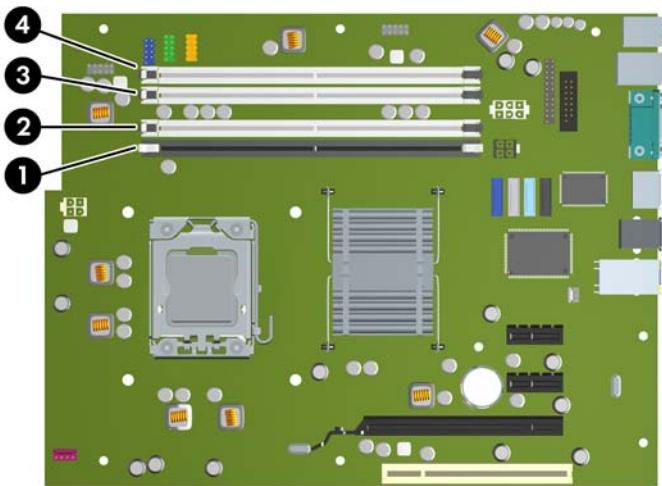


**NOTE:** The system will not operate properly if you install unsupported DIMMs.

## Populating DIMM Sockets

There are four DIMM sockets on the system board, with two sockets per channel. The sockets are labeled DIMM1, DIMM2, DIMM3, and DIMM4. Sockets DIMM1 and DIMM2 operate in memory channel A. Sockets DIMM3 and DIMM4 operate in memory channel B.

**Figure 2-8** DIMM Socket Locations



**Table 2-1** DIMM Socket Locations

Item	Description	Socket Color
1	DIMM1 socket, Channel A (populate first)	Black
2	DIMM2 socket, Channel A (populate third)	White
3	DIMM3 socket, Channel B (populate second)	White
4	DIMM4 socket, Channel B (populate fourth)	White

**NOTE:** A DIMM must occupy the black DIMM1 socket. Otherwise, the system will display a POST error message indicating that a memory module must be installed in the wrong socket.

The system will automatically operate in single channel mode, dual channel mode, or flex mode, depending on how the DIMMs are installed.

- The system will operate in single channel mode if the DIMM sockets are populated in one channel only.
- The system will operate in a higher-performing dual channel mode if the total memory capacity of the DIMMs in Channel A is equal to the total memory capacity of the DIMMs in Channel B. The technology and device width can vary between the channels. For example, if Channel A is populated with two 1-GB DIMMs and Channel B is populated with one 2-GB DIMM, the system will operate in dual channel mode.
- The system will operate in flex mode if the total memory capacity of the DIMMs in Channel A is not equal to the total memory capacity of the DIMMs in Channel B. In flex mode, the channel populated with the least amount of memory describes the total amount of memory assigned to dual channel

and the remainder is assigned to single channel. For optimal speed, the channels should be balanced so that the largest amount of memory is spread between the two channels. If one channel will have more memory than the other, the larger amount should be assigned to Channel A. For example, if you are populating the sockets with one 2-GB DIMM, and three 1-GB DIMMs, Channel A should be populated with the 2-GB DIMM and one 1-GB DIMM, and Channel B should be populated with the other two 1-GB DIMMs. With this configuration, 4-GB will run as dual channel and 1-GB will run as single channel.

- In any mode, the maximum operational speed is determined by the slowest DIMM in the system.

## Installing DIMMs

△ **CAUTION:** You must disconnect the power cord and wait approximately 30 seconds for the power to drain before adding or removing memory modules. Regardless of the power-on state, voltage is always supplied to the memory modules as long as the computer is plugged into an active AC outlet. Adding or removing memory modules while voltage is present may cause irreparable damage to the memory modules or system board. If you see an LED light on the system board, voltage is still present.

The memory module sockets have gold-plated metal contacts. When upgrading the memory, it is important to use memory modules with gold-plated metal contacts to prevent corrosion and/or oxidation resulting from having incompatible metals in contact with each other.

Static electricity can damage the electronic components of the computer or optional cards. Before beginning these procedures, ensure that you are discharged of static electricity by briefly touching a grounded metal object. For more information, refer to Appendix D, [Electrostatic Discharge on page 57](#).

When handling a memory module, be careful not to touch any of the contacts. Doing so may damage the module.

1. Remove/disengage any security devices that prohibit opening the computer.
2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
3. Turn off the computer properly through the operating system, then turn off any external devices.
4. Disconnect the power cord from the power outlet and disconnect any external devices.

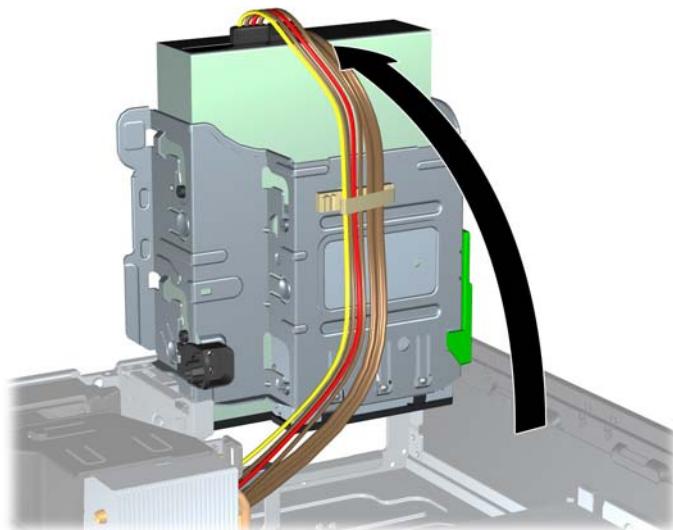
△ **CAUTION:** You must disconnect the power cord and wait approximately 30 seconds for the power to drain before adding or removing memory modules. Regardless of the power-on state, voltage is always supplied to the memory modules as long as the computer is plugged into an active AC outlet. Adding or removing memory modules while voltage is present may cause irreparable damage to the memory modules or system board. If you see an LED light on the system board, voltage is still present.

5. If the computer is on a stand, remove the computer from the stand.
6. Remove the access panel.

⚠ **WARNING!** To reduce risk of personal injury from hot surfaces, allow the internal system components to cool before touching.

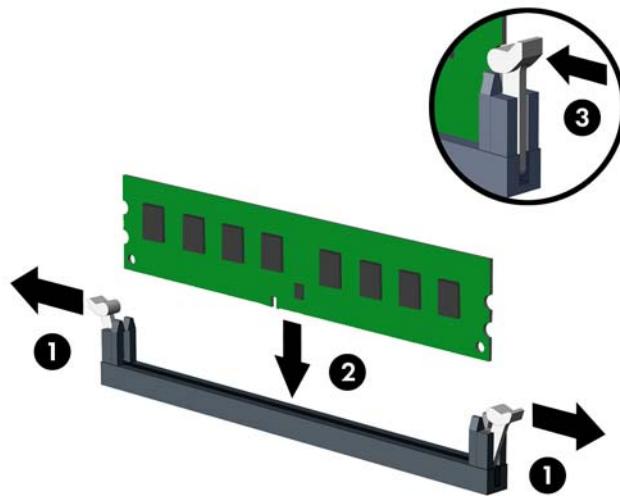
7. Rotate up the external drive bay housing to access the memory module sockets on the system board.

**Figure 2-9** Rotating the Drive Cage Up



8. Open both latches of the memory module socket (1), and insert the memory module into the socket (2).

**Figure 2-10** Installing a DIMM



 **NOTE:** A memory module can be installed in only one way. Match the notch on the module with the tab on the memory socket.

A DIMM must occupy the black DIMM1 socket.

Populate the DIMM sockets in the following order: DIMM1, DIMM3, DIMM2, then DIMM4.

For maximum performance, populate the sockets so that the memory capacity is spread as equally as possible between Channel A and Channel B. Refer to [Populating DIMM Sockets on page 18](#) for more information.

9. Push the module down into the socket, ensuring that the module is fully inserted and properly seated. Make sure the latches are in the closed position (3).
10. Repeat steps 8 and 9 to install any additional modules.
11. Replace the access panel.
12. If the computer was on a stand, replace the stand.
13. Reconnect the power cord and turn on the computer.
14. Lock any security devices that were disengaged when the access panel was removed.

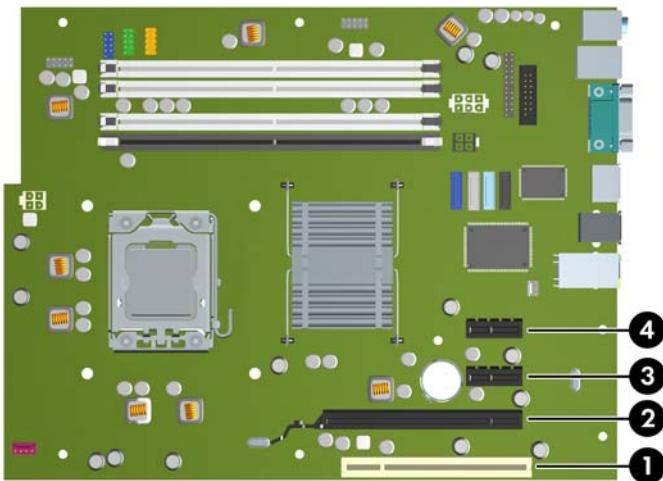
The computer should automatically recognize the additional memory the next time you turn on the computer.

# Removing or Installing an Expansion Card

The computer has one PCI expansion slot, two PCI Express x1 expansion slots, and one PCI Express x16 expansion slot.

 **NOTE:** The PCI and PCI Express slots support only low profile cards.

**Figure 2-11** Expansion Slot Locations



**Table 2-2** Expansion Slot Locations

Item	Description
1	PCI expansion slot
2	PCI Express x16 expansion slot
3	PCI Express x1 expansion slot
4	PCI Express x1 expansion slot

 **NOTE:** You can install a PCI Express x1, x4, x8, or x16 expansion card in the PCI Express x16 slot.

To install an expansion card:

1. Remove/disengage any security devices that prohibit opening the computer.
2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
3. Turn off the computer properly through the operating system, then turn off any external devices.
4. Disconnect the power cord from the power outlet and disconnect any external devices.

 **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.

5. If the computer is on a stand, remove the computer from the stand.

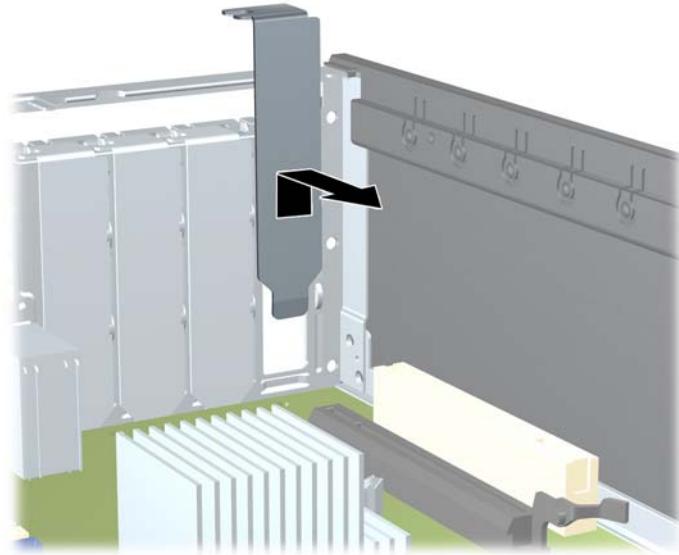
6. Remove the access panel.
7. Locate the correct vacant expansion socket on the system board and the corresponding expansion slot on the back of the computer chassis.
8. Release the slot cover retention latch that secures the PCI slot covers by lifting the green tab on the latch and rotating the latch to the open position.

**Figure 2-12** Opening the Expansion Slot Retainer



9. Before installing an expansion card, remove the expansion slot cover or the existing expansion card.
  - a. If you are installing an expansion card in a vacant socket, remove the appropriate expansion slot cover on the back of the chassis. Pull the slot cover straight up then away from the inside of the chassis.

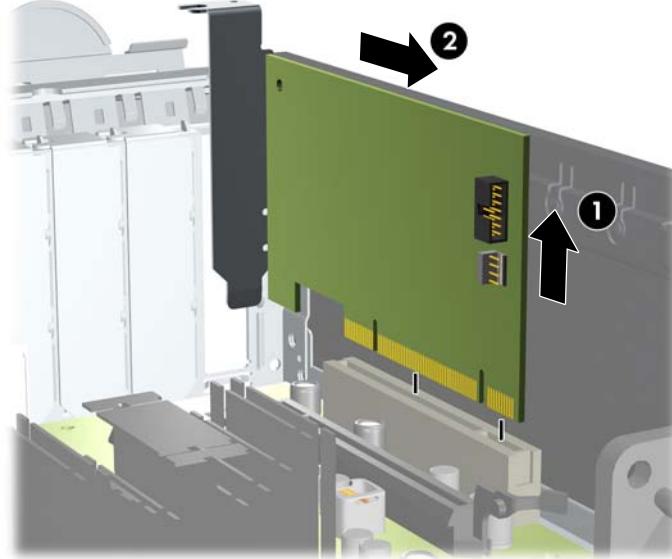
**Figure 2-13** Removing an Expansion Slot Cover



- b. If you are removing a standard PCI card or PCI Express x1 card, hold the card at each end, and carefully rock it back and forth until the connectors pull free from the socket. Pull the expansion card straight up from the socket (1) then away from the inside of the chassis to release it from the chassis frame (2). Be sure not to scrape the card against the other components.

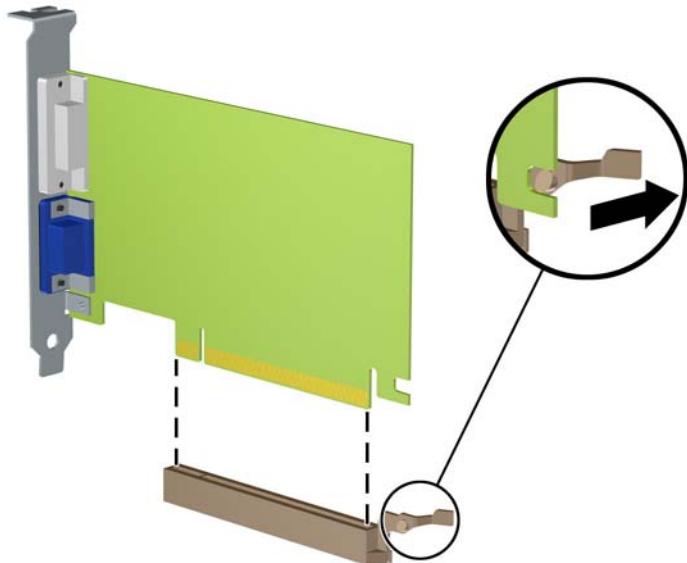
 **NOTE:** Before removing an installed expansion card, disconnect any cables that may be attached to the expansion card.

**Figure 2-14** Removing a Standard PCI Expansion Card



- c. If you are removing a PCI Express x16 card, pull the retention arm on the back of the expansion socket away from the card and carefully rock the card back and forth until the connectors pull free from the socket. Pull the expansion card straight up from the socket then away from the inside of the chassis to release it from the chassis frame. Be sure not to scrape the card against the other components.

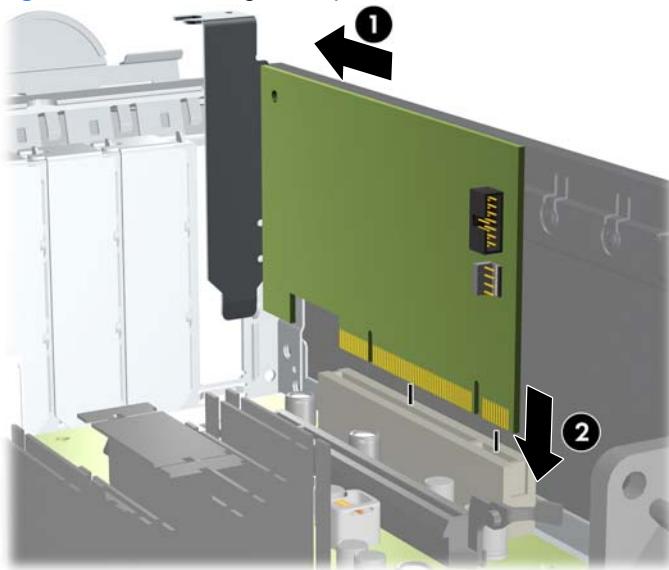
**Figure 2-15** Removing a PCI Express x16 Expansion Card



10. Store the removed card in anti-static packaging.
  11. If you are not installing a new expansion card, install an expansion slot cover to close the open slot.
- 
- △ **CAUTION:** After removing an expansion card, you must replace it with a new card or expansion slot cover for proper cooling of internal components during operation.

- 12.** To install a new expansion card, hold the card just above the expansion socket on the system board then move the card toward the rear of the chassis (1) so that the bracket on the card is aligned with the open slot on the rear of the chassis. Press the card straight down into the expansion socket on the system board (2).

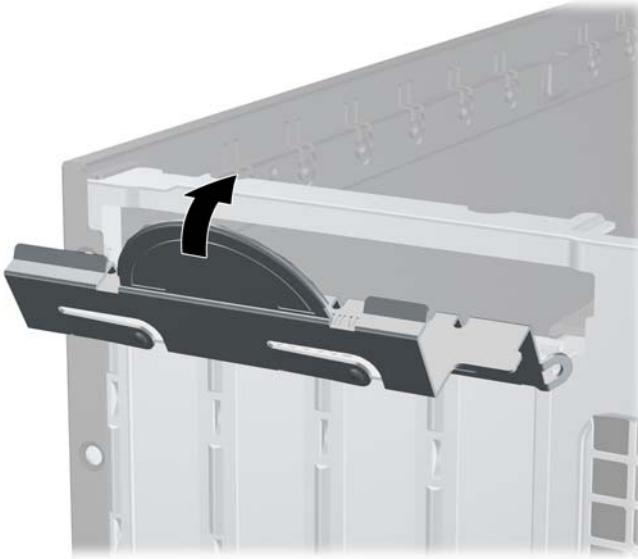
**Figure 2-16** Installing an Expansion Card



 **NOTE:** When installing an expansion card, press firmly on the card so that the whole connector seats properly in the expansion card slot.

- 13.** Rotate the slot cover retention latch back in place to secure the expansion card.

**Figure 2-17** Closing the Expansion Slot Retainer

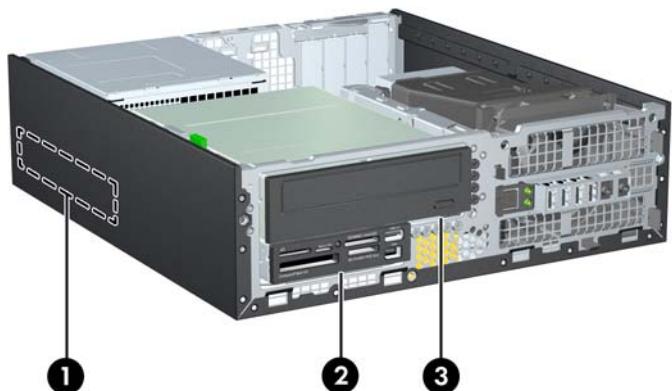


- 14.** Connect external cables to the installed card, if needed. Connect internal cables to the system board, if needed.
- 15.** Replace the access panel.

16. If the computer was on a stand, replace the stand.
17. Reconnect the power cord and turn on the computer.
18. Lock any security devices that were disengaged when the access panel was removed.
19. Reconfigure the computer, if necessary.

## Drive Positions

**Figure 2-18** Drive Positions



**Table 2-3** Drive Positions

1	3.5-inch internal hard drive bay
2	3.5-inch external drive bay for optional drives (media card reader shown)
3	5.25-inch external drive bay for optional drives (optical drive shown)

**NOTE:** The drive configuration on your computer may be different than the drive configuration shown above.

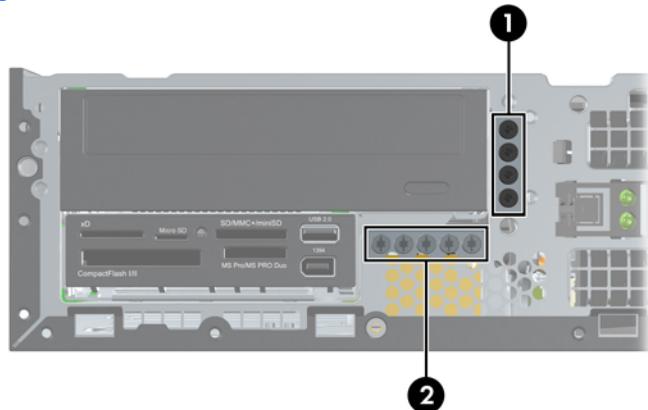
To verify the type, size, and capacity of the storage devices installed in the computer, run Computer Setup.

# Installing and Removing Drives

When installing additional drives, follow these guidelines:

- The primary Serial ATA (SATA) hard drive must be connected to the dark blue primary SATA connector on the system board labeled SATA0.
- Connect a SATA optical drive to the white SATA connector on the system board labeled SATA1.
- Connect devices in order of SATA0, SATA1, then SATA2
- Connect an optional eSATA adapter cable to the black ESATA connector on the system board.
- Connect a media card reader USB cable to the USB connector on the system board labeled MEDIA. If the media card reader has a 1394 port, connect the 1394 cable to the 1394 PCI card.
- The system does not support Parallel ATA (PATA) optical drives or PATA hard drives.
- You must install guide screws to ensure the drive will line up correctly in the drive cage and lock in place. HP has provided extra guide screws for the external drive bays (five 6-32 standard screws and four M3 metric screws), installed in the front of the chassis, under the front bezel. The 6-32 standard screws are required for a secondary hard drive. All other drives (except the primary hard drive) use M3 metric screws. The HP-supplied metric screws are black and the HP-supplied standard screws are silver. If you are replacing the primary hard drive, you must remove the four silver and blue 6-32 isolation mounting guide screws from the old hard drive and install them in the new hard drive.

**Figure 2-19** Extra Guide Screw Locations



No.	Guide Screw	Device
1	Black M3 Metric Screws	All Drives (except hard drives)
2	Silver 6-32 Standard Screws	Secondary Hard Drive

There are a total of five extra silver 6-32 standard screws. Four are used as guide screws for a secondary hard drive. The fifth is used for bezel security (see [Front Bezel Security on page 55](#) for more information).

△ **CAUTION:** To prevent loss of work and damage to the computer or drive:

If you are inserting or removing a drive, shut down the operating system properly, turn off the computer, and unplug the power cord. Do not remove a drive while the computer is on or in standby mode.

Before handling a drive, ensure that you are discharged of static electricity. While handling a drive, avoid touching the connector. For more information about preventing electrostatic damage, refer to Appendix D, [Electrostatic Discharge on page 57](#).

Handle a drive carefully; do not drop it.

Do not use excessive force when inserting a drive.

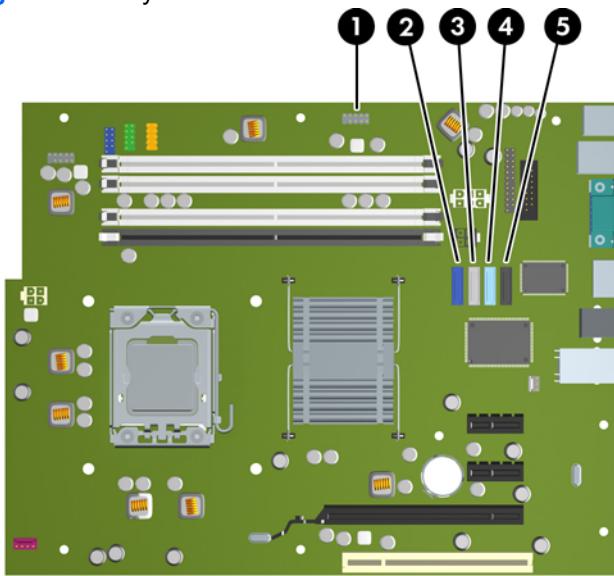
Avoid exposing a hard drive to liquids, temperature extremes, or products that have magnetic fields such as monitors or speakers.

If a drive must be mailed, place the drive in a bubble-pack mailer or other protective packaging and label the package “Fragile: Handle With Care.”

## System Board Drive Connections

Refer to the following illustration and table to identify the system board drive connectors.

**Figure 2-20** System Board Drive Connections



**Table 2-4** System Board Drive Connections

No.	System Board Connector	System Board Label	Color
1	Media Card Reader	MEDIA	black
2	SATA0	SATA0	dark blue
3	SATA1	SATA1	white
4	SATA2	SATA2	light blue
5	eSATA	ESATA	black

## Removing an External 5.25-inch Drive

△ **CAUTION:** All removable media should be taken out of a drive before removing the drive from the computer.

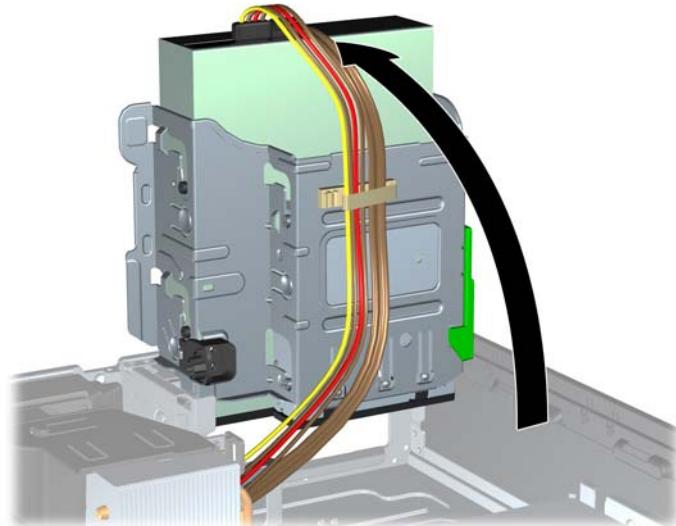
To remove a 5.25-inch external drive:

1. Remove/disengage any security devices that prohibit opening the computer.
2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
3. Turn off the computer properly through the operating system, then turn off any external devices.
4. Disconnect the power cord from the power outlet and disconnect any external devices.

△ **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.

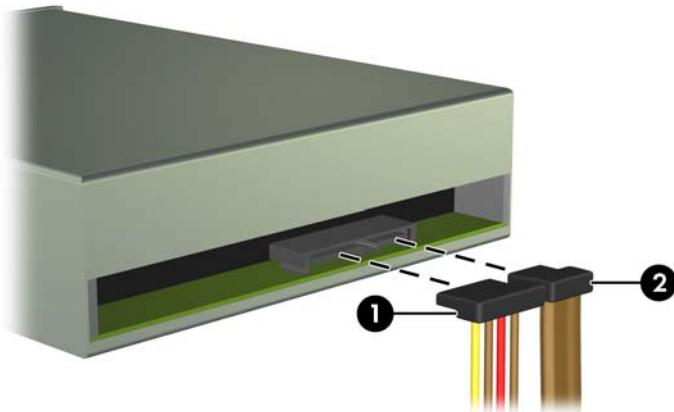
5. If the computer is on a stand, remove the computer from the stand.
6. Remove the access panel.
7. Rotate the drive cage to its upright position.

**Figure 2-21** Rotating the Drive Cage Up



8. If removing an optical drive, disconnect the power cable (1) and data cable (2) from the rear of the optical drive.

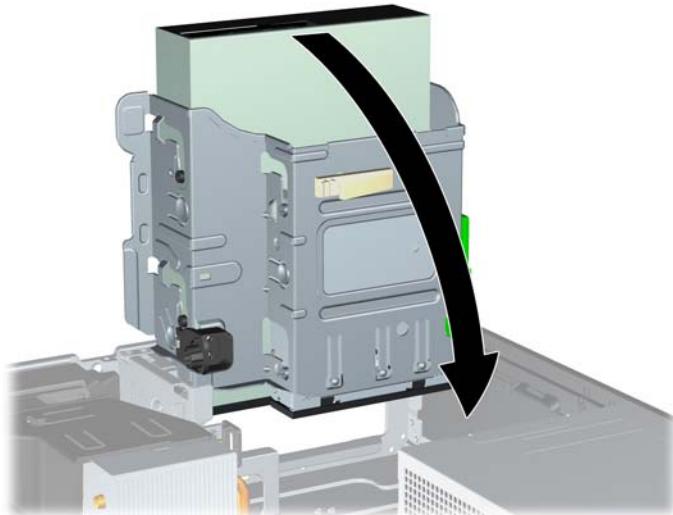
**Figure 2-22** Disconnecting the Power and Data Cables



9. Rotate the drive cage back down to its normal position.

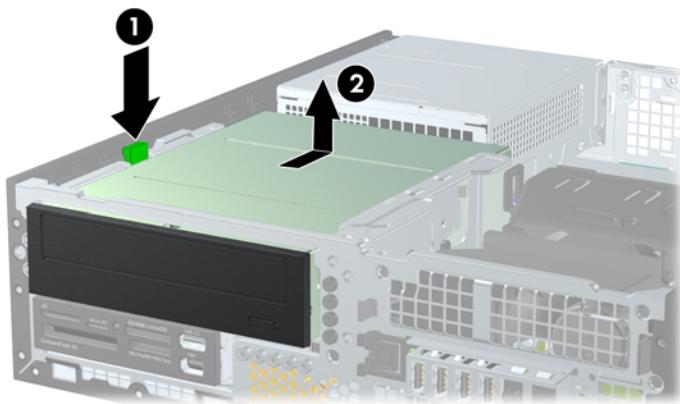
△ **CAUTION:** Be careful not to pinch any cables or wires when rotating the drive cage down.

**Figure 2-23** Rotating the Drive Cage Down



10. Press down on the green drive retainer button located on the left side of the drive to disengage the drive from the drive cage (1). While pressing the drive retainer button, slide the drive back until it stops, then lift it up and out of the drive cage (2).

**Figure 2-24** Removing the 5.25-inch Drive



 **NOTE:** To replace the drive, reverse the removal procedure. When replacing a drive, transfer the four guide screws from the old drive to the new one.

## Installing an Optical Drive into the 5.25-inch Drive Bay

To install an optional 5.25-inch optical drive:

1. Remove/disengage any security devices that prohibit opening the computer.
  2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
  3. Turn off the computer properly through the operating system, then turn off any external devices.
  4. Disconnect the power cord from the power outlet and disconnect any external devices.
-  **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.
5. If the computer is on a stand, remove the computer from the stand.
  6. Remove the access panel.
  7. If you are installing a drive in a bay covered by a bezel blank, remove the front bezel then remove the bezel blank. See [Removing Bezel Blanks on page 14](#) for more information.

8. Install four M3 metric guide screws in the lower holes on each side of the drive. HP has provided four extra M3 metric guide screws on the front of the chassis, under the front bezel. The M3 metric guide screws are black. Refer to [Installing and Removing Drives on page 29](#) for an illustration of the extra M3 metric guide screws location.

△ **CAUTION:** Use only 5-mm long screws as guide screws. Longer screws can damage the internal components of the drive.

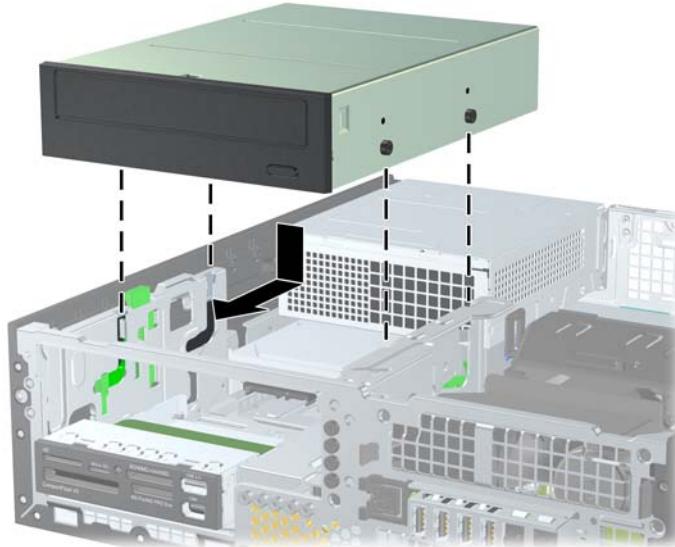
☒ **NOTE:** When replacing the drive, transfer the four M3 metric guide screws from the old drive to the new one.

**Figure 2-25** Installing Guide Screws in the Optical Drive



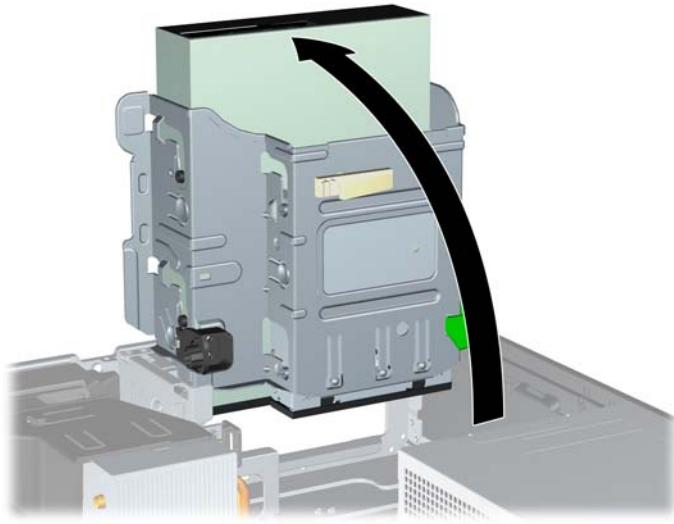
9. Position the guide screws on the drive into the J-slots in the drive bay. Then slide the drive toward the front of the computer until it locks into place.

**Figure 2-26** Installing the Optical Drive



10. Rotate the drive cage to its upright position.

**Figure 2-27** Rotating the Drive Cage Up



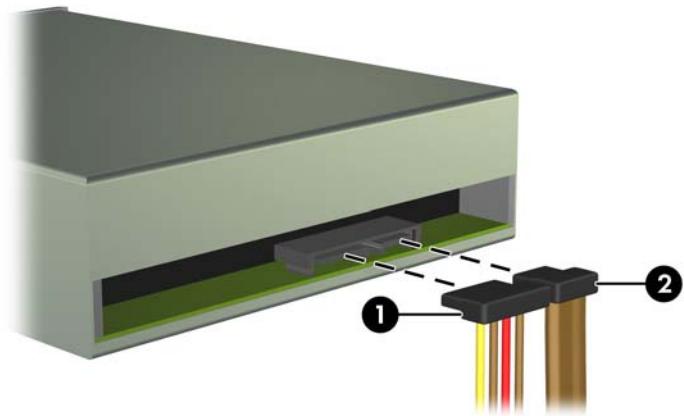
11. Connect the SATA data cable to the white system board connector labeled SATA1.

12. Route the data cable through the cable guides.

△ **CAUTION:** There are two cable guides that keep the data cable from being pinched by the drive cage when raising or lowering it. One is located on the bottom side of the drive cage. The other is located on the chassis frame under the drive cage. Ensure that the data cable is routed through these guides before connecting it to the optical drive.

13. Connect the power cable (1) and data cable (2) to the rear of the optical drive.

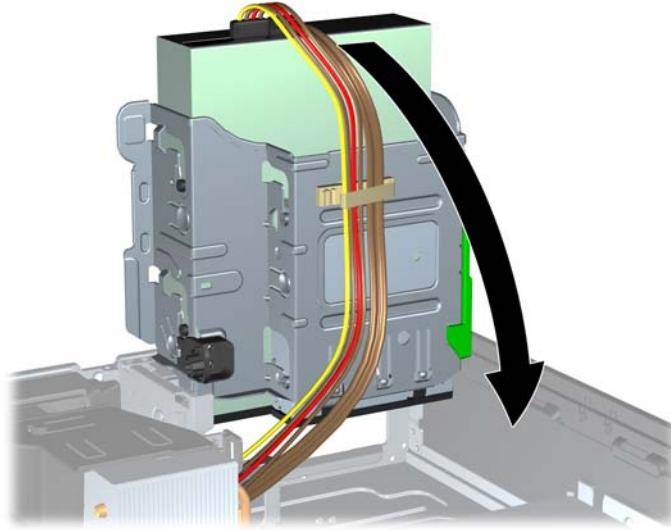
**Figure 2-28** Connecting the Power and Data Cables



14. Rotate the drive cage back down to its normal position.

△ **CAUTION:** Be careful not to pinch any cables or wires when rotating the drive cage down.

**Figure 2-29** Rotating the Drive Cage Down



15. Replace the access panel.
16. If the computer was on a stand, replace the stand.
17. Reconnect the power cord and turn on the computer.
18. Lock any security devices that were disengaged when the access panel was removed.

The system automatically recognizes the drive and reconfigures the computer.

## Removing an External 3.5-inch Drive

△ **CAUTION:** All removable media should be taken out of a drive before removing the drive from the computer.

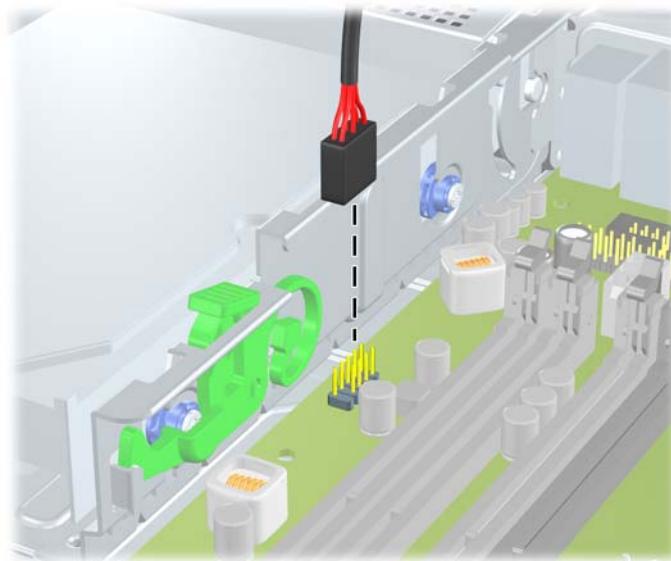
The 3.5-inch drive is located underneath the 5.25-inch drive. You must remove the external 5.25-inch drive before removing the external 3.5-inch drive.

1. Follow the procedure in [Removing an External 5.25-inch Drive on page 31](#) to remove the 5.25-inch drive and access the 3.5-inch drive.
- △ **CAUTION:** Ensure that the computer is turned off and that the power cord is disconnected from the electrical outlet before proceeding.

2. Disconnect the drive cables from the rear of the drive, or, if you are removing a media card reader, disconnect the USB and 1394 cables from the system board as indicated in the following illustrations.

 **NOTE:** On some models, the media card reader does not include a 1394 port or cable.

**Figure 2-30** Disconnecting the Media Card Reader USB Cable

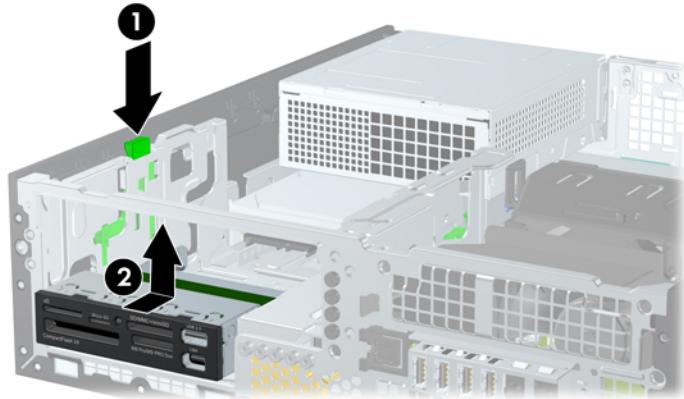


**Figure 2-31** Disconnecting the Media Card Reader 1394 Cable



3. Press down on the green drive retainer button located on the left side of the drive to disengage the drive from the drive cage (1). While pressing the drive retainer button, slide the drive back until it stops, then lift it up and out of the drive cage (2).

**Figure 2-32** Removing a 3.5-inch Drive (Media Card Reader Shown)



**NOTE:** To replace the 3.5-inch drive, reverse the removal procedure.

When replacing a 3.5-inch drive, transfer the four guide screws from the old drive to the new one.

## Installing a Drive into the 3.5-inch External Drive Bay

The 3.5-inch bay is located underneath the 5.25-inch drive. To install a drive into the 3.5-inch bay:

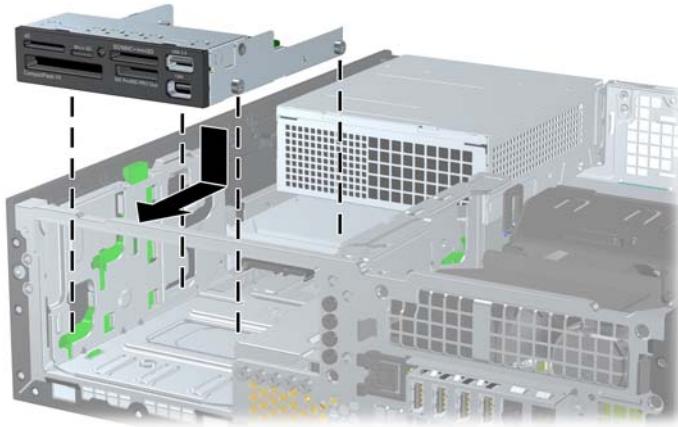
**NOTE:** Install guide screws to ensure the drive will line up correctly in the drive cage and lock in place. HP has provided extra guide screws for the external drive bays (four 6-32 standard screws and four M3 metric screws), installed in the front of the chassis, under the front bezel. A secondary hard drive uses 6-32 standard screws. All other drives (except the primary hard drive) use M3 metric screws. The HP-supplied M3 metric screws are black and the HP-supplied 6-32 standard screws are silver. Refer to [Installing and Removing Drives on page 29](#) for illustrations of the guide screw locations.

1. Follow the procedure in [Removing an External 5.25-inch Drive on page 31](#) to remove the 5.25-inch drive and access the 3.5-inch drive bay.

**CAUTION:** Ensure that the computer is turned off and that the power cord is disconnected from the electrical outlet before proceeding.
2. If you are installing a drive in a bay covered by a bezel blank, remove the front bezel then remove the bezel blank. See [Removing Bezel Blanks on page 14](#) for more information.

3. Position the guide screws on the drive into the J-slots in the drive bay. Then slide the drive toward the front of the computer until it locks into place.

**Figure 2-33** Installing a Drive into the 3.5-inch Drive Bay (Media Card Reader Shown)



4. Connect the appropriate drive cables:
  - a. If installing a second hard drive, connect the power and data cables to the rear of the drive and connect the other end of the data cable to the next available (unpopulated) SATA connector on the system board by following the numbered sequence of the connectors.
  - b. If installing a media card reader, connect the USB cable from the media card reader to the USB connector on the system board labeled MEDIA. If the media card reader includes a 1394 port, connect the 1394 cable to the 1394 PCI card.
5. Replace the 5.25-inch drive.
6. Replace the front bezel and access panel.
7. If the computer was on a stand, replace the stand.
8. Reconnect the power cord and turn on the computer.
9. Lock any security devices that were disengaged when the access panel was removed.

**NOTE:** Refer to [System Board Drive Connections on page 30](#) for an illustration of the system board drive connectors.

## Removing and Replacing the Primary 3.5-inch Internal SATA Hard Drive

**NOTE:** The system does not support Parallel ATA (PATA) hard drives.

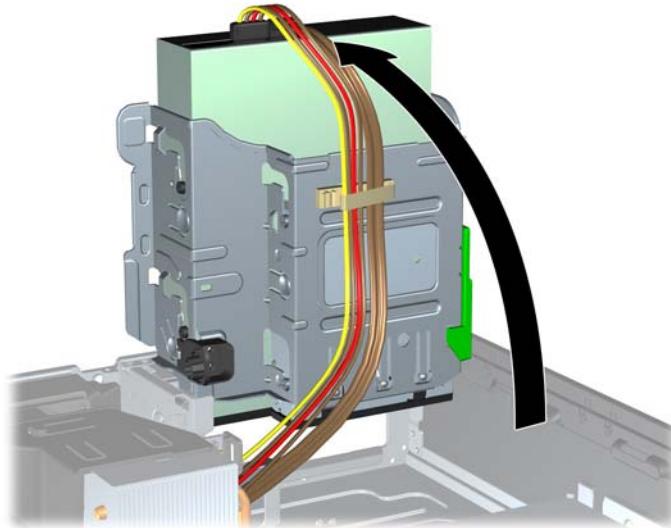
Before you remove the old hard drive, be sure to back up the data from the old hard drive so that you can transfer the data to the new hard drive.

The preinstalled 3.5-inch hard drive is located under the power supply. To remove and replace the hard drive:

1. Remove/disengage any security devices that prohibit opening the computer.
2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
3. Turn off the computer properly through the operating system, then turn off any external devices.

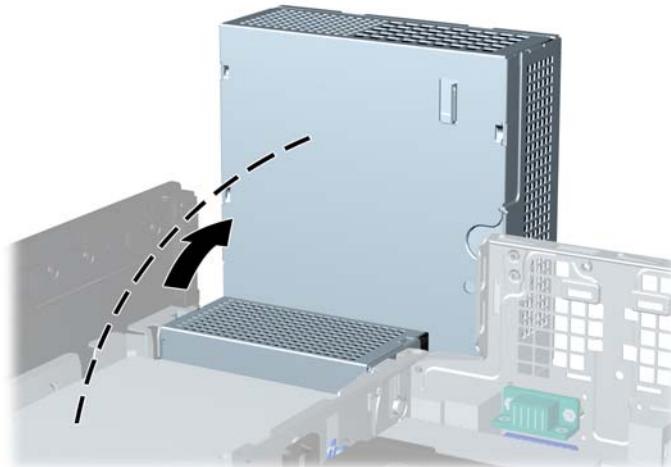
4. Disconnect the power cord from the power outlet and disconnect any external devices.
- △ **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.
5. If the computer is on a stand, remove the computer from the stand.
6. Remove the access panel.
7. Rotate the drive cage for external drives to its upright position.

**Figure 2-34** Rotating the Drive Cage Up



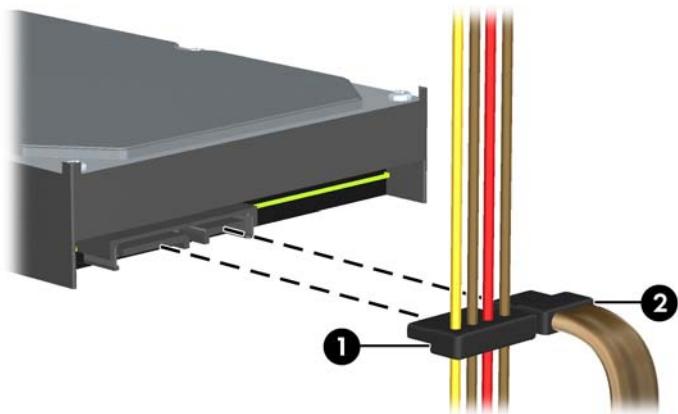
8. Rotate the power supply to its upright position. The hard drive is located beneath the power supply.

**Figure 2-35** Raising the Power Supply



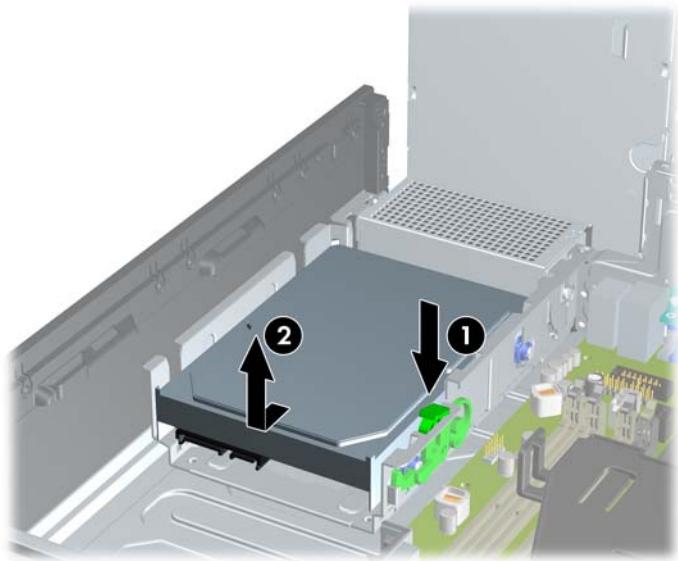
9. Disconnect the power cable (1) and data cable (2) from the back of the hard drive.

**Figure 2-36** Disconnecting the Hard Drive Power Cable and Data Cable



10. Press down on the green release latch next to the hard drive (1). While holding the latch down, slide the drive forward until it stops, then lift the drive up and out of the bay (2).

**Figure 2-37** Removing the Hard Drive



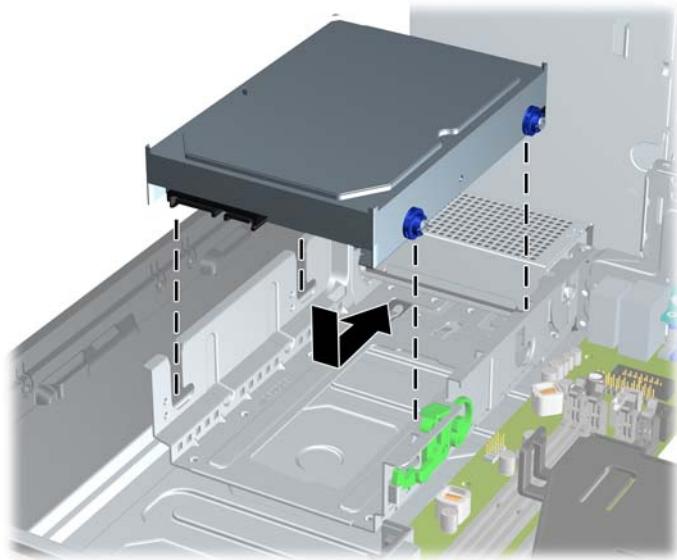
11. To install a hard drive, you must transfer the silver and blue isolation mounting guide screws from the old hard drive to the new hard drive.

**Figure 2-38** Installing Hard Drive Guide Screws



12. Align the guide screws with the slots on the chassis drive cage, press the hard drive down into the bay, then slide it back until it stops and locks in place.

**Figure 2-39** Installing the Hard Drive



13. Connect the power and data cables to the back of the hard drive.

**NOTE:** When replacing the primary hard drive, be sure to route the SATA and power cables through the cable guide on the bottom of the chassis frame behind the hard drive.

If the system has only one SATA hard drive, the data cable must be connected to the dark blue connector labeled SATA0 on the system board to avoid any hard drive performance problems.

14. Rotate the drive cage for external drives and the power supply down to their normal positions.
15. Replace the access panel.
16. If the computer was on a stand, replace the stand.
17. Reconnect the power cord and turn on the computer.
18. Lock any security devices that were disengaged when the access panel was removed.

## Removing and Replacing a Removable 3.5-inch SATA Hard Drive

Some models are equipped with a Removable SATA Hard Drive Enclosure in the 5.25-inch external drive bay. The hard drive is housed in a carrier that can be quickly and easily removed from the drive bay. To remove and replace a drive in the carrier:

**NOTE:** Before you remove the old hard drive, be sure to back up the data from the old hard drive so that you can transfer the data to the new hard drive.

1. Unlock the hard drive carrier with the key provided and slide the carrier out of the enclosure.

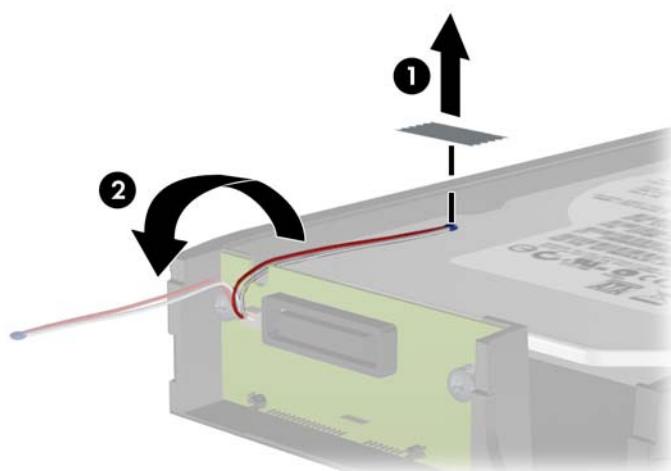
2. Remove the screw from the rear of the carrier (1) and slide the top cover off the carrier (2).

**Figure 2-40** Removing the Carrier Cover



3. Remove the adhesive strip that secures the thermal sensor to the top of the hard drive (1) and move the thermal sensor away from the carrier (2).

**Figure 2-41** Removing the Thermal Sensor



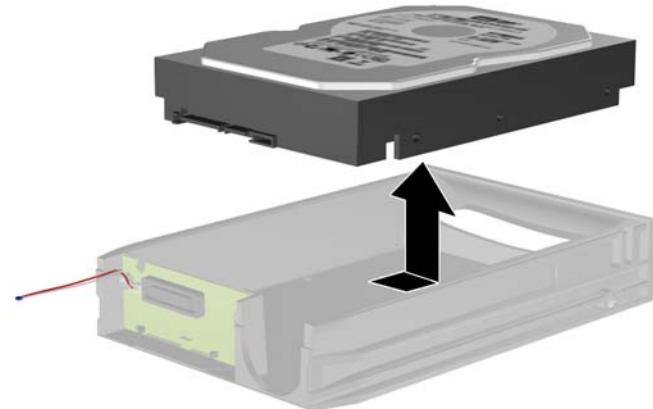
4. Remove the four screws from the bottom of the hard drive carrier.

**Figure 2-42** Removing the Security Screws



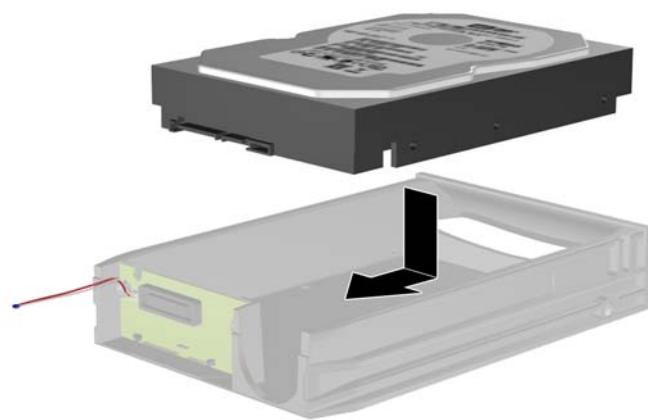
5. Slide the hard drive back to disconnect it from the carrier then lift it up and out of the carrier.

**Figure 2-43** Removing the Hard Drive



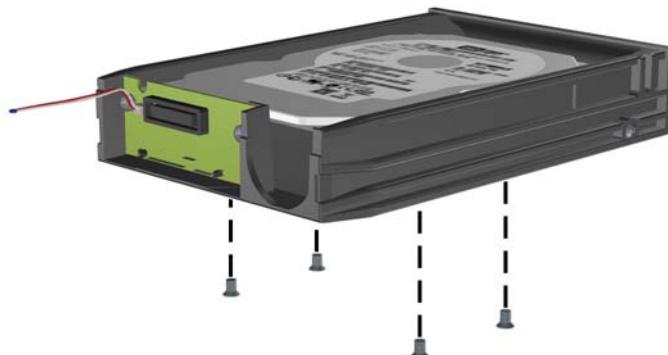
6. Place the new hard drive in the carrier then slide the hard drive back so that it seats in the SATA connector on the carrier's circuit board. Be sure the connector on the hard drive is pressed all the way into the connector on the carrier's circuit board.

**Figure 2-44** Replacing the Hard Drive



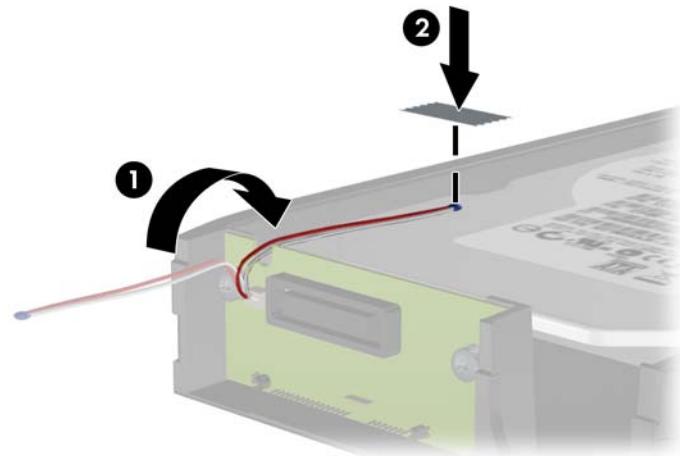
7. Replace the four screws in the bottom of the carrier to hold the drive securely in place.

**Figure 2-45** Replacing the Security Screws



8. Place the thermal sensor on top of the hard drive in a position that does not cover the label (1) and attach the thermal sensor to the top of the hard drive with the adhesive strip (2).

**Figure 2-46** Replacing the Thermal Sensor



9. Slide the cover on the carrier (1) and replace the screw on the rear of the carrier to secure the cover in place (2).

**Figure 2-47** Replacing the Carrier Cover



10. Slide the hard drive carrier into the enclosure on the computer and lock it with the key provided.

 **NOTE:** The carrier must be locked for power to be supplied to the hard drive.

# A Specifications

**Table A-1 Specifications**

Desktop Dimensions (in the desktop position)		
Height	3.95 in	10.0 cm
Width	13.3 in	33.8 cm
Depth	14.9 in	37.8 cm
Approximate Weight	16.72 lb	7.6 kg
Weight Supported (maximum distributed load in desktop position)	77 lb	35 kg
Temperature Range		
Operating	50° to 95°F	10° to 35°C
Nonoperating	-22° to 140°F	-30° to 60°C
<b>NOTE:</b> Operating temperature is derated 1.0° C per 300 m (1000 ft) to 3000 m (10,000 ft) above sea level; no direct sustained sunlight. Maximum rate of change is 10° C/Hr. The upper limit may be limited by the type and number of options installed.		
Relative Humidity (noncondensing)		
Operating	10-90%	10-90%
Nonoperating (38.7°C max wet bulb)	5-95%	5-95%
Maximum Altitude (unpressurized)		
Operating	10,000 ft	3048 m
Nonoperating	30,000 ft	9144 m
Heat Dissipation		
Max STD PS	1063 BTU/hr	268 kg-cal/hr
Typical STD PS idle	198 BTU/hr	50 kg-cal/hr
Max EPA 87/89/85% @ 20/50/100% load PS	941 BTU/hr	237 kg-cal/hr
Typical EPA 87/89/85% @ 20/50/100% load PS idle	150 BTU/hr	38 kg-cal/hr
Power Supply		
Operating Voltage Range (STD PS)	90-264 VAC	90-264 VAC
Operating Voltage Range (EPA 87/89/85% @ 20/50/100% load PS)	90-264 VAC	90-264 VAC
Rated Voltage Range (STD PS)	100-240 VAC	100-240 VAC
Rated Voltage Range (EPA 87/89/85% @ 20/50/100% load PS)	100-240 VAC	100-240 VAC

**Table A-1 Specifications (continued)**

Rated Line Frequency	50-60 Hz	50-60 Hz
<b>Power Output</b>	240W	240W
<b>Rated Input Current (maximum)<sup>1</sup></b>		
STD PS	4A @ 100 VAC	2A @ 230 VAC
EPA 87/89/85% @ 20/50/100% load PS	4A @ 100 VAC	2A @ 230 VAC

<sup>1</sup> This system utilizes an active power factor corrected power supply. This allows the system to pass the CE mark requirements for use in the countries of the European Union. The active power factor corrected power supply also has the added benefit of not requiring an input voltage range select switch.

---

## B Battery Replacement

The battery that comes with the computer provides power to the real-time clock. When replacing the battery, use a battery equivalent to the battery originally installed in the computer. The computer comes with a 3-volt lithium coin cell battery.

**⚠ WARNING!** The computer contains an internal lithium manganese dioxide battery. There is a risk of fire and burns if the battery is not handled properly. To reduce the risk of personal injury:

Do not attempt to recharge the battery.

Do not expose to temperatures higher than 60°C (140°F).

Do not disassemble, crush, puncture, short external contacts, or dispose of in fire or water.

Replace the battery only with the HP spare designated for this product.

**⚠ CAUTION:** Before replacing the battery, it is important to back up the computer CMOS settings. When the battery is removed or replaced, the CMOS settings will be cleared.

Static electricity can damage the electronic components of the computer or optional equipment. Before beginning these procedures, ensure that you are discharged of static electricity by briefly touching a grounded metal object.

**💡 NOTE:** The lifetime of the lithium battery can be extended by plugging the computer into a live AC wall socket. The lithium battery is only used when the computer is NOT connected to AC power.

HP encourages customers to recycle used electronic hardware, HP original print cartridges, and rechargeable batteries. For more information about recycling programs, go to <http://www.hp.com/recycle>.

1. Remove/disengage any security devices that prohibit opening the computer.
2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
3. Turn off the computer properly through the operating system, then turn off any external devices.
4. Disconnect the power cord from the power outlet and disconnect any external devices.

**⚠ CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.

5. If the computer is on a stand, remove the computer from the stand.
6. Remove the access panel.
7. Locate the battery and battery holder on the system board.

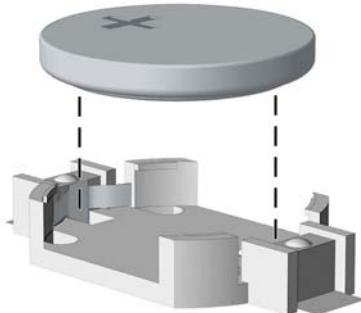
**NOTE:** On some computer models, it may be necessary to remove an internal component to gain access to the battery.

8. Depending on the type of battery holder on the system board, complete the following instructions to replace the battery.

#### Type 1

- a. Lift the battery out of its holder.

**Figure B-1** Removing a Coin Cell Battery (Type 1)

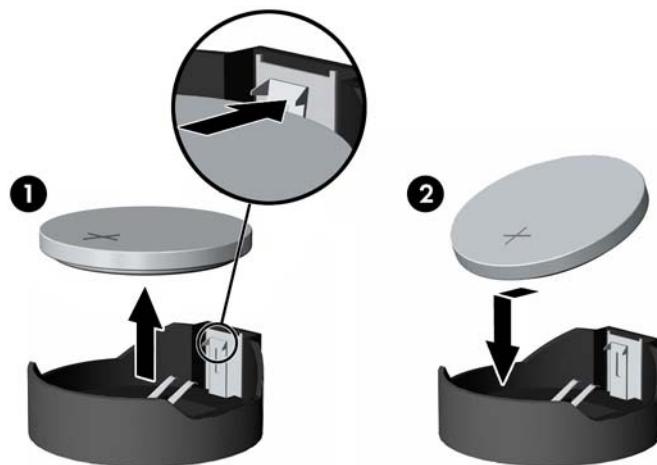


- b. Slide the replacement battery into position, positive side up. The battery holder automatically secures the battery in the proper position.

#### Type 2

- a. To release the battery from its holder, squeeze the metal clamp that extends above one edge of the battery. When the battery pops up, lift it out (1).
- b. To insert the new battery, slide one edge of the replacement battery under the holder's lip with the positive side up. Push the other edge down until the clamp snaps over the other edge of the battery (2).

**Figure B-2** Removing and Replacing a Coin Cell Battery (Type 2)

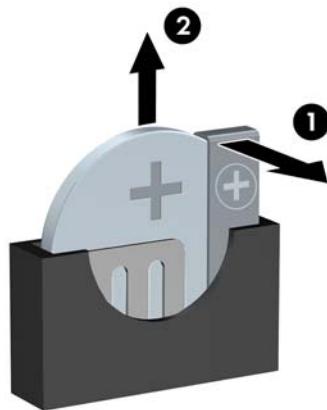


#### Type 3

- a. Pull back on the clip (1) that is holding the battery in place, and remove the battery (2).

- b. Insert the new battery and position the clip back into place.

**Figure B-3** Removing a Coin Cell Battery (Type 3)



 **NOTE:** After the battery has been replaced, use the following steps to complete this procedure.

9. Replace the access panel.
10. If the computer was on a stand, replace the stand.
11. Plug in the computer and turn on power to the computer.
12. Reset the date and time, your passwords, and any special system setups using Computer Setup.
13. Lock any security devices that were disengaged when the access panel was removed.

# C External Security Devices

 **NOTE:** For information on data security features, refer to the *Desktop Management Guide* and the *HP ProtectTools Security Manager Guide* (some models) at <http://www.hp.com>.

## Installing a Security Lock

The security locks displayed below and on the following pages can be used to secure the computer.

### HP/Kensington MicroSaver Security Cable Lock

**Figure C-1** Installing a Cable Lock



## Padlock

**Figure C-2** Installing a Padlock



## HP Business PC Security Lock

1. Fasten the security cable by looping it around a stationary object.

**Figure C-3** Securing the Cable to a Fixed Object



2. Thread the keyboard and mouse cables through the lock.

**Figure C-4** Threading the Keyboard and Mouse Cables



3. Screw the lock to the chassis using the screw provided.

**Figure C-5** Attaching the Lock to the Chassis



4. Insert the plug end of the security cable into the lock (1) and push the button in (2) to engage the lock. Use the key provided to disengage the lock.

**Figure C-6** Engaging the Lock



## Front Bezel Security

The front bezel can be locked in place by installing a security screw provided by HP. To install the security screw:

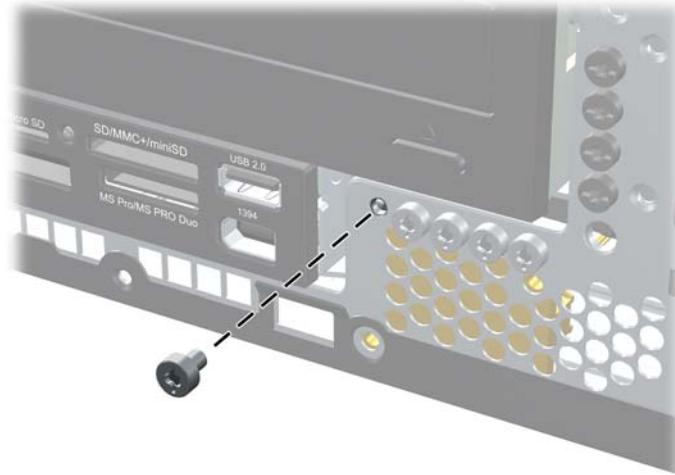
1. Remove/disengage any security devices that prohibit opening the computer.
2. Remove all removable media, such as compact discs or USB flash drives, from the computer.
3. Turn off the computer properly through the operating system, then turn off any external devices.
4. Disconnect the power cord from the power outlet and disconnect any external devices.

△ **CAUTION:** Regardless of the power-on state, voltage is always present on the system board as long as the system is plugged into an active AC outlet. You must disconnect the power cord to avoid damage to the internal components of the computer.

5. If the computer is on a stand, remove the computer from the stand.
6. Remove the access panel and front bezel.

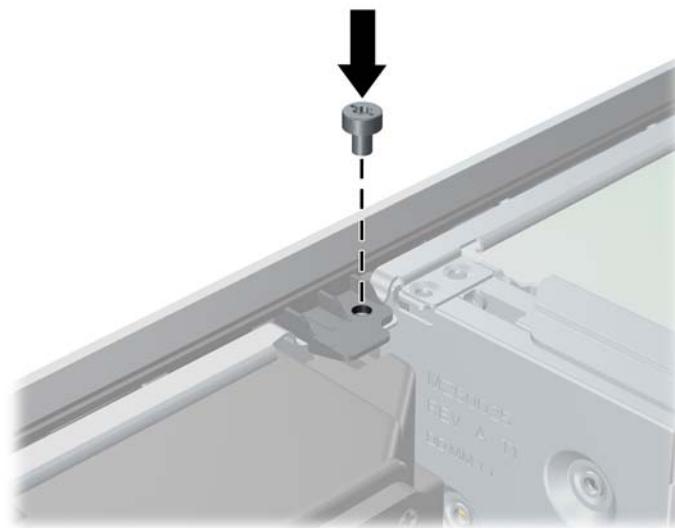
7. Remove one of the five silver 6-32 standard screws located on the front of the chassis behind the bezel.

**Figure C-7** Retrieving the Front Bezel Security Screw



8. Replace the front bezel.
9. Install the security screw next to the middle front bezel release tab to secure the front bezel in place.

**Figure C-8** Installing the Front Bezel Security Screw



10. Replace the access panel.
11. If the computer was on a stand, replace the stand.
12. Reconnect the power cord and turn on the computer.
13. Lock any security devices that were disengaged when the access panel was removed.

---

# D Electrostatic Discharge

A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

## Preventing Electrostatic Damage

To prevent electrostatic damage, observe the following precautions:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly.

## Grounding Methods

There are several methods for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm +/- 10 percent resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heelstraps, toestraps, or bootstraps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, contact an HP authorized dealer, reseller, or service provider.

---

 **NOTE:** For more information on static electricity, contact an HP authorized dealer, reseller, or service provider.

---

---

# E Computer Operating Guidelines, Routine Care and Shipping Preparation

## Computer Operating Guidelines and Routine Care

Follow these guidelines to properly set up and care for the computer and monitor:

- Keep the computer away from excessive moisture, direct sunlight, and extremes of heat and cold.
- Operate the computer on a sturdy, level surface. Leave a 10.2-cm (4-inch) clearance on all vented sides of the computer and above the monitor to permit the required airflow.
- Never restrict the airflow into the computer by blocking any vents or air intakes. Do not place the keyboard, with the keyboard feet down, directly against the front of the desktop unit as this also restricts airflow.
- Never operate the computer with the access panel or any of the expansion card slot covers removed.
- Do not stack computers on top of each other or place computers so near each other that they are subject to each other's re-circulated or preheated air.
- If the computer is to be operated within a separate enclosure, intake and exhaust ventilation must be provided on the enclosure, and the same operating guidelines listed above will still apply.
- Keep liquids away from the computer and keyboard.
- Never cover the ventilation slots on the monitor with any type of material.
- Install or enable power management functions of the operating system or other software, including sleep states.
- Turn off the computer before you do either of the following:
  - Wipe the exterior of the computer with a soft, damp cloth as needed. Using cleaning products may discolor or damage the finish.
  - Occasionally clean the air vents on all vented sides of the computer. Lint, dust, and other foreign matter can block the vents and limit the airflow.

# Optical Drive Precautions

Be sure to observe the following guidelines while operating or cleaning the optical drive.

## Operation

- Do not move the drive during operation. This may cause it to malfunction during reading.
- Avoid exposing the drive to sudden changes in temperature, as condensation may form inside the unit. If the temperature suddenly changes while the drive is on, wait at least one hour before you turn off the power. If you operate the unit immediately, it may malfunction while reading.
- Avoid placing the drive in a location that is subject to high humidity, extreme temperatures, mechanical vibration, or direct sunlight.

## Cleaning

- Clean the panel and controls with a soft, dry cloth or a soft cloth lightly moistened with a mild detergent solution. Never spray cleaning fluids directly on the unit.
- Avoid using any type of solvent, such as alcohol or benzene, which may damage the finish.

## Safety

If any object or liquid falls into the drive, immediately unplug the computer and have it checked by an authorized HP service provider.

## Shipping Preparation

Follow these suggestions when preparing to ship the computer:

1. Back up the hard drive files on PD discs, tape cartridges, CDs, or USB flash drives. Be sure that the backup media is not exposed to electrical or magnetic impulses while stored or in transit.

---

 **NOTE:** The hard drive locks automatically when the system power is turned off.

---

2. Remove and store all removable media.
3. Turn off the computer and external devices.
4. Disconnect the power cord from the electrical outlet, then from the computer.
5. Disconnect the system components and external devices from their power sources, then from the computer.

---

 **NOTE:** Ensure that all boards are seated properly and secured in the board slots before shipping the computer.

---

6. Pack the system components and external devices in their original packing boxes or similar packaging with sufficient packing material to protect them.

# Index

- A**  
access panel  
    locking and unlocking 9, 52  
audio connectors 2, 4
- B**  
battery replacement 49
- C**  
computer  
    specifications 47  
computer access panel  
    removing 11  
    replacing 12  
computer operating guidelines 58  
connecting drive cables 29
- D**  
DIMMs. See memory  
drives  
    connecting cables 29  
    installing 29  
    locations 28
- E**  
electrostatic discharge, preventing  
    damage 57  
expansion card  
    installing 22  
    removing 22  
    slot locations 22  
expansion slot cover  
    removing 24  
    replacing 26
- F**  
FailSafe Key 9  
front bezel  
    removing 13  
    removing blanks 14
- G**  
guide screws 29
- H**  
hard drive  
    installing 39  
    installing secondary 38  
    removing 39  
headphone connector 2
- I**  
installation guidelines 8  
installing  
    battery 49  
    drive cables 29  
    expansion card 22  
    guide screws 29  
    hard drive 39  
    media card reader 38  
    memory 17  
    optical drive 33  
    removable hard drive 42  
    security locks 52
- K**  
keyboard  
    components 5  
    connector 4
- L**  
line-in connector 4  
line-out connector 4  
locks  
    cable lock 52  
    front bezel 55
- M**  
HP Business PC Security Lock 53  
padlock 53  
Smart Cover Lock 9
- N**  
media card reader  
    features 3  
    installing 38  
    removing 36  
memory  
    installing 17  
    populating sockets 18  
    specifications 17  
microphone connector 2  
monitor connector  
    DisplayPort 4  
    VGA 4  
mouse connector 4
- O**  
optical drive  
    cleaning 59  
    installing 33  
    precautions 59  
    removing 31
- P**  
PCI card 22, 25  
PCI Express card 22, 26  
power supply 47  
product ID location 7
- R**  
rear panel components 4  
removable hard drive  
    replacing 42

removing  
battery 49  
bezel blanks 14  
computer access panel 11  
expansion card 22  
expansion slot cover 24  
front bezel 13  
hard drive 39  
media card reader 36  
optical drive 31  
PCI card 25  
PCI Express card 26  
Smart Cover Lock 9

## S

security  
cable lock 52  
front bezel 55  
HP Business PC Security  
Lock 53  
padlock 53  
Smart Cover Lock 9  
serial connector 4  
serial number location 7  
shipping preparation 59  
Smart Cover Lock 9  
specifications  
computer 47  
memory 17  
system board drive  
connections 30

## T

tower orientation 16

## U

unlocking access panel 9, 52  
USB ports  
front panel 2  
rear panel 4

## V

ventilation guidelines 58

## W

Windows Logo key 5

# **Nmap Security Scanner: The Definitive Guide**

**Fyodor**

**Edited by**

**Nmap Security Scanner: The Definitive Guide**

by Fyodor

Edited by

First Edition

Published (TBA)

# Table of Contents

Preface.....	i
1. Foreword.....	i
2. What's Inside.....	i
3. Style Conventions.....	i
4. Examples .....	i
5. Comments and Questions.....	i
6. Acknowledgments .....	ii
<b>1. Getting Started with Nmap .....</b>	<b>1</b>
1.1. Introduction .....	1
1.2. Nmap overview and demonstration.....	1
1.2.1. Avatar Online .....	1
1.2.2. Saving the Human Race.....	6
1.2.3. MadHat in Wonderland.....	9
1.3. Legal issues .....	11
1.3.1. Is unauthorized port scanning a crime? .....	11
1.3.2. Can port scanning crash the target computer/networks? .....	16
1.3.3. Misc: Copyright, license, (lack of) warranty, export control information .....	16
<b>2. Obtaining, Installing, and Removing Nmap.....</b>	<b>20</b>
2.1. Introduction .....	20
2.1.1. Testing whether Nmap is already installed.....	20
2.1.2. Verifying the integrity of Nmap downloads .....	20
2.1.3. Command-line and graphical interfaces .....	21
2.2. UNIX Compilation and installation from source code.....	22
2.2.1. Configure directives .....	23
2.2.2. If you encounter compilation problems .....	24
2.3. Linux Distributions.....	25
2.3.1. RPM-based distributions (Red Hat, Mandrake, Suse, Fedora).....	25
2.3.2. Debian Linux .....	26
2.3.3. Gentoo Linux .....	26
2.3.4. Other Linux distributions.....	26
2.4. Windows .....	27
2.4.1. Command line .zip binaries .....	27
2.4.2. Nmapwin.....	29
2.4.3. Compile from source code.....	29
2.5. Sun Solaris.....	30
2.6. Apple Mac OS X .....	31
2.7. FreeBSD / OpenBSD / NetBSD .....	31
2.7.1. OpenBSD binary packages and source ports instructions .....	31
2.7.2. FreeBSD binary package and source ports instructions .....	32
2.7.3. NetBSD binary package instructions.....	32
2.8. Amiga, HP-UX, IRIX, and Other Platforms .....	33
2.9. [RECIPE] Installing Nmap on a PDA .....	33
2.9.1. Installing Nmap on the Zaurus .....	34
2.9.2. Using Nmap and NmapFE on the Zaurus.....	35
2.10. Removing Nmap.....	37

<b>3. Host Enumeration ("Ping Scanning") .....</b>	<b>39</b>
3.1. Introduction .....	39
3.2. Specifying Target Hosts and Networks .....	39
3.3. Host Enumeration Controls .....	39
3.3.1. List Scan (-sL) .....	39
3.3.2. Ping Scan (-sP) .....	40
3.3.3. Disable Ping (-p0).....	41
3.4. Host Enumeration Techniques.....	42
3.4.1. TCP SYN Ping (-PS[portlist]).....	43
3.4.2. TCP ACK Ping (-PA[portlist]).....	44
3.4.3. UDP Ping (-PU[portlist]) .....	45
3.4.4. ICMP Ping Types (-PE, -PP, and -PM).....	45
3.4.5. Default Combination (-PB) .....	45
3.4.6. ARP Scan (-P?).....	46
3.5. Putting it All Together: Host Enumeration Strategies.....	46
3.5.1. Related Options .....	46
3.5.2. Choosing and Combining Ping Options .....	48
3.6. Finding an Organization's IP addresses to Scan .....	51
3.7. Host Enumeration Code Algorithms .....	51
<b>4. Port Scanning Overview .....</b>	<b>53</b>
4.1. Introduction to Port Scanning .....	53
4.1.1. What exactly is a port? .....	53
4.1.2. What is port scanning?.....	56
4.1.3. Why scan ports?.....	57
4.2. A Quick Port Scanning Tutorial .....	58
4.3. Command-line flags .....	60
4.3.1. Selecting scan techniques .....	60
4.3.2. Selecting ports to scan .....	62
4.3.3. Timing-related options.....	62
4.3.4. Output format and verbosity options .....	63
4.3.5. Firewall and IDS evasion options .....	64
4.3.6. Specifying targets .....	65
4.3.7. Miscellaneous options .....	65
4.4. IPv6 Scanning [-6] .....	66
4.5. [RECIPE] Scanning a large network for a certain open TCP port.....	66
4.5.1. Problem.....	67
4.5.2. Solution.....	67
4.5.3. Discussion.....	67
4.5.4. See Also .....	72
<b>5. Port Scanning Techniques and Algorithms .....</b>	<b>73</b>
5.1. Introduction .....	73
5.2. TCP SYN (Stealth) Scan .....	74
5.3. TCP Connect() Scan.....	77
5.4. UDP Scan .....	79
5.4.1. Disambiguating open from filtered UDP ports.....	80
5.4.2. Speeding up UDP scans.....	82
5.5. TCP Null, FIN, and Xmas Scans.....	83

5.6. Custom scan types with --scanflags .....	86
5.6.1. Custom SYN/FIN scan .....	86
5.6.2. PSH scan .....	87
5.7. TCP ACK Scan.....	88
5.8. TCP Window Scan .....	89
5.9. TCP Maimon Scan .....	91
5.10. TCP Idle Scan.....	92
5.10.1. Finding a working idle scan zombie host .....	94
5.10.2. Executing an Idle scan .....	94
5.10.3. Idle scan implementation algorithms.....	95
5.11. IP Protocol Scan .....	99
5.12. TCP FTP Bounce Scan.....	101
5.13. Scan Code and Algorithms.....	102
5.13.1. Network condition monitoring .....	102
5.13.2. Host and port parallelization.....	103
5.13.3. Round trip time estimation .....	103
5.13.4. Congestion control.....	104
5.13.5. Port scan pings.....	104
5.13.6. Inferred neighbor times.....	104
5.13.7. Adaptive retransmission .....	105
5.13.8. Scan delay .....	105
<b>6. Optimizing Nmap Performance.....</b>	<b>106</b>
<b>7. Service and Application Version Detection.....</b>	<b>107</b>
7.1. Introduction .....	107
7.2. Usage/Examples .....	108
7.3. Technique Described .....	110
7.4. Technique Demonstrated.....	111
7.5. Post-processors.....	114
7.5.1. RPC Grinding .....	114
7.5.2. SSL Post-processor notes .....	115
7.6. nmap-service-probes File Format .....	116
7.6.1. The probe directive .....	116
7.6.2. The match directive .....	117
7.6.3. The softmatch directive.....	118
7.6.4. The ports and sslports directives.....	118
7.6.5. The totalwaitms directive .....	119
7.6.6. Putting it all together .....	119
7.7. Community Contributions.....	119
7.8. [RECIPE] Find all servers running an insecure or nonstandard version of an application.....	121
7.9. [RECIPE] Hack version detection to suit custom needs, such as open proxy detection.....	121
<b>8. OS Fingerprinting.....</b>	<b>122</b>
<b>9. Detecting and Subverting Firewalls and Intrusion Detection Systems.....</b>	<b>123</b>
9.1. Introduction .....	123
9.2. Why would whitehats ever do this?.....	123
9.3. Determining Firewall Rules .....	124
9.3.1. Standard SYN scan.....	124
9.3.2. ACK scan.....	125

9.3.3. IPID tricks.....	127
9.3.4. UDP version scanning .....	129
9.4. Bypassing Firewall Rules.....	130
9.4.1. Exotic scan flags .....	130
9.4.2. Source port manipulation.....	131
9.4.3. IPv6 attacks.....	132
9.4.4. IPID Idle Scanning .....	133
9.4.5. Multiple ping probes.....	133
9.4.6. Fragmentation.....	134
9.4.7. Proxies .....	134
9.4.8. Source routing.....	135
9.4.9. FTP Bounce Scan .....	135
9.4.10. Take an alternative path .....	135
9.5. Subverting Intrusion Detection Systems .....	136
9.5.1. Intrusion detection system detection .....	136
9.5.2. Avoiding intrusion detection systems.....	138
9.5.3. Misleading intrusion detection systems.....	142
9.5.4. Exploiting intrusion detection systems.....	144
9.5.5. Ignoring intrusion detection systems .....	145
9.6. Detecting packet forgery by firewall and intrusion detection systems.....	145
9.6.1. Look for TTL consistency .....	146
9.6.2. Look for IPID and sequence number consistency .....	147
9.6.3. The Bogus Checksum trick.....	147
9.6.4. Close Analysis of packet headers and contents .....	148
9.6.5. Unusual network uniformity .....	148
<b>10. Defenses against Nmap .....</b>	<b>149</b>
10.1. Introduction .....	149
10.2. Proactive Scanning .....	149
10.3. Blocking and Slowing Nmap with Firewalls.....	149
10.4. Detecting Nmap Scans .....	150
10.5. Clever Trickery .....	151
10.5.1. Hiding Services on Obscure Ports .....	152
10.5.2. Port knocking.....	153
10.5.3. Honeypots and Honeynets .....	154
10.5.4. OS Spoofing.....	155
10.5.5. Tar pits .....	156
10.5.6. Reactive port scan detection .....	156
10.5.7. Escalating arms race .....	157
<b>11. Nmap Output Formats .....</b>	<b>158</b>
11.1. Introduction .....	158
11.2. Command-line flags .....	159
11.2.1. Controlling output type.....	159
11.2.2. Controlling verbosity of output .....	160
11.2.3. Enabling debugging output.....	163
11.2.4. Enabling packet tracing .....	164
11.2.5. Resuming canceled scans .....	165
11.3. Interactive output.....	165

11.4. Normal output (-oN) .....	165
11.5. \$crIpT kIddI3 0uTPut (-oS) .....	166
11.6. XML output (-oX).....	167
11.6.1. Using XML Output.....	169
11.7. Manipulating XML output with Perl.....	170
11.8. Output to a database .....	172
11.9. Creating HTML reports.....	173
11.10. Grepable output (-oG).....	173
11.10.1. Grepable output fields.....	174
11.10.2. Parsing grepable output on the command line.....	178
<b>12. Understanding and Customizing Nmap Data Files .....</b>	<b>179</b>
12.1. Introduction .....	179
12.2. nmap-services .....	179
12.3. nmap-service-probes.....	180
12.4. nmap-rpc.....	181
12.5. nmap-os-fingerprints.....	182
12.6. nmap-mac-prefixes .....	183
12.7. nmap-protocols.....	183
12.8. Using Customized Data Files.....	184
<b>13. Nmap Cookbook .....</b>	<b>186</b>
<b>14. The History and Future of Nmap .....</b>	<b>187</b>
<b>15. Nmap Reference Guide.....</b>	<b>188</b>
<b>A. Nmap XML Output DTD .....</b>	<b>189</b>
A.1. .....	189
<b>B. Appendix A: Complementary Tools .....</b>	<b>195</b>

# List of Tables

2-1. The Sharp Zaurus is an excellent platform for highly mobile security applications .....	33
3-1. Valuable TCP probe ports, in descending order of accessibility .....	48
5-1. ICMP destination unreachable (type 3) code values .....	74
5-2. How Nmap interprets responses to a SYN probe .....	76
5-3. How Nmap interprets responses to a UDP probe .....	79
5-4. How Nmap interprets responses to a Null, FIN, or Xmas scan probe .....	83
5-5. How Nmap interprets responses to an ACK scan probe .....	88
5-6. How Nmap interprets responses to a Window scan ACK probe .....	89
5-7. How Nmap interprets responses to a Maimon scan probe .....	91
5-8. How Nmap interprets responses to an IP protocol probe .....	100

# List of Figures

1-1. Trinity begins her assault .....	7
1-2. Trinity Scans the Matrix .....	8
1-3. Terminal-view of the hack .....	8
1-4. Strong opinions on port scanning legality and morality .....	11
2-1. NmapFE presents a simple graphical interface to Nmap .....	21
2-2. Executing Nmap from a Windows command shell .....	28
2-3. NmapWin provides a slick Windows interface to Nmap .....	29
2-4. The Sharp Zaurus SL-C760 PDA .....	36
2-5. The SL-C760 executing Nmap in a terminal window .....	36
4-1. IPv4 Header Layout .....	53
4-2. TCP Header Layout .....	53
4-3. UDP Header Layout .....	54
5-1. ICMPv4 Destination Unreachable Header Layout .....	73
5-2. SYN scan of open port 22 .....	75
5-3. SYN scan of closed port 113 .....	75
5-4. SYN scan of filtered port 139 .....	76
5-5. Connect scan of open port 22 ( <code>nmap -sT -p22 scanme.nmap.org</code> ) .....	78
5-6. Idle Scan Technique (Simplified) .....	92
9-1. BlackIce discovers an unusual intruder .....	137
9-2. An attacker masked by dozens of decoys .....	142
11-1. Reading XML in a web browser .....	169

# List of Examples

1-1. Nmap list scan against Avatar Online IP addresses .....	2
1-2. Nmap results against an AO firewall .....	4
1-3. Another interesting AO machine .....	5
1-4. Nmap-diff typical output .....	10
1-5. Nmap-report execution .....	11
2-1. Checking for Nmap and determining its version number .....	20

2-2. Verifying the Nmap download checksum.....	21
2-3. Installing Nmap from binary RPMs .....	25
2-4. Building and installing Nmap from source RPMs.....	26
3-1. Enumerating hosts surrounding WWW.Stanford.Edu with list scan.....	40
3-2. Attempts to ping popular Internet hosts .....	42
3-3. Retry Host Enumeration using port 80 SYN probes .....	43
3-4. Attempted ACK ping against Microsoft.....	44
3-5. Generating 50,000 IP Addresses, then ping scanning with default options .....	50
3-6. Repeating ping scan with extra probes .....	51
4-1. Viewing and increasing the ephemeral port range on Linux .....	55
4-2. Simple scan: nmap scanme.nmap.org.....	58
4-3. More complex: nmap -p0- -v -A -T4 scanme.nmap.org.....	59
4-4. A simple IPv6 scan.....	66
4-5. Discovering Playboy's IP space.....	67
4-6. Pinging Playboy's Web Server for a Latency Estimate .....	68
4-7. Digging through Playboy's DNS records .....	68
4-8. Pinging the MX servers .....	69
4-9. TCP Pinging the MX servers.....	70
4-10. Launching the scan .....	71
4-11. Egrep for open ports .....	71
5-1. A SYN Scan showing three port states.....	74
5-2. Using --packet_trace to understand a SYN scan.....	77
5-3. Connect scan example .....	78
5-4. UDP scan example.....	79
5-5. UDP scan example.....	80
5-6. Improving Felix's UDP scan results with version detection .....	80
5-7. Improving Scanme's UDP scan results with version detection .....	81
5-8. Attempting to disambiguate UDP ports with TTL discrepancies.....	81
5-9. Example FIN and Xmas scans.....	84
5-10. SYN scan of docsrv.caldera.com .....	85
5-11. FIN scan of docsrv.caldera.com .....	85
5-12. A SYN/FIN scan of Google.....	87
5-13. A custom PSH scan .....	87
5-14. A Typical ACK Scan .....	88
5-15. An ACK scan of Docsrv .....	89
5-16. Window scan of docsrv.caldera.com .....	90
5-17. A failed Maimon scan.....	91
5-18. An Idle scan against the RIAA .....	95
5-19. IPID scan packet trace .....	96
5-20. IP protocol scan of a router and a typical Linux 2.4 box.....	100
5-21. Attempting an FTP bounce scan.....	101
5-22. Successful FTP bounce scan.....	102
7-1. Simple usage of version detection .....	107
7-2. Version detection against WWW.Microsoft.Com .....	108
7-3. Complex version detection .....	109
7-4. Detailed trace of version detection .....	111
7-5. Enumerating RPC services with rpcinfo .....	114
7-6. Nmap direct RPC scan.....	115

7-7. Version scanning through SSL .....	116
9-1. Detection of closed and filtered TCP ports.....	124
9-2. ACK scan against Scanme.....	125
9-3. Contrasting SYN and ACK scans against Para .....	126
9-4. UDP scan against firewalled host .....	129
9-5. UDP version scan against firewalled host.....	130
9-6. FIN scan against stateless firewall .....	130
9-7. Bypassing Windows IPsec filter using source port 88.....	131
9-8. Comparing IPv4 and IPv6 scans.....	132
9-9. Exploiting a printer with the FTP bounce scan .....	135
9-10. Host names can be deceiving.....	137
9-11. Noting TTL gaps with traceroute .....	138
9-12. Slow scan to bypass the default Snort 2.2.0 Flow-portscan fixed time scan detection method .....	139
9-13. Default Snort rules referencing Nmap.....	141
9-14. Detection of closed and filtered TCP ports.....	146
9-15. Testing IPID sequence number consistency .....	147
10-1. An all-tcp-port version scan .....	152
10-2. Deceiving Nmap with IP Personality .....	155
11-1. Scanrand output against a local network .....	158
11-2. Grepding for verbosity conditionals .....	161
11-3. A comparison of interactive output with and without verbosity enabled.....	162
11-4. Some representative debugging lines .....	163
11-5. Using --packet_trace to detail a ping scan of Scanme .....	164
11-6. A typical example of normal output .....	166
11-7. A typical example of \$crIpt KiDDi3 0utPut.....	166
11-8. An example of Nmap XML output.....	167
11-9. Nmap XML port elements.....	168
11-10. Nmap::Parser sample code .....	171
11-11. Nmap::Scanner sample code .....	172
11-12. A typical example of grepable output.....	173
11-13. Grepable output for IP protocol scan.....	176
11-14. Ping scan grepable output.....	177
11-15. List scan grepable output.....	177
11-16. Parsing grepable output on the command line.....	178
12-1. Excerpt from nmap-services .....	179
12-2. Excerpt from nmap-service-probes .....	181
12-3. Excerpt from nmap-rpc .....	181
12-4. Excerpt from nmap-os-fingerprints.....	182
12-5. Excerpt from nmap-mac-prefixes .....	183
12-6. Excerpt from nmap-protocols.....	184

# Preface

## 1. Foreword

Blah blah blah ... see preface example from dblite distribution when I am ready to write this section

## 2. What's Inside

The book is organized into the following chapters:

## 3. Style Conventions

Items appearing in the book are sometimes given a special appearance to set them apart from the regular text. Here's how they look:

## 4. Examples

The examples from this book are freely downloadable from the book's web site at  
<http://www.oreilly.com/catalog/learnxml>.

## 5. Comments and Questions

We have tested and verified the information in this book to the best of our ability, but you may find that features have changed (or even that we have made mistakes!). Please let us know about any errors you find, as well as your suggestions for future editions, by writing to:

O'Reilly & Associates, Inc.  
101 Morris Street  
Sebastopol, CA 95472  
(800) 998-9938 (in the United States or Canada)  
(707) 829-0515 (international or local)  
(707) 829-0104 (fax)

We have a web page for this book, where we list errata, examples, or any additional information. You can access this page at:

<http://www.oreilly.com/catalog/learnxml>

To comment or ask technical questions about this book, send email to:

[bookquestions@oreilly.com](mailto:bookquestions@oreilly.com)

You can sign up for one or more of our mailing lists at:

<http://elists.oreilly.com>

For more information about our books, conferences, software, Resource Centers, and the O'Reilly Network, see our web site at:

<http://www.oreilly.com>

## **6. Acknowledgments**

Thanks to everyone who contributed.....

# Chapter 1. Getting Started with Nmap

## 1.1. Introduction

On September 1, 1997, I released a security scanner named Nmap in the fifty-first issue of Phrack magazine. My goal was to consolidate the fragmented field of special-purpose port scanners into one powerful and flexible free tool, providing a consistent interface and efficient implementation of all practicable port scanning techniques. Nmap then consisted of 3 files (barely 2,000 lines of code) and supported only the Linux operating system. It was written for my own purposes, and released in the hope that others would find it useful.

From these humble beginnings, and through the power of Open Source development, Nmap grew into the world's most popular network security scanner<sup>1</sup>. Over the years, Nmap has continued to add advanced functionality such as remote OS detection via TCP/IP fingerprinting, version/service detection, IPID Idle scanning, and fast multi-probe ping scanning. All major Windows and UNIX platforms are now supported. Nmap has been recognized as "security tool of the year" by publications including *Linux Journal*, *Info World*, *LinuxQuestions.Org*, and the *Codetalker Digest*. It was even featured in several movies, including the 2003 hit *The Matrix Reloaded*.

Nmap was designed for security auditors to explore a network and discover potential vulnerabilities. Many systems and network administrators have also found it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

This chapter uses fictional stories to provide a broad overview of Nmap and how it is typically used. An important legal section helps users avoid (or at least be aware of) controversial usage that could leave them expelled from their ISP or even facing civil or criminal charges. It also discusses the risks of crashing remote machines as well as miscellaneous issues such as the Nmap license (GNU GPL), copyright, and export control restrictions. Readers can then move to chapter two (download/installation) with an understanding of why to use Nmap and how to do so safely.

## 1.2. Nmap overview and demonstration

Sometimes the best way to understand something is to see it in action. This section includes examples of Nmap being used in (mostly) fictional yet typical circumstances. Nmap newbies should not expect to understand everything at once. This is simply a broad overview of features that are described in depth in later chapters. The "recipes" included throughout this book (index in Chapter 11) demonstrate many other common Nmap tasks for both security auditors and network administrators.

### 1.2.1. Avatar Online

Felix dutifully arrives at work on December 15th, although he does not expect many structured tasks. The small San Francisco penetration-testing firm he works for has been very quiet lately, due to impending holidays. Felix is able to spend business hours pursuing his latest hobby of building powerful Wi-Fi antennas for wireless assessments and war driving exploration. Nevertheless, Felix is hoping for more business. Hacking has been his hobby and fascination since a childhood spent learning everything he could about networking, security, UNIX, and phone systems. Occasionally his curiosity took him too far, and Felix was almost swept up in the 1990 Operation Sundevil prosecutions. Fortunately Felix emerged from adolescence without a criminal record, while retaining his expert knowledge of security weaknesses. As a professional, he is now able to perform the same types of network intrusions as before, but with the added benefit of contractual immunity from prosecution and even a paycheck! Rather than having to keep his creative exploits secret, he is able to brag about them to client management when presenting his

reports. So Felix was not disappointed when his boss interrupted his antenna soldering to announce that the sales department finally closed a pen-testing deal with the Avatar Online gaming company.

Avatar Online (AO) is a small company working to create the next generation of massive multi-player online role-playing games (MMORPGs). Their product, inspired by the Metaverse envisioned in Neil Stevenson's *Snow Crash*, is fascinating but still highly confidential. After witnessing the high-profile leak (<http://www.smh.com.au/articles/2003/10/03/1064988378345.html>) of Valve Software's upcoming game source code, AO quickly hired the security consultants. Felix's task is to initiate an external (from outside the firewall) vulnerability assessment while his partners work on physical security, source code auditing, social engineering, and so forth. Felix is permitted to exploit any vulnerabilities found.

The first step in a vulnerability assessment is network discovery. This reconnaissance stage determines what IP address ranges the target is using, what hosts are available and what services those hosts are offering, general network topology details, and what firewall/filtering policies are in effect.

Determining the IP ranges to scan would normally be an elaborate process involving ARIN (or other geographical registry) lookups, DNS queries and zone transfer attempts, various web sleuthing techniques, and more. But in this case, Avatar Online explicitly specified what networks they want tested: the corporate network on 6.209.42.0/24 and their production/DMZ systems residing on 6.207.0.0/22. Felix checks the ARIN IP allocation records anyway and confirms that these IP ranges belong to AO<sup>2</sup>. Felix subconsciously decodes the CIDR notation and recognizes this as 1,280 IP addresses. No problem.

Being the careful type, Felix first starts out with what is known as an Nmap list scan (-sL option). This Nmap feature simply enumerates every IP address in the given target netblock(s) and does a reverse-DNS lookup (unless -n was specified) on each. One reason to do this first is stealth. The names of the hosts can hint at potential vulnerabilities and allow for a better understanding of the target network, all without raising alarm bells<sup>3</sup>. Felix is doing this for another reason - to double-check that the IP ranges are correct. The systems administrator who provided the IPs might have made a mistake, and scanning the wrong company would be a disaster. The contract signed with Avatar Online may act as a get-out-of-jail-free card for penetrating their networks, but will not help if Felix accidentally roots another company's server! The command he uses and an excerpt of the results are shown in Example 1-1.

### **Example 1-1. Nmap list scan against Avatar Online IP addresses**

```
felix> nmap -sL 6.209.24.0/24 6.207.0.0/22

Starting nmap 3.49 ( http://www.insecure.org/nmap/ )
Host 6.209.24.0 not scanned
Host fw.corp.avataronline.com (6.209.24.1) not scanned
Host dev2.corp.avataronline.com (6.209.24.2) not scanned
Host 6.209.24.3 not scanned
Host 6.209.24.4 not scanned
Host 6.209.24.5 not scanned
...
Host dhcp-21.corp.avataronline.com (6.209.24.21) not scanned
Host dhcp-22.corp.avataronline.com (6.209.24.22) not scanned
Host dhcp-23.corp.avataronline.com (6.209.24.23) not scanned
Host dhcp-24.corp.avataronline.com (6.209.24.24) not scanned
Host dhcp-25.corp.avataronline.com (6.209.24.25) not scanned
Host dhcp-26.corp.avataronline.com (6.209.24.26) not scanned
...
Host 6.207.0.0 not scanned
Host gw.avataronline.com (6.207.0.1) not scanned
```

```

Host ns1.avataaronline.com (6.207.0.2) not scanned
Host ns2.avataaronline.com (6.207.0.3) not scanned
Host ftp.avataaronline.com (6.207.0.4) not scanned
Host 6.207.0.5 not scanned
Host 6.207.0.6 not scanned
Host www.avataaronline.com (6.207.0.7) not scanned
Host 6.207.0.8 not scanned
...
Host cluster-c120.avataaronline.com (6.207.2.120) not scanned
Host cluster-c121.avataaronline.com (6.207.2.121) not scanned
Host cluster-c122.avataaronline.com (6.207.2.122) not scanned
Host cluster-c123.avataaronline.com (6.207.2.123) not scanned
Host cluster-c124.avataaronline.com (6.207.2.124) not scanned
...
Host 6.207.3.253 not scanned
Host 6.207.3.254 not scanned
Host 6.207.3.255 not scanned
Nmap run completed -- 1280 IP addresses (0 hosts up) scanned in 330.694 seconds
felix>

```

Reading over the results, Felix finds that all of the machines with reverse-DNS entries resolve to Avatar Online. No other businesses seem to share the IP space. Moreover, these results give Felix a rough idea of how many machines are in use and a good idea of what many are used for. He is now ready to get a bit more intrusive and try a port scan. He uses Nmap features that try to determine the application and version number of each service listening on the network. He also requests that Nmap try to guess the remote operating system via a series of low-level TCP/IP probes known as OS fingerprinting. This sort of scan is not at all stealthy, but that does not concern Felix. He is interested in whether the admins of AO even notice these blatant scans. After a bit of consideration, Felix settles on the following command:

```
nmap -ss -p- -PS22,80,113,33334 -PA80,113,21000 -PU19000 -PE -A -T4 -oA
avatartcpscan-121503 6.209.24.0/24 6.207.0.0/22
```

These options are described in later chapters, but here is a quick summary of them.

**-sS**

Enables the efficient TCP port scanning technique known as SYN scan. Felix would have added a U at the end if he also wanted to do a UDP scan, but he is saving that for later. SYN scan is the default scan type, but stating it explicitly does not hurt.

**-p-**

Requests that Nmap scan *every* port from 1-65535. The default is to scan only ports one through 1024, plus about 600 others explicitly mentioned in the nmap-services database. This option format is simply a short cut for -p1-65535. He could have specified -p0-65535 if he wanted to scan the rather illegitimate port zero as well. The -p option has a very flexible syntax, even allowing the specification of a differing set of UDP and TCP ports.

**-PS22,80,113,33334 -PA80,113,21000 -PU19000 -PE**

These are all "ping" types used in combination to determine whether a host is really available and avoid wasting a lot of time scanning IP addresses that are not in use. This particular incantation sends a TCP SYN packet to ports 22, 80, 113, and 33334; a TCP ACK packet to ports 80, 113, and 21000; a UDP packet to port 19000; and

a normal ICMP echo request packet. If Nmap receives a response from the target host itself to any of these probes, it considers the host to be up and available for scanning. This is more extensive than the Nmap default, which simply sends an echo request and an ACK packet to port 80. In a pen-testing situation, you often want to scan every host even if they do not seem to be up. After all, they could just be heavily filtered in such a way that the probes you selected are ignored but some other obscure port may be available. To scan every IP whether it shows an available host or not, specify the `-P0` option instead of all of the above. Felix starts such a scan in the background, though it may take a day to complete.

#### `-A`

This shortcut option turns on *advanced* and *aggressive* features such as OS and service detection. At the time of this writing it is equivalent to `-sV -O` (version/service and remote operating system detection), though more features may be added to `-A` later.

#### `-T4`

Adjusts timing to the "aggressive" level (#4 of 5). This is the same as specifying `-T aggressive`, but does not require the same level of spelling competence. In general, the `-T4` option is recommended if the connection between you and the target networks are faster than modem dialups.

#### `-oA avatartcpscan-121503`

Outputs results in every format (normal, XML, grepable) to files named `avatartcpscan-121503.extension` where `extension` are `.nmap`, `.xml`, and `.gnmap` respectively. All of the output formats include the start date and time, but Felix likes to note the date explicitly in the filename. Normal output and errors are still sent to `stdout`<sup>4</sup> as well.

#### 6.209.24.0/24 6.207.0.0/22

These are the Avatar Online netblocks discussed above. They are given in CIDR notation, but Nmap allows them to be specified in many other formats. For example, `6.209.24.0/24` could instead be specified as `6.209.24.0-255`.

Since such a comprehensive scan against more than a thousand IP addresses could take a while, Felix simply starts it executing and resumes work on his Yagi antenna. A couple hours later he notices that it has finished and takes a peek at the results. Example 1-2 shows one of the machines discovered.

#### **Example 1-2. Nmap results against an AO firewall**

```
Interesting ports on fw.corp.avataronline.com (6.209.24.1):
(The 65530 ports scanned but not shown below are in state: filtered)
PORT      STATE    SERVICE        VERSION
22/tcp     open     ssh          OpenSSH 3.7.1p2 (protocol 1.99)
53/tcp     open     domain       ISC Bind 9.2.1
110/tcp    open     pop3         Courier pop3d
113/tcp    closed   auth
143/tcp    open     imap         Courier Imap 1.6.X - 1.7.X
3128/tcp   open     http-proxy   Squid webproxy 2.2.STABLE5
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 3.134 days (since Mon Dec 12 11:49:58 2003)
```

To the trained eye, this conveys substantial information about AO's security posture. Felix first notes the reverse DNS name - this machine is apparently meant to be a firewall for their corporate network. The next line is important, but all too often ignored. It states that the vast majority of the ports on this machine are in the `filtered` state. This means that Nmap is unable to reach the port because it is blocked by firewall rules. The fact that all ports except for a few chosen ones are in this state is a sign of security competence. Deny-by-default is a security mantra for good reasons - it means that even if someone accidentally left SunRPC (port 111) open on this machine, the firewall rules would prevent us (attackers) from communicating with it.

Felix then looks at every port line in turn. The first port is Secure Shell (OpenSSH). Version 3.7.1p2 is very recent (as of December 15, 2003). The administrators probably upgraded it because of the potentially exploitable buffer management bugs affecting earlier versions. This is another hint that the administrator knows what they are doing. A truly paranoid sysadmin would only allow ssh connections from certain trusted IP addresses, but one can argue for open access in case the administrator needs emergency access while far from home. Security often involves trade-offs, and this one may be justifiable. Felix makes a note to try his brute force password cracker and especially his private timing-based ssh user enumeration tool against the server.

Felix is not so charitable about port 53. It is running ISC bind, which has a long history of remotely exploitable security holes. Visit the Bind security page (<http://www.isc.org/products/BIND/bind-security.html>) for further details. Bind 9.2.1 even has a potentially exploitable buffer overflow, although the default build is not vulnerable. Felix checks and finds that this server is not vulnerable to the libbind issue, but that is besides the point. This server almost certainly should not be running an externally-accessible nameserver. A firewall should only run the bare essentials to minimize the risk of a disastrous compromise. Besides, this server is not authoritative for any domains - the real nameservers are on the production network. An administrator probably only meant for clients within the firewall to contact this nameserver, but he did not bother locking it down to only the internal interface. Felix will later try to gather important information from this unnecessary server using zone transfer requests and intrusive queries. He may attempt cache poisoning as well. By spoofing the IP of `windowsupdate.microsoft.com` or another important download server, Felix may be able to trick unsuspecting internal client users into running a trojan-horse program that provides him with full network access behind the firewall.

The next two open ports are 110 (pop3) and 143 (imap). Note that 113 (auth) in between them is `closed` instead of `open`. Pop3 and Imap are mail retrieval services which, like Named, have no legitimate place on this server. They are also a security risk in that they generally transfer the mail and (even worse) authentication credentials unencrypted. Users should probably VPN in and check their mail from an internal server. These ports could also be wrapped in SSL encryption. Nmap would have then listed the services as "ssl/pop3" and "ssl/imap". Felix will try his user enumeration and password guessing attacks on these services, which will probably be much more effective than against ssh.

The final open port is a Squid proxy. This is another service that may have been intended for internal client use and should not be accessible from the outside (and particularly not on the firewall). Felix's initially positive opinion of the AO security administrators drops further. Felix will test whether he can abuse this proxy to connect to other sites on the Internet. Spammers and malicious hackers often use proxies in this way to hide their tracks. Even more critical, Felix will try to proxy his way into the *internal* network. This common attack is how Adrian Lamo (<http://www.freelamo.org/>) broke into the New York Times internal network in 2002. Lamo was caught after he called reporters to brag about his exploits against the NY Times and other companies in detail (<http://www.securityfocus.com/news/340>).

The following lines disclose that this is a Linux box, which is valuable information when attempting exploitation. The low 3-day uptime was detected during OS fingerprinting by sending several probes for the TCP timestamp option value and extrapolating the line back to zero.

Felix then examines the Nmap output for another machine, as shown in Example 1-3

**Example 1-3. Another interesting AO machine**

```
Interesting ports on dhcp-23.corp.avataronline.com (6.209.24.23):
(The 65526 ports scanned but not shown below are in state: closed)
PORT      STATE     SERVICE      VERSION
135/tcp    filtered msrpc
136/tcp    filtered profile
137/tcp    filtered netbios-ns
138/tcp    filtered netbios-dgm
139/tcp    filtered netbios-ssn
445/tcp    open      microsoft-ds Microsoft Windows XP microsoft-ds
1002/tcp   open      windows-icfw?
1025/tcp   open      msrpc          Microsoft Windows msrpc
16552/tcp  open      unknown
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Professional RC1+ through final release
```

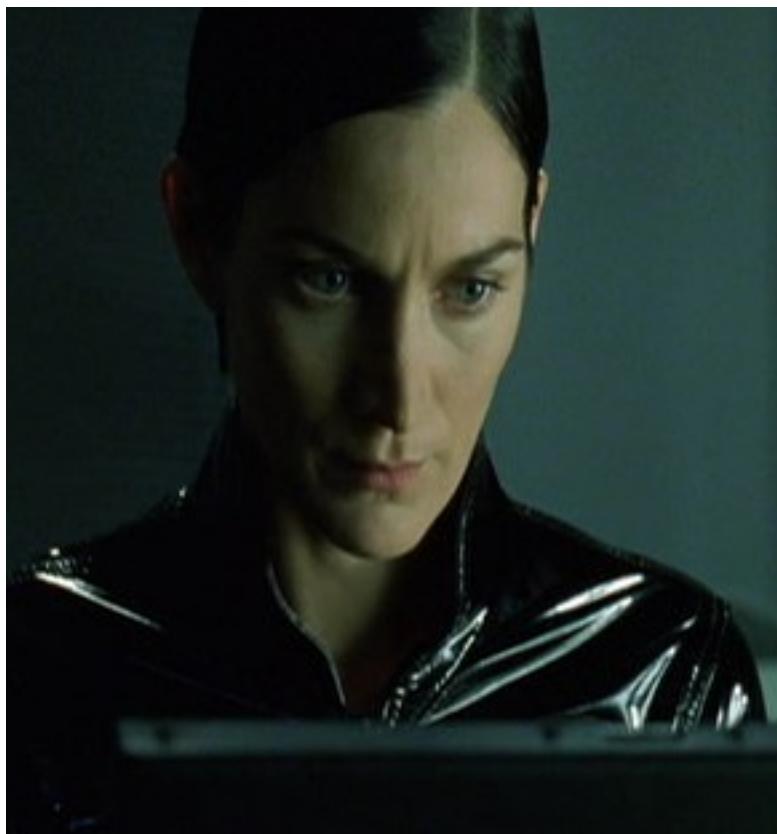
Felix smiles when he spies this Windows XP box on the Network. Thanks to a recent spate of MS RPC vulnerabilities, those machines are often trivial to compromise. The second line shows that the default state is closed, meaning the firewall does not have the same deny-by-default policy for this machine as for itself. Instead they tried to specifically block the Windows ports they consider dangerous on 135-139. This filter is woefully inadequate, as MS exports MS RPC functionality on many other ports in Windows XP. TCP ports 445 and 1025 are two examples on this scan. While Nmap failed to recognize 16552, Felix has seen this pattern enough to know that it is probably the MS Messenger Service. If AO had been using deny-by-default filtering, port 16552 would not be accessible in the first place. Looking through the results page, Felix sees several other Windows machines on this DHCP network. Felix cannot wait to try his favorite DCOM RPC exploit against them. It was written by HD Moore and is available at <http://www.metasploit.com/tools/dcom.c>. If that fails, there are a couple newer MS RPC vulnerabilities he will try.

Felix continues poring over the results for vulnerabilities he can leverage to compromise the network. On the production network, he sees that gw.avataronline.com is a Cisco router that also acts as a rudimentary firewall for the systems. They fall into the trap of only blocking "privileged ports" (those under 1024), which leaves a bunch of vulnerable SunRPC and other services accessible on that network. The machines with names like clust-\* each have dozens of ports open that Nmap does not recognize. There are probably custom daemons running the AO game engine. www.avataronline.com is a Linux box with an open Apache server on the http and https ports. Unfortunately, it is linked with an exploitable version of the OpenSSL library. Oops! Before the sun sets, Felix has gained privileged access to hosts on both the corporate and production networks.

*As Felix has demonstrated, Nmap is frequently used by security auditors and network administrators to help locate vulnerabilities on client/corporate networks. Subsequent chapters describe the techniques used by Felix, as well as many other Nmap features, in much greater detail.*

## 1.2.2. Saving the Human Race

**Figure 1-1. Trinity begins her assault**



Trinity is in quite a pickle! Having discovered that the world we take for granted is really a virtual "Matrix" run by machine overlords, Trinity decides to fight back and free the human race from this mental slavery. Making matters worse, her underground colony of freed humans (Zion) is under attack by 250,000 powerful alien sentinels. Her only hope involves deactivating the emergency power system for 27 city blocks in less than 5 minutes. The previous team died trying. In life's bleakest moments when all hope seems to be lost, what should you turn to? Nmap, of course! But not quite yet.

She first must defeat the perimeter security, which on many networks involves firewalls and intrusion detection systems (IDS). She is well aware of advanced techniques for circumventing these devices (covered later in this book). Unfortunately, the emergency power system admins knew better than to connect such a critical system to the Internet, even indirectly. No amount of source routing or IPID spoofed scanning will help Trinity overcome this "air gap" security. Thinking fast, she devises a clever plan that involves jumping her motorcycle off the rooftop of a nearby building, landing on the power station guard post, and then beating up all of the security guards. This advanced technique is not covered in any physical security manual, but proved highly effective. This demonstrates how clever hackers research and devise their own attacks, rather than always utilizing the script-kiddie approach of canned exploits.

Trinity fights her way to the computer room and sits down at a terminal. She quickly determines that the network is using the RFC1918-blessed 10.0.0.0/8 private network. A ping to the network address generates responses from dozens of machines. An Nmap "ping scan" would have provided a more comprehensive list of available machines,

but using the broadcast technique saved precious seconds. Then she whips out Nmap<sup>5</sup>. The terminal has version 2.54BETA25 installed. This version is ancient (2001) and less efficient than newer releases, but Trinity had no time to install a better version from the future. This job will not take long anyway. She runs the command **nmap -v -ss -o 10.2.1.3**. This executes a TCP SYN scan and OS detection against 10.2.1.3 and provides verbose output. The host appears to be a security disaster - AIX 3.2 with well over a dozen ports open. Unfortunately, this is not the machine she needs to compromise. So she runs the same command against 10.2.2.2. This time the target OS is unrecognized (she should have upgraded Nmap!) and only has port 22 open. This is the Secure Shell encrypted administration service. As any sexy PVC-clad hacker goddess knows, many SSH servers around that time (2001) had an exploitable vulnerability in the CRC32 compensation attack detector. Trinity whips out an all-assembly-code exploit written by her or her fallen comrade, and utilizes the exploit to change the root password of the target box to "Z10N0101". Trinity uses much more secure passwords under normal circumstances. She logs in as root and issues a command to disable the emergency backup power system for 27 city blocks, finishing just in time! Here are some shots of the action - squint just right and you should be able to read the text.

**Figure 1-2. Trinity Scans the Matrix**



**Figure 1-3. Terminal-view of the hack**

In addition, a terminal-view video showing the whole hack is available on the Internet. At least it will be until the MPAA finds out and sends sentinels or lawyers after the webmasters.

### 1.2.3. MadHat in Wonderland

This story differs from the previous ones in that it is actually true. Written by frequent Nmap user and contributor MadHat, it describes how he enhanced and customized Nmap for daily use in a large enterprise. In true open source spirit, he has released these valuable scripts on his Web site (<http://www.unspecific.com/.go/nmap/>). IP addresses have been changed to protect the corporate identity. The remainder of this section is in his own words.

After spending the past couple of decades learning computers and working my way up from tech support through sysadmin and into my dream job of Information Security Officer for a major Internet company, I found myself with a problem. I was handed the sole responsibility of security monitoring for our entire IP space. This was almost 50,000 hosts worldwide when I started several years ago, and it has doubled since then.

Scanning all of these machines for potential vulnerabilities as part of monthly or quarterly assessments would be tough enough, but management wanted it done daily. Attackers will not wait a week or month to exploit a newly exposed vulnerability, so I cannot wait that long either.

Looking around for tools, I quickly chose Nmap as my port scanner. It is widely considered to be the best scanner, and I had already been using it for years to troubleshoot networks and test security. Next I needed software to aggregate Nmap output and print differences between runs. I considered several existing tools, such as James Levine's NDiff (<http://www.vinecorp.com/ndiff/>), and HD Moore's Nlog (<http://www.secureaustin.com/nlog>). While these are great tools, they did not monitor changes in the way I desired. I had to know whenever a router or firewall access control list was misconfigured or a host was publicly sharing inappropriate content. I also worried about the scalability of these other solutions, so I decided to tackle the problem myself.

The first issue to come up was speed. Our networks are located worldwide, yet I was provided with only a single U.S.-based host to do the scanning. In many cases, firewalls between the sites slowed the scanning down significantly. Scanning all 100,000 hosts took over 30 hours, which is unacceptable for a daily scan. So I wrote a

script called nmap-wrapper which runs dozens of Nmap processes in parallel, reducing the scan time to fifteen hours, even including OS detection.

The next problem was dealing with so much data. A SQL database seemed like the best approach for scalability and data-mining reasons, but I had to abandon that idea due to time pressures. A future version may add this support. Instead, I used a flat file to store the results of each class C address range for each day. The most powerful and extensible way to parse and store this information was the Nmap XML format, but I chose the "grepable" (-oG option) format because it is so easy to parse from simple script. Per-host timestamps are also stored for reporting purposes. These have proven quite helpful when administrators try to blame machine or service crashes on the scanner. They cannot credibly claim a service crash at 7:12AM when I have proof that the scan ran at 9:45AM.

The describe process produces copious data, with no convenient access method. The standard UNIX **diff** tool is not smart enough to report only the changes I care about, so I wrote a Perl script named nmap-diff to provide daily change reports. A typical output report is shown in Example 1-4.

#### Example 1-4. Nmap-diff typical output

```
> nmap-diff.pl -c3
  5 IPs showed changes

  10.12.4.8 (ftp-box.foocompany.biz)
    21/tcp    open   ftp
    80/tcp    open   http
    443/tcp   open   https
    1027/tcp  open   IIS
    + 1029/tcp open   ms-lsa
    38292/tcp open   landesk-cba
  OS: Microsoft Windows Millennium Edition (Me)
      Windows 2000 Professional or Advanced Server
      or Windows XP

  10.16.234.3 (media.foocompany.biz)
    80/tcp    open   http
    + 554/tcp  open   rtsp
    + 7070/tcp open   realserver

  192.168.10.186 (testbox.foocompany.biz)
    + 8082/tcp open   blackice-alerts
  OS: Linux Kernel 2.4.0 - 2.5.20

  172.24.12.58 (mtafoocompany.biz)
    + 25/tcp    open   smtp
  OS: FreeBSD 4.3 - 4.4PRERELEASE

  172.23.76.22 (media2.foocorp.biz)
    80/tcp    open   http
    1027/tcp  open   IIS
    + 1040/tcp open   netsaint
    1755/tcp  open   wms
    3372/tcp  open   msdtc
    6666/tcp  open   irc-serv
    7007/tcp  open   afs3-bos
  OS: Microsoft Windows Millennium Edition (Me)
```

Windows 2000 Professional or Advanced Server  
or Windows XP

Management and staff were impressed when I demonstrated this new system at an internal company security symposium. But instead of allowing me to rest on my laurels, they began asking for new features. They wanted counts of mail and web servers, growth estimates, and more. This data was all available from the scans, but was difficult to access. So I created yet another Perl script, nmap-report, which made querying the data much easier. It takes specifications such as open ports or operating systems and finds all the systems that matched on a given day.

One problem with this approach to security monitoring is that employees do not always place services on their IANA-registered official ports. For example, they might put a web server on port 22 (ssh) or vice versa. Just as I was debating how to address this problem, Nmap came out with an advanced service and version detection system (see Chapter 7). Nmap-report now has a rescan feature that uses version scanning to report the true services rather than guessing based on port number. I hope to further integrate version detection in future versions. Example 1-5 shows nmap-report listing FTP servers.

#### **Example 1-5. Nmap-report execution**

```
> nmap-report -p21 -rV
[...]
172.21.199.76 (ftp1.foocorp.biz)
  21/tcp  open  ssl|ftp Serv-U ftpd 4.0

192.168.12.56 (ftp2.foocorp.biz)
  21/tcp  open  ftp      NcFTPD

192.168.13.130 (dropbox.foocorp.biz)
  21/tcp  open  ftp      WU-FTPD 6.00LS
```

While being far from perfect, these scripts have proven themselves quite valuable at monitoring large networks for security-impacting changes. Since Nmap itself is open source, it only seemed fair to release my scripts to the public as well. I have made them freely available at <http://www.unspecific.com/.go/nmap>.

## **1.3. Legal issues**

### **1.3.1. Is unauthorized port scanning a crime?**

The legal ramifications of scanning networks with Nmap are complex and so controversial that third-party organizations have printed T-shirts and bumper stickers promulgating opinions on the matter<sup>6</sup>.

**Figure 1-4. Strong opinions on port scanning legality and morality**



While I agree with the sentiment that port scanning *should not* be illegal, it is rarely wise to take legal advice from a T-shirt. Indeed, taking it from a software engineer and author is only slightly better. Speak to a competent lawyer within your jurisdiction for a better understanding of how the law applies to your particular situation. With that important disclaimer out of the way, here is some general information that may prove helpful.

The best way to avoid controversy when using Nmap is to always secure written authorization from the target network representatives before initiating any scanning. There is still a chance that your ISP will give you trouble if they notice it (or if the target admins accidentally send them an abuse report), but this is usually not terribly difficult to resolve. When you are performing a penetration test, this authorization should be in the Statement of Work. When testing your own company, make certain that this activity clearly falls within your job description. Security consultants should be familiar with the excellent Open Source Security Testing Methodology Manual (OSSTMM) (<http://www.osstmm.org/>), which provides current best practices for these situations.

While civil and (especially) criminal court cases are the nightmare scenario for Nmap users, these happen very rarely. After all, no US federal laws explicitly make port scanning illegal. A much more frequent occurrence is that the target network will notice a scan and then send a complaint to the network service provider where the scan initiated (your ISP). Most network admins do not seem to care or notice the many scans bouncing off their networks daily. But a few complain. The scanner's ISP may track down the user corresponding to the reported IP address and time, then chide the user or even kick them off the service. Port scanning without authorization is sometimes against the provider's acceptable use policy (AUP). For example, the AUP for the huge cable-modem ISP Comcast presently says<sup>7</sup>:

<sup>7</sup>"Network probing or port scanning tools are only permitted when used in conjunction with a residential home network, or if

explicitly authorized by the destination host and/or network. Unauthorized port scanning, for any reason, is strictly prohibited."

Even if an ISP does not explicitly ban unauthorized port scanning, they might claim that some "anti-hacking" provision applies. Of course this does *not* make port scanning illegal. Many perfectly legal and (in the United States) constitutionally protected activities are banned by ISPs. For example, the AUP quoted from above also prohibits users from transmitting, storing, or posting "any information or material which a reasonable person could deem to be objectionable, offensive, indecent, pornographic, ... embarrassing, distressing, vulgar, hateful, racially or ethnically offensive, or otherwise inappropriate, regardless of whether this material or its dissemination is unlawful." In other words, some ISPs ban any behavior that could possibly offend or annoy someone. Indiscriminate scanning of other people's networks/computers does have the potential to do so. If you decide to perform such controversial scanning anyway, never do it from work, school, or any other service provider that has substantial control over your well-being. Use a dialup or commercial broadband provider instead. Losing your DSL connection and having to change providers is a slight nuisance, but it is immeasurably preferable to being expelled or fired.

While legal cases involving port scanning (without follow-up hacking attacks) are rare, they do happen. One of the most notable cases involved a man named Scott Moulton who had an ongoing consulting contract to maintain the Cherokee County, Georgia emergency 911 system. In December 1999, he was tasked with setting up a router connecting the Canton, Georgia Police Department with the E911 Center. Concerned that this might jeopardize the E911 Center security, Moulton initiated some preliminary port scanning of the networks involved. In the process he scanned a Cherokee County web server that was owned and maintained by a competing consulting firm named VC3. They noticed the scan and emailed Moulton, who replied that he worked for the 911 Center and was testing security. VC3 then reported the activity to the police. Moulton lost his E911 maintenance contract and was arrested for allegedly violating the Computer Fraud and Abuse Act of America Section 1030(a)(5)(B)<sup>8</sup>. This act applies against anyone who "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage" (and meets other requirements). The damage claimed by VC3 involved time spent investigating the port scan and related activity. VC3 also filed a civil suit against Moulton claiming violation of the same act as well as the Georgia Computer Systems Protection Act, after Moulton sued VC3 for defamation.

The civil case against Moulton was dismissed before trial, implying a complete lack of merit. The ruling made many Nmap users smile:

"Court holds that plaintiff's act of conducting an unauthorized port scan and throughput test of defendant's servers does not constitute a violation of either the Georgia Computer Systems Protection Act or the Computer Fraud and Abuse Act." -- Civ. Act. No. 1:00-CV-434-TWT (N.D. Ga. November 6, 2000)

This was an exciting victory in the civil case, but Scott still had the criminal charges hanging over his head. Fortunately he kept his spirits high, sending the following note to the nmap-hackers mailing list<sup>9</sup>:

"I am proud that I could be of some benefit to the computer society in defending and protecting the rights of specialists in the computer field, however it is EXTREMELY costly to support such an effort, of which I am not happy about. But I will continue to fight and prove that there is nothing illegal about port scanning especially when I was just doing my job."

Eventually, the criminal court came to the same conclusion and all charges were dropped. While Moulton was vindicated in the end, he suffered six-figure legal bills and endured stressful years battling through the court system. While his case does set a good example (if not legal precedent), different courts or situations could still lead to worse outcomes. Remember that many states have their own computer abuse laws, some of which can arguably make even pinging a remote machine without authorization illegal<sup>10</sup>.

Laws in other nations obviously differ as well. For example, A 17-year-old youth was convicted in Finland (<http://www.osborneclarke.com/publications/text/ITM0903f.htm>) of attempted computer intrusion for simply port scanning a bank. He was fined to cover the target's investigation expenses. The Moulton court might also have ruled differently if the VC3 machine had actually crashed and they were able to justify the \$5,000 damage figure required by the act.

At the other extreme, an Israeli judge acquitted (<http://www.haaretz.com/hasen/spages/399602.html>) Avi Mizrahi in early 2004 for vulnerability scanning the Mossad secret service. Judge Abraham Tennenbaum even praised Avi as follows:

“In a way, Internet surfers who check the vulnerabilities of Web sites are acting in the public good. If their intentions are not malicious and they do not cause any damage, they should even be praised.”

ISP accounts will continue to be terminated regardless of the legal status of port scanning if too many complaints are generated. The best way to avoid ISP abuse reports or civil/criminal charges is to avoid annoying the target network admins in the first place. Here are some practical suggestions:

- Probably at least 90% of network scanning is non-controversial. You are rarely badgered for scanning your own machine or the networks you administer. The controversy comes when scanning other networks. There are many reasons (good and bad) for doing this sort of network exploration. Perhaps you are scanning the other systems in your dorm or department to look for publicly shared files (FTP, SMB, WWW, etc.). Or maybe you are just trying to find the IP of a certain printer. You scanned your favorite web site to see if they are offering any other services, or because you were curious what OS they run. Perhaps you are just trying to test connectivity, or maybe you wanted to do a quick security sanity check before handing off your credit card details to that e-commerce company. You might be conducting Internet research. Or are you performing initial reconnaissance in preparation for a break-in attempt? The remote administrators rarely know your true intentions, and do sometimes get suspicious. The best approach is to get permission first. I have seen a few people with non-administrative roles land in hot water after deciding to “prove” network insecurity by launching an intrusive scan of the entire company or campus. Admins tend to be more cooperative when asked in advance than when woken up at 3AM by an IDS alarm claiming they are under massive attack. So whenever possible, obtain written authorization before scanning a network. Adrian Lamo would probably not be in jail at the time of this writing if he had asked the New York Times to test their security rather than telling reporters about the flaws afterward. Unfortunately they would likely have said no. Be prepared for this answer.
- Target your scan as tightly as possible. Any machine connected to the Internet is scanned regularly enough that most admins ignore such Internet “white noise”. But scanning enough networks or executing very noisy/intrusive scans increases the probability of generating complaints. So if you are only looking for web servers, specify -p80 rather than scanning all 65,535 TCP ports on each machine. If you are only trying to find available hosts, do an Nmap ping scan rather than full port scan. Do not scan a CIDR /16 (65K hosts) when a /24 netblock suffices. The random scan mode now takes an argument specifying the number of hosts, rather than running forever. So consider -iR 1000 rather than -iR 10000 if the former is sufficient. Use the default timing (or even “-T Polite”) rather than “-T Insane”. Avoid noisy and relatively intrusive scans such as version detection (-sV). Similarly, a SYN scan (-sS) is quieter than a connect() scan (-sT) while providing the same information and often being faster.
- As noted previously, do not do anything controversial from your work or school connections. Even though your intentions may be good, you have too much to lose if someone in power (e.g. boss, dean) decides you are a malicious cracker. Do you really want to explain your actions to someone who may not even understand the terms “port scanner” or “packet”? Spend \$10-\$50 bucks a month for a dialup, shell, or residential broadband account. Not only are the repercussions less severe if you offend someone from such an account, but target network admins

are less likely to even bother complaining to mass-market providers. Also read the relevant AUP and choose a provider accordingly. If your provider (like Comcast discussed above) bans any unauthorized port scanning and posting of "offensive" material, do not be surprised if you are kicked off for this activity. In general, the more you pay to a service provider the more accommodating they are. A T1 provider is highly unlikely to yank your connection without notice because someone reported being port scanned. A dialup or residential DSL/cable provider very well might. This can happen even when the scan was forged by someone else.

- Nmap offers many options for stealthy scans, including source-IP spoofing, decoy scanning, and the more recent Idle Scan technique. These are discussed in the IDS evasion chapter. But remember that there is always a trade-off. You are harder to find if you launch scans from an open WAP far from your house, with 17 decoys, while doing subsequent probes through a chain of 9 open proxies. But if anyone does track you down, they will be mighty suspicious of your intentions.
- Always have a legitimate reason for performing scans. An offended admin might write to you first (or your ISP might forward his complaint to you) expecting some sort of justification for the activity. In the Moulton case discussed above, VC3 first emailed Moulton to ask what was going on. If they had been satisfied with his answer, matters might have stopped there rather than escalating into civil and criminal litigation. Groups scanning large portions of the Internet for research purposes often use a reverse-DNS name that describes their project and runs a web server with detailed information and opt-out forms.

Also remember that ancillary and subsequent actions are often used as evidence of intent. A port scan by itself does not always signify an attack. A port scan followed closely by an IIS exploit, however, broadcasts the intention loud and clear. This is important because decisions to prosecute (or fire, expel, complain, etc.) are often based on the whole event and not just one component (such as a port scan). One dramatic case involved a Canadian man named Walter Nowakowski, who was apparently the first person to be charged in Canada with theft of communications<sup>11</sup> for accessing the Internet through an someone's unsecured Wi-Fi network. Thousands of Canadian "war drivers" do this every day, so why was he singled out? Because of ancillary actions and intent. He was allegedly caught driving the wrong way on a one-way street, naked from the waist down, with laptop in hand, while downloading child pornography through the aforementioned unsecured wireless access point<sup>12</sup>. The police apparently considered his activity egregious enough that they brainstormed for relevant charges and tacked on theft of communications to the many child pornography-related charges. Similarly, charges involving port scanning are usually reserved for the most egregious cases. Even when paranoid administrators notify the police that they have been port scanned, prosecution (or any further action) is exceedingly rare. The fact that a 911 emergency service was involved is likely what motivated prosecutors in the Moulton case. Your author has scanned hundreds of thousands of Internet hosts and has only been contacted by police and investigative agencies when they file bug reports and feature requests.

To summarize this whole section, the question of whether port scanning is legal does not have a simple answer. I cannot unequivocally say "port scanning is never a crime", as much as I would like to. Laws differ dramatically between jurisdictions, and cases hinge on their particular details. Even when facts are nearly identical, different judges and prosecutors do not always interpret them the same way. I can only urge caution and reiterate the suggestions above.

For testing purposes, you have permission to scan the host `scanme.nmap.org`. You may have noticed that it was used in several examples already. Note that this permission only includes scanning via Nmap and not testing exploits or denial of service attacks. To conserve bandwidth, please do not initiate more than a dozen scans against that host per day. If this free scanning target service is abused, it will be taken down and Nmap will report `Failed to resolve given hostname/IP: scanme.nmap.org`. These permissions also apply to the hosts `scanme2.nmap.org`, `scanme3.nmap.org`, and so on, though those hosts do not currently exist.

This section provides an overview of legal issues related to port scanning, but cannot hope to cover everything. A valuable forum for discussing legal issues related to security is the `seclegal` mailing list. Details are available at

<http://seclegal.jscript.dk>

### 1.3.2. Can port scanning crash the target computer/networks?

Nmap does not have any features designed to crash target networks. It usually tries to tread lightly. For example, Nmap detects dropped packets and slows down when they occur in order to avoid overloading the network. Nmap also does not send any corrupt packets. The headers and such are always appropriate although the destination host is not necessarily expecting the packets. For these reasons, no application, host, or network component *should* ever crash based on an Nmap scan. If they do, that is a bug in the system which should be repaired by the vendor.

Reports of systems being crashed by Nmap are rare, but they do happen. Many of these systems were probably unstable in the first place and Nmap either pushed them over the top or they crashed at the same time as an Nmap scan by pure coincidence. In other cases, poorly written applications, TCP/IP stacks, and even operating systems have been demonstrated to crash reproducibly given a certain Nmap command. These are usually older legacy devices, as newer equipment is rarely released with these problems. Smart companies use Nmap and many other common network tools to test devices prior to shipment. Even those who don't often find out about the problem in early beta tests when a box is first deployed on the Internet. It rarely takes long for a given IP to be scanned as part of Internet white noise. Keeping systems and devices up-to-date with the latest vendor patches and firmware should reduce the susceptibility of your machines to these problems, while also improving the security and usability of your network.

In many cases, finding that a machine crashes from a certain scan is valuable information. After all, attackers can do anything Nmap can do by using Nmap itself or their own custom scripts. They should not be allowed to crash your devices, and a patch should be demanded of vendors if devices do suffer. In other Nmap usage scenarios, you may want to do very light scanning in order to reduce the risk of these problems. Here are a few suggestions:

- Use SYN scan (-sS) instead of Connect() scan (-sT). User-mode applications such as web servers can rarely even detect the former because it is all handled in kernel space (some older Linux kernels are an exception) and thus the services have no excuse to crash.
- Version scanning (-sV) risks crashing poorly written applications. Similarly, some lame operating systems have been reported to crash when OS fingerprinted (-O). Omit these options for particularly sensitive environments or where you do not care about the results.
- Using -T2 or slower (-T1, -T0) timing modes can reduce the chances that a port scan will harm a system, though they slow your scan dramatically. Older Linux boxes had an identd that would block services temporarily if they were accessed too frequently. This could happen in a port scan, as well as during legitimate high-load situations. Slower timing might help here.
- Limit the number of ports and machines scanned to the fewest that are required. Every machine scanned has a minuscule chance of crashing, and so cutting the number of machines down improves your odds. Reducing the number of ports scanned reduces the risks to end hosts as well as network devices. Many NAT/Firewall devices keep a state entry for every port probe. Most of them expire old entries when the table fills out, but occasional (pathetic) implementations crash instead. Reducing the ports/hosts scanned reduces the number of state entries and thus might help those sorry devices stay up.

### 1.3.3. Misc: Copyright, license, (lack of) warranty, export control information

These important legal notices come from the Nmap manual page.

The Nmap Security Scanner is (C) 1996-2004 Insecure.Com LLC. Nmap is also a registered trademark of Insecure.Com LLC. This program is free software; you may redistribute and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; Version 2. This guarantees your right to use, modify, and redistribute this software under certain conditions. If you wish to embed Nmap technology into proprietary software, we may be willing to sell alternative licenses (contact sales@insecure.com). Many security scanner vendors already license Nmap technology such as our remote OS fingerprinting database and code, service/version detection system, and port scanning code.

Note that the GPL places important restrictions on "derived works", yet it does not provide a detailed definition of that term. To avoid misunderstandings, we consider an application to constitute a "derivative work" for the purpose of this license if it does any of the following:

- Integrates source code from Nmap
- Reads or includes Nmap copyrighted data files, such as nmap-os-fingerprints or nmap-service-probes.
- Executes Nmap and parses the results (as opposed to typical shell or execution-menu apps, which simply display raw Nmap output and so are not derivative works.)
- Integrates/includes/aggregates Nmap into a proprietary executable installer, such as those produced by InstallShield.
- Links to a library or executes a program that does any of the above

The term "Nmap" should be taken to also include any portions or derived works of Nmap. This list is not exclusive, but is just meant to clarify our interpretation of derived works with some common examples. These restrictions only apply when you actually redistribute Nmap. For example, nothing stops you from writing and selling a proprietary front-end to Nmap. Just distribute it by itself, and point people to <http://www.insecure.org/nmap/> to download Nmap.

We don't consider these to be added restrictions on top of the GPL, but just a clarification of how we interpret "derived works" as it applies to our GPL-licensed Nmap product. This is similar to the way Linus Torvalds has announced his interpretation of how "derived works" applies to Linux kernel modules. Our interpretation refers only to Nmap - we don't speak for any other GPL products.

If you have any questions about the GPL licensing restrictions on using Nmap in non-GPL works, we would be happy to help. As mentioned above, we also offer alternative license to integrate Nmap into proprietary applications and appliances. These contracts have been sold to many security vendors, and generally include a perpetual license as well as providing for priority support and updates as well as helping to fund the continued development of Nmap technology. Please email sales@insecure.com for further information.

As a special exception to the GPL terms, Insecure.Com LLC grants permission to link the code of this program with any version of the OpenSSL library which is distributed under a license identical to that listed in the included COPYING.OpenSSL file, and distribute linked combinations including the two. You must obey the GNU GPL in all respects for all of the code used other than OpenSSL. If you modify this file, you may extend this exception to your version of the file, but you are not obligated to do so.

If you received these files with a written license agreement or contract stating terms other than the terms above, then that alternative license agreement takes precedence over these comments.

Source is provided to this software because we believe users have a right to know exactly what a program is going to do before they run it. This also allows you to audit the software for security holes (none have been found so far).

Source code also allows you to port Nmap to new platforms, fix bugs, and add new features. You are highly encouraged to send your changes to fyodor@insecure.org for possible incorporation into the main distribution. By sending these changes to Fyodor or one the Insecure.Org development mailing lists, it is assumed that you are

offering Fyodor and Insecure.Com LLC the unlimited, non-exclusive right to reuse, modify, and relicense the code. Nmap will always be available Open Source, but this is important because the inability to relicense code has caused devastating problems for other Free Software projects (such as KDE and NASM). We also occasionally relicense the code to third parties as discussed above. If you wish to specify special license conditions of your contributions, just say so when you send them.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details (it is included as an appendix, and is also available from <http://www.gnu.org/copyleft/gpl.html>).

It should also be noted that Nmap has been known to crash certain poorly written applications, TCP/IP stacks, and even operating systems (see previous section). Nmap should never be run against mission critical systems unless you are prepared to suffer downtime. We acknowledge here that Nmap may crash your systems or networks and we disclaim all liability for any damage or problems Nmap could cause.

Because of the slight risk of crashes and because a few black hats like to use Nmap for reconnaissance prior to attacking systems, there are administrators who become upset and may complain when their system is scanned. Thus, it is often advisable to request permission before doing even a light scan of a network.

Nmap should never be run with privileges (e.g. suid root) for security reasons.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). The Libpcap portable packet capture library is distributed along with nmap. Libpcap was originally copyrighted by Van Jacobson, Craig Leres and Steven McCanne, all of the Lawrence Berkeley National Laboratory, University of California, Berkeley, CA. It is now maintained at <http://www.tcpdump.org>.

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. See <http://www.pcre.org/>.

Nmap can optionally link to the OpenSSL cryptography toolkit, which is available from [http://www.openssl.org/](http://www.openssl.org).

**US Export Control:** Insecure.Com LLC believes that Nmap falls under US ECCN (export control classification number) 5D992. This category is called "'Information Security" "software" not controlled by 5D002'. The only restriction of this classification is AT (anti-terrorism), which applies to almost all goods and denies export to a handful of rogue nations such as Iran and North Korea. Thus exporting Nmap does not require any special license, permit, or other governmental authorization.

## Notes

1. Based on having the highest download frequency, number of Google hits, and Freshmeat.Net software "popularity" ranking.
2. These IP addresses are actually registered to the United States Army Yuma Proving Ground, which is used to test a wide variety of artillery, missiles, tanks, and other deadly weapons. The moral is to be very careful about who you scan, lest you accidentally hit a highly sensitive network. The scan results in this story are not actually from this IP range.
3. It is possible that the target nameserver will log a suspicious bunch of reverse-DNS queries from Felix's nameserver, but most organizations don't even keep such logs, much less analyze them.
4. stdio is the "C" notation for representing the standard output mechanism for a system, such as to the UNIX xterm or Windows command window in which Nmap was initiated.

5. A sexy leather-clad attacker from the previous team actually started the session. It is unclear at what point she died and left the remaining tasks to Trinity.
6. These are from <http://www.americansushi.com/>. I have no affiliation with them except that they were cool enough to send me samples.
7. <http://www.comcast.net/terms/use.jsp>
8. <http://www4.law.cornell.edu/uscode/18/1030.html>
9. <http://seclists.org/lists/nmap-hackers/2001/Apr-Jun/0011.html>
10. An excellent paper on this topic by lawyer Ethan is available at <http://grove.ufl.edu/~techlaw/vol6/Preston.html>  
He has also written an excellent paper relating to the legal risks of publishing security information and exploits at <http://www.mcndl.com/computer-security.html>.
11. Canadian Criminal Code Section S.342.1 - [http://www.digitaldefence.ca/Canada\\_CriminalCode\\_S342.1.htm](http://www.digitaldefence.ca/Canada_CriminalCode_S342.1.htm)
12. <http://www.canoe.ca/NewsStand/LondonFreePress/News/2003/11/22/264890.html>

# Chapter 2. Obtaining, Installing, and Removing Nmap

## 2.1. Introduction

This chapter describes how to install Nmap on many platforms, from Windows to OpenBSD, including both source code compilation and binary installation methods. Graphical and command-line versions of Nmap are described and contrasted. A recipe describes how to install and use Nmap on the Sharp Zaurus PDA. Finally, Nmap removal instructions are provided in case you change your mind.

### 2.1.1. Testing whether Nmap is already installed

The first step toward obtaining Nmap is to check whether you already have it. Many free operating system distributions (including most Linux and BSD systems) come with Nmap, although it may not be installed by default. On UNIX systems, open a terminal window and try executing the command `nmap --version`. If Nmap exists and is in your \$PATH, you should see output similar to Example 2-1.

#### Example 2-1. Checking for Nmap and determining its version number

```
felix~>nmap --version  
  
nmap version 3.50 ( http://www.insecure.org/nmap )  
felix~>
```

If Nmap does *not* exist on the system (or if your PATH is incorrectly set), an error message such as `nmap: Command not found` displays. As the example above shows, Nmap responds to the command by printing its version number (here 3.50).

Even if your system already has a copy of Nmap, you should consider upgrading to the latest version available from [http://www.insecure.org/nmap/nmap\\_download.html](http://www.insecure.org/nmap/nmap_download.html). Newer versions often run faster, fix important bugs, and feature updated operating system and service version detection databases. A list of changes since the version already on your system can be found at [http://www.insecure.org/nmap/nmap\\_changelog.html](http://www.insecure.org/nmap/nmap_changelog.html). Nmap output examples in this book usually include a version number near the top, and they may not work with older versions.

### 2.1.2. Verifying the integrity of Nmap downloads

It often pays to be paranoid about the integrity of files downloaded from the Internet. While nobody has ever compromised Insecure.Org or (as far as I know) distributed a trojaned version of Nmap, one should always be cautious. Popular packages such as Sendmail<sup>1</sup>, OpenSSH<sup>2</sup>, tcpdump, libpcap, BitchX, Fragrouter, and many others have been infected with malicious trojans. Popular software distributions sites at the Free Software Foundation, Debian, and SourceForge have also been successfully compromised. To help people verify the authenticity of Nmap releases, I always send a PGP-signed announcement to the nmap-hackers list. That announcement includes MD5 cryptographic checksums of the source code and binaries. Visit <http://seclists.org/> for subscription information and archives. The message should be signed by my key, which is available from the public keyservers or from [http://www.insecure.org/fyodor\\_gpgkey.txt](http://www.insecure.org/fyodor_gpgkey.txt). The KeyID is 0x53587D95 and the fingerprint is

972F:93AB:9CB0:0980:D951:406B:B9BC:E17E. The checksum can be verified with the md5sum or md5 utilities available on most UNIX boxes. Example 2-2 demonstrates this.

#### **Example 2-2. Verifying the Nmap download checksum**

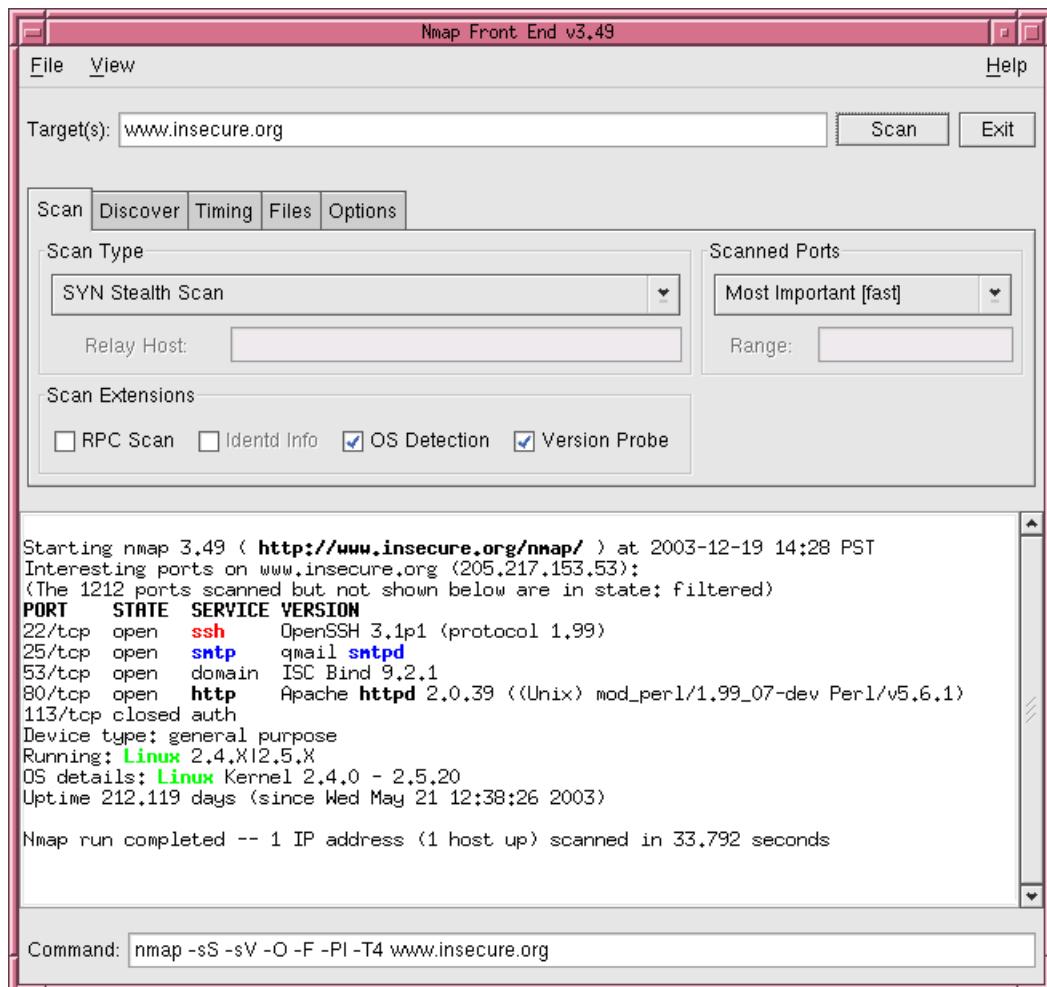
```
felix~> gpg --verify Nmap-3.50-announce-email.txt
gpg: Warning: using insecure memory!
gpg: Signature made Wed 21 Jan 2004 02:54:38 PM PST using RSA key ID 53587D95
gpg: Good signature from "Fyodor <fyodor@insecure.org>" 
gpg:                               aka "Fyodor <fyodor@dhp.com>" 
felix~> md5sum nmap-3.50.tgz
9823bcd72f87051707e6e1c2b10d5d62  nmap-3.50.tgz
felix~>
```

While releases from Insecure.Org are signed as described above, certain Nmap add-ons, interfaces, and platform-specific binaries are developed and distributed by other parties. They may have different mechanisms for establishing the authenticity of their downloads.

### **2.1.3. Command-line and graphical interfaces**

Nmap has traditionally been a command-line application run from a UNIX shell or (more recently) Windows command prompt. This allows experts to quickly execute a command that does exactly what they want without having to maneuver through a bunch of configuration panels and scattered option fields. This also makes Nmap easier to script and enables easy sharing of useful commands among the user community.

One downside of the command-line approach is that it can be intimidating for new and infrequent users. Nmap offers more than a hundred command-line options, although many are obscure features or debugging controls that most users can ignore. Many graphical frontends have been created for those users who prefer a GUI interface. The most common GUI for UNIX is NmapFE, which is distributed as part of the Nmap project. It offers a number of option panes (**Scan**, **Discover**, **Timing**, **Files**, and **Options**), which are all used to build an appropriate Nmap command. The Nmap command-line is shown at the bottom of the window as it is constructed. This feature helps people learn the syntax in case they wish to migrate to the command-line version. There is not presently a field for entering arbitrary Nmap options, but one trick is to stick them in the big **Target(s)** field. Once the command is constructed to your liking, press the **Scan** button to launch Nmap. Raw Nmap output (with added color for service emphasis) is shown in a large white window, as seen in Figure 2-1.

**Figure 2-1.** NmapFE presents a simple graphical interface to Nmap

Unfortunately, NmapFE does not yet work well on the Windows platform. The good news is that Jens Vogt has created a popular Windows Nmap GUI named Nmapwin. It is organized a little differently than NmapFE, but retains the same paradigm of constructing a command-line from multiple tabbed option panes and then displaying the raw output in a big scrollable box. Instructions for installing Nmapwin are provided in Section 2.4.2.

This book focuses almost exclusively on command-line invocations of Nmap. Once you understand how the command-line options work and can interpret the output, using any of the available Nmap GUIs is trivial. The options are all the same whether you choose them from radio buttons and menus or type them at a command-line.

## 2.2. UNIX Compilation and installation from source code

While binary packages discussed in later sections are available for most platforms, compilation and installation from source code is the traditional and most powerful way to install Nmap. This insures that the latest version is available and allows Nmap to adapt to the library availability and directory structure of your system. For example, Nmap uses the OpenSSL cryptography libraries for version detection (Chapter 7) when available, but most binary packages do

not include this functionality. On the other hand, binary packages are generally quicker and easier to install, and allow for consistent management (installation, removal, upgrading, etc.) of all packaaged software on the system.

Source installation is usually a painless process - the build system is designed to auto-detect as much as possible. Here are the steps required for a default install:

1. Download the latest version of Nmap in .tar.bz2 (bzip2 compression) or .tgz (gzip compression) format from [http://www.insecure.org/nmap/nmap\\_download.html](http://www.insecure.org/nmap/nmap_download.html).

2. Decompress the downloaded tarball with a command such as:

```
bzip2 -cd nmap-VERSION.tar.bz2 | tar xvf -
```

If you downloaded the .tgz version, replace bzip2 with gzip in the command above.

3. Change into the newly created directory: **cd nmap-VERSION**

4. Configure the build system: **./configure**

5. Build Nmap (and GUI nmapfe if requirements met): **make**

6. Become a privileged user for systemwide install: **su root**

7. Install Nmap, support files, docs, etc.: **make install**

As you can see above, a simple source compilation and install consists of little more than **./configure;make;make install**. However, there are a number of options available to configure that affect the way Nmap is built.

### 2.2.1. Configure directives

Most of the UNIX build options are controlled by the **configure** script, as used in step number four above. There are dozens of command-line parameters and environmental variables which affect the way Nmap is built. Run **./configure --help** for a huge list with brief descriptions. Here are the ones that are specific to Nmap or particularly important:

**--prefix=directoryname**

This option, which is standard to the configure scripts of most software, determines where Nmap and its components are installed. By default, the prefix is `/usr/local`, meaning that nmap is installed in `/usr/local/bin`, the man page (`nmap.1`) is installed in `/usr/local/man/man1`, and the data files (`nmap-os-fingerprints`, `nmap-services`,`nmap-service-probes`, etc.) are installed under `/usr/local/share/nmap`. If you only wish to change the path of certain components, use the options `--bindir`, `--datadir`, and/or `--mandir`. An example usage of `--prefix` would be to install Nmap in my account as an unprivileged user. I would run **./configure --prefix=/home/fyodor**. Nmap creates subdirs like `/home/fyodor/man/man1` in the install stage if they do not already exist.

**--without-nmapfe**

This option prevents the NmapFE graphical X-Window frontend from being built. Normally the build system checks your system for requirements such as the GTK graphical widget library and then build NmapFE if they are all available.

--with-openssl=*directoryname*

The version detection subsystem of Nmap is able to probe SSL-encrypted services using the free OpenSSL libraries. Normally the Nmap build system looks for these libraries on your system and include this capability if they are found. If they are in a location your compiler does not search for by default, but you still want them to be used, specify --with-openssl=*directoryname*. Nmap then looks in *directoryname*/libs for the OpenSSL libraries themselves and *directoryname*/include for the necessary header files.

--with-libpcap=*directoryname*

Nmap uses the Libpcap library (<http://www.tcpdump.org>) for capturing raw IP packets. Nmap normally looks for an existing copy of Libpcap on your system and use that if the version number and platform is appropriate. Otherwise Nmap includes its own recent copy of Libpcap, which has been modified for improved Linux functionality. The specific changes are described in libpcap-possiblymodified/CHANGES in the Nmap source directory. Because of these Linux-related changes, Nmap always uses its own Libpcap by default on that platform. If you wish to force Nmap to link with your own Libpcap, pass the option --with-libpcap=*directoryname* to configure. Nmap then expects the Libpcap library to be in *directoryname*/lib/libpcap.a and the include files to be in *directoryname*/include.

--with-libpcre=*directoryname*

LibPCRE is a Perl-compatible regular expression library available from <http://www.pcre.org>. Nmap normally looks for a copy on your system, and then fall back to its own copy if that fails. If your PCRE library is not in your compiler's standard search path, Nmap probably will not find it. In that case you can tell Nmap where it can be found by specifying the option --with-libpcre=*directoryname* to configure. Nmap then expects the library files to be in *directoryname*/lib and the include files to be in *directoryname*/include. In some cases, you may wish to use the PCRE libraries included with Nmap in preference to those already on your system. In that case, specify --with-libpcre=included.

--with-localdirs

This simple option tells Nmap to look in /usr/local/lib and /usr/local/include for important library and header files. This should never be necessary, except that some people put such libraries in /usr/local without configuring their compiler to find them. If you are one of those people, use this option.

## 2.2.2. If you encounter compilation problems

In an ideal world, software would always compile perfectly (and quickly) on every system you maintain. Unfortunately, society has not yet reached that state of nirvana. Despite all the efforts to make Nmap portable, compilation issues occasionally arise. Here are some suggestions in case the source distribution compilation fails.

Upgrade to the latest Nmap

Check [http://www.insecure.org/nmap/nmap\\_download.html](http://www.insecure.org/nmap/nmap_download.html) to make sure you are using the latest version of Nmap. The problem may have already been fixed.

Read the error message carefully

Scroll up in the output screen and examine the error messages given when commands fail. It is often best to find the first error message, as that often causes a cascade of further errors. Read the error message carefully, as it could indicate a system problem such as low disk space or a broken compiler. Users with programming skills may be able to resolve a wider range of problems themselves. If you make code changes to fix the problem,

please send a patch (created with **diff -uw oldfile newfile**) and any details about your problem and platform to me at <fyodor@insecure.org>. Integrating the change into the base Nmap distribution allows many other users to benefit, and prevents you from having to make the changes with each new Nmap version.

#### Ask Google and other Internet resources

Try searching for the exact error message on Google or other search engines. You might also want to browse recent activity on the Nmap development (nmap-dev) list -- archives are available at <http://seclists.org>.

#### Ask nmap-dev

If none of your research has led to a solution for your problem, try sending a report to the Nmap development (nmap-dev) list. If you subscribe first, your message gets through faster because it does not go through moderation. Subscribe by sending a blank email to <nmap-dev-subscribe@insecure.org> and post to the list by mailing <nmap-dev@insecure.org>. Be sure to describe your problem in full, including the Nmap version number, platform you are running on, and any relevant output snippets showing the error.

#### Consider binary packages

Binary packages of Nmap are available on most platforms and are usually easy to install. The downsides are that they may not be as up-to-date and you lose some of the flexibility of self-compilation. Previous sections of this chapter describe how to find binary packages on many platforms, and even more are available via Internet searching.

## 2.3. Linux Distributions

Linux is far and away the most popular platform for running Nmap. In a 2003 survey of roughly 2000 Nmap users, 86% said that Linux was at least one of the platforms on which they run Nmap.

Linux users can choose between a source code install or using binary packages provided by their distribution. The binary packages are generally quicker and easier to install, and are often slightly customized to use the distribution's standard directory paths and such. These packages also allow for consistent management in terms of upgrading, removing, or surveying software on the system. A downside is that packages created by the distributions are necessarily behind the Insecure.Org source releases. Most Linux distributions (particularly Debian and Gentoo) keep their Nmap package relatively current, though a few are way out of date. Choosing the source install allows for more flexibility in determining how Nmap is built and optimized for your system. To build Nmap from source, see Section 2.2. Here are simple package instructions for the most common distributions.

### 2.3.1. RPM-based distributions (Red Hat, Mandrake, Suse, Fedora)

I build RPM packages for every release of Nmap and post them to the Nmap download page at [http://www.insecure.org/nmap/nmap\\_download.html](http://www.insecure.org/nmap/nmap_download.html). I build two packages: The `nmap` package contains just the command-line executable and data files, while the `nmap-frontend` package contains the optional X-Window graphical frontend named `nmapfe`. The `nmap-frontend` package is optional and only necessary for those who want a GUI interface to Nmap. It does require that the `nmap` package be installed first.

Installing via rpm is quite easy - it even downloads the package for you when given the proper URLs. The following example downloads and installs Nmap 3.48, including the frontend. Of course you should use the latest version at the download site above instead. Any existing RPM-installed versions are upgraded. Example 2-3 demonstrates this installation process.

**Example 2-3. Installing Nmap from binary RPMs**

```
# rpm -vhU http://download.insecure.org/nmap/dist/nmap-3.48-1.i386.rpm
Retrieving http://download.insecure.org/nmap/dist/nmap-3.48-1.i386.rpm
Preparing... #####
1:nmap #####
# rpm -vhU http://download.insecure.org/nmap/dist/nmap-frontend-3.48-1.i386.rpm
Retrieving http://download.insecure.org/nmap/dist/nmap-frontend-3.48-1.i386.rpm
Preparing... #####
1:nmap-frontend #####
core/home/fyodor#
```

As the filenames above imply, these binary RPMs were created for normal PCs (X86 architecture). So they do not work for the relatively few Linux users on other platforms such as SPARC, Alpha, or PowerPC. They also may refuse to install if your library versions are sufficiently different from what the RPMs were initially built on. One option in these cases would be to find binary RPMs prepared by your Linux vendor for your specific distribution. The original install CDs or DVD are a good place to start. Unfortunately, those may not be current or available. Another option is to install Nmap from source code as described previously, though you lose the binary package maintenance consistency benefits. A third option is to build and install your own binary RPMs from the source RPMs distributed from the download page above. Example 2-4 demonstrates this technique with Nmap 3.48.

**Example 2-4. Building and installing Nmap from source RPMs**

```
> rpm --rebuild http://download.insecure.org/nmap/dist/nmap-3.48-1.src.rpm
[ hundreds of lines cut ]
Wrote: /home/fyodor/rpmdir/RPMS/i386/nmap-3.48-1.i386.rpm
Wrote: /home/fyodor/rpmdir/RPMS/i386/nmap-frontend-3.48-1.i386.rpm
[ cut ]
> su
Password:
# rpm -vhU /home/fyodor/rpmdir/RPMS/i386/nmap-*3.48-1.i386.rpm
Preparing... #####
1:nmap #####
2:nmap-frontend #####
#
```

Removing RPM packages is as easy as **rpm -e nmap nmap-frontend**.

**2.3.2. Debian Linux**

LaMont Jones does a fabulous job maintaining the Nmap .deb packages, including keeping them reasonably up-to-date. The proper upgrade/install command is **apt-get install nmap**. Information on the latest Debian "stable" Nmap package is available at <http://packages.debian.org/stable/net/nmap.html> and the development ("unstable") package info is available from <http://packages.debian.org/unstable/net/nmap.html>.

**2.3.3. Gentoo Linux**

\* I believe Gentoo uses "emerge nmap" or some such. Can anyone send me details?

### 2.3.4. Other Linux distributions

There are far too many Linux distributions available to list here, but even many of the obscure ones include Nmap in their package tree. Even if they do not, you can simply compile from source code as described in Section 2.2.

*\* If I am missing any important distributions, please send me details on installing their Nmap binary package*

## 2.4. Windows

Although Windows support is a relatively recent Nmap phenomenon, it has quickly grown into the second most popular Nmap platform. Because of this popularity and the fact that many Windows users do not have a compiler, binary executables are distributed for each major Nmap release. While it is improving rapidly, the Windows port is still not as efficient or stable as on UNIX. Here are some known limitations (at the time of this writing):

- You cannot generally scan your own machine from itself (using a loopback IP such as 127.0.0.1 or any of its registered IP addresses)
- Most scanning over RAS connections (such as PPP dialups) are only supported under Windows 2000/XP.
- Version detection cannot use SSL scan-through (discussed in Chapter 6)
- Scans from Windows often take longer than on UNIX

I would like to thank Ryan Permeh of eEye, Andy Lutomirski, and Jens Vogt for their hard work on the Nmap Windows port. For many years, Nmap was a UNIX-only tool, and it would likely still be that way if not for their efforts.

Windows users have three choices for installing Nmap, all of which are available from the download page at [http://www.insecure.org/nmap/nmap\\_download.html](http://www.insecure.org/nmap/nmap_download.html).

### 2.4.1. Command line .zip binaries

Every major "stable" Nmap release comes with Windows command-line binaries and associated files in a Zip archive. No graphical interface is included, so you need to run `nmap.exe` from a DOS/command window. Or you can download and install a superior command shell such as those included with the free Cygwin system available from <http://www.cygwin.com>. Here are the step-by-step instructions for installing and executing the Nmap .Zip binaries.

#### 2.4.1.1. Installing the Nmap .Zip binaries

1. Read the Nmap Win32 support page (<http://www.insecure.org/nmap/data/README-WIN32>) for the latest updates
2. Download the .Zip binaries from [http://www.insecure.org/nmap/nmap\\_download.html](http://www.insecure.org/nmap/nmap_download.html).
3. Uncompress the zip-file into the directory you want Nmap to reside in. An example would be "C:\Program Files\". A directory called `nmap-VERSION` should be created, which includes the Nmap executable and data files. If you do not have a Zip decompression program, there is one (called `unzip`) in Cygwin above, or you can download the open source and free 7-zip utility from <http://www.7-zip.org>. Commercial alternatives are Winzip and PKZIP from <http://www.winzip.com> and <http://www.pkware.com> respectively.

4. For improved performance, apply the Nmap registry changes by clicking on nmap\_performance.reg in the new Nmap directory. This increases the number of ephemeral ports reserved for user applications (such as Nmap) and decreases the amount of time before a closed connection can be reused.
5. Nmap requires the free WinPcap packet capture library. Obtain and install the latest version from <http://winpcap.polito.it>. They distribute an executable installer which makes this easy. At the time of this writing, the latest version is 3.01 and is known to work. Downloading the newest version available is recommended.

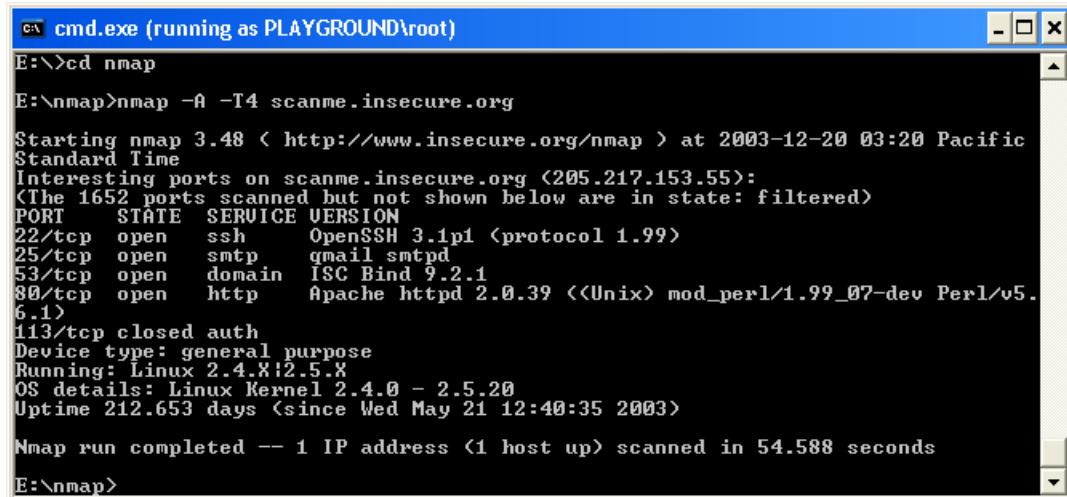
#### 2.4.1.2. Executing Nmap as installed above

1. Make sure the user you are logged in as has administrative privileges in the box (should be in the administrators group).
2. Open a command/DOS Window. Though it can be found in the program menu tree, the simplest approach is to choose Start -> Run and type cmd<enter>. Opening a Cygwin window (if you installed it) by clicking on the Cygwin icon on the desktop works too, although the necessary commands differ slightly from those shown below.
3. Change to the directory you installed Nmap into. Assuming the example directory name used in the install section above, type the following commands.

```
c:  
cd "\program files\nmap-VERSION" (replace VERSION with the Nmap version number)
```

4. Execute nmap.exe. Figure 2-2 is a screen shot showing a simple example

**Figure 2-2. Executing Nmap from a Windows command shell**



```
cmd.exe (running as PLAYGROUND\root)
E:\>cd nmap
E:\nmap>nmap -A -T4 scanme.insecure.org
Starting nmap 3.48 < http://www.insecure.org/nmap > at 2003-12-20 03:20 Pacific
Standard Time
Interesting ports on scanme.insecure.org (205.217.153.55):
(The 1652 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 3.1p1 <protocol 1.99>
25/tcp    open  smtp   gmail smtpd
53/tcp    open  domain ISC Bind 9.2.1
80/tcp    open  http   Apache httpd 2.0.39 <<Unix> mod_perl/1.99_07-dev Perl/v5.
6.1>
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.4.8!2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 212.653 days <since Wed May 21 12:40:35 2003>
Nmap run completed -- 1 IP address (1 host up) scanned in 54.588 seconds
E:\nmap>
```

If you execute Nmap frequently, you can the Nmap directory (c:\program files\nmap-VERSION in this case) to your command execution path. The exact place to set this varies by Windows platform. On my Windows XP box, I do the following:

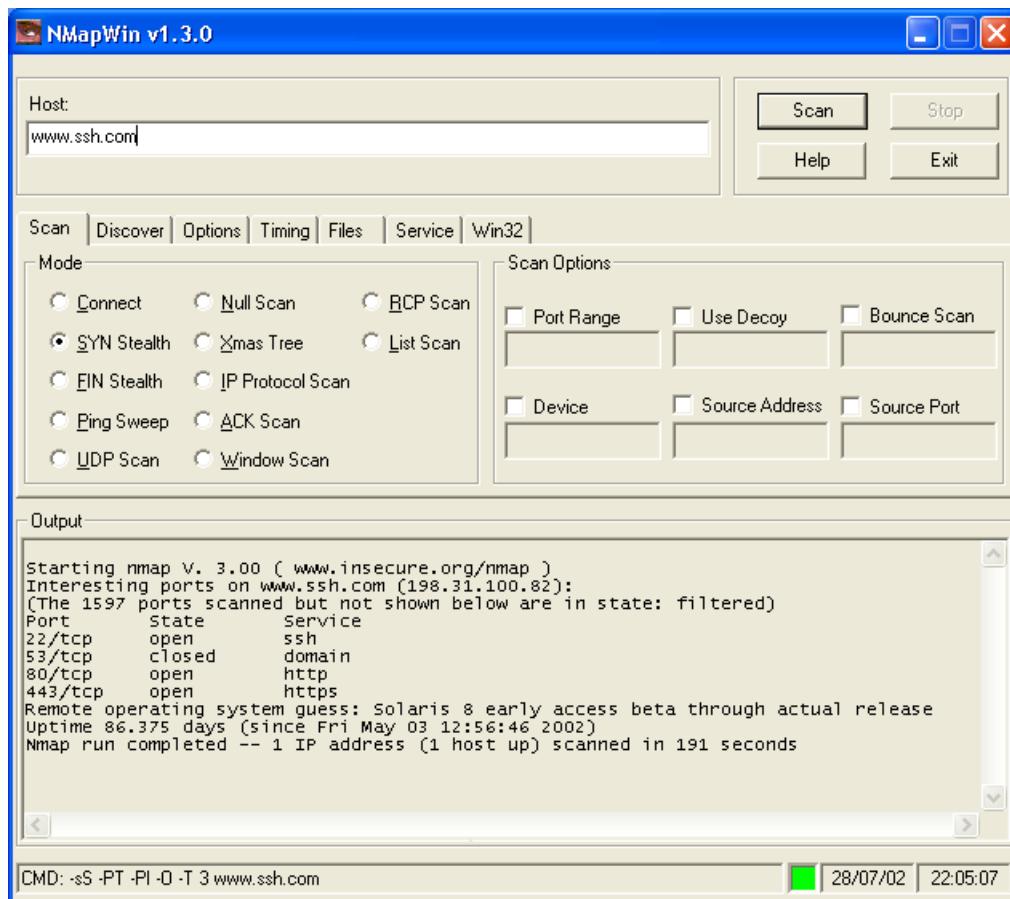
1. From the desktop, right click on My Computer and then click properties.

2. In the System Properties window, click the Advanced tab.
3. Click the Environment Variables button.
4. Choose Path from the System variables section, then hit edit.
5. Add a semi-colon and then your Nmap directory (such as c:\program files\nmap-VERSION) to the end of the value.
6. Open a new DOS window and you should be able to execute a command such as **nmap scanme.nmap.org** from any directory.

## 2.4.2. Nmapwin

\* I am going to save this until later in case the Nmapwin landscape changes. When I do cover it, I should note instructions for upgrading the Nmap version that comes in the Nmapwin installer.

**Figure 2-3. NmapWin provides a slick Windows interface to Nmap**



### 2.4.3. Compile from source code

Most Windows users prefer to use the Nmap binary distribution, but compilation from source code is an option. Compilation presently requires certain versions of the commercial Microsoft Visual C++ compiler (part of MS Visual Studio). The following steps are required.

#### Compiling Nmap on Windows from Source.

1. Read the Nmap Win32 support page at <http://www.insecure.org/nmap/data/README-WIN32> for the latest updates. The Windows compilation instructions do change occasionally.
2. Make sure you have installed Microsoft Visual Studio .Net 2003 or later. Apparently the "solution files" with build instructions do not even work in the 2002 version of the software. This is typical Microsoft behavior and it exemplifies why most Windows users use the binary package while many UNIX users prefer source compilation.
3. Download the latest Nmap source distribution from [http://www.insecure.org/nmap/nmap\\_download.html](http://www.insecure.org/nmap/nmap_download.html). It has the name nmap-*version*.tgz or nmap-*version*.tar.bz2 . Those are the same tar file compressed using gzip or bzip2, respectively.
4. Uncompress the source code file you just downloaded. Recent releases of the free Cygwin distribution (<http://www.cygwin.com/>) can handle both the .tgz and .tar.bz2 . Use the command **tar xvzf nmap-*version*.tgz** or **tar xvjf nmap-*version*.tar.bz2**, respectively. Alternatively, the common Winzip application can decompress the .tgz version.
5. Open Visual Studio and the Nmap solution file ( nmap-VERSION/mswin32/nmap.sln )
6. From the Build Menu, select Configuration Manager and set Active Solution Configuration to Release.
7. Choose Build Solution from the Build Menu. Nmap should begin compiling, and end with the line "-- Done --" saying that all projects built successfully and there were 0 failures.
8. The executable and data files can be found in nmap-VERSION/mswin32/Release/ . You can copy them to a preferred directory as long as they are all kept together.
9. Nmap requires the free WinPcap packet capture library. Obtain and install the latest version from <http://winpcap.polito.it>. They distribute an executable installer which makes this easy.
10. Instructions for executing your compiled Nmap are the same as given above for the .zip binaries.

Many people have asked whether Nmap can be compiled with the gcc/g++ included with Cygwin or other compilers. At this time, only Visual Studio is supported because that is what the original Windows porters used. If someone develops a clean patch which allows for compilation by free compilers, it is likely to be integrated into the project build system. Because of this unfortunate requirement for commercial tools to build Nmap on Windows, new binaries are frequently made available on the download page.

## 2.5. Sun Solaris

Solaris has long been well-supported by Nmap. Sun even donated a complete SPARCstation to the project, which is still being used to test new Nmap builds. For this reason, many Solaris users compile and install from source code as described in Section 2.2.

Users who prefer native Solaris packages will be pleased to learn that Steven Christensen does an excellent job of maintaining Nmap packages over at <http://www.sunfreeware.com>. Instructions are on his site, and are generally very simple: download the appropriate Nmap package for your version of Solaris, decompress it, and then run **pkgadd -d packagename**. As is generally the case with contributed binary packages, these Solaris packages are simple and quick to install. The advantages of compiling from source are that a newer version may be available and you have more flexibility in the build process. Certain optional features such as OpenSSL version detection are often not available in prebuilt packages.

## 2.6. Apple Mac OS X

Thanks to several people graciously donating shell accounts on their OS X boxes, Nmap usually compiles on that platform without problems. Doing this does require the Apple Developer Tools system. If you are not careful, Apple tries to charge for them. Brian Hatch sent me the following steps for obtaining the Developer Tools for free (as of September 2003).

1. Browse to <http://connect.apple.com> and join the ADC (Apple Developer Connection)
2. Fill out several forms to create a new account
3. Eventually you reach a page for buying support and/or CD media. Ignore this page and return to <http://connect.apple.com>.
4. Log in with your new account credentials.
5. Hit the Download link on the left and then choose Developer Tools.
6. Download the most recent Dev Tools and install.
7. Download the most recent Dev Tools Updates and install.

\* Verify that these steps have not changed shortly before release

These exact steps may change, but it is hoped that this general approach will continue to work.

Once you have the developer tools installed, you can follow the compilation instructions found in Section 2.2. Note that on some older versions of Mac OS X, you may have to replace the command **./configure** with **./configure CPP=/usr/bin/cpp**.

Users who prefer binary packages may want to have a look at the Fink project (<http://fink.sourceforge.net>). Their stated goal is “to bring the full world of Unix Open Source software to Darwin and Mac OS X,” and so they offer Nmap and hundreds of other useful packages. As with all contributed binary packages, the disadvantage is that they may not be up-to-date with the latest Nmap releases and you have less flexibility in the build process. But it is certainly worth a look if you want to install many popular UNIX tools at once.

## 2.7. FreeBSD / OpenBSD / NetBSD

The BSD flavors are well supported by Nmap, so you can simply compile it from source as described in Section 2.2. This provides the normal advantages of always having the latest version and a flexible build process. If you prefer binary packages, these \*BSD variants each maintain their own Nmap packages. Many BSD systems also have a “ports” tree which standardizes the compilation of popular applications. Instructions for installing Nmap on the most popular \*BSD variants follow.

### 2.7.1. OpenBSD binary packages and source ports instructions

According to the OpenBSD FAQ (<http://www.openbsd.org/faq/>), users “are HIGHLY advised to use packages over building an application from ports. The OpenBSD ports team considers packages to be the goal of their porting work, not the ports themselves.”. That same FAQ contains detailed instructions for each method. Here is a summary.

#### Installation using binary packages

1. Choose a mirror from <http://www.openbsd.org/ftp.html>. FTP in and grab the Nmap package from `/pub/OpenBSD/version/packages/platform/nmap-version.tgz`. Or obtain it from the OpenBSD distribution CD-ROM.
2. As root, execute: `pkg_add -v nmap-version.tgz`

#### Installation using the source ports tree

1. If you do not already have a copy of the ports tree, obtain it via CVS using instructions at <http://www.openbsd.org/faq/faq8.html#CVS>.
2. As root, execute the following command (replace /usr/ports with your local ports directory if it differs):

```
cd /usr/ports/net/nmap && make install clean
```

### 2.7.2. FreeBSD binary package and source ports instructions

The FreeBSD has a whole chapter ([http://www.freebsd.org/doc/en\\_US.ISO8859-1/books/handbook/ports.html](http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/ports.html)) in their Handbook describing the package and port installation processes. A brief summary of the process follows.

#### 2.7.2.1. Installation of the binary packages

The easiest way to install the binary Nmap package is to run `pkg_add -r nmap`. You can then run the same command with an `nmapfe` option if you want the X-Window front-end. If you wish to obtain the package manually instead, retrieve it from <http://www.freebsd.org/cgi/ports.cgi?query=nmap> or the CDROM and run `pkg_add packagename.tgz`.

#### Installation using the source ports tree

1. The ports tree is often installed with the system itself (usually in /usr/ports). If you do not already have it, specific installation instructions are provided in the FreeBSD Handbook chapter referenced above.
2. As root, execute the following command (replace /usr/ports with your local ports directory if it differs):

```
cd /usr/ports/security/nmap && make install clean
```

### 2.7.3. NetBSD binary package instructions

NetBSD has packaged Nmap for an enormous number of platforms, from the normal i386 to Playstation 2, PowerPC, Vax, SPARC, MIPS, Amiga, ARM, and several platforms that I have never even heard of! Unfortunately they are not very up-to-date. A list of NetBSD Nmap packages is available from

<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/net/nmap/README.html> and a description of using their package system to install applications is available at <http://www.netbsd.org/Documentation/pkgsrc/using.html#id2956484>.

## **2.8. Amiga, HP-UX, IRIX, and Other Platforms**

One of the wonders of Open Source development is that resources are often biased towards what people find exciting rather than having an exclusive focus on profits as most corporations do. It is along those lines that the Amiga port came about. Diego Casorran performed most of the work and sent in a clean patch which was integrated into the main Nmap distribution. In general, AmigaOS users should be able to simply follow the source compilation instructions in Section 2.2. You may encounter a few hurdles on some systems, but I presume that must be part of the fun for Amiga fanatics.

Nmap supports many proprietary UNIX flavors such as HP-UX and SGI IRIX. The Nmap project mostly depends on the user community to maintain adequate support for these systems. If you have trouble, try sending a report with full details to the nmap-dev mailing list (<[nmap-dev@insecure.org](mailto:nmap-dev@insecure.org)>). If you develop a patch which improves support on your platform, please email it to me at <[fyodor@insecure.org](mailto:fyodor@insecure.org)>.

## **2.9. [RECIPE] Installing Nmap on a PDA**

Previous sections have described the installation of Nmap on notebook and desktop computers running a wide variety of operating systems. However, some users want greater portability and stealth than even the smallest notebook computers provide. They wish to do their security auditing from a personal digital assistant (PDA) small enough to fit in their pocket or to hide near an ethernet jack in a corporate office or datacenter. Walking around while using a notebook can raise eyebrows. With a PDA, passers by may assume you are just checking your calendar or shopping list while you locate insecure wireless access points or scan their internal network for vulnerabilities. Thanks in a large part to enthusiastic user communities, Nmap supports numerous PDAs. Two of the best supported are the Sharp Zaurus and Compaq IPAQ. Nmap has not been ported to PalmOS systems.

**Table 2-1. The Sharp Zaurus is an excellent platform for highly mobile security applications**

---



This recipe focuses on the Sharp Zaurus because it is the most popular PDA for running Nmap. Users of the Compaq IPAQ may wish to investigate the Familiar Linux distribution for similar functionality. Many other PDAs have active developer communities that are easily found with Google or through sites such as <http://www.handhelds.org>. The Zaurus is popular with mobile security auditors for many reasons.

### Advantages of the Sharp Zaurus for hackers

- Keyboard (sliding or folding) allows easy use of Linux console commands
- Lightweight, compact form factor is convenient and inconspicuous
- Reasonably fast (200Mhz+) ARM processor and adequate RAM (32MB+) provide plenty of power for running Nmap and other security tools
- A wide variety of CF networking cards are supported without bulky adapters. Secure Digital cards are also supported for extra flash storage.
- Ships with Linux pre-installed, making it compatible with a wide variety of popular free security tools (and other software).
- The OpenZaurus project provides convenient support for Nmap, NmapFE, and many other security tools

Many thanks go to Kevin Milne, Adrian Crenshaw (AKA IronGeek), and David Malcher (KillingJoke), avid Zaurus users who provided much of the content and screenshots for this recipe.

#### 2.9.1. Installing Nmap on the Zaurus

Before beginning, make sure you have sufficient hardware.

##### System Requirements

- A Sharp Zaurus (any model)
- 64MB or larger Compact Flash (CF) card for the OpenZaurus ROMS

- A CF networking card such as a basic ethernet card and/or wireless 802.11X. Wireless cards with the Prism2 chipset are recommended. Kevin uses a Xircom 10MB ethernet card and a Netgear MA701 wireless card. Adrian uses an Ambicom WL1100C-CF Wi-Fi card and an TRENDnet/TRENDware TE-CF100 ethernet card.

The most common way to install Nmap is using the OpenZaurus project (<http://www.openzaurus.org>). They provide an alternative ROM image (Linux kernel and filesystem) with a greater emphasis on development and open source tools than the ROM Sharp provides. OpenZaurus is based on the popular Debian Linux distribution. Many other Zaurus Linux distributions are available to suit different needs and preferences. The OpenZaurus project may be subsumed by the more general OpenEmbedded distribution.

Rather than describe the installation process here, readers are advised to follow the directions in the OpenZaurus Install Guide available from [http://www.openzaurus.org/oz\\_website/content/installguide](http://www.openzaurus.org/oz_website/content/installguide). Follow those directions carefully to avoid damaging your Zaurus.

Once OpenZaurus is installed, thousands of open source applications are available for easy installation as IPK files (the file extensions should be .ipk). These are available for download from the OpenZaurus site, or a number of 3rd party sites such as <http://www.killefiz.de/zaurus/>. While finding IPK files on the Internet is quite convenient, they are not always up-to-date. At the time of this writing, the latest IPK of Nmap available via the sites OpenZaurus.Org and Killefiz.de is almost 2 years old. A bit of Internet searching turned up IronGeek's excellent resource site at <http://www.irongeek.com/all.php>. He includes instructions for installing the very latest Nmap version. As with many emerging technologies, browsing and searching specialized web sites is highly recommended as a supplement to book information. Even an efficient dead-tree publisher like O'Reilly cannot hope to disseminate news as quickly as (some) Web sites can.

After downloading IPK files to the Zaurus, they can be installed with the ipkg program. An example execution would be **ipkg install nmap\_3.27-1\_armv4l-strongarm.ipk**. Type **ipkg** with no arguments for help.

A convenient alternative to manually downloading and installing IPK files is the Zaurus Package Manager. It makes installing a large number of packages simple and quick.

### **Installing Nmap using the Zaurus Package Manager**

1. Click on the **Settings** tab and choose **Packages**.
2. The first time you start the Package Manager, activate the feeds through the **Options -> Configure** screen and configure the stable, testing, and/or unstable feeds. Nmap is currently part of the testing feed.
3. Since the available packages are frequently updated, perform a feed update by choosing **Actions** and then **Update Lists**.
4. A huge list of available software is provided. You may have to switch to the **testing** feed to obtain Nmap and NmapFE. NmapFE is the official UNIX GUI frontend that is distributed with Nmap. What OpenZaurus.Org calls NmapFE is actually Qopenmapfe (<http://home.midsouth.rr.com/zaurus/>), a simplified clone written by Dennis Webb. Scroll down the list of software packages and check Nmap, NmapFE, and anything else that catches your fancy. Many excellent security tools are available.
5. After selecting all of the appropriate software, click the GO (green arrow) icon on the top right hand of the screen. The installation manager screen shows the progress of software download and installation.

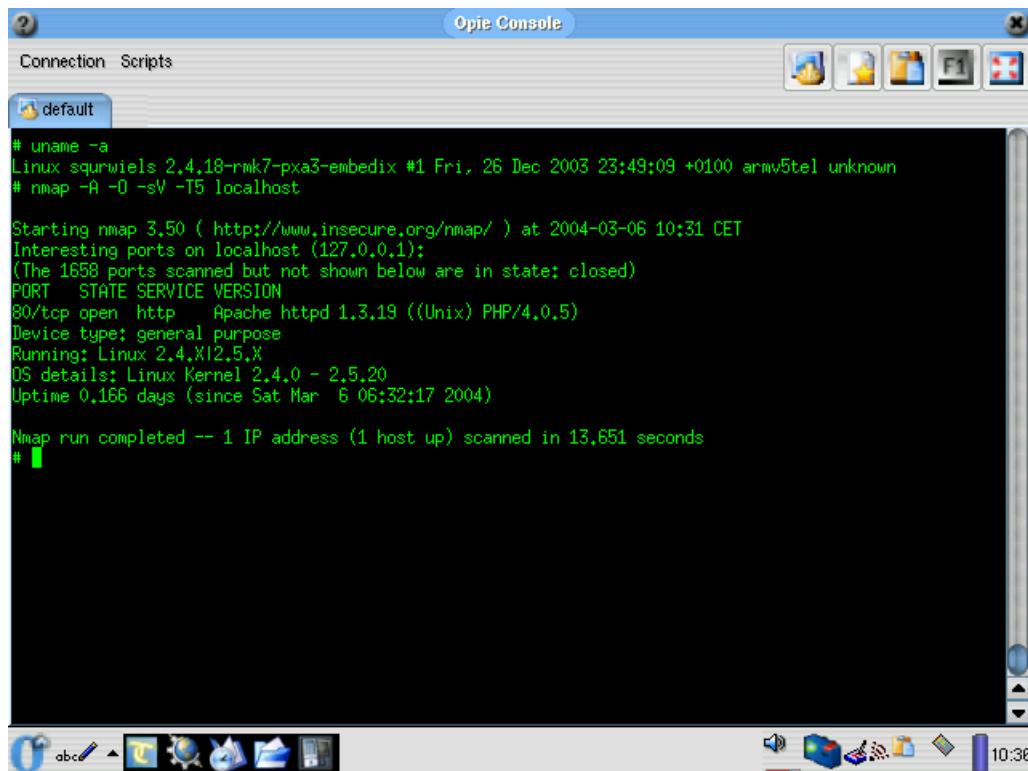
### **2.9.2. Using Nmap and NmapFE on the Zaurus**

Once NmapFE and Nmap have been properly installed, a new NmapFE icon should appear in the Applications menu. If it does not appear, try restarting Opie. Simply click the icon to use it. If you prefer the command-line version of Nmap, start the console and execute the appropriate command. The screenshots at the top of this recipe demonstrate

both methods. Except for a simplified option set in qopenmapfe, usage of Nmap is the same as described in the rest of this book. The following figures show another type of Zaurus (the SL-C760) and how to run Nmap on it.

**Figure 2-4. The Sharp Zaurus SL-C760 PDA**



**Figure 2-5.** The SL-C760 executing Nmap in a terminal window

## 2.10. Removing Nmap

If your purpose for removing Nmap is simply to upgrade to the latest version, you can usually use the "upgrade" option provided by most binary package managers. Similarly, installing the latest source code (as described in Section 2.2) generally overwrites any previous from-source installations. Removing Nmap is a good idea if you are changing install methods (such as from source to RPM or vice versa) or if you are not using Nmap anymore and you care about a few megabytes of disk space.

How to remove Nmap depends on how you installed it initially (see previous sections). Ease of removal (and other maintenance) is a major advantage of most binary packages. For example, when Nmap is installed using the RPM system common on Linux distributions, it can be removed by running the command **rpm -e nmap nmap-frontend** as root. Analogous options are offered by most other package managers -- consult their documentation for further information.

If you installed Nmap from source code, removal is slightly more difficult. If you still have the build directory available (where you initially ran **make install**), you can remove Nmap by running **make uninstall**. If you no longer have that build directory, type **nmap -v** to obtain the Nmap version number. Then download that source tarball for that version of Nmap from <http://download.insecure.org/nmap/dist/>. Uncompress the tarball and change into the newly created directory (**nmap-VERSION**). Run **./configure**, including any install-path options that you specified the first time (such as **--prefix** or **--datadir**). Then run **make uninstall**. Alternatively, you can simply delete all the Nmap-related files. If you used a default source install of Nmap versions 3.00 or higher, the following command

removes it.

```
# cd /usr/local  
# rm -f bin/nmap bin/nmapfe bin/xnmap  
# rm -f man/man1/nmap.1 man/man1/nmapfe.1 man/man1/xnmap.1  
# rm -rf share/nmap share/gnome/apps/Utilities/nmapfe.desktop
```

You may have to adjust the above commands slightly if you specified `--prefix` or other install-path option when first installing Nmap. The files relating to nmapfe/xnmap do not exist if you did not install the NmapFE frontend initially.

## Notes

1. <http://www.cert.org/advisories/CA-2002-28.html>
2. <http://www.cert.org/advisories/CA-2002-24.html>

# Chapter 3. Host Enumeration ("Ping Scanning")

## 3.1. Introduction

One of the very first steps in any network reconnaissance mission is to reduce a (sometimes huge) set of IP ranges into a list of active or interesting hosts. Scanning every port of every single IP address is slow and usually unnecessary. Of course what makes a host interesting depends greatly on the scan purposes. Network administrators may only be interested in hosts running a certain service, while security auditors may care about every single device with an IP address. An administrator may be comfortable using just an ICMP ping to locate hosts on his internal network, while an external penetration tester may use a diverse set of dozens of probes in an attempt to evade firewall restrictions.

Because host enumeration needs are so diverse, Nmap offers a wide variety of options for customizing the techniques used. Despite the name ping scan, this goes well beyond the simple ICMP echo request packets associated with the ubiquitous ping tool. Users can skip the ping step entirely with a list scan (`-sL`) or by disabling ping (`-P0`), or engage the network with arbitrary combinations of multi-port TCP SYN/ACK, UDP, and ICMP probes. The goal of these probes is to solicit responses which demonstrate that an IP address is actually active (is being used by a host or network device). On many networks, only a small percentage of IP addresses are active at any given time. This is particularly common with RFC1918-blessed private address space such as 10.0.0.0/8. That network has 16 million IPs, but I have seen it used by companies with less than a thousand machines. Host enumeration can find those machines in a sparsely allocated sea of IP addresses.

This chapter first discusses how Nmap ping scanning works overall, with high-level control options. Then specific techniques are covered, including how they work and when each is most appropriate. Nmap offers many ping techniques because it often takes carefully crafted combination to get through a series of firewalls and router filters leading to a target network. Effective overall ping scanning strategies are discussed, followed by a low-level look at the algorithms used.

## 3.2. Specifying Target Hosts and Networks

## 3.3. Host Enumeration Controls

By default, Nmap will include a ping scanning stage prior to more intrusive probes such as port scans, OS detection, or version detection. Nmap usually only performs intrusive scans on machines that are shown to be available in the ping scan stage. This saves substantial time and bandwidth over trying to scan every single IP address. However, this approach is not ideal for all circumstances. There are times when you *do* want to scan every IP (`-P0`), and other times when you want to do host enumeration and nothing more (`-sP`). There are even times when you want to print out the target hosts and exit prior to even sending ping probes (`-sL`). Nmap offers several high-level options to control this behavior.

### 3.3.1. List Scan (`-sL`)

The list scan is a degenerate form of host enumeration that simply lists each host of the network(s) specified, without sending any packets to the target hosts. By default, Nmap still does reverse-DNS resolution on the hosts to learn their names. Nmap also reports the total number of IP addresses at the end. The list scan is a good sanity check to ensure

that you have proper IP addresses for your targets. If the hosts sport domain names you do not recognize, it is worth investigating further to prevent scanning the wrong company's network.

There are many reasons target IP ranges can be incorrect. Even network administrators can mistype their own netblocks, and pen-testers have even more to worry about. In some cases, security consultants are given the wrong addresses. In others, they try to find proper IP ranges through resources such as whois databases and routing tables. The databases can be out of date, or the company could be loaning IP space to other organizations. Whether to scan corporate parents, siblings, service providers, and subsidiaries is an important issue that should be worked out with the customer in advance. A preliminary list scan helps confirm exactly what targets are being scanned.

Another reason for an advance list scan is stealth. In some cases, you do not want to begin with a full-scale assault on the target network that is likely to trigger IDS alerts and bring unwanted attention. A list scan is unobtrusive and provides information that may be useful in choosing which individual machines to target. It is possible, though highly unlikely, that the target will notice all of the reverse-DNS requests.

A list scan is specified with the `-sL` command-line option. Since the idea is to simply print a list of target hosts, options for higher level functionality such as port scanning, OS detection, or ping scanning cannot be combined with this. If you wish to disable ping scanning while still performing such higher level functionality, read up on the `-p0` option described in the next section. Example 3-1 shows list scan being used to enumerate the CIDR<sup>1</sup> /28 network range (16 IP addresses) surrounding the main Stanford webserver.

### **Example 3-1. Enumerating hosts surrounding WWW.Stanford.Edu with list scan**

```
felix~> nmap -sL www.stanford.edu/28

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Host www9.Stanford.EDU (171.67.16.80) not scanned
Host www10.Stanford.EDU (171.67.16.81) not scanned
Host scriptorium.Stanford.EDU (171.67.16.82) not scanned
Host coursework-a.Stanford.EDU (171.67.16.83) not scanned
Host coursework-e.Stanford.EDU (171.67.16.84) not scanned
Host www3.Stanford.EDU (171.67.16.85) not scanned
Host leland-dev.Stanford.EDU (171.67.16.86) not scanned
Host coursework-preprod.Stanford.EDU (171.67.16.87) not scanned
Host stanfordwho-dev.Stanford.EDU (171.67.16.88) not scanned
Host workgroup-dev.Stanford.EDU (171.67.16.89) not scanned
Host courseworkbeta.Stanford.EDU (171.67.16.90) not scanned
Host www4.Stanford.EDU (171.67.16.91) not scanned
Host coursework-i.Stanford.EDU (171.67.16.92) not scanned
Host leland2.Stanford.EDU (171.67.16.93) not scanned
Host coursework-j.Stanford.EDU (171.67.16.94) not scanned
Host 171.67.16.95 not scanned
Nmap run completed -- 16 IP addresses (0 hosts up) scanned in 0.384 seconds
```

### **3.3.2. Ping Scan (-sP)**

This option tells Nmap to *only* perform a ping scan, then print out the available hosts that responded to the scan. No further testing (such as port scanning or OS detection) is performed. This is one step more intrusive than the list scan, and can often be used for the same purposes. It allows light reconnaissance of a target network without attracting much attention. Knowing how many hosts are up is more valuable to attackers than the list of every single IP and host name provided by list scan.

Systems administrators often find this option valuable as well. It can easily be used to count available machines on a network or monitor server availability. This is often called a ping sweep, and is more reliable than pinging the broadcast address because many hosts do not reply to broadcast queries.

The following example shows a quick ping sweep against the CIDR /24 (256 IPs) surrounding one of my favorite Linux web sites, LWN.Net.

```
# nmap -sP -T4 www.lwn.net/24

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Host 66.216.68.0 seems to be a subnet broadcast address (returned 1 extra pings).
Host 66.216.68.1 appears to be up.
Host 66.216.68.2 appears to be up.
Host 66.216.68.3 appears to be up.
Host server1.camnetsec.com (66.216.68.10) appears to be up.
Host akqa.com (66.216.68.15) appears to be up.
Host asria.org (66.216.68.18) appears to be up.
Host webcubic.net (66.216.68.19) appears to be up.
Host dizzy.yellowdog.com (66.216.68.22) appears to be up.
Host www.outdoorwire.com (66.216.68.23) appears to be up.
Host www.inspectorhosting.com (66.216.68.24) appears to be up.
Host jwebmedia.com (66.216.68.25) appears to be up.
[...]
Host rs.lwn.net (66.216.68.48) appears to be up.
Host 66.216.68.52 appears to be up.
Host cuttlefish.laughingsquid.net (66.216.68.53) appears to be up.
[...]
Nmap run completed -- 256 IP addresses (105 hosts up) scanned in 12.691 seconds
```

This example only took 13 seconds, but provides valuable information. In that class C sized address range, 105 hosts are up. From the unrelated domain names all packed into such a small IP space, it is clear that LWN uses a colocation or dedicated server provider. If the LWN machines turned out to be highly secure, an attacker might go after one of those neighbor machines and then perform a local ethernet attack with tools such as Ettercap or Dsniff. A white-hat use of this data would be a network administrator considering moving machines to this provider. He might e-mail a few of the listed organizations and ask their opinion of the service before signing a long-term contract or making the expensive and disruptive datacenter move.

The `-sP` option sends an ICMP echo request and a TCP packet to port 80 by default (except when executed by an unprivileged UNIX user). It can be combined with any of the techniques discussed in the next section for greater flexibility. If any of those probe type and port number options are used, these default probes are overridden. When strict firewalls are in place between the source host running Nmap and the target network, using those advanced techniques is recommended. Otherwise hosts could be missed when the firewall drops probes or their responses.

### 3.3.3. Disable Ping (-P0)

Another option is to skip the Nmap enumeration stage altogether. Normally, Nmap uses this stage to determine active machines for heavier scanning. By default, Nmap only performs heavy probing such as port scans, version detection, or OS detection against hosts that are found to be up. Disabling host enumeration with `-P0` causes Nmap to attempt the requested scanning functions against *every* target IP address specified. So if a class B sized target address space (/16) is specified on the command line, all 65,536 IP addresses are scanned. That second option character in `-P0` is a

zero and not the letter O. Proper host enumeration is skipped as with the list scan, but instead of stopping and printing the target list, Nmap continues to perform requested functions as if each target IP is active.

There are many reasons for disabling the Nmap ping tests. One of the most common is intrusive vulnerability assessments. One can specify dozens of different ping probes in an attempt to elicit a response from all available hosts, but it is still possible that an active yet heavily firewalled machine might not reply to any of the probes. So to avoid missing anything, auditors frequently perform intense scans, such as for all 65,536 TCP ports, against every IP on the target network. It may seem wasteful to send hundreds of thousands of packets to IP addresses that probably have no host listening, and it can slow scan times by an order of magnitude or more. Nmap must send retransmissions to every port in case the original probe was dropped in transit, and Nmap must spend substantial time waiting for responses because it has no round-trip-time (RTT) estimate for these non-responsive IP addresses. But serious penetration testers are willing to pay this price to avoid even a slight risk of missing active machines. They can always do a quick scan as well, leaving the massive `-P0` scan to run in the background while they work. Chapter 6 provides substantial performance advice.

Another frequent reason for using `-P0` is that the tester has a list of machines that are already known to be up. There is no point wasting time with the host enumeration stage, the reasoning goes. The user creates their own list of active hosts and then passes it to Nmap using the `-iL` (take input from list) option. This strategy is rarely beneficial from a time-saving perspective. Even one unresponsive IP address in a large list will often take more time to scan than a whole ping scanning stage would have, due to the retransmission and RTT estimate issues discussed in the previous paragraph. In addition, the ping stage allows Nmap to gather RTT samples that can speed up the following port scan, particularly if the target host has strict firewall rules. While specifying `-P0` is rarely helpful as a time saver, it is important if some of the machines on your list block all of the enumeration techniques that would otherwise be specified. Users must strike a balance between scan speed and the possibility of missing a heavily cloaked machine.

## 3.4. Host Enumeration Techniques

There was a day when finding whether an IP address was registered to an active host was easy. Simply send an ICMP echo request ("ping") packet and wait for a response. Firewalls rarely blocked these requests, and the vast majority of hosts obediently responded. Such a response has been required since 1989 by RFC 1122 (<http://www.rfc-editor.org/rfc/rfc1122.txt>), which clearly states that "Every host MUST implement an ICMP Echo server function that receives Echo Requests and sends corresponding Echo Replies".

Unfortunately for network explorers, many administrators have decided that security concerns trump RFC requirements and have blocked ICMP ping messages. Example 3-2 uses an ICMP-only Nmap ping scan against six popular Web sites, but receives only two responses. This demonstrates that hosts can no longer be assumed unavailable based on failure to elicit an ICMP ping response. The `-sP -PE` options specify an ICMP-only ping scan and will soon be discussed. `-R` tells Nmap to perform reverse-DNS resolution against all hosts, even down ones.

### Example 3-2. Attempts to ping popular Internet hosts

```
# nmap -sP -PE -R -v microsoft.com ebay.com citibank.com google.com slashdot.org yahoo.com

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Host origin2.microsoft.com (207.46.250.252) appears to be down.
Host pages.ebay.com (66.135.192.87) appears to be down.
Host ld1-www.citicorp.com (192.193.195.132) appears to be down.
Host 216.239.57.99 appears to be up.
Host slashdot.org (66.35.250.150) appears to be down.
```

```
Host w3.rc.dcn.yahoo.com (216.109.127.30) appears to be up.  
Nmap run completed -- 6 IP addresses (2 hosts up) scanned in 3.762 seconds
```

Fortunately, Nmap offers a wide variety of host enumeration techniques beyond the standard ICMP echo request. They are described in the following sections.

### 3.4.1. TCP SYN Ping (-PS[portlist])

This option sends an empty TCP packet with the SYN flag set. The default destination port is 80 (configurable at compile time by changing DEFAULT\_TCP\_PROBE\_PORT in `nmap.h`), but an alternate port can be specified as a parameter. A comma separated list of ports can even be specified (e.g. `-PS22,23,25,80,113,1050,35000`), in which case probes will be attempted against each port in parallel.

The SYN flag suggests to the remote system that you are attempting to establish a connection. Normally the destination port will be closed, and a RST (reset) packet sent back. If the port happens to be open, the target will take the second step of a TCP 3-way-handshake by responding with a SYN|ACK TCP packet. The machine running Nmap then tears down the nascent connection by responding with a RST rather than sending an ACK packet which would complete the 3-way-handshake and establish a full connection.

Nmap does not care whether the port is open or closed. Either the RST or SYN|ACK response discussed previously tell Nmap that the host is available and responsive. However, Nmap does note the distinction in certain cases, allowing for a "turbo-mode" single-port sweep discussed in Chapter 4.

On UNIX boxes, only the privileged user `root` is generally able to send and receive raw TCP packets. For unprivileged users, a workaround is automatically employed whereby the `connect()` system call is initiated against each target port. This has the effect of sending a SYN packet to the target host, in an attempt to establish a connection. If `connect()` returns with a quick success or an ECONNREFUSED failure, the underlying TCP stack must have received a SYN|ACK or RST and the host is marked available. If the connection attempt is left hanging until a timeout is reached, the host is marked as down. This workaround is also used for IPv6 connections, as raw IPv6 packet building support is not yet available in Nmap.

Example 3-2 failed to detect four out of six machines because they did not respond to ICMP echo requests. Repeating the experiment using a SYN probe to port 80 (`http`) garners responses from all six, as shown in Example 3-3.

#### Example 3-3. Retry Host Enumeration using port 80 SYN probes

```
# nmap -sP -PS80 -R -v microsoft.com ebay.com citibank.com google.com slashdot.org yahoo.com  
  
Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )  
Host origin2.microsoft.com (207.46.249.252) appears to be up.  
Host pages.ebay.com (66.135.192.87) appears to be up.  
Host ld1-www.citicorp.com (192.193.195.132) appears to be up.  
Host 216.239.57.99 appears to be up.  
Host slashdot.org (66.35.250.150) appears to be up.  
Host w3.rc.dcn.yahoo.com (216.109.127.30) appears to be up.  
Nmap run completed -- 6 IP addresses (6 hosts up) scanned in 0.479 seconds
```

In addition to detecting all six machines, the second run is much faster. It takes less than half a second because the machines are scanned in parallel and it never times out waiting for a response. This test is not entirely fair because these are all popular web servers and thus can be expected to listen on port 80. However, it demonstrates the point that different types of hosts respond to different probe types. Nmap supports the usage of many scan types in parallel to enable effective scanning of diverse networks.

### 3.4.2. TCP ACK Ping (-PA[portlist])

The TCP ACK ping is quite similar to the just-discussed SYN ping. The difference, as you could likely guess, is that the TCP ACK flag is set instead of the SYN flag. Such an ACK packet purports to be acknowledging data over an established TCP connection, but no such connection exists. So remote hosts should always respond with a RST packet, disclosing their existence in the process.

The -PA option uses the same default port as the SYN probe (80) and can also take a list of destination ports in the same format. If an unprivileged user tries this, or an IPv6 target is specified, the connect() workaround discussed previously is used. This workaround is imperfect because connect() is actually sending a SYN packet.

The reason for offering both SYN and ACK ping probes is to maximize the chances of bypassing firewalls. Many administrators configure routers and other simple firewalls to block incoming SYN packets except for those destined for public services like the company web site or mail server. This prevents other incoming connections to the organization, while allowing users to make unobstructed outgoing connections to the Internet. This non-stateful approach takes up few resources on the firewall/router and is widely supported by hardware and software filters. As just one example of the prevalence of this method, the Linux Netfilter/iptables firewall software offers the --syn convenience option, which the man page describes as follows.

“ Only match TCP packets with the SYN bit set and the ACK and RST bits cleared. Such packets are used to request TCP connection initiation; for example, blocking such packets coming in an interface will prevent incoming TCP connections, but outgoing TCP connections will be unaffected. It is equivalent to --tcp-flags SYN,RST,ACK SYN. ”

When firewall rules such as this are in place, SYN ping probes (-PS) are likely to be blocked when sent to closed target ports. In such cases, the ACK probe shines as it cuts right through these rules.

Another common type of firewall uses stateful rules that drop unexpected packets. This feature was initially found mostly on high-end firewalls, though it has become much more common over the years. The Linux Netfilter/iptables system supports this through the --state option, which categorizes packets based on connection state as described in the following man page excerpt.

“ Possible states are INVALID meaning that the packet is associated with no known connection, ESTABLISHED meaning that the packet is associated with a connection which has seen packets in both directions, NEW meaning that the packet has started a new connection, or otherwise associated with a connection which has not seen packets in both directions, and RELATED meaning that the packet is starting a new connection, but is associated with an existing connection, such as an FTP data transfer, or an ICMP error. ”

The ACK probe is unlikely to work against firewalls taking this approach, as such an unexpected packet will be classified in the INVALID state and probably dropped. Example 3-4 shows an attempted ACK ping against Microsoft. Their stateful firewall drops the packet, leading Nmap to wrongly conclude that the host is down. The SYN probe has a much better chance of working in such cases. This begs the question of which technique to use when the firewall rules of the target networks are unknown or inconsistent. The proper answer is usually both. Nmap can send SYN and ACK probes to many ports in parallel, as well as performing other host enumeration techniques at the same time. This is further discussed in Section 3.5.

#### Example 3-4. Attempted ACK ping against Microsoft

```
# nmap -sP -PA www.microsoft.com
Starting nmap 3.51-TEST4 ( http://www.insecure.org/nmap/ )
```

```
Note: Host seems down. If it is really up, but blocking our ping probes, try -PO
Nmap run completed -- 1 IP address (0 hosts up) scanned in 37.949 seconds
```

### 3.4.3. UDP Ping (-PU[portlist])

Another host enumeration option is the UDP ping, which sends an empty (unless `--data_length` is specified) UDP packet to the given ports. The portlist takes the same format as with the previously discussed `-PS` and `-PA` options. If no ports are specified, the default is 31338. This default can be configured at compile-time by changing `DEFAULT_UDP_PROBE_PORT` in `nmap.h`. A highly uncommon port is used by default because sending to open ports is often undesirable for this particular scan type.

Upon hitting a closed port on the target machine, the UDP probe should elicit an ICMP port unreachable packet in return. This signifies to Nmap that the machine is up and available. Many other types of ICMP errors, such as host/network unreachables or TTL exceeded are indicative of a down or unreachable host. A lack of response is also interpreted this way. If an open port is reached, most services simply ignore the empty packet and fail to return any response. This is why the default probe port is 31338, which is highly unlikely to be in use. A few services, such as chargen, will respond to an empty UDP packet, and thus disclose to Nmap that the machine is available.

The primary advantage of this scan type is that it bypasses firewalls and filters that only screen TCP. For example, I once owned a Linksys BEFW11S4 wireless broadband router. The external interface of this device filtered all TCP ports by default, but UDP probes would still elicit port unreachable messages and thus give away the device.

### 3.4.4. ICMP Ping Types (-PE, -PP, and -PM)

In addition to the unusual TCP and UDP host enumeration types discussed previously, Nmap can send the standard packets sent by the ubiquitous ping program. Nmap sends an ICMP type 8 (echo request) packet to the target IP addresses, expecting a type 0 (Echo Reply) in return from available hosts. As noted at the beginning of this chapter, many hosts and firewalls now block these packets, rather than responding as required by RFC 1122. For this reason, ICMP-only scans are rarely reliable enough against unknown targets over the Internet. But for system administrators monitoring an internal network, this can be a practical and efficient approach. Use the `-PE` option to enable this echo request behavior.

While echo request is the standard ICMP ping query, Nmap does not stop there. The ICMP standard (RFC 792 (<http://www.rfc-editor.org/rfc/rfc792.txt>)) also specifies timestamp request, information request, and address mask request packets as codes 13, 15, and 17, respectively. While the ostensible purpose for these queries is to learn information such as address masks and current times, they can easily be used for host enumeration. A system that replies is up and available. Nmap does not currently implement information request packets, as they are not widely supported. RFC 1122 insists that "a host SHOULD NOT implement these messages". Timestamp and address mask queries can be sent with the `-PP` and `-PM` options, respectively. A timestamp reply (ICMP code 14) or address mask reply (code 18) discloses that the host is available. These two queries can be valuable when admins specifically block echo request packets, but forget that other ICMP queries can be used for the same purpose.

### 3.4.5. Default Combination (-PB)

If none of these host enumeration techniques are chosen, Nmap uses a default which is equivalent to the `-PA -PE` arguments for Windows or privileged (root) UNIX users. Attentive readers know that this means a TCP ACK packet to port 80 and an ICMP Echo Request query are sent to each machine. For unprivileged UNIX shell users, the default

is equivalent to `-PS` (a TCP connect() call against port 80 of the target hosts). For security auditing, I recommend using a more comprehensive set of ping types, such as those discussed in Section 3.5.2.4.

### 3.4.6. ARP Scan (`-P?`)

This scan *does not yet exist*, but implementing it is high on the desired feature priority list. It sends an ethernet ARP request for every target IP given. If a response is received, that host is available. Of course this only works for targets on a local ethernet network, but that covers a substantial portion of Nmap usage. This scan should be much faster and even a little more reliable than other ping scan types under these circumstances. The technique and implementation plans are described further in Chapter 13.

## 3.5. Putting it All Together: Host Enumeration Strategies

### 3.5.1. Related Options

Previous sections describe the major options used to control the Nmap host enumeration phase and customize the techniques used. However, there are many more general Nmap options which are relevant here. This section provides a brief description of how these option flags relate to ping scanning. See the Nmap Reference Guide (Chapter 14) for complete descriptions of each option.

`-v` (same as `--verbose`)

By default, Nmap usually only prints active, responsive hosts. Verbose mode causes Nmap to print down hosts, as well as extra information about active ones.

`--source_port <portnum>`(same as `-g`)

Setting a constant source port works for ping scanning (TCP and UDP) as it does with other Nmap features. Some naive firewall administrators make a ruleset exception in order keep DNS (port 53) or FTP-DATA (port 20) working. Of course this opens a hole big enough to drive an Nmap ping scan through. Chapter 9 provides further details on this technique.

`-n, -R`

The `-n` option disables all DNS resolution, while the `-R` option enables DNS queries for all hosts, even down ones. The default behavior is to limit DNS resolution to active hosts. These options are particularly important for ping scanning because DNS resolution can greatly affect scan times.

`--data_length <length>`

This option adds `length` random bytes of data to every packet, and works with the TCP, UDP, and ICMP ping scan types (for privileged users scanning IPv4). This helps make the scan less conspicuous and more like the packets generated by the ubiquitous ping diagnostics program. Several intrusion detection systems (IDS), including Snort, have alerts for zero-byte ping packets. This option evades those alerts. An option value of 32 makes an echo request look more like it came from Windows, while 56 simulates the default Linux ping.

--ttl

Setting the outgoing TTL is supported for privileged users doing IPv4 ping scans. This could be useful as a safety precaution to ensure a scan does not propagate beyond the local network. It can also be used to simulate a native ping program even more convincingly.

Canned timing options (-T3, -T4, -T5, etc.)

As with Nmap functions in general, higher -T values speed up scanning. With a moderately fast and reliable connection between the source and target networks (i.e. anything more than a dial-up modem), the -T4 option is recommended.

--max\_parallelism, --min\_parallelism

These affect how many probes may be outstanding at once. With the default ping type (2-probes), the parallelism value is roughly the number of machines scanned in parallel. Reducing the ping techniques to one probe per host (e.g. -PE) will double the number of hosts scanned at once for a given parallelism level, while increasing to four probes per host (e.g. -PE -PS22,113,50000) halves it. Most users simply stick to the canned timing options such as -T4.

--min\_rtt\_timeout, --max\_rtt\_timeout, --initial\_rtt\_timeout

These options control how long Nmap waits for a ping response.

Input options (-iL, -iR)

Host input options are supported as in the rest of Nmap. Users often combine the input-from-list (-iL) option with -P0 to avoid ping-scanning hosts that are already known to be up. Read Section 3.3.3 before doing this in an attempt to save time. The -iR chooses hosts at random from allocated Internet IP space. It takes as an argument the number of random hosts you wish to scan. Use zero for a never-ending (until you abort or kill the Nmap process) scan.

Output options (-oA, -oN, -oG, -oX, etc.)

All of the Nmap output types (normal, grepable, and XML) support ping scanning. Chapter 11 further describes how they work.

--randomize\_hosts (same as -rH)

Shuffling the host scan order with this option may make the scan less conspicuous, though it also can make the scan output a bit more difficult to follow.

--packet\_trace

The normal Nmap output indicates whether a host is up or not, but does not describe which enumeration test(s) the host responded to. This is because Nmap uses a short-circuit algorithm for performance reasons. As soon as it receives any one response from a host, it stops listening for more. Printing the response might mislead users into thinking that the host only responded to one certain test, when the reality is that Nmap stopped paying attention after that point. Scanning several times might produce different results, depending on which response comes in first. To avoid this confusion, Nmap omits the ping response type altogether. Users who really need that information can rescan with --packet\_trace and see exactly what is going on at the packet level.

-D

Decoys are fully supported for privileged IPv4 ping scans, camouflaging the true attacker. Decoys are not used in DNS requests, so -n may be advisable for ultra-sensitive scans.

-6

The TCP connect()-based ping scans (-PS) support the IPv6 protocol, including multi-port mode.

-S <source IP address>, -e <sending device name>

As with other functions of Nmap, the source address and sending device can be specified with these options.

#### General options

By default, or if -P0 is specified, Nmap moves onto more intrusive scanning after the host enumeration stage. Thus many dozens of general port scanning, OS detection, and version detection options can be used. See the reference guide or relevant chapters for further information.

### 3.5.2. Choosing and Combining Ping Options

Effective scanning requires more than knowing all of the options described in this and previous sections. Users must understand how and when to use them to suit the target network topology and scanning goals.

#### 3.5.2.1. TCP probe and port selection

The TCP ping options are some of the most powerful enumeration techniques in Nmap. An administrator may be able to get away with blocking ICMP echo request packets without affecting most users, but a server absolutely must respond to SYN packets sent to the public services it provides. Meanwhile, ACK packets often get through non-stateful firewalls. I would recommend using both of SYN and ACK probes, using lists of ports based on any knowledge you might have of the target networks as well as more generally popular ports. A quick scan of more than 10,000 IP addresses across the Internet showed the ports in Table 3-1 to be particularly valuable. Of hosts with a default-drop filter (the hardest type to reach), these are the ports most likely to be accessible (open or closed).

**Table 3-1. Valuable TCP probe ports, in descending order of accessibility.**

Port number / Service	Reasoning
80/http	The prevalence of Web servers on the Internet leads many newbies to believe that the Web <i>is</i> the Internet.
25/smtp	Mail is another Internet "killer app" that companies allow through their firewalls.
22/ssh	SSH seems to have finally surpassed telnet as the standard for remote terminal administration.
443/https	SSL is a popular way for web sites to protect confidential information.
21/ftp	This file transfer protocol lives on, though many firewall administrators would not mourn its passing.

Port number / Service	Reasoning
113/auth	The auth (identd) service allows servers (usually mail or IRC) to request the username of clients connected to them. Administrators often leave this port unfiltered to avoid long timeouts that can occur when firewall rules prevent servers from connecting back to port 113. Using this port for ping scanning can sometimes lead to false positives, as some admins have been known to configure their firewalls to forge RST packets back in response to auth queries to any IP on their network, even when no machine exists at that IP. Administrators do this to avoid server timeouts while still preventing the ports from being accessed.
23/telnet	Many devices still offer this administrative interface, though it is a security nightmare.
53/domain	Domain Name servers are extremely widespread.
554/rtsp	Real Time Stream Control Protocol is used by media servers, including Quicktime and RealServer.
3389/ms-term-server	Microsoft Terminal Services
1723/pptp	Point-to-Point Tunneling Protocol is often used to implement VPN solutions on Microsoft Windows.
389/ldap	The Lightweight Directory Access Protocol is often used to store contact directories and the like.
636/ldapssl	LDAP over SSL is popular for accessing confidential information.
256/FW1-secureremote	Checkpoint Firewall-1 devices often have this administration port open.

In addition to popular ports such as the ones in the list above, choosing at least one high-numbered port is recommended. Many poorly configured firewalls only have default-deny for the "reserved ports", meaning those below 1024. I usually pick a high numbered port out of the air, such 40,000 or 10,042, to catch machines behind this sort of firewall.

In choosing the ports to probe, remember to emphasize platform diversity. If you are limiting your ping scan to two ports, http (80) and ssh (22) are probably better than http and https (443) because the latter two are related web services, and many machines that have https will often have http available anyway. Finding two accessible ports on the same machine is no better for ping scanning purposes than finding one. Choosing ports so that a broad set of hosts will match at least one of them is the goal.

Note that the valuable port table does not include many client-oriented ports such as the ubiquitous Windows SMB port 135. The primary reason is that this table only looked at hosts behind default-deny firewalls, where the vast majority of ports are filtered. In those situations, Windows ports such as 135-139 and 445 are usually blocked. When these machines are not behind a firewall, the open ports are unimportant for ping scanning because the thousands of closed ports work just as well.

### 3.5.2.2. UDP port selection

In selecting UDP ports, remember that an open port is unlikely to respond to the probes. Unfiltered ports are desired. To avoid open ports, you might consider excluding common UDP services like DNS (port 53) and SNMP (161). On the other hand, firewall rules are often so broad that those probes (particularly to port 53) might get through and hit a closed port. So I would recommend choosing at least port 53 and an arbitrarily selected high-numbered port.

### 3.5.2.3. ICMP probe selection

For ICMP, the standard ping (echo request) is usually worth trying. Many administrators specifically allows this because it is useful for debugging or because RFC 1122 requires it. I would also use at least one of the address mask or timestamp requests. These are valuable for networks where administrators intentionally block echo request packets, but forget about other ICMP queries.

### 3.5.2.4. Designing the ideal combinations of probes

How all of these ping types are combined into a ping scan strategy depends on characteristics of the target network and on the scan goals. For internal networks, the default ping type usually works well. The default is also fine for most casual scanning, where missing an occasional host is no big deal. Adding more probes can help catch those occasional stealthy machines, at the expense of making the ping scan take a bit longer. Time taken is roughly proportional to the number of probes sent to each machine. For security scans of target networks over the Internet, adding more probes is usually advisable. Try to include a diverse set of the techniques discussed previously. Here is a set of ping options that should catch the vast majority of hosts: `-PE -PT -PS21,22,23,25,80,113,31339 -PA80,113,443,10042`. Adding in `--source_port 53` might be worthwhile as well. How much better will the results be, and how much longer will it take? That depends on the target network, of course, but the Nmap random target selection option (`-iR`) makes it easy to perform a quick test. Example 3-5 shows Nmap generating 50,000 random IP addresses and then performing a default ping scan. You should remember that the default is a TCP ACK packet to port 80, and an ICMP echo request packet.

#### Example 3-5. Generating 50,000 IP Addresses, then ping scanning with default options

```
#nmap -n -sL -iR 50000 -oN - | grep "not scanned" | awk '{print $2}' > 50K_Test_IPs
# head -5 50K_Test_IPs
186.247.186.175
57.190.183.219
152.249.87.150
208.149.189.242
43.210.154.84
# nmap -sP -T4 -iL 50K_Test_IPs -oA 50KHosts_Defaultping

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Host 64.38.217.78 appears to be up.
Host pD954B8C2.dip.t-dialin.net (217.84.184.194) appears to be up.
Host 218.88.159.224 appears to be up.
[ Thousands of lines cut ]
Host d84.public.swarthmore.edu (130.58.248.84) appears to be up.
Host ip24-250-44-170.ri.ri.cox.net (24.250.44.170) appears to be up.
Host host121-52.apgea.army.mil (131.92.121.52) appears to be up.
Nmap run completed -- 50000 IP addresses (1732 hosts up) scanned in 3008.070 seconds
```

Scanning the 50,000 address took fifty minutes, and 1,732 hosts were detected. Most of the DNS names were already in cache due to a previous scratch run, though it still would have likely been much faster had DNS resolution been disabled with `-n`. To determine the effects of using a wider range of ping techniques, the same 50K hosts were rescanned with 13 probes per port rather than the default of two. As shown in Example 3-6, Nmap was able to detect 396 more hosts (23%). It took 45 minutes (90%) longer, but that is acceptable in many cases. Note that not all of the new hosts may be legitimate. Increasing the number of ping probes increases the chances that Nmap will hit network artifacts that make a non-existent host appear to be active. Firewalls that return a RST for SYN or ACK packets to port 113 are one example of this.

#### **Example 3-6. Repeating ping scan with extra probes**

```
# nmap -sP -PE -PT -PS21,22,23,25,80,113,31339 -PA80,113,443,10042 -T4 \
--source_port 53 -iL 50K_Test_IPs -oA 50KHosts_extendedping

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Host 64.38.217.78 appears to be up.
Host pD954B8C2.dip.t-dialin.net (217.84.184.194) appears to be up.
Host YahooBB220053236002.bbtec.net (220.53.236.2) appears to be up.
[ Thousands of lines cut ]
Host d84.public.swarthmore.edu (130.58.248.84) appears to be up.
Host ip24-250-44-170.ri.ri.cox.net (24.250.44.170) appears to be up.
Host sdn-ap-007castocP0414.dialsprint.net (63.187.65.160) appears to be up.
Host host121-52.apgea.army.mil (131.92.121.52) appears to be up.
Nmap run completed -- 50000 IP addresses (2128 hosts up) scanned in 5709.445 seconds
```

When performing security audits for clients, I normally start with port scan against about 1700 common ports (the default) with comprehensive ping scan options like those shown in Example 3-6. Such a scan does not take particularly long, allowing me to quickly start working. I also launch `-P0` (ping disabled) scans against all 65K ports in the background while I work. When they finish, which may be days later, I compare them to my initial quick scan and investigate any new ports or machines found.

## **3.6. Finding an Organization's IP addresses to Scan**

\* Need to actually write this section

## **3.7. Host Enumeration Code Algorithms**

One of the greatest benefits of Open Source software like Nmap is that curious users are always able to study the source code when they want answers about its operation. In the case of host enumeration, almost all of the important algorithms are contained in `targets.cc`. The highest level ping scanning function is `nexthost()`, which calls `massping()` to coordinate the actual packet-level techniques chosen. `massping()`, in turn, relies on lower level functions such as aptly named `sendrawtcpudppingqueries()`, `sendpingqueries()`, and `get_connecttcpscan_results()`. Unlike port scanning, which has numerous algorithms based on the technique chosen (such as SYN scan vs. FIN scan), host enumeration is all handled the same way at a high level.

While source code analysis is the only way to truly get the complete picture of Nmap operation down to every trivial detail, it is not always the easiest approach to understanding Nmap. In many cases, the most effective way to quickly

peek at Nmap's behavior given a set of command-line options is to add the `--packet_trace` option, which prints out all of the packets sent and received by Nmap.

Because these are excellent resources for learning the nitty-gritty details of Nmap operation, I'll only discuss the host enumeration algorithm at a high level here. When Nmap is executed, it may be passed networks containing hundreds of thousands or even millions of hosts. So Nmap breaks them into blocks that are small enough to deal with at one time (hundreds up to a couple thousand hosts). The ping scanner then pulls out a group of the first dozen or so hosts from the block. The exact initial group size depends on Nmap parameters used. The probes requested by the user are then sent to each member of the group in one spurt, and Nmap begins waiting for responses. When a conclusive response is received, that host is marked as up or down as appropriate, and Nmap resumes waiting for further responses. Nmap waits until it receives a conclusive response from every group member (unlikely for large groups), or it times out. Upon timeout, Nmap tests whether any group members have already been through the maximum number of retransmissions. If so, they are marked as down. All of the hosts which left the group because of a response or because Nmap gave up on retransmissions are then replaced by new members from the block. Nmap starts the cycle again, sending initial probes to the new group members and retransmissions to the existing ones. Eventually, Nmap runs out of new hosts in the block and the group size dwindles to zero as retransmissions complete. The ping scanning subsystem returns the results so that Nmap can begin port scanning or any other requested probing of the target machines. When Nmap finishes with them, it passes the next block to the ping scanner.

This parallelization allows the Nmap ping scanning subsystem to work very quickly. Multiple hosts, usually with multiple probes per host, are handled in parallel. The group size and timeout periods are modified in real-time based on packet latency timers and dropped packet detection. Most other components of Nmap can handle just one target host at a time. Upgrading the DNS resolver, port scanners, and possibly even OS detection to deal with multiple hosts at once, like the ping scanner and version detection can, is an ongoing project.

## Notes

1. Classless Inter-Domain Routing (CIDR) notation is a method for describing networks with more granularity than class A (CIDR /8), class B (CIDR /16), or class C (CIDR /24) notation. An excellent description is available at <http://public.pacbell.net/dedicated/cidr.html> .

# Chapter 4. Port Scanning Overview

## 4.1. Introduction to Port Scanning

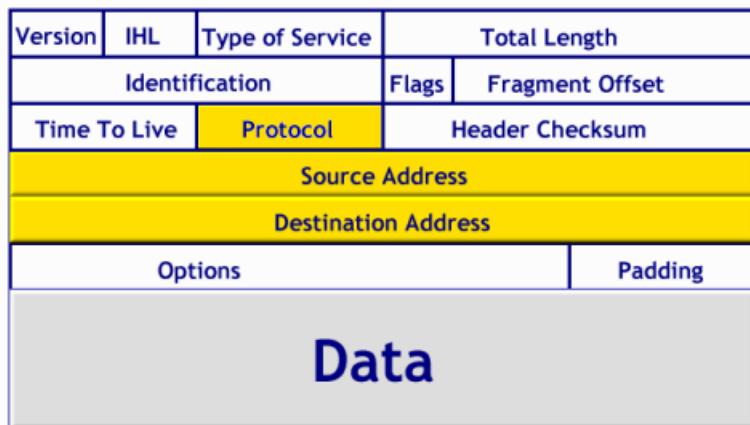
While Nmap has grown in functionality over the years, it began as an efficient port scanner, and that remains its core function. The simple command `nmap target` scans more than 1660 TCP ports on the host `target`, classifying each port into the state open, closed, or filtered.

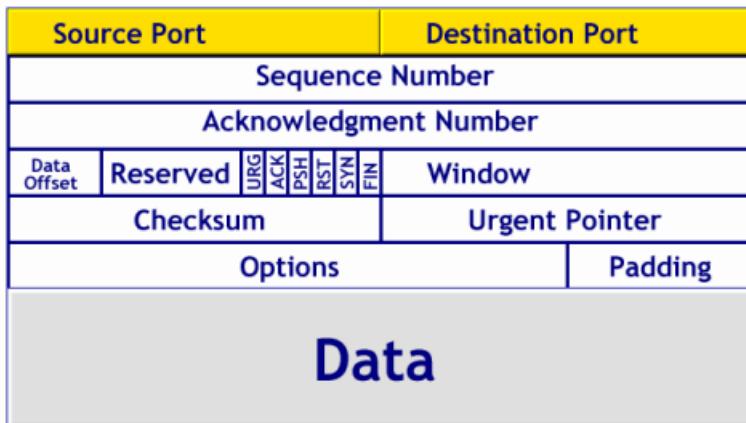
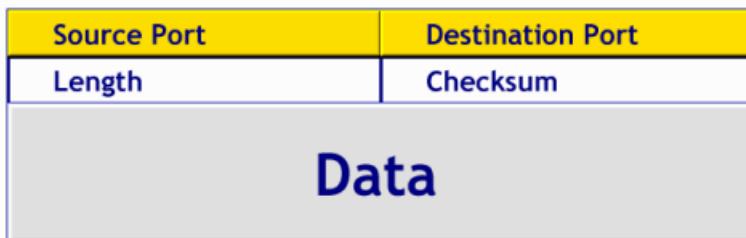
### 4.1.1. What exactly is a port?

Ports are simply a software abstraction, used to distinguish between communication channels. Similar to the way IP addresses are used to identify machines on the Internet, ports identify specific applications in use on a single machine. For example, your web browser will by default connect to TCP port 80 of machines in http URLs. If you specify the secure https protocol instead, the browser will try port 443 by default.

Nmap works with two protocols that use ports: TCP and UDP. A connection for each protocol is uniquely identified by four elements: source and destination IP addresses and corresponding source and destination ports. All of these elements are simply numbers placed in the headers of each packet sent between hosts. The protocol is an 8-bit field, which specifies what type of packet is contained in the IP data (payload) section. For example, TCP is protocol number 6, and UDP is 17. IPv4 addresses at 32-bits wide (128 with IPv6), and ports are each 16-bits long. The following figures, which are courtesy of Linux-France.Org (<http://www.linux-france.org/>), display the header layout.

Figure 4-1. IPv4 Header Layout



**Figure 4-2. TCP Header Layout****Figure 4-3. UDP Header Layout**

\* I highlighted IP protocol myself in quick, cheesy way. Should fix, or redo the whole images. Maybe include ECN bits. Images from <http://www.linux-france.org/prj/inetdoc/articles/transport/protocoles.transport.html> (GNU FDL). Maybe remove Data section, or make it smaller. Specify bit positions on top (32-bits wide). Nice 3-D eye candy :). Maybe make it clearer that TCP or UDP header goes in IP data section.

Because most popular services are registered to a well-known port number, one can often guess what services open ports represent. Nmap includes an `nmap-services` (<http://www.insecure.org/nmap/data/nmap-services>) file, containing the well-known service for registered port and protocol numbers, as well as common ports for trojan backdoors and other applications that don't bother registering with the Internet Assigned Numbers Authority (IANA). Nmap prints this service name for reference along with the port number.

Because the port number field is 16-bits wide, values can reach 65,535. The lowest possible value, zero, is invalid. The Berkeley sockets API, which defines how programs are usually written for network communication, does not allow port zero to be used as such. Instead, it interprets a port zero request as a wildcard, meaning that the programmer does not care which is used. The system then chooses an available port number. For example, programmers rarely care what source port number is used for an outgoing connection. So they set it to zero and let the operating system choose one.

While port zero is invalid, nothing stops someone from specifying it in the header field. Some malicious backdoor trojans listen on port zero of compromised systems as a stealthy way to offer illegitimate access without appearing on most port scans. To combat this, Nmap does allow scanning of port zero when it is specified explicitly (e.g. `-p0-65535`).

The first class of valid ports, numbers one through 1023, are known as reserved ports. UNIX systems (unlike Windows) require that applications have special (root) privileges in order to bind to and listen on these ports. The idea is to allow remote users to trust that they are connecting to a valid service started by an administrator and not by some wicked, unprivileged user. If the well-known port for ssh was 2222 instead of 22, a malicious user could start up a rogue ssh daemon on that port, collecting passwords of anyone who connects. As most common server applications listen on reserved ports, these are often the most fruitful to scan. So Nmap scans all 1023 reserved ports by default.

The ephemeral port range is another class of ports. This pool of ports is available by the system for allocation as needed. When an application specifies port zero ("any port"), the system chooses a port from this range. The range varies by operating system, and is usually configurable. It should contain at least a couple thousand ports to avoid running out when many concurrent connections are open. The Nmap connect() scan can use hundreds at a time as it scans every specified port on each target machine. On Linux, you can view or set the range using the file `/proc/sys/net/ipv4/ip_local_port_range`. Example 4-1 shows that on my Linux system, the range is 32,768 to 61,000. Such a large range should be sufficient in almost all cases, but I expand it just to demonstrate how to do so.

#### **Example 4-1. Viewing and increasing the ephemeral port range on Linux**

```
felix/# cat /proc/sys/net/ipv4/ip_local_port_range
32768   61000
felix/# echo "10000 65000" > /proc/sys/net/ipv4/ip_local_port_range
felix/# cat /proc/sys/net/ipv4/ip_local_port_range
10000   65000
felix/#
```

By default, Nmap only scans ports over 1024 if they are registered to a service in `nmap-services`. Specify `-p0-65535` to scan every single port. SunRPC ports are often found in the ephemeral range. Other applications open ephemeral ports temporarily for a file transfer or other event. FTP clients often do this when requesting an active mode transfer. Some P2P and instant messaging clients do so as well.

The IANA has their own port classification scheme, which differs slightly from vernacular of this book. Their authoritative port list at <http://www.iana.org/assignments/port-numbers> divides the space into the following three classes:

##### **well known ports**

These are reserved ports (within the range 1 to 1023, as discussed above) which have been registered with the IANA for a certain service. Familiar examples are ports 22, 25, and 80 for the services ssh, smtp, and http, respectively.

##### **registered ports**

These are ports fall within the range 1024 to 49,151 and have been registered with the IANA in the same way the well known ports have. Most of these are not as commonly used as the well known ports. The key difference is that unprivileged users can bind to these ports and thus run the services on their registered port. Users cannot do so on most platforms for well known ports, since they reside in the reserved port range.

##### **dynamic and/or private ports**

The IANA reserves the port numbers from 49152 through 65535 for dynamic uses such as those discussed in the ephemeral ports section. Proprietary services that are only used within a company may also use these ports.

When this book mentions registered or well known ports without any reference to the IANA, it usually means ports registered with Nmap in the `nmap-services` file, regardless of whether they fall in the reserved port range.

### **4.1.2. What is port scanning?**

Port scanning is the act of remotely testing numerous ports to determine what state they are in. The most interesting state is usually open, meaning that an application is listening and accepting connections on the port. Many techniques are available for conducting such a scan. Chapter 5 explains the circumstances under which each is most appropriate.

While many port scanners have traditionally lumped all ports into the open or closed states, Nmap is much more granular. It divides ports into five states. These states are not intrinsic properties of the port itself, but describe how Nmap sees them. For example, an Nmap scan from the same network as the target may show port 135/tcp as open, while a scan at the same time with the same options from across the Internet might show that port as filtered.

## **The five port states recognized by Nmap**

### **open**

An application is actively accepting TCP connections or UDP packets on this port. Finding these is often the primary goal of port scanning. Security-minded people know that each open port is an avenue for attack.

Attackers and pen-testers want to exploit the open ports, while administrators try to close or protect them with firewalls without thwarting legitimate users. Open ports are also interesting for non-security scans because they show services available for use on the network.

### **closed**

A closed port is accessible (it receives and responds to Nmap probe packets), but there is no application listening on it. They can be helpful in showing that a host is up on an IP address (host enumeration, or ping scanning), and as part of OS detection. Because closed ports are reachable, it may be worth scanning later in case some open up. Administrators may want to consider blocking such ports with a firewall. Then they would appear in the filtered state, discussed next.

### **filtered**

Nmap cannot determine whether the port is open because packet filtering prevents its probes from reaching the port. The filtering could be from a dedicated firewall device, router rules, or host-based firewall software. These ports frustrate attackers because they provide so little information. Sometimes they respond with ICMP error messages such as type 3 code 13 (destination unreachable: communication administratively prohibited), but filters that simply drop probes without responding are far more common. This forces Nmap to retry several times just in case the probe was dropped due to network congestion rather than filtering. It slows down the scan dramatically, further adding to the attacker's frustration.

### **unfiltered**

The unfiltered state means that a port is accessible, but Nmap is unable to determine whether it is open or closed. Only the ACK scan, which is used to map firewall rulesets, classifies ports into this state. Scanning unfiltered ports with other scan types such as Window scan, SYN scan, or FIN scan, may help resolve whether the port is open.

**open|filtered**

Nmap places ports in this state when it is unable to determine whether a port is open or filtered. This occurs for scan types in which open ports give no response. Of course the lack of response could also mean that a packet filter dropped the probe or any response it elicited. So Nmap does not know for sure whether the port is open or being filtered. The scans UDP, IP Protocol, FIN, Null, and Xmas scan classify ports this way.

**closed|filtered**

This state is used when Nmap is unable to determine whether a port is closed or filtered. It is only used for the IPID Idle scan discussed in Section 5.10.

While Nmap attempts to produce accurate results, keep in mind that all of its insights are based on packets returned by the target machines (or firewalls in front of them). Such hosts may be untrustworthy and send responses intended to confuse or mislead Nmap. Much more common are non-rfc-compliant hosts that do not respond as they should to Nmap probes. FIN, Null, and Xmas scans are particularly susceptible to this problem. Such issues are specific to certain scan types (particularly FIN, Null, and Xmas scans) and so are discussed in the relevant sections of Chapter 5.

### **4.1.3. Why scan ports?**

Port scanning is not done only for fun and amusement. There are numerous practical benefits to regularly scanning your networks. Foremost among these is security. One of the central tenants of network security is that reducing the number and complexity of services offered reduces the opportunity for attackers to break in. Most remote network compromises come from exploiting a server application listening on a TCP or UDP port. In many cases, the exploited application is not even used by the targeted organization, but was enabled by default when the machine was set up. Had that service been disabled, or protected by a firewall, the attack would have been thwarted.

Realizing that every open port is an opportunity for compromise, attackers regularly scan targets, taking an inventory of all open ports. They compare this list of listening services with their list of favorite exploits for vulnerable software. It takes just one match to compromise a machine, creating a foothold that is often used to infest the whole network. Attackers who are less discriminate about who they target will often scan for just the default port of an exploitable application. This is much faster than scanning every port, though the service will be missed when running on a non-default port. Such attackers are often derided as “script kiddies”, because they often know little more about security than how to run an exploit script written by someone more skilled. Across many organizations, such attackers are bound to find vulnerable hosts. They can be quite a nuisance, though their sheer numbers and relentless pounding against Internet-accessible machines often drive people to patch systems quickly. This reduces the likelihood of more serious, targeted attacks succeeding.

An important defense against these crackers is for systems administrators to scan their own networks regularly with tools such as Nmap. Take the list of open ports, and shut down any services that aren’t used. Ensure that those which must remain available are fully patched and that you are on the vendor’s security notification list. Firewall rules should be added where possible, limiting access to only legitimate users. Hardening instructions are available on the web for most popular applications, reducing the cracker’s opportunity even further. Nmap cannot do most of this for you, but it creates the list of available services to start out with. Some admins try to use netstat instead, but that doesn’t scale well. It requires access to every machine, and some mobile machines are easy to miss. Plus, you can’t run netstat on your average wireless access point, VOIP phone, or printer. There is also always the risk that a compromised machine will have a trojaned netstat which gives out false information. Most of the modern rootkits installed by attackers include this functionality. Relying solely on Nmap is a mistake too. A combination of careful design, configuration auditing, and regular scanning is well advised.

While security is the most common reason for port scanning, administrators often find that it suits other purposes as well. Creating an inventory of machines and the services they offer can be useful for asset tracking, network design, policy compliance checks, software license tracking, availability testing, network debugging, and more.

## 4.2. A Quick Port Scanning Tutorial

One of my goals in developing Nmap is to keep the most common usage simple, while retaining the flexibility for custom and advanced scans. This is accomplished with the command-line interface by offering dozens of options, but choosing sane defaults when they are not specified. A newbie can start out with a command as simple as **nmap *targetname***. Meanwhile, advanced users sometimes specify so many options that their terminal line wraps around.

A similar balance must be struck with command output. The most important results should stick out even to the occasional user who hasn't even read the man page. Yet the output should be comprehensive and concise enough to suit professional penetration testers who run Nmap against thousands of machines daily. Users smart enough to read this book or the Nmap source code benefit from greater control of the scanner and insights into what Nmap output really means.

This tutorial demonstrates some common Nmap port scanning scenarios and explains the output. Rather than attempt to be comprehensive, the goal is simply to acquaint new users well enough to understand the rest of this chapter.

The simplest Nmap command is simply **nmap** by itself. This prints a cheat sheet of common Nmap options and syntax. A more interesting command is **nmap *targetname***, which does the following:

1. Converts *targetname* from a hostname into an IPv4 address using DNS. I could have specified an IP address instead to skip this step.
2. Pings the host, by default with an ICMP echo request packet and a TCP ACK packet to port 80, to determine whether it is up and running. If not, Nmap reports that fact and exits. I could have specified **-P0** to skip this test. See Chapter 3.
3. Converts the target IP address back to the name using a reverse-DNS query. Because of the way DNS works, the reverse name may not be the same as the *targetname* specified on the command-line. This query can be skipped with the **-n** option to improve speed and stealthiness.
4. Launches a TCP port scan of ports 1-1024, plus all ports above 1024 which are registered in **nmap-services**. About 1660 ports are scanned if the default **nmap-services** is used. A SYN stealth scan is usually used, but **connect()** scan is substituted instead for non-root UNIX users who lack the privileges necessary to send raw packets.
5. Prints the results to standard output in normal human-readable format, and exits. Other output formats and locations (files) can be specified, as described in Chapter 11. Example 4-2 displays the results where **scanme.nmap.org** is used as *targetname*.

### Example 4-2. Simple scan: nmap scanme.nmap.org

```
# nmap scanme.nmap.org

Starting nmap 3.70 ( http://www.insecure.org/nmap/ ) at 2004-09-17 22:21 PDT
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 1655 ports scanned but not shown below are in state: filtered)
PORT      STATE      SERVICE
```

```

22/tcp  open  ssh
25/tcp  open  smtp
53/tcp  open  domain
80/tcp  open  http
113/tcp closed auth

Nmap run completed -- 1 IP address (1 host up) scanned in 20.596 seconds

```

The first output line in Example 4-2 simply gives the Nmap version number, URL for downloading it, and the time Nmap started. The Nmap version number is important for interpreting the results, as Nmap behavior and output does change occasionally. The time is critical, since Nmap only captures a snapshot of the network during the period in which it runs. If a new host plugs in or a port opens two minutes later, it obviously won't be included in the results until the next Nmap run. Times are removed from most examples to avoid line wrapping. The version number betrays the rough timeframe anyway.

The next line provides the target IP address (IPv4 in this case), and reverse DNS name (also known as the PTR record) if it is available. Nmap promises to show the "Interesting ports", though all ports scanned are accounted for. The ports considered most interesting because they are open or in a rarely-seen state for that host are itemized individually. When many ports are in a single non-open state, they are considered a default state, and aggregated onto a single line to avoid diluting the results with thousands of uninteresting entries. In this case, Nmap notes that 1,655 ports are filtered.

The interesting ports table comes next, and provides the key scan results. The columns vary depending on options used, but in this case provide the port number and protocol, state, and service protocol for each port. The service here is just a guess made by looking up the port in `nmap-services`. The service would be listed as unknown if any of the ports were not registered in that file. Four of these ports are open, with the remaining one being closed.

Finally, Nmap reports some basic timing stats before it exits. These stats are the number of targets specified, the number of those that the ping scan found to be up, and the total time taken.

While this simple command is often all that is needed, advanced users often go much further. In Example 4-3, the scan is modified with four options. `-p0-` asks Nmap to scan every possible TCP port, `-v` asks Nmap to be verbose about it, `-A` enables aggressive tests such as remote OS and service/version detection, and `-T4` enables a more aggressive timing policy to speed up the scan.

### **Example 4-3. More complex: nmap -p0- -v -A -T4 scanme.nmap.org**

```

# nmap -p0- -v -A -T4 scanme.nmap.org

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Initiating SYN Scan against scanme.nmap.org (205.217.153.55) [65536 ports] at 23:15
Discovered open port 80/tcp on 205.217.153.55
Discovered open port 22/tcp on 205.217.153.55
Discovered open port 25/tcp on 205.217.153.55
Discovered open port 53/tcp on 205.217.153.55
SYN Stealth Scan Timing: About 4.58% done; ETC: 23:26 (0:10:25 remaining)
The SYN Stealth Scan took 680.40s to scan 65536 total ports.
Initiating service scan against 4 services on scanme.nmap.org (205.217.153.55) at 23:26
The service scan took 5.14s to scan 4 services on 1 host.
For OSScan assuming port 22 is open, port 113 closed, and neither are firewalled
Host scanme.nmap.org (205.217.153.55) appears to be up ... good.
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 65531 ports scanned but not shown below are in state: filtered)

```

```

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.1p1 (protocol 1.99)
25/tcp    open  smtp    qmail smptd
53/tcp    open  domain  ISC Bind 9.2.1
80/tcp    open  http    Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.4.20
Uptime 158.050 days (since Mon Apr 12 22:14:55 2004)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=3296835 (Good luck!)
IPID Sequence Generation: All zeros

Nmap run completed -- 1 IP address (1 host up) scanned in 689.127 seconds

```

Nmap certainly provided the requested verbosity in Example 4-3! Fortunately the extra output is easy to understand. The first eleven new lines are runtime information letting the user know what is happening as she stares expectantly at the terminal, hoping for good news. What constitutes good news depends on whether she is a systems administrator who has to fix problems, a pen-tester who needs some issues to report on, or a black-hat cracker trying to exploit them. The "discovered open port" lines provide as-it-happens notification of open ports so that she can start banging on them before the scan even finishes. The "scan timing" line provides a completion time estimate, so she knows whether to keep staring at the screen or have lunch. Because network conditions (latency, congestion, bandwidth, etc.) and packet filtering rules vary so much, the same scan options may take 30 seconds to complete against one host and 45 minutes against another.

The port table shows no new ports. All the extra ports scanned are in the filtered state, raising the filtered port total from 1,655 to 65,531. While there are no new itemized ports, the entries have changed. A new VERSION column provides the application name and (in three of the four cases) version number of each open port. This comes from service detection, one of the features enabled by `-A`. Another feature of service detection is that all of the service protocols in the SERVICE column have actually been verified. In the previous scan, they were based on the relatively flimsy heuristic of an `nmap-services` lookup. That table lookup happened to be correct this time, but it won't always be.

The remaining new lines come from OS detection (also enabled by `-A`), which is discussed in depth in Chapter 8. The final line shows that all this extra info came at a price -- the scan took thirty times longer than Example 4-2 to complete.

## 4.3. Command-line flags

While the tutorial showed how simple executing an Nmap port scan can be, dozens of command-line flags are available to make the system more powerful and flexible. This section covers only options that relate to port scans, and often describes only the port-scanning-related functionality of those options. See Chapter 15 for a comprehensive list of option flags and everything they do.

### 4.3.1. Selecting scan techniques

One of the first considerations when contemplating a port scan is deciding what techniques to use. Nmap offers about a dozen such methods. This section provides a brief summary of them, and full coverage comes in the next chapter.

Only one scan method may be used at a time, except that UDP scan (`-sU`) may be combined with any one of the TCP scan types. As a memory aid, port scan type options are of the form `-sC`, where *C* is a prominent character in the scan name, usually the first. The one exception to this is the deprecated FTP bounce scan (`-b`). By default, Nmap performs a SYN Scan, though it substitutes a Connect() scan if the user does not have proper privileges to send raw packets (requires root access on UNIX) or if IPv6 targets were specified.

## **Port scanning methods supported by Nmap**

### TCP SYN Stealth (-`sS`)

This is far and away the most popular scan type because it is the fastest way to scan ports of the most popular protocol (TCP). It is stealthier than connect() scan, and it works against all functional TCP stacks (unlike some special-purpose scans such as FIN scan).

### TCP Connect() (-`sT`)

Connect() scan uses the system call of the same name to scan machines, rather than relying on raw packets as most of the other methods do. It is usually used by unprivileged UNIX users and against IPv6 targets because SYN scan doesn't work in those cases.

### UDP (-`sU`)

Don't forget UDP ports -- they offer plenty of security holes too.

### TCP FIN, Xmas, and Null (-`sF`, -`sX`, -`sN`)

These special purpose scan types are adept at sneaking past firewalls to explore the systems behind them. Unfortunately they rely on target behavior that some systems (particularly Windows variants) don't exhibit.

### TCP ACK (-`sA`)

ACK scan is commonly used to map out firewall rulesets. In particular, it helps understand whether firewall rules are stateful or not. The downside is that it cannot distinguish open from closed ports.

### TCP Window (-`sW`)

Window scan is like ACK scan, except that it is able to detect open versus closed ports against certain machines.

### TCP Maimon (-`sM`)

Another obscure firewall-evading scan type. It is similar to a FIN scan, but includes the ACK flag as well. This allows it to get by more packet filtering firewalls, with the downside that it works against even fewer systems than FIN scan.

### TCP Idle (-`sI <zombie host>`)

The stealthiest scan type of all, even if it is slow and complex. Can exploit trusted IP address relationships.

### IP protocol (-`sO`)

Determines which IP protocols (TCP, ICMP, IGMP, etc.) are supported by the target machine. This isn't technically a port scan, since it cycles through IP protocol numbers rather than TCP or UDP port numbers. Yet it still uses the `-p` option to select scanned protocol numbers, reports its results with the normal port table format, and even uses the same underlying scan engine as the true port scanning methods. So it is close enough to a port scan that it belongs here.

TCP FTP bounce (-b <FTP bounce proxy>)

A way to trick FTP servers into performing a port scan by proxy. Unfortunately, most FTP servers are now patched to prevent this. It is a good way to sneak through restrictive firewalls when it works.

### 4.3.2. Selecting ports to scan

By default, Nmap scans ports 1-1024, plus every higher port that is registered in the `nmap-services` file. The total is about 1475 UDP ports and 1660 TCP ports. The `-F` (stands for fast) option will scan only those registered ports regardless of whether they are reserved (under 1024). The speed difference is not dramatic because this still leaves about 1000 UDP ports and 1200 TCP. One solution is to specify your own `nmap-services` file, as described in Chapter 12, though specifying the desired ports on the command-line with the `-p` option may be a better approach. The syntax of the `-p` option can be complex, and is best described with examples.

#### Port selection examples with the `-p` option

`-p22`

Scan a single port (in this case port 22) by specifying just that number as the `-p` argument.

`-p22,25,80`

Multiple ports may be separated with commas. Note that no protocol is specified, so these same port numbers will be used for whatever scan methods are specified on the command-line. If a TCP scan such as SYN scan (`-sS`) is specified, TCP ports 22, 25, and 80 are scanned. Those correspond to the services ssh, smtp, and http, respectively. If a UDP scan is selected (`-sU`), those three UDP ports are scanned. If both are specified, those three ports are scanned for each protocol, for a total of six scanned ports. With IP protocol scan (`-sO`), those three IP protocols (corresponding to xns-idp, leaf-1, and iso-ip) are scanned.

`-p80-85,443,8000-8005,8080-8085`

Port ranges may be specified by separating the beginning and end port with a hyphen. Multiple ranges or individual ports can be specified with commas. This option scans ports 80, 81, 82, 83, 84, 85, 443, 8000, etc. Based on the port numbers, this user is probably scanning TCP and looking for web servers.

`-p100,60000-`

You can omit the beginning of a range to imply port one, or the end to imply the last port possible (65535 for TCP and UDP, 255 for protocol scan). This example scans ports one through 100, and all ports greater or equal to 60,000.

`-p-`

Omit beginning and end numbers to scan the whole range (excluding zero).

`-pT:21,23,110,U:53,111,137,161`

Separate lists of TCP and UDP ports can be given by preceding the lists with T: (for TCP) or U:. This example scans three TCP ports (ftp, telnet, and pop3), and four UDP services (DNS, rpcbind, netbios, and snmp). Specifying both TCP and UDP ports only matters if you also tell Nmap to do a UDP scan (`-sU`) and one of the TCP scan methods, such as `-sS`, `-sA`, or `-sF`.

### 4.3.3. Timing-related options

Port scanning often takes more time than all of the other elements in a comprehensive Nmap scan (version detection, OS detection, ping scanning, DNS resolution, etc.) put together. Optimizing with the timing options can help substantially. This list summarizes the options that affect port scan timing. Chapter 6 offers a much more complete treatment.

`--min_rtt_timeout, --max_rtt_timeout, --initial_rtt_timeout`

The minimum, maximum, and initial amount of time in milliseconds that Nmap will wait for a port scan probe response.

`--min_hostgroup, --max_hostgroup`

Sets the minimum and maximum number of hosts that Nmap will port scan in parallel.

`--min_parallelism, --max_parallelism`

Limits the minimum or maximum number of port scan probes (across all hosts scanned concurrently) that Nmap may have outstanding.

`--host_timeout`

Asks Nmap to give up on hosts that take more than a given number of milliseconds to scan.

`--scan_delay, --max_scan_delay`

Asks Nmap to wait at least the given number of milliseconds between sending probes to any individual host. The scan delay can grow as Nmap detects packet loss, so a maximum may be specified with `--max_scan_delay`.

`-T0 through -T5`

These timing templates affect many variables, offering a simple way to adjust overall Nmap speed from very slow (`-T0`) to extremely aggressive (`-T5`).

### 4.3.4. Output format and verbosity options

Nmap offers the ability to write its reports in its standard format, a simple line-oriented “grepable” format, or XML. These reports are enabled with the `-oN` (normal), `-oG` (grepable), and `-oX` (XML) options. Each option takes a filename, and they may be combined to output in several formats at once. Several options are also available to increase output verbosity. These options are summarized in the following list, and fully covered in Chapter 11. That chapter also documents the output formats themselves.

`-v`

Increases the verbosity level, causing Nmap to print more information about the scan in progress. Open ports are shown as they are found and completion time estimates are provided when Nmap thinks a scan will take more than a few minutes. Use it twice for even greater verbosity. Using it more than twice has no effect.

`-d`

Increases the debugging level, causing Nmap to print out details about its operation that can be useful in tracking down bugs or simply understanding how it works. Higher levels result in massive amounts of data. Using the option once sets the debugging level to one, and it is incremented for each additional `-d`. Or you may

follow the `-d` with the desired level, as in `-d5`. If you don't see enough information, try a higher level. The maximum effective level is 9. If your screen is flooded with too much debugging data, reduce the level. Redusing scan intensity, such as the number of ports or targets and the features used, can also help to isolate only the debug messages you want.

#### `--packet_trace`

Causes Nmap to print a summary of every packet sent or received. This is often used for debugging, but is also a valuable way for new users to understand exactly what Nmap is doing under the covers. To avoid printing thousands of lines, you may want to specify a limited number of ports to scan, such as `-p20-30`.

#### `-oN <filename>`

Write output in Nmap's normal format to `filename`. This format is roughly the same as the standard output printed by Nmap at runtime.

#### `-oX <filename>`

Write output in Nmap's XML format to `filename`. Normal (human readable) output will still be printed to stdout unless you ask for XML to be directed there by specifying `-` as `filename`. This is the preferred format for use by scripts and programs that process Nmap results.

#### `-oG <filename>`

Write output in Nmap's so-called grepable format to `filename`. This tabular format fits the output of each host on a single line, making it easy to grep for open ports, certain operating systems, application names, or other data. Normal output will still be printed to stdout unless you ask for the grepable output to be directed there by specifying `-` as `filename`. While this format works well for parsing with simple grep and awk command-lines, significant scripts and programs should use the XML output instead. The XML format contains substantial information that grepable format has no place for, and extensibility makes XML easier to update with new information without breaking tools that rely on it.

#### `--resume <filename>`

Resume an aborted scan by specifying the normal (`-oN`) or grepable (`-oG`) output file which was created during the ill-fated scan. Don't use any options other than `--resume`, as Nmap will use the ones specified in the output file. It then parses the file and resumes scanning (and logging to the file) at the host which the previous Nmap execution was working on when it ceased.

#### `--append_output`

Tells Nmap to append scan results to any output files specified (with arguments such as `-oN` or `-oX`) rather than overwriting them.

### 4.3.5. Firewall and IDS evasion options

Nmap offers many options for sneaking past IDSs undetected or evading firewall rules. They are discussed in depth in Chapter 9, and this list gives a quick summary. Some of these options (particularly `-S` and `-e`) are useful for more mundane purposes as well.

**-f**

Asks Nmap to fragment the packets it uses for a port scan. This is usually done in an attempt to evade firewall or IDS systems. Unfortunately the option does not work when Nmap is running on recent versions of Linux. See Section 9.4.6 for a discussion of this technique.

**-D <decoy1[,decoy2][,ME],...>**

Enables decoys which hide the real attacker amongst a flurry of decoy IP addresses. See Section 9.5.3.1 for decoy scanning examples and suggestions.

**-S <IP Address>**

Sets the source address of port scan packets. This can be used on hosts with many IP addresses to select the one that packets are sent from. Or it can be used for more sinister purposes -- to spoof the scan so that some other party takes the blame. This sort of spoofing is described in Section 9.5.3.2.

**-e**

Tells Nmap which interface to send and receive packets on. This may be required if the -S option is used to spoof someone else's IP address. It can also be useful on multi-homed hosts to select the most desirable interface when several can route to the target networks.

**--source\_port (-g)**

Sets the source port used in scans. This is usually done to bypass poorly-implemented firewalls, as described in Section 9.4.2.

**--data\_length <numbytes>**

Rather than send packet headers with empty data sections as port scan probes, this option causes each probe packet to be padded with the given number of random data bytes.

### 4.3.6. Specifying targets

To scan a single host (or a few of them), simply add their names or IP addresses to the end of your Nmap command line. Nmap also has a structured syntax to make scanning large networks easy. You can give Nmap a file listing targets, or even ask Nmap to generate them randomly. This is all described in Section 3.2.

### 4.3.7. Miscellaneous options

Here are some options that can be quite handy even though they don't fit into specific categories. The descriptions focus on how each option relates to port scanning. See the Nmap Reference Guide in Chapter 15 for more comprehensive coverage.

**-6**

Asks Nmap to scan the target using the IPv6 protocol. This process is described in Section 4.4.

**-r**

Nmap randomizes the port scan order by default to make detection slightly harder. The -r option causes them to be scanned in numerical order instead.

```
--ttl <numHops>
```

Sets the IP time-to-live to the given number of hops. This can be used to avoid scanning hosts beyond a limited network. It can also be useful as a sort of poor man's traceroute to discover network topology, though that is usually easier to accomplish with hping2 (<http://www.hping.org>).

```
-P0
```

Tells Nmap to skip the ping test and simply scan every target host provided. Other options for controlling host enumeration are described in Chapter 3.

## 4.4. IPv6 Scanning [-6]

Since 2002, Nmap has offered IPv6 support for its most popular features. In particular, ping scanning (TCP-only), connect() scanning, and version detection all support IPv6. The command syntax is the same as usual except that you also add the `-6` option. Of course, you must use IPv6 syntax if you specify an address rather than a hostname. An address might look like `3ffe:501:4819:2000:210:f3ff:fe03:4d0`, so hostnames are recommended. Example 4-4 shows a typical port scanning session. The output looks the same as it usually does, with the IPv6 address on the “interesting ports” line being the only IPv6 give away.

### Example 4-4. A simple IPv6 scan

```
# nmap -6 -sV www.eurov6.org

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Interesting ports on ns1.euro6ix.com (2001:800:40:2a03::3):
(The 1656 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Pure-FTPd
22/tcp    open  ssh      OpenSSH 3.5p1 (protocol 2.0)
53/tcp    open  domain   ISC Bind 9.2.1
80/tcp    open  http     Apache httpd

Nmap run completed -- 1 IP address (1 host up) scanned in 56.782 seconds
```

While IPv6 hasn't exactly taken the world by storm, it gets significant use in some (usually Asian) countries and most modern operating systems support it. To use the Nmap `-6` feature, both the source and target of your scan must be configured for IPv6. If your ISP (like most of them) does not allocate IPv6 addresses to you, free tunnel brokers are widely available and work fine with Nmap. One of the better ones is run by BT Exact at <https://tb.ipv6.btexact.com/>. I have also used one that Hurricane Electric provides at <http://ipv6tb.he.net/>. 6to4 tunnels are another popular, free approach.

Systems that support IPv6 don't always have their IPv4 and IPv6 firewall rules in sync. Section 9.4.3 shows a real-life example of reaching ports through IPv6 that are filtered in IPv4.

## 4.5. [RECIPE] Scanning a large network for a certain open TCP port

### 4.5.1. Problem

You wish to quickly find all machines on a network that have a certain TCP port open. For example, after a new Microsoft IIS vulnerability is found, you might want to scan for all machines with TCP port 80 open and ensure that they aren't running a vulnerable version of that software. Or if you investigate a compromised box and find that the attacker left a backdoor running on port 31337, scanning your whole network for that port might quickly identify other compromised systems. A full scan would be done later.

### 4.5.2. Solution

The straightforward way is to run:

```
nmap -P0 -p<portnumber> -oG <logfilename.gnmap> <target networks>
```

Here is a concrete example of searching 4096 IPs for web servers (port 80 open):

```
nmap -P0 -p80 -oG logs/pb-port80scan-092304.gnmap 216.163.128.0/20
```

While this works, a little effort choosing appropriate timing values for the network being scanned reduces scan time substantially. The scan above took 1,236 seconds, while the optimized version below provided the same results in 869 seconds:

```
nmap -T4 -P0 -p80 --max_rtt_timeout 200 --initial_rtt_timeout 150 --min_hostgroup 512 -oG  
logs/pb-port80scan2-092304.gnmap 216.163.128.0/20
```

And much of that time is spent doing reverse-DNS resolution. Excluding that by adding `-n` to the command-line above reduces the 4096-host scan time to 193 seconds. Being patient for 3 minutes is far easier than for the 21 minutes taken before.

The commands above store grepable-format results in the specified file. A simple egrep command will then find the machines with port 80 open:

```
egrep '[^0-9]80/open' logs/pb-port80scan2-092304.gnmap
```

The egrep pattern is preceded with `[^0-9]` to avoid bogus matching ports such as 3180. Of course that can't happen since we are only scanning port 80, but it is a good practice to remember for many-port scans. If you only want the IP addresses and nothing else, pipe the egrep output to `awk '{print $2}'`.

### 4.5.3. Discussion

Sometimes a story is the best way to understand decisions, so this is how I decided upon the command lines in the solution section. I was bored at home, and finding myself curious as to whether the popular magazine *Playboy* had any secret (unadvertised) web servers on their network. Such web servers might offer exciting free content, such as Linux distribution ISOs! Those really turn me on. The way to find out is a single-port scan across their network for hosts with TCP port 80 open.

The first step is determining which IP addresses to scan. I perform a whois search of the American Registry for Internet Numbers for organizations named *Playboy*. The results are shown in Example 4-5.

**Example 4-5. Discovering Playboy's IP space**

```
core~> whois -h whois.arin.net n playboy
[Querying whois.arin.net]
[whois.arin.net]

OrgName:      Playboy
OrgID:        PLAYBO
Address:      680 N. Lake Shore Drive
City:         Chicago
StateProv:    IL
PostalCode:   60611
Country:      US

NetRange:     216.163.128.0 - 216.163.143.255
CIDR:         216.163.128.0/20
NetName:      PLAYBOY-BLK-1
NetHandle:    NET-216-163-128-0-1
Parent:       NET-216-0-0-0-0
NetType:      Direct Assignment
NameServer:   NS1-CHI.PLAYBOY.COM
NameServer:   NS2-CHI.PLAYBOY.COM
[...]
```

This shows 4096 IPs (the net range 216.163.128.0/20) registered to Playboy. Using techniques discussed in Section 3.6 I could have found many more netblocks they control, but 4096 IPs are sufficient for this example.

Next I want to estimate latency to these machines, so that Nmap will know what to expect. This isn't required, but feeding Nmap appropriate timing values can speed it up. This is particularly true for single-port -P0 scans, such as this one. Nmap does not receive enough responses from each host to accurately estimate latency and packet drop rate, so I will help it out on the command line. My first thought is to ping their main web server, as shown in Example 4-6.

**Example 4-6. Pinging Playboy's Web Server for a Latency Estimate**

```
# ping -c5 www.playboy.com
PING www.phat.playboy.com (209.247.228.201) from 205.217.153.56 : 56(84) bytes of data.
64 bytes from free-chi.playboy.com (209.247.228.201): icmp_seq=1 ttl=245 time=57.5 ms
64 bytes from free-chi.playboy.com (209.247.228.201): icmp_seq=2 ttl=245 time=56.7 ms
64 bytes from free-chi.playboy.com (209.247.228.201): icmp_seq=3 ttl=245 time=56.9 ms
64 bytes from free-chi.playboy.com (209.247.228.201): icmp_seq=4 ttl=245 time=57.0 ms
64 bytes from free-chi.playboy.com (209.247.228.201): icmp_seq=5 ttl=245 time=56.6 ms

--- www.phat.playboy.com ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 4047ms
rtt min/avg/max/mdev = 56.652/57.004/57.522/0.333 ms
```

The maximum round trip time is 58 milliseconds. Unfortunately, this IP address (209.247.228.201) is not within the 216.163.128.0/20 netblock I wish to scan. I would normally add this new netblock to the target list, but have already decided to limit my scan to the original 4096 IPs. These times are probably perfectly fine to use, but finding actual values from IPs on the target network would be even better. I use dig to obtain Playboy's public DNS records from a nameserver shown in the previous whois query. The output is shown in Example 4-7.

**Example 4-7. Digging through Playboy's DNS records**

```

core<~>dig @ns1-chi.playboy.com playboy.com. any
; <>> DiG 8.3 <>> @ns1-chi.playboy.com playboy.com. any
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6
;; flags: qr aa rd; QUERY: 1, ANSWER: 9, AUTHORITY: 0, ADDITIONAL: 4
;; QUERY SECTION:
;;      playboy.com, type = ANY, class = IN

;; ANSWER SECTION:
playboy.com.          1D IN A      209.247.228.201
playboy.com.          1D IN MX     10 mx.la.playboy.com.
playboy.com.          1D IN MX     5 mx.chi.playboy.com.
playboy.com.          1D IN NS      ns15.customer.level3.net.
playboy.com.          1D IN NS      ns21.customer.level3.net.
playboy.com.          1D IN NS      ns29.customer.level3.net.
playboy.com.          1D IN NS      ns1-chi.playboy.com.
playboy.com.          1D IN NS      ns2-chi.playboy.com.
playboy.com.          1D IN SOA     ns1-chi.playboy.com. dns.playboy.com. (
2004092010           ; serial
12H                  ; refresh
2h30m                ; retry
2wld                ; expiry
1D )                 ; minimum

;; ADDITIONAL SECTION:
mx.chi.playboy.com.   1D IN A      216.163.143.4
mx.la.playboy.com.    1D IN A      216.163.128.15
ns1-chi.playboy.com.  1D IN A      209.247.228.135
ns2-chi.playboy.com.  1D IN A      64.202.105.36

;; Total query time: 107 msec

```

The DNS query reveals two MX (mail) servers within the target 216.163.128.0/20 netblock. Since the names mx.chi and mx.la imply that they are in different regions (Chicago and Los Angeles), I decide to test them both for latency. The ping results are shown in Example 4-8.

**Example 4-8. Pinging the MX servers**

```

core~> ping -c5 mx.chi.playboy.com
PING mx.chi.playboy.com (216.163.143.4) 56(84) bytes of data.

--- mx.chi.playboy.com ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4000ms

core~> ping -c5 mx.la.playboy.com
PING mx.la.playboy.com (216.163.128.15) 56(84) bytes of data.

--- mx.la.playboy.com ping statistics ---

```

```
5 packets transmitted, 0 received, 100% packet loss, time 4011ms
```

Well, that attempt was a miserable failure. The hosts seem to be blocking ICMP ping packets. Since they are mail servers, they must have TCP port 25 open, so I try again using hping2 (<http://www.hping2.org>) to perform a TCP ping against port 25, as demonstrated in Example 4-9.

### Example 4-9. TCP Pinging the MX servers

```
core# hping2 --syn -p 25 -c 5 mx.chi.playboy.com
eth0 default routing interface selected (according to /proc)
HPING mx.chi.playboy.com (eth0 216.163.143.4): S set, 40 headers + 0 data bytes
46 bytes from 216.163.143.4: flags=SA seq=0 ttl=51 id=14221 win=65535 rtt=56.8 ms
46 bytes from 216.163.143.4: flags=SA seq=1 ttl=51 id=14244 win=65535 rtt=56.9 ms
46 bytes from 216.163.143.4: flags=SA seq=2 ttl=51 id=14274 win=65535 rtt=56.9 ms
46 bytes from 216.163.143.4: flags=SA seq=3 ttl=51 id=14383 win=65535 rtt=61.8 ms
46 bytes from 216.163.143.4: flags=SA seq=4 ttl=51 id=14387 win=65535 rtt=57.5 ms

--- mx.chi.playboy.com hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 56.8/58.0/61.8 ms

core# hping2 --syn -p 25 -c 5 mx.la.playboy.com
eth0 default routing interface selected (according to /proc)
HPING mx.la.playboy.com (eth0 216.163.128.15): S set, 40 headers + 0 data bytes
46 bytes from 216.163.128.15: flags=SA seq=0 ttl=52 id=58728 win=57344 rtt=16.0 ms
46 bytes from 216.163.128.15: flags=SA seq=1 ttl=52 id=58753 win=57344 rtt=15.4 ms
46 bytes from 216.163.128.15: flags=SA seq=2 ttl=52 id=58790 win=57344 rtt=15.5 ms
46 bytes from 216.163.128.15: flags=SA seq=3 ttl=52 id=58870 win=57344 rtt=16.4 ms
46 bytes from 216.163.128.15: flags=SA seq=4 ttl=52 id=58907 win=57344 rtt=15.5 ms

--- mx.la.playboy.com hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 15.4/15.8/16.4 ms
```

These are the results I was looking for. The LA host never takes more than 16 milliseconds to respond, while the Chicago one takes up to 62 milliseconds. This is not surprising, given that I am probing from a machine in California. It pays to be cautious, and latency can increase during heavy scanning, so I decide to let Nmap wait up to 200 milliseconds for responses. I'll have it start with a timeout of 150ms. So I pass it the options `--max_rtt_timeout 200 --initial_rtt_timeout 150`. To set a generally aggressive timing mode, I specify `-T4` at the beginning of the line. It is important the `-T4` comes before those other timing options, or the `-T4` canned RTT values (500ms initial rtt timeout, 1250ms max) will override the ones I explicitly specified.

Since I value minimizing completion time of the whole scan over minimizing the amount of time before the first batch of host results is returned, I specify a large scan group size. The option `--min_hostgroup 512` is specified so that at least 512 IPs will be scanned in parallel (when possible). Using an exact factor of the target network size (4096) prevents the small and less efficient 96-host block which would occur at the end if I specified `--min_hostgroup 500`. All of these timing issues are explained in much more depth in Chapter 6.

There is no need to waste time with a prior ping stage, since a ping would take as long as the single-port scan itself. So `-P0` is specified to disable that stage. Substantial time is saved by skipping reverse-DNS resolution with the `-n` argument. Otherwise, with ping scanning disabled, Nmap would try to look up all 4096 IPs. Nmap does not yet offer parallelized DNS subsystem, so that would be painfully slow. I am searching for webservers, so I request port eighty

with `-p80`. Of course I will miss any http servers running on non-standard ports such as 81 or 8080. SSL servers on port 443 won't be found either. One could add them to the `-p` option, but even one more port would double the scan time, which is roughly proportional to the number of ports scanned.

The final option is `-oG` followed by the filename in which I want grepable results stored. I append the target network to the command, then press enter to execute Nmap. The output is shown in Example 4-10.

#### **Example 4-10. Launching the scan**

```
# nmap -T4 -p80 -P0 --max_rtt_timeout 200 --initial_rtt_timeout 150 \
--min_hostgroup 512 -n -oG pb-port80scan-092304.gnmap 216.163.128.0/20
Warning: You specified a highly aggressive --min_hostgroup.
Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Interesting ports on 216.163.128.0:
PORT      STATE      SERVICE
80/tcp     filtered  http

Interesting ports on 216.163.128.1:
PORT      STATE      SERVICE
80/tcp     filtered  http

Interesting ports on 216.163.128.2:
PORT      STATE      SERVICE
80/tcp     filtered  http

Interesting ports on 216.163.128.3:
PORT      STATE      SERVICE
80/tcp     filtered  http
[ ... ]
Interesting ports on 216.163.143.255:
PORT      STATE      SERVICE
80/tcp     filtered  http

Nmap run completed -- 4096 IP addresses (4096 hosts up) scanned in 192.968 second
```

Nmap scans all 4096 IPs in about three minutes. The normal output shows a bunch of ports in the `filtered` state. Most of those IPs are probably not active hosts -- the port simply appears filtered because Nmap receives no response to its SYN probes. I obtain the list of web servers with a simple egrep on the output file, as shown in Example 4-11.

#### **Example 4-11. Egrep for open ports**

```
# egrep '[^0-9]80/open' pb-port80scan-092304.gnmap
Host: 216.163.140.20 () Ports: 80/open/tcp//http///
Host: 216.163.142.135 ()      Ports: 80/open/tcp//http///
```

After all that effort, only two accessible web servers are found out of 4096 IPs! Sometimes that happens. The first one, 216.163.140.20 (no reverse DNS name) brings me to a Microsoft Outlook Web Access (webmail) server. That might excite me if I was trying to compromise their network, but it isn't gratifying now. The next server (reverse name `mirrors.playboy.com`) is much better. It offers those Linux ISOs I was hoping for, as well as substantial FreeBSD, CPAN, and Apache archives! I download the latest Fedora Core ISOs at a smoking-fast 4Mbps. I suppose

an abundance of bandwidth at Playboy is not surprising. Later I scan other Playboy netblocks, finding dozens more web servers, though some of their content is inappropriate for this book.

While this is an unusual reason for port scanning, single port sweeps are common for many other purposes expressed previously. The techniques described here can be easily applied to any single-port TCP sweep.

#### **4.5.4. See Also**

Version detection can be used to find specific applications listening on a network. For example, you could seek a certain vulnerable version of OpenSSH rather than find all hosts with port 22 open. This is also useful for single-port UDP scans, as the techniques in this recipe only work well for TCP. Instructions are provided in Section 7.8.

Chapter 6 looks at scan speed optimization in much more depth.

# Chapter 5. Port Scanning Techniques and Algorithms

## 5.1. Introduction

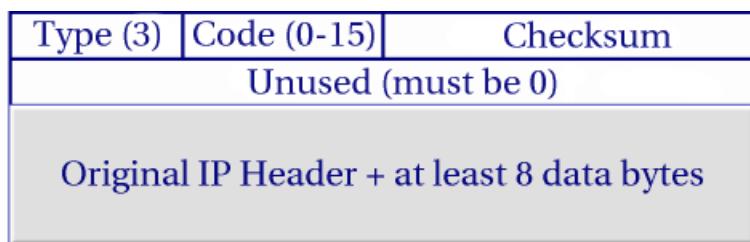
As a novice performing automotive repair, I can struggle for hours trying to fit my rudimentary tools (hammer, duct tape, wrench, etc.) to the task at hand. When I fail miserably and tow my jalopy to a real mechanic, he invariably fishes around in a huge tool chest until pulling out the perfect gizmo which makes the job seem effortless. The art of port scanning is similar. Experts understand the dozens of scan techniques and choose the appropriate one (or combination) for a given task. Inexperienced users and script kiddies, on the other hand, try to solve every problem with the default SYN scan. Since Nmap is free, the only barrier to port scanning mastery is knowledge. That certainly beats the automotive world, where it may take great skill to determine that you need a strut spring compressor, then you still have to pay thousands of dollars for it.

The previous chapter described port scanning with Nmap in general terms, including a brief summary of Nmap's supported scan types in Section 4.3.1. This chapter describes each of those scan types in depth. Typical usage scenarios and instructions are given for each scan type, as are on-the-wire packet traces illustrating how they work. Then the `ultra_scan` algorithm (which most scan methods use) is discussed, with an emphasis on aspects that can be tweaked to improve performance.

Most of the scan types are only available to privileged users. This is because they send and receive raw packets, which requires root access on UNIX systems. Using an administrator account on Windows is recommended, though it sometimes works for unprivileged users on that platform when Winpcap has already been loaded into the OS. Requiring root privileges was a serious limitation when Nmap was released in 1997, as many users only had access to shared shell accounts. Now, the world is different. Computers are cheaper, far more people have always-on direct Internet access, and desktop UNIX systems (including Linux and MAC OS X) are prevalent. A Windows version of Nmap is now available, allowing it to run on even more desktops. For all these reasons, users have less need to run Nmap from limited shared shell accounts. This is fortunate, as the privileged options make Nmap far more powerful and flexible.

When discussing how Nmap handles probe responses, many sections discuss ICMP error messages by their type and code numbers. The type and code are each 8-bit fields in ICMP headers that describe the message's purpose. Nmap port scanning techniques are concerned only with ICMP type 3, which are destination unreachable messages. Figure 5-1 shows the ICMP header layout of such a packet (it is encapsulated in the data section of an IP packet, as shown in Figure 4-1).

**Figure 5-1. ICMPv4 Destination Unreachable Header Layout**



\* This needs to be redone in the same fashion as the headers in previous chapter.

There are sixteen codes representing different destination unreachable messages. They are all shown in Table 5-1, though Nmap only cares about codes 0-3, 9, 10, and 13, which are marked with an asterisk.

**Table 5-1. ICMP destination unreachable (type 3) code values**

Code	Description
0*	Network unreachable
1*	Host unreachable
2*	Protocol unreachable
3*	Port unreachable
4	Fragmentation needed but don't-fragment bit set
5	Source route failed
6	Destination network unknown
7	Destination host unknown
8	Source host isolated (obsolete)
9*	Destination network administratively prohibited
10*	Destination host administratively prohibited
11	Network unreachable for type of service (TOS)
12	Host unreachable for TOS
13*	Communication administratively prohibited by filtering
14	Host precedence violation
15	Precedence cutoff in effect

## 5.2. TCP SYN (Stealth) Scan

SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls. SYN scan is relatively unobtrusive and stealthy, since it never completes TCP connections. It also works against any compliant TCP stack rather than depending on idiosyncrasies of specific platforms as Nmap's Fin/Null/Xmas, Maimon and Idle scans do. It also allows clear, reliable differentiation between open, closed, and filtered states.

SYN scan may be requested by passing the `-sS` option to Nmap. It requires raw-packet privileges, and is the default TCP scan when they are available. So when running Nmap as root or Administrator, `-sS` is usually omitted. This default SYN scan behavior is shown in Example 5-1, which finds a port in each of the three major states.

### Example 5-1. A SYN Scan showing three port states

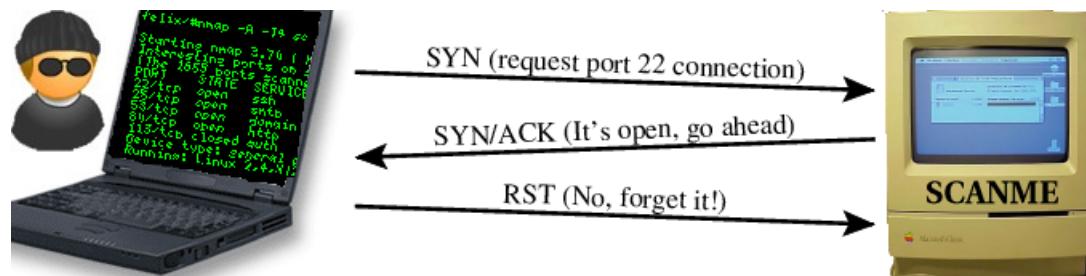
```
krad# nmap -p22,113,139 scanme.nmap.org

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
PORT      STATE      SERVICE
22/tcp    open       ssh
113/tcp   closed    auth
139/tcp   filtered  netbios-ssn
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 1.345 seconds
```

While SYN scan is pretty easy to use without any low-level TCP (<http://www.rfc-editor.org/rfc/rfc793.txt>) knowledge, understanding the technique helps when interpreting unusual results. Fortunately for us, the fearsome black-hat cracker Ereet Hagiwara has taken a break from terrorizing Japanese Windows users ([http://www.microsoft.com/japan/security/security\\_bulletins/MS04-003e.asp](http://www.microsoft.com/japan/security/security_bulletins/MS04-003e.asp)) to illustrate the Example 5-1 SYN scan for us at the packet level. First, the behavior against open port 22 is shown in Figure 5-2.

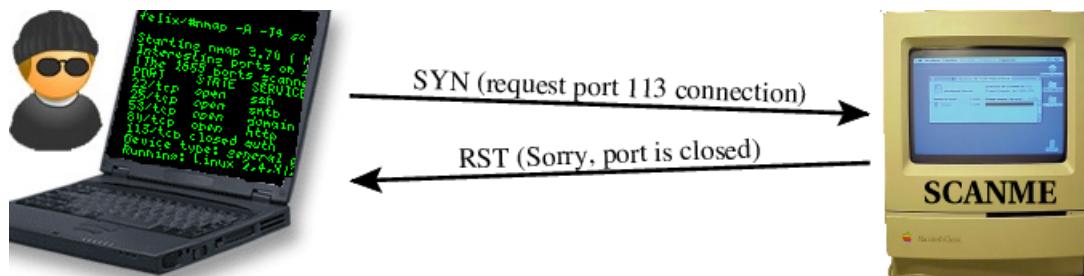
**Figure 5-2. SYN scan of open port 22**



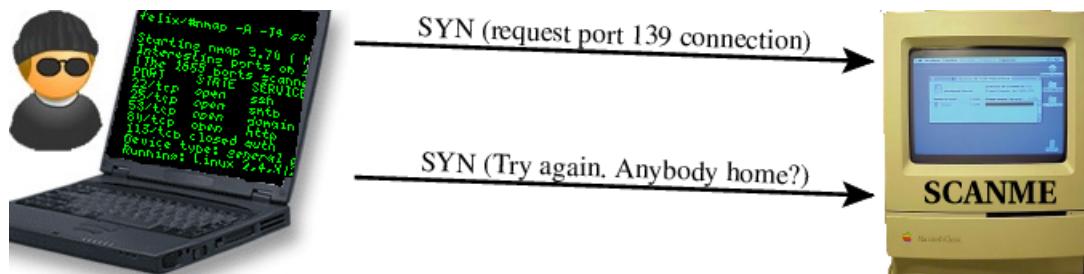
\* When illustrators create final versions of these, Ereet may have to be redrawn for copyright reasons. And the hostname should be krad.

As this example shows, Nmap starts by sending a TCP packet with the SYN flag set (see Figure 4-2 if you have forgotten what packet headers look like) to port 22. This is the first step in the TCP three-way handshake that any legitimate connection attempt takes. Since the target port is open, Scanme takes the second step by sending a response with the SYN and ACK flags back. In a normal connection, Ereet's machine (named krad) would complete the three-way handshake by sending an ACK packet acknowledging the SYN/ACK. Nmap does not need to do this, since the SYN/ACK response already told it that the port is open. If Nmap completed the connection, it would then have to worry about closing it. This usually involves another three-way handshake, using FIN packets rather than SYN. So an ACK is a bad idea, yet something still has to be done. If the SYN/ACK is ignored completely, Scanme will assume it was dropped and keep resending it. The proper response, since we don't want to make a full connection, is a RST packet as shown in the diagram. This tells Scanme to forget about (reset) the attempted connection. Nmap could send this RST packet easily enough, but it actually doesn't need to. The OS running on krad also receives the the SYN/ACK, which it doesn't expect because Nmap crafted the SYN probe itself. So the OS responds to the unexpected SYN/ACK with a RST packet. All RST packets described in this chapter also have the ACK bit set because they are always sent in response to (and acknowledge) a received packet. So that bit is not shown explicitly for RST packets. Because the three-way handshake is never completed, SYN scan is sometimes called half-open scanning.

Figure 5-3 shows how Nmap determines that port 113 is closed. This is even simpler than the open case. The first step is always the same -- Nmap sends the SYN probe to Scanme. But instead of receiving a SYN/ACK back, a RST is returned. That settles it -- the port is closed. No more communication regarding this port is necessary.

**Figure 5-3. SYN scan of closed port 113**

Finally, Ereet shows us how a filtered port appears to Nmap in Figure 5-4. The initial SYN is sent first, as usual, but Nmap sees no reply. The response could simply be slow. From previous responses (or timing defaults), Nmap knows how long to wait and eventually gives up on receiving one. A nonresponsive port is usually filtered (blocked by a firewall device, or perhaps the host is down), but this one test is not conclusive. Perhaps the port is open but the probe or response were simply dropped. Networks can be pretty flaky. So Nmap tries again, sending another SYN probe. After yet another timeout period, Nmap gives up and marks the port `filtered`. In this case, only one retransmission was attempted. As described in Section 5.13, Nmap keeps careful packet loss statistics and will attempt more retransmissions when scanning less reliable networks.

**Figure 5-4. SYN scan of filtered port 139**

Nmap will also consider a port `filtered` if it receives certain ICMP error messages back. Table 5-2 shows how Nmap assigns port states based on responses to a SYN probe.

**Table 5-2. How Nmap interprets responses to a SYN probe**

Probe Response	Assigned State
TCP SYN/ACK response	open
TCP RST response	closed
No response received	filtered (if probe retransmissions also fail to elicit responses)
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

While the pretty illustrations in this section are useful when you have them, Nmap reports exactly what it is doing at the packet level when you specify the `--packet_trace` option in addition to any other desired options. This is a great way for newbies to understand Nmap's behavior when Ereet is not around to help. Even advanced users find it

handy when Nmap produces results they don't expect. You may want to increase the debug level with `-d` (or even `-d5`) as well. Then scan the minimum number of ports and hosts necessary for your purpose or you could end up with literally millions of output lines. Example 5-2 repeats Ereet's 3-port SYN scan with packet tracing enabled (output edited for brevity). Read the command-line, then test yourself by figuring out what packets will be sent before reading on. Then once you read the trace up to "The SYN Stealth Scan took 1.25s", you should know from the RCVD lines what the port state table will look like before continuing on to read it.

### **Example 5-2. Using --packet\_trace to understand a SYN scan**

```
krad# nmap -d --packet_trace -p22,113,139 scanme.nmap.org

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
SENT (0.0130s) ICMP krad > scanme Echo request (type=8/code=0) ttl=52 id=1829
SENT (0.0160s) TCP krad:63541 > scanme:80 A iplen=40 seq=3191911070 ack=2499850910
RCVD (0.0280s) ICMP scanme > krad Echo reply (type=0/code=0) iplen=28
We got a ping packet back from scanme: id = 48821 seq = 714 checksum = 16000
massping done: num_hosts: 1 num_responses: 1
Initiating SYN Stealth Scan against scanme.nmap.org (scanme) [3 ports] at 00:53
SENT (0.1340s) TCP krad:63517 > scanme:113 S iplen=40 seq=1610438635
SENT (0.1370s) TCP krad:63517 > scanme:22 S iplen=40 seq=1610438635
SENT (0.1400s) TCP krad:63517 > scanme:139 S iplen=40 seq=1610438635
RCVD (0.1460s) TCP scanme:113 > krad:63517 RA iplen=40 seq=0 ack=1610438636
RCVD (0.1510s) TCP scanme:22 > krad:63517 SA iplen=44 seq=4275897108 ack=1610438636
SENT (1.2550s) TCP krad:63518 > scanme:139 S iplen=40 seq=1610373098 win=3072
The SYN Stealth Scan took 1.25s to scan 3 total ports.
Interesting ports on scanme.nmap.org (205.217.153.55):
PORT      STATE      SERVICE
22/tcp    open       ssh
113/tcp   closed    auth
139/tcp   filtered  netbios-ssn

Nmap run completed -- 1 IP address (1 host up) scanned in 1.403 seconds
```

SYN scan has long been called the stealth scan because it is subtler than TCP connect() scan (discussed next), which was the most common scan type before Nmap was released. Despite that moniker, don't count on a default SYN scan slipping undetected through sensitive networks. Widely deployed intrusion detection systems, personal firewalls, and similar systems are all quite capable of detecting default SYN scans. More effective techniques for stealthy scanning are demonstrated in Chapter 9.

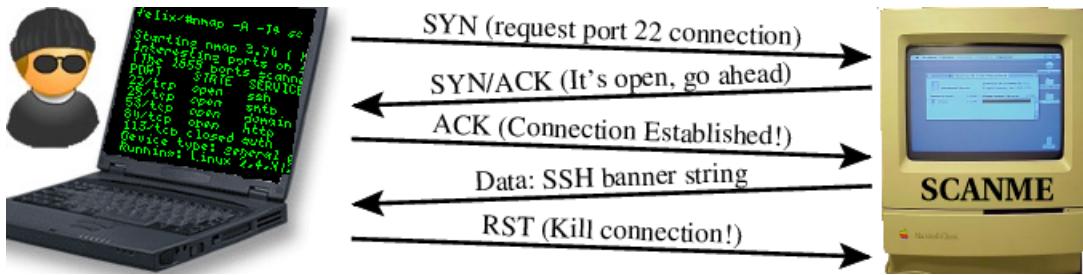
## **5.3. TCP Connect() Scan**

TCP Connect() scan is the default TCP scan type when SYN scan is not an option. This is the case when a user does not have raw packet privileges or is scanning IPv6 networks. Instead of writing raw packets as most other scan types do, Nmap asks the underlying operating system to establish a connection with the target machine and port by issuing the `connect()` system call. This is the same high-level system call that web browsers, P2P clients, and most other network-enabled applications use to establish a connection. It is part of a programming interface known as the Berkeley Sockets API. Rather than read raw packet responses off the wire, Nmap uses this API to obtain status information on each connection attempt. This and the FTP bounce scan (Section 5.12) are the only scan types available to unprivileged users.

When SYN scan is available, it is usually a better choice. Nmap has less control over the high level `connect()` call than with raw packets, making it less efficient. The system call completes connections to open target ports rather than performing the half-open reset that SYN scan does. Not only does this take longer and require more packets to obtain the same information, but target machines are more likely to log the connection. A decent IDS will catch either, but most machines have no such alarm system. Many services on your average UNIX system will add a note to syslog, and sometimes a cryptic error message, when Nmap connects and then closes the connection without sending data. Truly pathetic services crash when this happens, though that is uncommon. An administrator who sees a bunch of connection attempts in his logs from a single system should know that he has been `connect()` scanned.

Figure 5-5 shows a `connect()` scan in action against open port 22 of `scanme.nmap.org`. Recall that this only required three packets for the SYN scan in Example 5-1. The exact behavior against an open port depends on the platform Nmap runs on and the service listening at the other end, but this six packet example is typical.

**Figure 5-5. Connect scan of open port 22 (nmap -sT -p22 scanme.nmap.org)**



The first two steps (SYN and SYN/ACK) are exactly the same as with a SYN scan. Then, instead of aborting the half-open connection with a RST packet, krad acknowledges the SYN/ACK with its own ACK packet, completing the connection. In this case, Scanme even had time to send its SSH banner string (`SSH-1.99-OpenSSH_3.1p1\\n`) through the now-open connection. As soon as Nmap hears from its host OS that the connection was successful, it terminates the connection. TCP connections usually end with another three-way handshake involving the FIN flag, but Nmap asks the host OS to terminate the connection immediately with a RST packet.

While this `connect()` scan example took twice as many packets as a SYN scan, the bandwidth differences are rarely so substantial. The vast majority of ports in a large scan will be closed or filtered. The packet traces for those are the same as described for SYN scan in Figure 5-3 and Figure 5-4. Only open ports generate more network traffic.

The output of a `connect()` scan doesn't differ significantly from a SYN scan. Example 5-3 shows a `connect()` scan of Scanme. The `-sT` option could have been omitted since Nmap is being run from a non-privileged account so `connect()` scan is the default type. This scan takes 30-seconds, while a SYN scan performed afterward between the two machines took only 20 seconds.

### Example 5-3. Connect scan example

```
krad~$ nmap -T4 -sT scanme.nmap.org

Starting nmap 3.75 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 1658 ports scanned but not shown below are in state: filtered)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    open     smtp
53/tcp    open     domain
```

```

80/tcp  open  http
113/tcp closed auth

Nmap run completed -- 1 IP address (1 host up) scanned in 30.205 seconds

```

## 5.4. UDP Scan

While most popular services on the Internet run over the TCP protocol, UDP (<http://www.rfc-editor.org/rfc/rfc768.txt>) services are not uncommon. DNS, SNMP, and DHCP (registered ports 53, 161/162, and 67/68) are three of the most common. Because UDP scanning is generally slower and more difficult than TCP, some security auditors ignore these ports. This is a mistake, as exploitable UDP services are quite common and attackers certainly don't ignore the whole protocol. Fortunately, Nmap can help inventory UDP ports.

UDP scan is activated with the `-sU` option. It can be combined with a TCP scan type such as SYN scan (`-sS`) to check both protocols during the same run.

UDP scan works by sending an empty (no data) UDP header to every targeted port. Based on the response, or lack thereof, the port is assigned to one of four states, as shown in Table 5-3.

**Table 5-3. How Nmap interprets responses to a UDP probe**

Probe Response	Assigned State
Any UDP response from target port (unusual)	open
No response received	open filtered (if probe retransmissions also fail to elicit responses)
ICMP port unreachable error (type 3, code 3)	closed
Other ICMP unreachable errors (type 3, code 1, 2, 9, 10, or 13)	filtered

The most curious element of this table may be the `open|filtered` state. It is a symptom of the biggest challenges with UDP scanning: open ports rarely respond to these probes. The target TCP/IP stack simply passes the (empty) packet up to the listening application, which usually discards it immediately as invalid. If ports in all other states would respond, then open ports could all be deduced by elimination. Unfortunately, firewalls and filtering devices are *also* known to drop packets without responding. So when Nmap receives no response after several attempts, it cannot determine whether the port is `open` or `filtered`. When Nmap was released, filtering devices were rare enough that Nmap could (and did) simply assume that the port was `open`. The Internet is better guarded now, so Nmap changed in 2004 (version 3.70) to report nonresponsive UDP ports as `open|filtered` instead. We can see that in Example 5-4, which shows Ereet scanning a Linux box named Felix.

### Example 5-4. UDP scan example

```

krad# nmap -sU -v -F felix

Starting nmap 3.75 ( http://www.insecure.org/nmap/ )
Interesting ports on felix.yuma.net (192.168.0.42):
(The 1005 ports scanned but not shown below are in state: closed)
PORT      STATE          SERVICE
53/udp    open|filtered domain

```

```

67/udp open|filtered dhcpserver
111/udp open|filtered rpcbind
MAC Address: 00:02:E3:14:11:02 (Lite-on Communications)

Nmap run completed -- 1 IP address (1 host up) scanned in 999.250 seconds

```

This scan of Felix demonstrates the `open|filtered` ambiguity issue as well as another problem: UDP scanning can be *slow*. Scanning a thousand ports took almost 17 minutes in this case. Nmap provides ways to work around both problems, as described by the following two sections.

### 5.4.1. Disambiguating open from filtered UDP ports

In the case of the Felix scan, all but the three `open|filtered` ports were `closed`. So the scan was still successful in narrowing down potentially open ports to a handful. That is not always the case. Example 5-5 shows a UDP scan against the heavily filtered site Scanme.

#### Example 5-5. UDP scan example

```

krad# nmap -sU -F scanme.nmap.org

Starting nmap 3.75 ( http://www.insecure.org/nmap/ )
All 1008 scanned ports on scanme.nmap.org (205.217.153.55) are: open|filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 23.187 seconds

```

In this case, the scan didn't narrow down the open ports at all. All 1008 are `open|filtered`. A new strategy is called for.

Table 5-3 shows that the `open|filtered` state occurs when Nmap fails to receive any responses from its UDP probes to a particular port. Yet it also shows that, on rare occasions, the UDP service listening on a port will respond in kind, proving that the port is open. The reason these services don't respond often is that the empty packets Nmap sends are considered invalid. Unfortunately, UDP services generally define their own packet structure rather than adhering to some common general format that Nmap could always send. An SNMP packet looks completely different than a SunRPC, NFS, or DNS request packet.

To send the proper packet for every popular UDP service, Nmap would need a large database defining their probe formats. Fortunately, Nmap has that in the form of `nmap-versions`, which is part of the service and version detection subsystem described in Chapter 7.

When version scanning is enabled with `-sV` (or `-A`), it will send UDP probes to every `open|filtered` port (as well as known open ones). If any of the probes elicit a response from an `open|filtered` port, the state is changed to `open`. The results of adding `-sV` to the Felix scan are shown in Example 5-6.

#### Example 5-6. Improving Felix's UDP scan results with version detection

```

krad# nmap -sUV -F felix.yuma.net

Starting nmap 3.75 ( http://www.insecure.org/nmap/ )
Interesting ports on felix.yuma.net (192.168.0.42):
(The 1005 ports scanned but not shown below are in state: closed)
PORT      STATE         SERVICE      VERSION
53/udp    open          domain      ISC Bind 9.2.1

```

```

67/udp open|filtered dhcpserver
111/udp open rpcbind 2 (rpc #100000)
MAC Address: 00:02:E3:14:11:02 (Lite-on Communications)

Nmap run completed -- 1 IP address (1 host up) scanned in 1037.570 seconds

```

This new scan shows that port 111 and 53 are definitely open. The system isn't perfect though -- port 67 is still open|filtered. In this particular case, the port is open but Nmap does not have a working version probe for dhcp. Another tough service is SNMP, which usually only responds when the correct community string is given. Many devices are configured with the community string public, but not all are. While these results aren't perfect, learning the true state of two out of three tested ports is still helpful.

After the success in disambiguating Felix results, Ereet turns his attention back to Scanme, which listed all ports as open|filtered last time. He tries again with version detection, as shown in Example 5-7.

### **Example 5-7. Improving Scanme's UDP scan results with version detection**

```

krad# nmap -sUV -F scanme.nmap.org

Starting nmap 3.75 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 1007 ports scanned but not shown below are in state: open|filtered)
PORT      STATE SERVICE VERSION
53/udp    open  domain  ISC Bind 9.2.1

Nmap run completed -- 1 IP address (1 host up) scanned in 3053.411 seconds

```

This result took 50 minutes, versus 23 seconds for the previous Scanme scan, but these results are actually useful. Ereet's smile widens and eyes sparkle at this evidence of an open ISC Bind nameserver on a machine he wants to compromise. That software has a long history of security holes, so perhaps he can find a flaw in this recent version.

While Ereet will focus his UDP attacks on port 53 since it is confirmed open, he does not forget about the other ports. Those 1007 are listed as open|filtered. As we witnessed with the dhcpserver port on Felix, certain open UDP services can hide even from Nmap version detection. He has also only scanned the default ports so far, there are 64529 others that could possibly be open. For the record, 53 is the only open UDP port on Scanme.

While this version detection technique is the only way for Nmap to automatically disambiguate open|filtered ports, there are a couple tricks that can be tried manually. Sometimes a specialized traceroute can help. You could do a traceroute against a known-open TCP or UDP port with a tool such as hping2 (<http://www.hping.org>). Then try the same against the questionable UDP port. Differences in hop counts can differentiate open from filtered ports. Ereet attempts this against Scanme in Example 5-8. The first hping2 command does a UDP traceroute against known-open port 53. The -t 8 option tells hping2 to start at hop 8 and is only used here to save space. The second command does the same thing against presumed-closed port 54.

### **Example 5-8. Attempting to disambiguate UDP ports with TTL discrepancies**

```

krad# hping2 --udp --traceroute -t 8 -p 53 scanme.nmap.org
HPING scanme.nmap.org (ppp0): udp mode set, 28 headers + 0 data bytes
hop=8 TTL 0 during transit from ip=206.24.211.77 name=dcr2.SanFranciscosfo.savvis.net
hop=9 TTL 0 during transit from ip=208.172.147.94 name=bpr2.PaloAltoPaix.savvis.net
hop=10 TTL 0 during transit from ip=206.24.240.194 name=meernet.PaloAltoPaix.savvis.net
hop=11 TTL 0 during transit from ip=205.217.152.21 name=vlan21.sv.meer.net

```

```

--- scanme.nmap.org hping statistic ---
12 packets transmitted, 4 packets received, 67% packet loss
round-trip min/avg/max = 13.4/13.8/14.1 ms

krad# hping2 --udp --traceroute -t 8 -p 54 scanme.nmap.org
HPING scanme.nmap.org (ppp0): udp mode set, 28 headers + 0 data bytes
hop=8 TTL 0 during transit from ip=206.24.211.77 name=dcr2.SanFranciscosfo.savvis.net
hop=9 TTL 0 during transit from ip=208.172.147.94 name=bpr2.PaloAltoPaix.savvis.net
hop=10 TTL 0 during transit from ip=206.24.240.194 name=meernet.PaloAltoPaix.savvis.net
hop=11 TTL 0 during transit from ip=205.217.152.21 name=vlan21.sv.meer.net

--- scanme.nmap.org hping statistic ---
12 packets transmitted, 4 packets received, 67% packet loss
round-trip min/avg/max = 12.5/13.6/14.7 ms

```

In this example, Ereet was only able to reach hop eleven of both the open and closed ports. So these results can't be used to distinguish port states against this host. It was worth a try, and does work in a significant number of cases. It is more likely to work in situations where the screening firewall is at least a hop or two before the target host. Scanme, on the other hand, is running its own Linux iptables host-based firewall. So there is no difference in hopcount between filtered and open ports.

Another technique is to try application-specific tools against common ports. For example, a brute force SNMP community string cracker could be tried against port 161. As Nmap's version detection probe database grows, the need to augment its results with external specialized tools is reduced. They will still be useful for special cases, such as SNMP devices with a custom community string.

### 5.4.2. Speeding up UDP scans

The other big challenge with UDP scanning is doing so quickly. Open and filtered ports rarely send any response, leaving Nmap to time out and then conduct retransmissions just in case the probe or response were lost. Closed ports are often an even bigger problem. They usually send back an ICMP port unreachable error. But unlike the RST packets sent by closed TCP ports in response to a SYN or Connect scan, many hosts rate limit ICMP port unreachable messages by default. Linux and Solaris are particularly strict about this. For example, the Linux 2.4.20 kernel on Felix limits destination unreachable messages to one per second (in `net/ipv4/icmp.c`). This explains why the scan in Example 5-4 is so slow.

Nmap detects rate limiting and slows down accordingly to avoid flooding the network with useless packets that the target machine will drop. Unfortunately, a Linux-style limit of one packet per second makes a 65,536-port scan take more than 18 hours. Here are some suggestions specific to this problem. Also read Chapter 6 for more detailed discussion and general advise.

Increase host parallelism

If Nmap receives just one port unreachable error from a single target host per second, it could receive 100/second just by scanning 100 such hosts at once. Implement this by passing a large value (such as 100) to `--min_hostgroup`.

Scan popular ports first

Very few UDP port numbers are commonly used. A scan of a hundred common ports will go quite quickly. You can then investigate those results while you launch a multi-day 65K-port sweep of the network in the background.

Scan from behind the firewall

As with TCP, packet filters can slow down scans dramatically. Many modern firewalls make setting packet rate limits easy. If you can bypass that problem by launching the scan from behind the firewall rather than across it, do so.

Use `-v` and chill out

With verbosity (`-v`) enabled, Nmap provides estimated time for scan completion of each host. There is no need to watch it closely. Get some sleep, head to your favorite pub, read a book, finish other work, or otherwise amuse yourself while Nmap tirelessly scans on your behalf.

## 5.5. TCP Null, FIN, and Xmas Scans

These three scan types (even more are possible with the `--scanflags` option described in the next section) exploit a subtle loophole in the TCP RFC (<http://www.rfc-editor.org/rfc/rfc793.txt>) to differentiate between open and closed ports. Page 65 says that “if the [destination] port state is CLOSED .... an incoming segment not containing a RST causes a RST to be sent in response.” Then the next page discusses packets sent to open ports without the SYN, RST, or ACK bits set, stating that: “you are unlikely to get here, but if you do, drop the segment, and return.”

When scanning systems compliant with this RFC text, any packet not containing SYN, RST, or ACK bits will result in a returned RST if the port is closed and no response at all if the port is open. As long as none of those three bits are included, any combination of the other three (FIN, PSH, and URG) are OK. Nmap exploits this with three scan types:

Null scan (`-sN`)

Does not set any bits (tcp flag header is 0)

FIN scan (`-sF`)

Sets just the TCP FIN bit.

Xmas scan (`-sX`)

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

These three scan types are exactly the same in behavior except for the TCP flags set in probe packets. Responses are treated as shown in Table 5-4.

**Table 5-4. How Nmap interprets responses to a Null, FIN, or Xmas scan probe**

Probe Response	Assigned State
No response received	open filtered (if probe retransmissions also fail to elicit responses)
TCP RST packet	closed

Probe Response	Assigned State
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

The key advantage to these scan types is that they can sneak through certain non-stateful firewalls and packet filtering routers. Such firewalls try to prevent incoming TCP connections (while allowing outbound ones) by blocking any TCP packets with the SYN bit set and ACK cleared. This configuration is common enough that the Linux iptables firewall command offers a special `--syn` option to implement it. The Null, FIN, and Xmas scans clear the SYN bit and thus fly right through those rules.

Another advantage is that these scan types are a little more stealthy than even a SYN scan. Don't count on this though -- most modern IDS products can be configured to detect them.

The big downside is that not all systems follow RFC 793 to the letter. A number of systems send RST responses to the probes regardless of whether the port is open or not. This causes all of the ports to be labeled `closed`. Major operating systems that do this are Microsoft Windows, many Cisco devices, BSDI, and IBM OS/400. This scan does work against most UNIX-based systems though. Since Nmap OS detection tests for this quirk, you can learn whether the scan works against a particular type of system by examining the `nmap-os-fingerprints` file. Test T2 sends a NULL packet to an open port. So if you see a line like `T2 (Resp=N)`, that system seems to support the RFC and one of these scans should work against it. If the T2 line is longer, the system violated the RFC by sending a response and these scans won't work. Chapter 8 explains OS fingerprinting in further detail.

Another downside of these scans is that they can't distinguish open ports from certain filtered ones. If the packet filter sends an ICMP destination prohibited error, Nmap knows that a port is filtered. But most filters simply drop banned probes without any response, making the ports appear open. Since Nmap cannot be sure which is the case, it marks nonresponsive ports as `open|filtered`. Adding version detection (`-sV`) can disambiguate as it does with UDP scans, but that defeats much of the stealthy nature of this scan. If you are willing and able to connect to the ports anyway, you might as well use a SYN scan.

Using these scan methods is simple. Just add the `-sN`, `-sF`, or `-sX` options to specify the scan type. Example 5-9 shows two examples. The first one, a FIN scan against Para, identifies all 5 open ports (as `open|filtered`). The next execution, an Xmas scan against `scanme.nmap.org` doesn't work so well. Since it is unable to differentiate the 1658 filtered ports from the 4 open ones, all 1662 are listed as `open|filtered`. This demonstrates why Nmap offers so many scan methods. No single technique is preferable in all cases. Ereet will simply have to try another method to learn more about Scanme.

### Example 5-9. Example FIN and Xmas scans

```
krad# nmap -sF -T4 para

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on para (192.168.10.191):
(The 1658 ports scanned but not shown below are in state: closed)
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
53/tcp    open|filtered domain
111/tcp   open|filtered rpcbind
515/tcp   open|filtered printer
6000/tcp  open|filtered X11
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 4.644 seconds
```

```
krad# nmap -sX -T4 scanme.nmap.org
```

```
Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 1662 ports scanned but not shown below are in state: open|filtered)
PORT      STATE SERVICE
113/tcp    closed auth
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 23.112 seconds
```

Demonstrating the full, firewall-bypassing power of these scans requires a rather lame target firewall configuration. Unfortunately, those aren't hard to find. Example 5-10 shows a SYN scan of a SCO/Caldera machine named Docsrv.

**Example 5-10. SYN scan of docsrv.caldera.com**

```
# nmap -sS -T4 docsrv.caldera.com
```

```
Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on docsrv.caldera.com (216.250.128.247):
(The 1660 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed auth
507/tcp   open  crs
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 28.624 seconds
```

This example looks OK. Only two ports are open and the rest (except for 113) are filtered. With a modern stateful firewall, a FIN scan should not produce any extra information. Yet I try it anyway, obtaining the output in Example 5-11.

**Example 5-11. FIN scan of docsrv.caldera.com**

```
# nmap -sF -T4 docsrv.caldera.com
```

```
Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on docsrv.caldera.com (216.250.128.247):
(The 1624 ports scanned but not shown below are in state: closed)
PORT      STATE      SERVICE
7/tcp     open|filtered echo
9/tcp     open|filtered discard
11/tcp    open|filtered systat
13/tcp    open|filtered daytime
15/tcp    open|filtered netstat
19/tcp    open|filtered chargen
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
23/tcp    open|filtered telnet
25/tcp    open|filtered smtp
```

```

37/tcp    open|filtered time
79/tcp    open|filtered finger
80/tcp    open|filtered http
110/tcp   open|filtered pop3
111/tcp   open|filtered rpcbind
135/tcp   open|filtered msrpc
143/tcp   open|filtered imap
360/tcp   open|filtered scoi2odialog
389/tcp   open|filtered ldap
465/tcp   open|filtered smtps
507/tcp   open|filtered crs
512/tcp   open|filtered exec
513/tcp   open|filtered login
514/tcp   open|filtered shell
515/tcp   open|filtered printer
636/tcp   open|filtered ldapssl
712/tcp   open|filtered unknown
955/tcp   open|filtered unknown
993/tcp   open|filtered imaps
995/tcp   open|filtered pop3s
1434/tcp  open|filtered ms-sql-m
2000/tcp  open|filtered callbook
2766/tcp  open|filtered listen
3000/tcp  open|filtered ppp
3306/tcp  open|filtered mysql
6112/tcp  open|filtered dtspc
32770/tcp open|filtered sometimes-rpc3
32771/tcp open|filtered sometimes-rpc5
32772/tcp open|filtered sometimes-rpc7

```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 7.635 seconds
```

Wow! That is a lot of apparently open ports. Most of them are probably open, because having just these 39 filtered and the other 1624 closed (sending a RST packet) would be unusual. Yet it is still possible that some or all are filtered instead of open. FIN scan cannot determine for sure. We will revisit this case and learn more later in this chapter.

## 5.6. Custom scan types with `--scanflags`

Truly advanced Nmap users need not limit themselves to the canned scanned types offered. The `--scanflags` allows you to design your own scan by specifying arbitrary TCP flags. Let your creative juices flow, while evading intrusion detection systems whose vendors simply paged through the Nmap man page adding specific rules!

The `--scanflags` argument can be a numerical flag value such as 9 (PSH and FIN), but using symbolic names is easier. Just mash together any combination of URG, ACK, PSH, RST, SYN, and FIN. For example, `--scanflags URGACKPSHRSTSYNFIN` sets everything, though it's not very useful for scanning. The order these are specified in is irrelevant.

In addition to specifying the desired flags, you can specify a TCP scan type (such as `-sA` or `-sF`). That base type tells Nmap how to interpret responses. For example, a SYN scan considers no-response to indicate an `filtered` port, while a FIN scan treats the same as `open|filtered`. Nmap will behave the same way it does for the base scan type, except that it will use the TCP flags you specify instead. If you don't specify a base type, SYN scan is used.

### 5.6.1. Custom SYN/FIN scan

One interesting custom scan type is SYN/FIN. Sometimes a firewall admin or device manufacturer will attempt to block incoming connections with a rule such as “drop any incoming packets with only the SYN flag set”. They limit it to *only* the SYN flag because they don’t want to block the SYN/ACK packets which are returned as the second step of an outgoing connection.

The problem with this approach is that most end systems will accept initial SYN packets that contain other (non-ACK) flags as well. For example, the Nmap OS fingerprinting system sends a SYN/FIN/URG/PSH packet to an open port. More than half of the fingerprints in the database respond with a SYN/ACK. Thus they allow port scanning with this packet and generally allow making a full TCP connection too. Some systems have even been known to respond with SYN/ACK to a SYN/RST packet! The TCP RFC is ambiguous as to which flags are acceptable in an initial SYN packet, though SYN/RST certainly seems bogus.

Example 5-12 shows Ereet conducting a successful SYN/FIN scan of Google. Apparently he is getting bored with scanme.nmap.org.

#### Example 5-12. A SYN/FIN scan of Google

```
krad# nmap -sS --scanflags SYNFIN -T4 www.google.com

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on www.google.com (216.239.57.103):
(The 1660 ports scanned but not shown below are in state: filtered)
PORT      STATE    SERVICE
80/tcp    open     http
179/tcp   closed   bgp
443/tcp   open     https

Nmap run completed -- 1 IP address (1 host up) scanned in 22.914 seconds
```

Similar scan types, such as SYN/URG or SYN/PSH/URG/FIN will generally work as well. If you aren’t getting through, don’t forget the already mentioned SYN/RST option.

### 5.6.2. PSH scan

Section 5.5 noted that RFC-compliant systems allow one to scan ports using any combination of the FIN, PSH, and URG flags. While there are eight possible permutations, Nmap only offers three canned modes (Null, FIN, and Xmas). Show some personal flair by trying a PSH/URG or FIN/PSH scan instead. Results rarely differ from the three canned modes, but there is a small chance of evading scan detection systems.

To perform such a scan, just specify your desired flags with `--scanflags` and specify FIN scan (`-sF`) as the base type (choosing Null or Xmas would make no difference). Example 5-13 demonstrates a PSH scan against a Linux machine on my local network.

#### Example 5-13. A custom PSH scan

```
krad# nmap -sF --scanflags PSH  para

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on para (192.168.10.191):
(The 1658 ports scanned but not shown below are in state: closed)
```

```

PORT      STATE           SERVICE
22/tcp    open|filtered ssh
53/tcp    open|filtered domain
111/tcp   open|filtered rpcbind
515/tcp   open|filtered printer
6000/tcp  open|filtered X11
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap run completed -- 1 IP address (1 host up) scanned in 5.953 seconds

```

Because these scans all work the same way, I could keep just one of `-sF`, `-sN`, and `-sX` options, letting users emulate the others with `--scanflags`. There are no plans to do this because the shortcut options are easier to remember and use. You can still try the emulated approach to show off your Nmap skills. Execute `nmap -sF --scanflags FINPSHURG target` rather than the more mundane `nmap -sX target`.

### Warning

In my experience, needlessly complex Nmap command-lines don't impress girls. They usually respond with a condescending sneer, presumably because they recognize that the command is redundant.

## 5.7. TCP ACK Scan

This scan is different than the others discussed so far in that it never determines open (or even `open|filtered`) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

ACK scan is enabled by specifying the `-sA` option. Its probe packet has only the ACK flag set (unless you use `--scanflags`). When scanning unfiltered systems, open and closed ports will both return a RST packet. Nmap then labels them as unfiltered, meaning that they are reachable by the ACK packet, but whether they are open or closed is undetermined. Ports that don't respond, or send certain ICMP error messages back, are labeled filtered. Table 5-5 provides the full details.

**Table 5-5. How Nmap interprets responses to an ACK scan probe**

Probe Response	Assigned State
TCP RST response	unfiltered
No response received	filtered (if probe retransmissions also fail to elicit responses)
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

ACK scan usage is similar to most other scan types in that you simply add a single option flag, `-sA` in this case. Example 5-14 shows an ACK scan against Scanme.

#### Example 5-14. A Typical ACK Scan

```
krad# nmap -sA -T4 scanme.nmap.org
```

```

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 1658 ports scanned but not shown below are in state: filtered)
PORT      STATE      SERVICE
22/tcp    UNfiltered ssh
25/tcp    UNfiltered smtp
53/tcp    UNfiltered domain
80/tcp    UNfiltered http
113/tcp   UNfiltered auth

Nmap run completed -- 1 IP address (1 host up) scanned in 19.823 seconds

```

One of the most interesting uses of ACK scanning is to differentiate between stateful and stateless firewalls. Section 9.3.2 describes how to do this and why you would want to.

Sometimes a combination of scan types can be used to glean extra information from a system. As an example, start by reviewing the FIN scan of Docsvr in Example 5-11. Nmap finds the closed ports in that case, but 39 of them are listed as open|filtered because Nmap cannot determine between those two states with a FIN scan. Now look at the ACK scan of the same host in Example 5-15. Two of those 39 previously unidentified ports are shown to be filtered. The other 37 (based on the default port line above the table) are in the state unfiltered. That means open or closed. If one scan type identifies a port as open or filtered and another identifies it as open or closed, logic dictates that it must be open. By combining both scan types, we have learned that 37 ports on Docsvr are open, 2 are filtered, and 1624 are closed. While logical deduction worked well here to determine port states, that technique can't always be counted on. It assumes that different scan types always return a consistent state for the same port, which is inaccurate. Firewalls and TCP stack properties can cause different scans against the same machine to differ markedly. Against Docsvr, we have seen that a SYN scan considers the SSH port (tcp/22) filtered, while an ACK scan considers it unfiltered. When exploring boundary conditions and strangely configured networks, interpreting Nmap results is an art that benefits from experience and intuition.

### Example 5-15. An ACK scan of Docsvr

```

# nmap -sA -T4 docsvr.caldera.com

Starting nmap 3.77 ( http://www.insecure.org/nmap/ )
Interesting ports on docsvr.caldera.com (216.250.128.247):
(The 1661 ports scanned but not shown below are in state: UNfiltered)
PORT      STATE      SERVICE
135/tcp   filtered msrpc
1434/tcp  filtered ms-sql-m

Nmap run completed -- 1 IP address (1 host up) scanned in 7.207 seconds

```

## 5.8. TCP Window Scan

Window scan is exactly the same as ACK scan except that it exploits an implementation detail of certain systems to differentiate open ports from closed ones, rather than always printing UNfiltered when a RST is returned. It does this by examining the TCP Window value of the RST packets returned. On some systems, open ports use a positive window size (even for RST packets) while closed ones have a zero window. Window scan sends the same bare ACK probe as ACK scan, interpreting the results as shown in Table 5-6.

**Table 5-6. How Nmap interprets responses to a Window scan ACK probe**

Probe Response	Assigned State
TCP RST response with non-zero window field	open
TCP RST response with zero window field	closed
No response received	filtered (if probe retransmissions also fail to elicit responses)
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

This scan relies on an implementation detail of a minority of systems out on the Internet, so you can't always trust it. Systems that don't support it will usually return all ports `closed`. Of course, it is possible that the machine really has no open ports. If most scanned ports are `closed` but a few common port numbers (such as 22, 25, 53) are `filtered`, the system is most likely susceptible. Occasionally, systems will even show the exact opposite behavior. If your scan shows 1000 open ports and 3 closed or filtered ports, then those three may very well be the truly open ones.

While this scan is not suited for every situation, it can be quite useful on occasion. Recall Example 5-11, which shows many `open|filtered` ports not found in a basic SYN scan. The problem is that we can't distinguish between open and filtered ports with that FIN scan. The previous section showed that we could distinguish them by combining FIN and ACK scan results. In this case, a Window scan makes it even easier by not requiring the FIN scan results, as shown in Example 5-16.

#### Example 5-16. Window scan of docsrv.caldera.com

```
# nmap -sW -T4 docsrv.caldera.com

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on docsrv.caldera.com (216.250.128.247):
(The 1624 ports scanned but not shown below are in state: closed)
PORT      STATE     SERVICE
7/tcp      open      echo
9/tcp      open      discard
11/tcp     open      systat
13/tcp     open      daytime
15/tcp     open      netstat
19/tcp     open      chargen
21/tcp     open      ftp
22/tcp     open      ssh
23/tcp     open      telnet
25/tcp     open      smtp
37/tcp     open      time
79/tcp     open      finger
80/tcp     open      http
110/tcp    open      pop3
111/tcp    open      rpcbind
135/tcp    filtered msrpc
143/tcp    open      imap
360/tcp    open      scoi2odialog
389/tcp    open      ldap
465/tcp    open      smtps
507/tcp    open      crs
```

```

512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
515/tcp  open  printer
636/tcp  open  ldapssl
712/tcp  open  unknown
955/tcp  open  unknown
993/tcp  open  imaps
995/tcp  open  pop3s
1434/tcp filtered ms-sql-m
2000/tcp open  callbook
2766/tcp open  listen
3000/tcp open  ppp
3306/tcp open  mysql
6112/tcp open  dtspc
32770/tcp open  sometimes-rpc3
32771/tcp open  sometimes-rpc5
32772/tcp open  sometimes-rpc7

```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 7.304 seconds
```

These results are exactly what we wanted! The same 39 interesting ports are shown as with the FIN scan, but this time it distinguishes between the two filtered ports (MS-SQL and MSRPC) and the 37 that are actually open. These are the same results we obtained by combining FIN and ACK scan results together in the previous section. Verifying results for consistency is another good reason for trying multiple scan types against a target network.

## 5.9. TCP Maimon Scan

The Maimon scan is named after its discoverer, Uriel Maimon. He described the technique in Phrack Magazine issue #49 (November 1996). Nmap, which included this technique, was released two issues later. This technique is exactly the same as Null, FIN, and Xmas scan, except that the probe is FIN/ACK. According to RFC 793 (TCP), a RST packet should be generated in response to such a probe whether the port is open or closed. However, Uriel noticed that many BSD-derived systems simply drop the packet if the port is open. Nmap takes advantage of this to determine open ports, as shown in Table 5-7.

**Table 5-7. How Nmap interprets responses to a Maimon scan probe**

Probe Response	Assigned State
No response received	open filtered (if probe retransmissions also fail to elicit responses)
TCP RST packet	closed
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

The Nmap flag for a Maimon scan is `-sM`. While this option was quite useful in 1996, modern systems rarely exhibit this bug. They send a RST back for all ports, making every port appear closed. This result is shown in Example 5-17

**Example 5-17. A failed Maimon scan**

```
# nmap -sM -T4 para

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
All 1663 scanned ports on para (192.168.10.191) are: closed
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap run completed -- 1 IP address (1 host up) scanned in 4.189 seconds
```

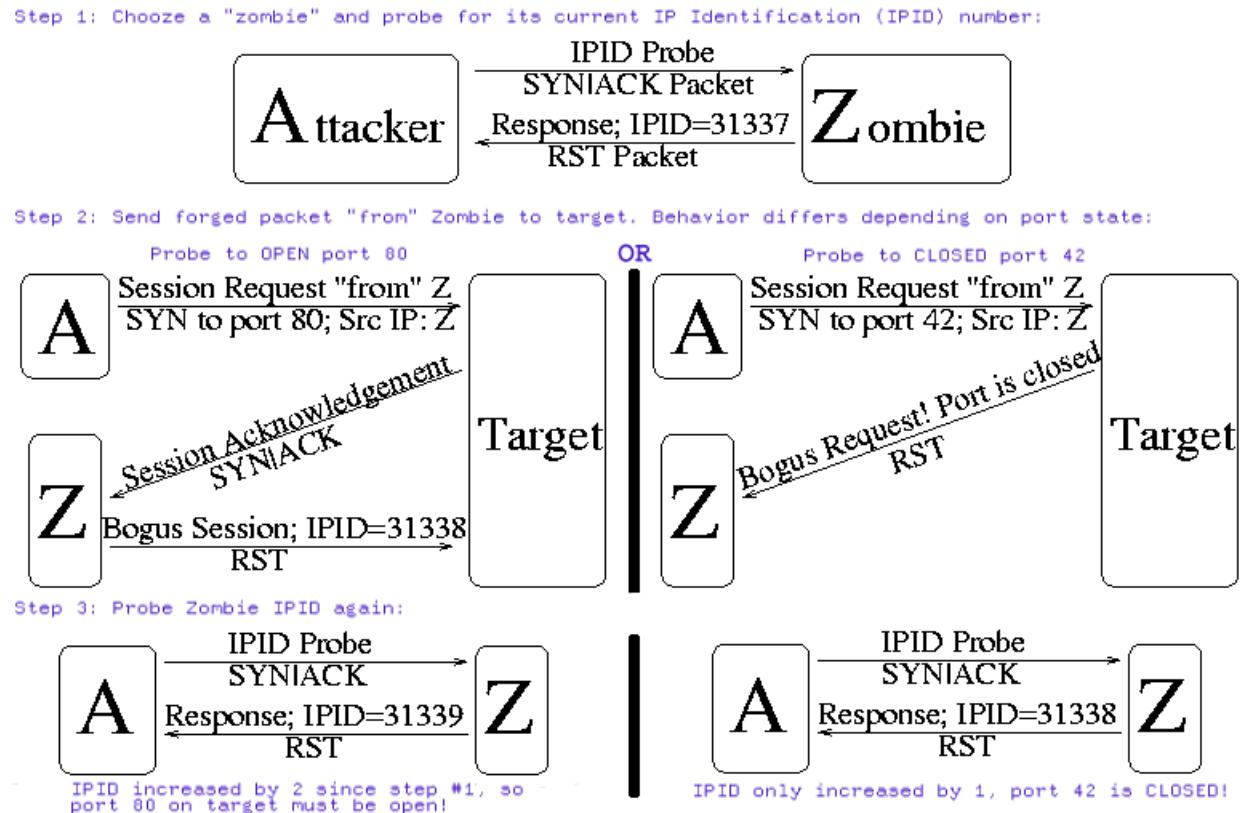
## 5.10. TCP Idle Scan

In 1998, security researcher Antirez (who also wrote the hping2 tool frequently used in this book) posted to the Bugtraq mailing list an ingenious new port scanning technique. Idle scan, as it has become known, allows for completely blind port scanning. Attackers can actually scan a target without sending a single packet to the target from their own IP address! Instead, a clever side-channel attack allows for the scan to be bounced off a dumb "zombie" host. Intrusion detection system (IDS) reports will finger the innocent zombie as the attacker. Besides being extraordinarily stealthy, this scan type permits mapping out IP-based trust relationships between machines.

While Idle scanning is more complex than any of the techniques discussed so far, you don't need to be a TCP/IP expert to understand it. It can be put together from these basic TCP/IP facts:

- One way to determine whether a TCP port is open is to send a SYN (session establishment) packet to the port. The target machine will respond with a SYN/ACK (session request acknowledgment) packet if the port is open, and RST (reset) if the port is closed. This is the basis of the previously discussed SYN scan.
- A machine which receives an unsolicited SYN|ACK packet will respond with a RST. An unsolicited RST will be ignored.
- Every IP packet on the Internet has a fragment identification number (IPID). Many operating systems simply increment this number for each packet they send. So probing for this number can tell an attacker how many packets have been sent since the last probe.

By combining these traits, it is possible to scan a target network while forging your identity so that it looks like an innocent "zombie" machine did the scanning. This technique is easiest to describe with a diagram. In Figure 5-6, an attacker, A, is scanning a Target machine, while blaming the scan on some Zombie, Z. The boxes represent machines, and the lines represent packets. Brief English descriptions of the packets are printed on top of the lines, while actual TCP flags and distinctive packet information is printed below them.

**Figure 5-6. Idle Scan Technique (Simplified)**

\* When this figure is redone, it should either show a filtered port case, or at least note at the bottom-right that port 42 is closed or filtered.

As this diagram demonstrates, the target hosts respond differently to the zombie depending on port state. If the probed port is open, the target sends a SYN/ACK to the zombie. The zombie does not expect this SYN/ACK, so it sends a RST back. By sending the RST, the zombie causes its IPID sequence number to increment. If the port is closed, the target sends a RST to the zombie. Zombies ignore this unsolicited RST packet and do not increment their IPID sequence number. In step three, the attacker simply probes for the Zombie's latest IPID. If the IPID value is just one higher than the previous probe, the new response accounts for that increment and the target port must be closed or filtered. Nmap versions starting with 3.78 label such a port as `closed|filtered`, while previous versions considered it `closed`. If the IPID value increased by two, that extra increment was due to the zombie sending back a RST to the target and so the port is open.

Idlescan is the ultimate stealth scan. Nmap offers decoy scanning (`-D`) to help users shield their identity, but that (unlike Idle scan) still requires an attacker to send some packets to the target from his real IP address to get scan results back. One upshot of Idle scan is that intrusion detection systems will generally send alerts claiming that the zombie machine has launched a scan against them. So it can be used to frame some other party for a scan. Keep this possibility in mind when reading alerts from your IDS.

A unique advantage of Idle scan is that it can be used to defeat certain packet filtering firewalls and routers. IP source address filtering is a common (though weak) security mechanism for limiting machines that may connect to a sensitive host or network. For example, a company database server might only allow connections from the public web server which accesses it. Or a home user might only allow ssh (interactive login) connections from his work

machines.

A more disturbing scenario occurs when some company bigwig demands that network administrators open a firewall hole so he can access internal network resources from his home IP address. This can happen when executives are unwilling or unable to use secure VPN alternatives.

Idle scanning can sometimes be used to map out these trust relationships. The key factor is that Idlescan results list open ports from the zombie host's perspective. A normal scan against the aforementioned database server might show no ports open, but performing an Idle scan while using the web server's IP as the zombie could expose the trust relationship by showing the database-related service ports open.

Mapping out these trust relationships can be very useful to attackers for prioritizing targets. The web server discussed above may seem mundane to an attacker until she notices its special database access.

A disadvantage to Idle scanning is that it takes far longer than most other scan types. Despite the optimized algorithms described in Section 5.10.3, A 15-second SYN scan could take 15 minutes or more as an Idle scan. Another issue is that you must be able to spoof packets as if they are coming from the zombie and have them reach the target machine. Many ISPs (particularly dialup and residential broadband providers) now implement egress filtering to prevent this sort of packet spoofing. Higher end providers (such as colocation and T1 service) are much less likely to do this. If this filtering is in effect, Nmap will print a quick error message for every zombie you try. If changing ISPs is not an option, you might try using another IP on the same ISP network. Sometimes the filtering only blocks spoofing of IP addresses that are *outside* the range used by customers. Another challenge with idle scan is that you must find a working zombie host, as described in the next section.

### 5.10.1. Finding a working idle scan zombie host

The first step in executing an IPID Idle scan is to find an appropriate zombie. It needs to assign IPID packets incrementally on a global (rather than per-host it communicates with) basis. It should be idle (hence the scan name), as extraneous traffic will bump up its IPID sequence, confusing the scan logic. The lower the latency between the attacker and the zombie, and between the zombie and the target, the faster the scan will proceed.

When an Idle scan is attempted, Nmap tests the proposed Zombie and reports any problems with it. If one doesn't work, try another. Enough Internet hosts are vulnerable that zombie candidates aren't hard to find. Since the hosts need to be idle, choosing a well-known host such as [www.yahoo.com](http://www.yahoo.com) or [google.com](http://google.com) will almost never work.

A common approach is to simply execute a Nmap ping scan of some network. You could use Nmap's random IP selection mode (`-iR`), but that is likely to result in far away zombies with substantial latency. Choosing a network near your source address, or near the target, should produce better results. You can try an Idle scan using each available host from the ping scan results until you find one that works. As usual, it is best to ask permission before using someone's machines for unexpected purposes such as idle scanning.

Performing a port scan and OS identification (`-O`) on the zombie candidate network rather than just a ping scan helps in selecting a good zombie. As long as verbose mode (`-v`) is enabled, OS detection will usually determine the IPID sequence generation method and print a line such as "IPID Sequence Generation: Incremental". If the type is given as Incremental or Broken little-endian incremental, the machine is a good zombie candidate. That is still no guarantee that it will work, as Solaris and some other systems create a new IPID sequence for each host they communicate with. The host could also be too busy. OS detection and the open port list can also help in identifying systems that are likely to be idle.

While identifying a suitable zombie takes some initial work, you can keep re-using the good ones.

### 5.10.2. Executing an Idle scan

Once a suitable zombie has been found, performing a scan is easy. Simply specify the zombie hostname to the `-sI` option and Nmap does the rest. Example 5-18 shows an example of Ereet scanning the Recording Industry Association of America by bouncing an Idle scan off an Adobe machine named Kiosk.

#### Example 5-18. An Idle scan against the RIAA

```
# nmap -P0 -p- -sI kiosk.adobe.com www.riaa.com

Starting nmap V. 3.10ALPHA3 ( www.insecure.org/nmap/ )
Idlescan using zombie kiosk.adobe.com (192.150.13.111:80); Class: Incremental
Interesting ports on 208.225.90.120:
(The 65522 ports scanned but not shown below are in state: closed)
Port      State       Service
21/tcp    open        ftp
25/tcp    open        smtp
80/tcp    open        http
111/tcp   open        sunrpc
135/tcp   open        loc-srv
443/tcp   open        https
1027/tcp  open        IIS
1030/tcp  open        iad1
2306/tcp  open        unknown
5631/tcp  open        pcanywheredata
7937/tcp  open        unknown
7938/tcp  open        unknown
36890/tcp open        unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 2594.472 seconds
```

From the scan above, we learn that the RIAA is not very security conscious (note the open PC Anywhere, portmapper, and Legato nsexec ports). Since they apparently have no firewall, it is unlikely that they have an IDS. But if they do, it will show kiosk.adobe.com as the scan culprit. The `-P0` option prevents Nmap from sending an initial ping packet to the RIAA machine. That would have disclosed Ereet's true address. The scan took a long time because `-p-` was specified to scan all 65K ports. Don't try to use kiosk for your scans, as it has already been removed.

By default, Nmap forges probes to the target from the source port 80 of the zombie. You can choose a different port by appending a colon and port number to the zombie name (e.g. `-sI kiosk.adobe.com:113`). The chosen port must not be filtered from the attacker or the target. A SYN scan of the zombie should show the port in the open or closed state.

### 5.10.3. Idle scan implementation algorithms

While Figure 5-6 describes Idle scan at the fundamental level, the Nmap implementation is far more complex. Key differences are parallelism for quick execution and redundancy to reduce false positives.

Parallelizing idle scan is trickier than with other scan techniques due to indirect method of deducing port states. If Nmap sends probes to many ports on the target and then checks the new IPID value of the zombie, the number of IPID increments will expose how many target ports are open, but not which ones. This isn't actually a major

problem, as the vast majority of ports in a large scan will be `closed|filtered`. Since only open ports cause the IPID value to increment, Nmap will see no intervening increments and can mark the whole group of ports as `closed|filtered`. Nmap can scan groups of up to 100 ports in parallel. If Nmap probes a group then finds that the zombie IPID has increased  $N$  times, there must be  $N$  open ports among that group. Nmap then finds the open ports with a binary search. It splits the group into two and separately sends probes to each. If a subgroup shows zero open ports, that group's ports are all marked `closed|filtered`. If a subgroup shows one or more open ports, it is divided again and the process continues until those ports are identified. While this technique adds complexity, it can reduce scan times by an order of magnitude over scanning just one port at a time.

Reliability is another major idle scanning concern. If the zombie host sends packets to any unrelated machines during the scan, its IPID increments. This causes Nmap to think it has found an open port. Fortunately, parallel scanning helps here too. If Nmap scans 100 ports in a group and the IPID increase signals two open ports, Nmap splits the group into two fifty-port subgroups. When Nmap does an IPID scan on both subgroups, the total zombie IPID increase better be two again! Otherwise, Nmap will detect the inconsistency and rescan the groups. It also modifies group size and scan timing based on the detected reliability rate of the zombie. If Nmap detects too many inconsistent results, it will quit and ask the user to provide a better zombie.

Sometimes a packet trace is the best way to understand complex algorithms and techniques such as these. Once again, the Nmap `--packet_trace` makes these trivial to produce when desired. Example 5-19 provides an annotated packet trace of an actual seven port idle scan. The IP addresses have been changed to Attacker, Zombie, and Target (as in Figure 5-6) and some irrelevant aspects of the trace lines (such as TCP window size) have been removed for clarity.

#### **Example 5-19. IPID scan packet trace**

```
Attacker# nmap -sI Zombie -P0 -p20-25,110 -r --packet_trace -v Target
```

*-P0 is necessary for stealth, otherwise ping packets would be sent to the target from Attacker's real address. Version scanning would also expose the true address, and so -sV is not specified. -r (turns off port randomization) is only used to make this example easier to follow.*

```
Starting nmap 3.78 ( http://www.insecure.org/nmap/ )
```

*Nmap firsts tests the Zombie IPID sequence generation by sending 6 SYN/ACK to it and analyzing the responses. This helps Nmap immediately weed out bad zombies. It is also necessary because some systems (usually Microsoft Windows machines, though not all Windows boxes do this) increment the IPID by 256 for each packet sent rather than by one. This happens on little-endian machines when they don't convert the IPID to network byte order (big-endian). Nmap uses these initial probes to detect and work around this problem.*

```
SENT (0.0060s) TCP Attacker:51824 > Zombie:80 SA id=35996
SENT (0.0900s) TCP Attacker:51825 > Zombie:80 SA id=25914
SENT (0.1800s) TCP Attacker:51826 > Zombie:80 SA id=39591
RCVD (0.1550s) TCP Zombie:80 > Attacker:51824 R id=15669
SENT (0.2700s) TCP Attacker:51827 > Zombie:80 SA id=43604
RCVD (0.2380s) TCP Zombie:80 > Attacker:51825 R id=15670
SENT (0.3600s) TCP Attacker:51828 > Zombie:80 SA id=34186
```

```
RCVD (0.3280s) TCP Zombie:80 > Attacker:51826 R id=15671
SENT (0.4510s) TCP Attacker:51829 > Zombie:80 SA id=27949
RCVD (0.4190s) TCP Zombie:80 > Attacker:51827 R id=15672
RCVD (0.5090s) TCP Zombie:80 > Attacker:51828 R id=15673
RCVD (0.5990s) TCP Zombie:80 > Attacker:51829 R id=15674
Idlescan using zombie Zombie (Zombie:80); Class: Incremental
```

*For this next test, Nmap spoofs four packets to Zombie as if they are coming from Target. Then it probes the zombie to insure that the IPID increased. If it hasn't, then it is likely that either the attacker's ISP is blocking the spoofed packets or the zombie uses a separate IPID sequence counter for each host it communicates with. Both are common occurrences, so Nmap always performs this test. The last-known Zombie IPID was 15674, as shown above.*

```
SENT (0.5990s) TCP Target:51823 > Zombie:80 SA id=1390
SENT (0.6510s) TCP Target:51823 > Zombie:80 SA id=24025
SENT (0.7110s) TCP Target:51823 > Zombie:80 SA id=15046
SENT (0.7710s) TCP Target:51823 > Zombie:80 SA id=48658
SENT (1.0800s) TCP Attacker:51987 > Zombie:80 SA id=27659
RCVD (1.2290s) TCP Zombie:80 > Attacker:51987 R id=15679
```

*The four spoofed packets coupled with the probe from Attacker caused the Zombie to increase its IPID from 15674 to 15679. Perfect! Now the real scanning begins. Remember that 15679 is the latest Zombie IPID.*

```
Initiating Idlescan against Target
SENT (1.2290s) TCP Zombie:80 > Target:20 S id=13200
SENT (1.2290s) TCP Zombie:80 > Target:21 S id=3737
SENT (1.2290s) TCP Zombie:80 > Target:22 S id=65290
SENT (1.2290s) TCP Zombie:80 > Target:23 S id=10516
SENT (1.4610s) TCP Attacker:52050 > Zombie:80 SA id=33202
RCVD (1.6090s) TCP Zombie:80 > Attacker:52050 R id=15680
```

*Nmap probes ports 20-23. Then it probes Zombie and finds that the new IPID is 15680, only one higher than the previous value of 15679. There were no IPID increments in between those two known packets, meaning ports 20-23 are probably closed/filtered. It is also possible that a SYN/ACK from a Target port has simply not arrived yet. In that case, Zombie has not responded with a RST and thus its IPID has not incremented. To ensure accuracy, Nmap will try these ports again later.*

```
SENT (1.8510s) TCP Attacker:51986 > Zombie:80 SA id=49278
RCVD (1.9990s) TCP Zombie:80 > Attacker:51986 R id=15681
```

*Nmap probes again because four tenths of a second has gone by since the last probe it sent. The Zombie (if not truly idle) could have communicated with other hosts during this period, which would screw up later results if not detected here. Fortunately, that has not happened: the next IPID is 15681 as expected.*

```

SENT (2.0000s) TCP Zombie:80 > Target:24 S id=23928
SENT (2.0000s) TCP Zombie:80 > Target:25 S id=50425
SENT (2.0000s) TCP Zombie:80 > Target:110 S id=14207
SENT (2.2300s) TCP Attacker:52026 > Zombie:80 SA id=26941
RCVD (2.3800s) TCP Zombie:80 > Attacker:52026 R id=15684

```

*Nmap probes ports 24, 25, and 110 then queries the Zombie IPID. It has jumped from 15681 to 15684. It skipped 15682 and 15683, meaning that two of those three ports are likely open. Nmap cannot tell which two are open, and it could also be a false positive. So Nmap drills down deeper, dividing the scan into subgroups.*

```

SENT (2.6210s) TCP Attacker:51867 > Zombie:80 SA id=18869
RCVD (2.7690s) TCP Zombie:80 > Attacker:51867 R id=15685
SENT (2.7690s) TCP Zombie:80 > Target:24 S id=30023
SENT (2.7690s) TCP Zombie:80 > Target:25 S id=47253
SENT (3.0000s) TCP Attacker:51979 > Zombie:80 SA id=12077
RCVD (3.1480s) TCP Zombie:80 > Attacker:51979 R id=15687

```

*The first subgroup is ports 24 and 25. The IPID jumps from 15685 to 15687, meaning that one of these two ports is most likely open. Nmap tries the divide and conquer approach again, probing each port separately.*

```

SENT (3.3910s) TCP Attacker:51826 > Zombie:80 SA id=32515
RCVD (3.5390s) TCP Zombie:80 > Attacker:51826 R id=15688
SENT (3.5390s) TCP Zombie:80 > Target:24 S id=47868
SENT (3.7710s) TCP Attacker:52012 > Zombie:80 SA id=14042
RCVD (3.9190s) TCP Zombie:80 > Attacker:52012 R id=15689

```

*A port 24 probe shows no jump in the IPID. So that port is closed. From the results so far, Nmap has tentatively determined:*

- 1) Ports 20-23 are closed/filtered
- 2) Two of the ports 24, 25, and 110 are open
- 3) One of the ports 24 and 25 are open
- 4) Port 24 is closed/filtered

*Stare at this puzzle long enough and you'll find only one solution: ports 25 and 110 are open while the other five are closed/filtered. Using this logic, Nmap could cease scanning and print results now. It used to do so, but that produced too many false positive open ports when the Zombie wasn't truly idle. So Nmap continues scanning to verify its results*

```

SENT (4.1600s) TCP Attacker:51858 > Zombie:80 SA id=6225
RCVD (4.3080s) TCP Zombie:80 > Attacker:51858 R id=15690
SENT (4.3080s) TCP Zombie:80 > Target:25 S id=35713
SENT (4.5410s) TCP Attacker:51856 > Zombie:80 SA id=28118
RCVD (4.6890s) TCP Zombie:80 > Attacker:51856 R id=15692
Discovered open port 25/tcp on Target
SENT (4.6900s) TCP Zombie:80 > Target:110 S id=9943
SENT (4.9210s) TCP Attacker:51836 > Zombie:80 SA id=62254

```

```
RCVD (5.0690s) TCP Zombie:80 > Attacker:51836 R id=15694
Discovered open port 110/tcp on Target
```

*Probes of ports 25 and 110 show that they are open, as we deduced previously.*

```
SENT (5.0690s) TCP Zombie:80 > Target:20 S id=8168
SENT (5.0690s) TCP Zombie:80 > Target:21 S id=36717
SENT (5.0690s) TCP Zombie:80 > Target:22 S id=4063
SENT (5.0690s) TCP Zombie:80 > Target:23 S id=54771
SENT (5.3200s) TCP Attacker:51962 > Zombie:80 SA id=38763
RCVD (5.4690s) TCP Zombie:80 > Attacker:51962 R id=15695
SENT (5.7910s) TCP Attacker:51887 > Zombie:80 SA id=61034
RCVD (5.9390s) TCP Zombie:80 > Attacker:51887 R id=15696
```

*Just to be sure, Nmap tries ports 20-23 again. A Zombie IPID query shows no sequence jump. On the off chance that a SYN/ACK from Target to Zombie came in late, Nmap tries another IPID query. This again shows no open ports. Nmap is now sufficiently confident with its results to print them.*

The Idlescan took 5 seconds to scan 7 ports.

Interesting ports on Target:

PORt	STATE	SERVICE
20/tcp	closed filtered	ftp-data
21/tcp	closed filtered	ftp
22/tcp	closed filtered	ssh
23/tcp	closed filtered	telnet
24/tcp	closed filtered	priv-mail
25/tcp	open	smtp
110/tcp	open	pop3

```
Nmap run completed -- 1 IP address (1 host up) scanned in 5.949 seconds
```

For complete details on the Nmap idle scan implementation, read `idle_scan.cc` from the Nmap source code distribution.

While port scanning is a clever abuse of predictable IPID sequences, they can be exploited for many other purposes as well. Examples are peppered throughout this book, particularly in Chapter 9.

## 5.11. IP Protocol Scan

IP Protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by target machines. This isn't technically a port scan, since it cycles through IP protocol numbers rather than TCP or UDP port numbers. Yet it still uses the `-p` option to select scanned protocol numbers, reports its results within the normal port table format, and even uses the same underlying scan engine as the true port scanning methods. So it is close enough to a port scan that it belongs here.

Besides being useful in its own right, protocol scan demonstrates the power of open source software. While the fundamental idea is pretty simple, I had not thought to add it nor received any requests for such functionality. Then in the summer of 2000, Gerhard Rieger conceived the idea, wrote an excellent patch implementing it, and sent it to the

nmap-hackers mailing list. I incorporated that patch into the Nmap tree and released a new version the next day. Few pieces of commercial software have users enthusiastic enough to design and contribute their own improvements!

Protocol scan works in a similar fashion to UDP scan. Instead of iterating through the port number field of a UDP packet, it sends IP packet headers and iterates through the 8-bit IP protocol field. The headers are usually empty, containing no data and not even the proper header for the claimed protocol. The three exceptions are TCP, UDP, and ICMP. A proper protocol header for those is included since some systems won't send them otherwise and because Nmap already has functions to create them. Instead of watching for ICMP port unreachable messages, protocol scan is on the lookout for ICMP *protocol* unreachable messages. Table 5-8 shows how responses to the IP probes are mapped to port states.

**Table 5-8. How Nmap interprets responses to an IP protocol probe**

Probe Response	Assigned State
Any response in any protocol from target host	open (for protocol used by response, not necessarily probe protocol)
ICMP protocol unreachable error (type 3, code 2)	closed
Other ICMP unreachable errors (type 3, code 1, 3, 9, 10, or 13)	filtered (though they prove ICMP is open if sent from the target machine)
No response received	open filtered (if probe retransmissions also fail to elicit responses)

Like open ports in the TCP or UDP protocols, every open protocol is a potential exploitation vector. In addition, protocol scan results help determine the purpose of a machine and what sort of packet filtering is in place. End hosts usually have little more than icmp, tcp, udp, and (sometimes) igmp open, while routers often offer much more, including routing-related protocols such as GRE and EGP. Firewalls and VPN gateways may show encryption-related protocols such as IPSec and SWIPE.

Like the ICMP port unreachable messages received during a UDP scan, ICMP protocol unreachable messages are often rate limited. For example, no more than one ICMP destination unreachable response is sent per second from a default Linux 2.4.20 box. Since there are only 256 possible protocol numbers, this is less of a problem than with a 65,536-port UDP scan. The suggestions in Section 5.4.2 apply to speeding up IP protocol scans as well.

Protocol scan is used the same way as most other scan techniques. Just specify `-sO` in addition to whatever general Nmap options please you. The normal port (`-p`) option is used to select protocol numbers. Or you can use `-F` to scan all protocols listed in the `nmap-protocols` database. By default, Nmap scans all 256 possible values. Example 5-20 shows Ereet scanning a router in Poland followed by a typical Linux box on my local network.

#### **Example 5-20. IP protocol scan of a router and a typical Linux 2.4 box**

```
# nmap -sO 62.233.173.90 para

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting protocols on ntwklan-62-233-173-90.devs.futuro.pl (62.233.173.90):
(The 240 protocols scanned but not shown below are in state: closed)
PROTOCOL STATE          SERVICE
1      open              icmp
4      open|filtered     ip
6      open              tcp
8      open|filtered     egp
```

```

9      open|filtered  igrp
17     filtered      udp
47     open|filtered gre
53     filtered      swipe
54     open|filtered narp
55     filtered      mobile
77     filtered      sun-nd
80     open|filtered iso-ip
88     open|filtered eigrp
89     open|filtered ospfigrp
94     open|filtered ipip
103    filtered      pim

Interesting protocols on para (192.168.10.191):
(The 252 protocols scanned but not shown below are in state: closed)
PROTOCOL STATE           SERVICE
1      open            icmp
2      open|filtered igmp
6      open            tcp
17     filtered       udp
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap run completed -- 2 IP addresses (2 hosts up) scanned in 458.040 seconds

```

## 5.12. TCP FTP Bounce Scan

An interesting feature of the FTP protocol (RFC 959 (<http://www.rfc-editor.org/rfc/rfc959.txt>)) is support for so-called proxy ftp connections. This allows a user to connect to one FTP server, then ask that files be sent to a third-party server. Such a feature is ripe for abuse on many levels, so most servers have ceased supporting it. One of the abuses this feature allows is causing the FTP server to port scan other hosts. Simply ask the FTP server to send a file to each interesting port of a target host in turn. The error message will describe whether the port is open or not. This is a good way to bypass firewalls because organizational FTP servers are often behind firewalls where they have more access than any old Internet host would. Nmap supports ftp bounce scan with the `-b` option. It takes an argument of the form `username:password@server:port`. *Server* is the name or IP address of a vulnerable FTP server. As with a normal URL, you may omit `username:password`, in which case anonymous login credentials (`user: anonymous password:-wwwuser@`) are used. The port number (and preceding colon) may be omitted as well, in which case the default FTP port (21) on *server* is used.

In Example 5-21, I attempt to bounce off the main Microsoft FTP server to scan Google.

### Example 5-21. Attempting an FTP bounce scan

```
# nmap -P0 -b ftp.microsoft.com google.com

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Your ftp bounce server doesn't allow privileged ports, skipping them.
Your ftp bounce server sucks, it won't let us feed bogus ports!
```

Frequent users of the FTP bounce scan better get used to that error message. This vulnerability was widespread in 1997 when Nmap was released, but has largely been fixed. Vulnerable servers are still around, so it is worth trying

when all else fails. If bypassing a firewall is your goal, scan the target network for open port 21 (or even for any ftp services if you scan all ports with version detection), then try a bounce scan using each. Nmap will tell you whether the host is vulnerable or not. If you are just trying to cover your tracks, you don't need to (and, in fact, shouldn't) limit yourself to hosts on the target network. Before you go scanning random Internet addresses for vulnerable FTP servers, consider that sysadmins may not appreciate you abusing their servers in this way.

Example 5-22 shows a successful bounce scan against a few interesting ports on Scanme. The verbose option (-v) was given to provide extra detail. The given server type of "JD FTP Server" means that this is an HP JetDirect print server.

### Example 5-22. Successful FTP bounce scan

```
krad~> nmap -p 22,25,135 -P0 -v -b XXX.YY.111.2 scanme.nmap.org

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Attempting connection to ftp://anonymous:-wwwuser@XXX.YY.111.2:21
Connected:220 JD FTP Server Ready
Login credentials accepted by ftp server!
Initiating TCP ftp bounce scan against scanme.nmap.org (205.217.153.55)
Adding open port 22/tcp
Adding open port 25/tcp
Scanned 3 ports in 12 seconds via the Bounce scan.
Interesting ports on scanme.nmap.org (205.217.153.55):
PORT      STATE      SERVICE
22/tcp    open       ssh
25/tcp    open       smtp
135/tcp   filtered  msrpc

Nmap run completed -- 1 IP address (1 host up) scanned in 21.790 seconds
```

## 5.13. Scan Code and Algorithms

In 2004, Nmap's primary port scanning engine was rewritten for greater performance and accuracy. The new engine, known as `ultra_scan` after its function name, handles SYN, Connect, UDP, Null, FIN, Xmas, ACK, Window, Maimon, and IP Protocol scans. That leaves only Idle scan and FTP bounce scan using their own engines.

While the diagrams throughout this chapter show how each scan type works, the Nmap implementation is far more complex since it has to worry about port and host parallelization, latency estimation, packet loss detection, timing profiles, abnormal network conditions, packet filters, response rate limits, and much more.

This section doesn't provide every low-level detail of the `ultra_scan` engine. If you are inquisitive enough to want that, you are better off getting it from the source. You can find `ultra_scan()` and its high-level helper functions defined in `scan_engine.cc` from the Nmap tarball. Here I cover the most important algorithmic features. Understanding these helps in optimizing your scans for better performance, as described in Chapter 6.

### 5.13.1. Network condition monitoring

Some authors brag that their scanners are faster than Nmap because of stateless operation. They simply blast out a flood packets then listen for responses and hope for the best. While this may have value for quick surveys and other cases where speed is more important than comprehensiveness and accuracy, I don't find it appropriate for security

scanning. A stateless scanner cannot detect dropped packets in order to retransmit and throttle its send rate. If a busy router half way along the network path drops 80% of the scanner's packet flood, the scanner will still consider the run successful and print results that are woefully incomplete. Nmap, on the other hand, saves extensive state in RAM while it runs. There is usually plenty of memory available, even on a PDA. Nmap marks each probe with sequence numbers, source or destination ports, ID fields, or other aspects (depending on probe type) which allow it to recognize responses (and thus drops). It then adjusts its speed appropriately to stay as fast as the network (and given command-line options) allow without crossing the line and suffering inaccuracy or unfairly hogging the shared network. Some administrators who have not installed an IDS might not notice an Nmap SYN scan of their whole network. But you better believe the admin will investigate if you use a brute packet flooding scanner that affects his Quake ping time!

### **5.13.2. Host and port parallelization**

Most of the diagrams in this chapter illustrate using a technique to determine the state of a single port. Sending a probe and receiving the response requires a round trip time (rtt) between the source and target machines. If your rtt is 200ms and you are scanning 65,536 ports on a machine, handling them serially would take at least 3.6 hours. Scan a network of 20,000 machines that way and the wait balloons to more than 8 years. Clearly, this is unacceptable. So Nmap parallelizes its scans, and is capable of scanning hundreds of ports on each of dozens of machines at the same time. This improves speeds by several orders of magnitude. The number of hosts and ports it scans at a time is dependent on arguments described in Chapter 6, such as `--min_hostgroup`, `--min_parallelism`, `-T4`, and `--max_rtt_timeout`, among many others. It also depends on network conditions detected by Nmap.

When scanning multiple machines, Nmap tries to efficiently spread the load between them. If a machine appears overwhelmed (drops packets or its latency increases), Nmap slows down for that host while continuing against others at full speed.

### **5.13.3. Round trip time estimation**

Every time a probe response is received, Nmap calculates the microseconds elapsed since the probe was sent. We'll call this the instanceRTT, and Nmap uses it to keep a running tally of three crucial timing-related values: srtt, rttvar, and timeout. Nmap keeps separate values for each host and also merged values for a whole group of hosts scanned in parallel. They are calculated as follows:

srtt

The smoothed average round trip time. This is what Nmap uses as its most accurate rtt guess. Rather than use a true arithmetic mean, the formula favors more recent results because network conditions change frequently. The formula is:  $\text{newsrtt} = \text{oldsrtt} + (\text{instanceRTT} - \text{oldsrtt}) / 8$

rttvar

This is the observed variance or deviation in the round trip time. The idea is that if rtt values are quite consistent, Nmap can give up shortly after waiting the srtt. If the variance is quite high, Nmap must wait much longer than the srtt before giving up on a probe because relatively slow responses are common. The formula is:  $\text{newrttvar} = \text{AbsoluteValue}(\text{instanceRTT} - \text{oldsrtt}) - \text{oldrttvar}$

timeout

This is the amount of time Nmap is willing to wait before giving up on a probe. It is calculated as: timeout = newsrtt + newrttvar \* 4

When a probe times out, Nmap may retransmit the probe or assign a port state such as `filtered` (depending on scan type). Nmap keeps some state information even after a timeout just in case a late response arrives while the overall scan is still in progress.

\* What does O'Reilly want to do with these formulas? Keep ghetto ASCII or display them nicely? MathML?

These simple time estimation formulas seem to work quite well. I did not make them up, but found them in networking literature. TCP implementations use very similar techniques, as discussed in RFC2988 -- Computing TCP's Retransmission Timer (<http://www.rfc-editor.org/rfc/rfc2988.txt>).

#### 5.13.4. Congestion control

Retransmission timers are far from the only technique Nmap gleaned from TCP. Since Nmap is most commonly used with TCP, it is only fair to follow many of the same rules. Particularly since those rules are the result of substantial research into maximizing throughput without degrading into a tragedy of the commons where everyone selfishly hogs the Network. With its default options, Nmap is reasonably polite. Three reasons are the congestion window, exponential backoff, and slow start algorithms. The congestion window controls how many probes Nmap may have outstanding at once. If the window is full, Nmap won't send any more until a response is received or a probe times out. Exponential backoff means that Nmap slows itself down dramatically when it detects dropped packets. The congestion window is usually reduced to one whenever drops are detected. Slow start is an algorithm for gradually increasing the scan speed to determine the performance limits of the network.

All of these techniques are described in RFC 2581 -- TCP Congestion Control (<http://www.rfc-editor.org/rfc/rfc2581.txt>). That document was written by networking gurus Richard Stevens, Vern Paxson, and Mark Almman. It is only 10 pages long and anyone interested in implementing efficient TCP stacks (or other network protocols, or port scanners) should find it fascinating.

#### 5.13.5. Port scan pings

Every technique discussed in this algorithms section involves (at some level) network monitoring to detect and estimate network packet loss and latency. That really is critical to obtaining fast scan times. Unfortunately, good data is often difficult to come by when scanning heavily firewalled systems. These filters often drop the overwhelming majority of packets without any response. Nmap may have to send 20,000 probes or more to find one responsive port, making it difficult to monitor network conditions.

To combat this problem, Nmap 3.70 introduced the idea of port scan pings. If Nmap has found at least one port responsive on a heavily filtered host, it will send a probe to that port every five seconds that it goes without receiving responses from any other ports. This allows Nmap to conduct a sufficient level of monitoring to speed up or slow down its scans as network conditions allow.

### **5.13.6. Inferred neighbor times**

Sometimes even port scan pings won't help because no responsive ports at all have been found. The machine could be down (and scanned with `-P0`), or every single port could be filtered. Or perhaps the target does have a couple responsive ports, but Nmap has not been lucky enough to find them yet. In these cases, Nmap uses timing values that it maintains for the whole group of machines it is scanning at the same time. As long as at least one response has been received from any machine in the group, Nmap has something to work with. Of course Nmap cannot assume that hosts in a group always share similar timing characteristics. So Nmap tracks the timing variances between responsive hosts in a group. If they differ wildly, Nmap infers long timeouts for neighboring hosts to be on the safe side.

### **5.13.7. Adaptive retransmission**

The simplest of scanners (and the stateless ones) generally don't retransmit probes at all. They simply send a probe to each port and report based on the response or lack thereof. Slightly more complex scanners will retransmit a set number of times. Nmap tries to be smarter by keeping careful packet loss statistics for each scan against a target. If no packet loss is detect, Nmap may retransmit only once when it fails to receive a probe response. When massive packet loss is evident, Nmap may retransmit ten or more times. This allows Nmap to scan hosts on fast, reliable networks quickly, while preserving accuracy (at the expense of some speed) when scanning problematic networks or machines. Even Nmap's patience isn't unlimited though. At a certain point (twelve retransmissions with Nmap 3.75), Nmap will print a warning and give up on further retransmissions. This prevents malicious hosts from slowing Nmap down too much with intentional packet drops, slow responses, and similar responses. Such an attack is known as tarpitting and is commonly used against spammers.

### **5.13.8. Scan delay**

Packet response rate limiting is perhaps the most pernicious problem faced by port scanners such as Nmap. For example, Linux 2.4 kernels limit ICMP error messages returned during a UDP (`-sU`) or IP protocol (`-sO`) scan to one per second. If Nmap counted these as normal drops, it would be continually slowing down (remember exponential backoff) but still end up having the vast majority of its probes dropped. Instead, Nmap tries to detect this situation. When a large proportion of packets are being dropped, it implements a short delay (as little as 5 milliseconds) between each probe sent to a single target. If drops continue to be a major problem, Nmap will keep doubling the delay until the drops cease or Nmap hits the maximum allowed scan delay. The maximum scan delay defaults to one second between probes. The scan delay is sometimes enabled when a slow host can't keep up, even when that host has no explicit rate limiting rules. This can reduce total network traffic substantially by reducing wasted (dropped) probe packets. Unfortunately even small scan delay values can make a scan takes several times as long. Nmap is conservative by default, allowing second-long scan delays for TCP and UDP probes. If your priorities differ, you can configure maximum scan delays as discussed in Chapter 5.

## **Chapter 6. Optimizing Nmap Performance**

# Chapter 7. Service and Application Version Detection

## 7.1. Introduction

Previous chapters discussed many techniques for port scanning -- determining the TCP or UDP port numbers that are listening for connections on a system. Point Nmap at a remote machine, and it might tell you that ports 25/tcp, 80/tcp, and 53/udp are open. Using its nmap-services database of more than 2,200 well-known services, Nmap would report that those ports probably correspond to a mail server (SMTP), web server (HTTP), and name server (DNS) respectively. This lookup is usually accurate -- the vast majority of daemons listening on TCP port 25 are, in fact, mail servers. However, you should not bet your security on this! People can and do run services on strange ports. Perhaps their main web server was already on port 80, so they picked a different port for a staging or test server. Maybe they think hiding a vulnerable service on some obscure port prevents "evil hackers" from finding it. Even more common lately is that people choose ports based not on the service they want to run, but on what gets through the firewall. When ISPs blocked port 80 after major Microsoft IIS worms CodeRed and Nimda, hordes of users responded by moving their personal web servers to another port. When companies block telnet access due to its horrific security risks, I have seen users simply run telnetd on the Secure Shell (SSH) port instead.

Even if Nmap is right, and the hypothetical server above is running SMTP, HTTP, and DNS servers, that is not a lot of information. When doing vulnerability assessments (or even simple network inventories) of your companies or clients, you really want to know which mail and DNS servers and versions are running. Having an accurate version number helps dramatically in determining which exploits a server is vulnerable to. Do keep in mind that security fixes are often backported to earlier versions of software, so you cannot rely solely on the version number to prove a service is vulnerable.

Another good reason for determining the service types and version numbers is that many services share the same port number. For example, port 258/tcp is used by both the Checkpoint Firewall-1 GUI management interface and the yak Windows chat client. This makes a guess based on the nmap-services table even less accurate. Anyone who has done much scanning knows that you also often find services listening on unregistered ports - these are a complete mystery without version detection. A final problem is that filtered UDP ports often look the same to a simple port scanner as open ports (see Chapter 3 - Mainstream Port Scanning Techniques). But if they respond to the service-specific probes sent by Nmap version detection, you know for sure that they are open (and often exactly what is running).

The Nmap version scanning subsystem (introduced in version 3.45) tries to answer all these questions by connecting to open ports and interrogating them for further information using probes that the specific services understand. This allows Nmap to give a detailed assessment of what is really running, rather than just what port numbers are open. Example 7-1 shows the actual output.

### Example 7-1. Simple usage of version detection

```
# nmap -A -T4 -F www.insecure.org

Starting nmap 3.40PVT16 ( http://www.insecure.org/nmap/ )
Interesting ports on www.insecure.org (205.217.153.53):
(The 1206 ports scanned but not shown below are in state: filtered)
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh      OpenSSH 3.1pl1 (protocol 1.99)
```

```

25/tcp  open  smtp    Qmail smptd
53/tcp  open  domain  ISC Bind 9.2.1
80/tcp  open  http    Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)
113/tcp closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 108.307 days (since Wed May 21 12:27:44 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 34.962 seconds

```

Nmap version detection offers the following advanced features (fully described later):

- High speed, parallel operation via non-blocking sockets and a probe/match definition grammar designed for efficient yet powerful implementation.
- Determines the application name and version number where available -- not just the service protocol.
- Supports both the TCP and UDP protocols, as well as both textual ASCII and packed binary services.
- Multi-platform support, including Linux, Windows, Mac OS X, FreeBSD/NetBSD/OpenBSD, Solaris, and all the other platforms on which Nmap is known to work.
- If SSL is detected, Nmap connects using OpenSSL (if available) and tries to determine what service is listening behind the encryption. This allows it to discover services like https, pop3s, imaps, etc. as well as providing version details.
- If a SunRPC service is discovered, Nmap launches its brute-force RPC grinder to find the program number, name, and version number.
- IPv6 is supported, including TCP, UDP, and SSL over TCP.
- Community contributions - If Nmap gets data back from a service that it does not recognize, a "service fingerprint" is printed along with a submission URL. This system is patterned after the extremely successful Nmap OS Detection (Chapter 7) fingerprint submission process. New probes and corrections can also be submitted.
- Comprehensive database - Nmap recognizes more than one thousand service signatures, covering more than 180 unique service protocols from acap, afp, and aim to xml-rpc, zebadee, and zebra.

## 7.2. Usage/Examples

Before delving into the technical details of how version detection is implemented, here are some examples demonstrating its usage and capabilities. To enable version detection, just add `-sv` to whatever Nmap flags you normally use. Or use the `-A` option, which also turns on OS detection (`-O`, Chapter 7) and may enable other advanced and aggressive features later. It is really that simple, as shown in Example 7-2.

### Example 7-2. Version detection against WWW.Microsoft.Com

```

# nmap -A -T4 -F www.microsoft.com

Starting nmap 3.40PVT16 ( http://www.insecure.org/nmap/ )
Interesting ports on 80.67.68.30:
(The 1208 ports scanned but not shown below are in state: closed)

```

```

PORT      STATE     SERVICE      VERSION
22/tcp    open      ssh          Akamai-I SSH (protocol 1.5)
80/tcp    open      http         AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
443/tcp   open      ssl/http    AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
Device type: general purpose
Running: Linux 2.1.X|2.2.X
OS details: Linux 2.1.19 - 2.2.25
Uptime 22.924 days (since Fri Aug 15 03:34:27 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 19.223 seconds

```

This preceding scan demonstrates a couple things. First of all, it is gratifying to see WWW.Microsoft.Com served off one of Akamai's Linux boxes. More relevant to this chapter is that the "service" for port 443 is "ssl/http". That means that service detection first discovered that the port was SSL, then it loaded up OpenSSL and performed service detection again through SSL connections to discover a web server running AkamiGHost behind the encryption. Recall that -T4 causes Nmap to go faster (more aggressive timing) and -F tells Nmap to scan only ports registered in nmap-services.

Example 7-3 is a longer and more diverse example.

### Example 7-3. Complex version detection

```

./nmap -A -T4 localhost

Starting nmap 3.40PVT16 ( http://www.insecure.org/nmap/ )
Interesting ports on felix (127.0.0.1):
(The 1640 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          WU-FTPD wu-2.6.1-20
22/tcp    open  ssh          OpenSSH 3.1pl1 (protocol 1.99)
53/tcp    open  domain       ISC Bind 9.2.1
79/tcp    open  finger       Linux fingerd
111/tcp   open  rpcbind     2 (rpc #100000)
443/tcp   open  ssl/http    Apache httpd 2.0.39 ((Unix) mod_perl/1.99_04-dev [cut])
515/tcp   open  printer      CUPS 1.1
631/tcp   open  ipp          CUPS 1.1
953/tcp   open  rndc?       -
5000/tcp   open  ssl/ftp     WU-FTPD wu-2.6.1-20
5001/tcp   open  ssl/ssh     OpenSSH 3.1pl1 (protocol 1.99)
5002/tcp   open  ssl/domain ISC Bind 9.2.1
5003/tcp   open  ssl/finger  Linux fingerd
6000/tcp   open  X11         (access denied)
8000/tcp   open  http-proxy  Junkbuster webproxy
8080/tcp   open  http        Apache httpd 2.0.39 ((Unix) mod_perl/1.99_04-dev [cut])
8081/tcp   open  http        Apache httpd 2.0.39 ((Unix) mod_perl/1.99_04-dev [cut])
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 8.653 days (since Fri Aug 29 11:16:40 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 42.494 seconds

```

You can see here the way RPC services are treated, with the brute force RPC scanner being used to determine that port 111 is rpcbind version 2. You may also notice that port 515 gives the service as "printer", but that version column is empty. This means that Nmap did determine the service name via its probing, but was not able to determine anything else. On the other hand, port 953 gives the service as "rndc?". The question mark tells us that Nmap was not even able to determine the service name through probing. As a fallback, rndc is mentioned because that has port 953 registered in `nmap-services`. Unfortunately, none of Nmap's probes elicited any sort of response from rndc. If they had, Nmap would have printed a service fingerprint and a submission URL so that it could be recognized in the next version. As it is, Nmap requires a special probe. One might even be available by the time you read this. The upcoming "community contributions" section provides details on writing your own probes.

It is also worth noting that some services provide much more information than just the version number. Examples above include whether X11 permits connections, the SSH protocol number, and the Apache module versions list. Some of the Apache modules even had to be cut from the output to fit on this page.

A few early reviewers questioned the sanity of running services such as SSH and finger over SSL. This was actually just fun with stunnel (<http://www.stunnel.org/>), in part to ensure that parallel SSL scans actually work.

### 7.3. Technique Described

Nmap version scanning is actually rather straightforward. It was designed to be as simple as possible while still being scalable, fast, and accurate. The truly nitty-gritty details are best discovered by downloading and reviewing the source code, but a synopsis of the techniques used follows.

Nmap first does a port scan as per your instructions, and then passes all the open TCP and/or UDP ports to the service scanning module. Those ports are then interrogated in parallel, although a single port is described here for simplicity.

1. If the port is TCP, Nmap starts by connecting to it.
2. Once the TCP connection is made, Nmap listens for roughly 5 seconds. Many common services, including most ftp, ssh, smtp, telnet, pop3, and imap servers, identify themselves in an initial welcome banner. Nmap refers to this as the "NULL probe", because Nmap just listens for responses without sending any probe data. If any data is received, Nmap compares it to hundreds of signature regular expressions in its `nmap-service-probes` file (described in Section 7.6). If the service is fully identified, we are done with that port! The regular expression includes substrings that can be used to pick version numbers out of the response. In some cases, Nmap gets a "soft match" on the service type, but no version info. In that case, Nmap continues but only send probes that are known to recognize the soft-matched service type.
3. At this point, Nmap UDP probes start, and TCP connections end up here if the NULL probe above fails or soft-matches. Since the reality is that most ports are used by the service they are registered to in `nmap-services`, every probe has a list of port numbers that are considered "good bets". For example, the probe called GetRequest that recognizes web servers (among other services) lists 80-85, 8000-8010, and 8080-8085 as probable ports. Nmap sequentially executes the probe(s) that match the port number being scanned. Each probe includes a probe string (which can be arbitrary ASCII text or \xHH escaped binary), which is sent to the port. Responses that come back are compared to a list of regular expressions of the same type as discussed in the NULL probe description above. As with the NULL probe, these tests can either result in a full match (ends processing for the remote service), a soft match (limits future probes to those which match a certain service), or no match at all.
4. In most cases, the "NULL probe" or the probable port probe(s) (there is usually only one) described above matches the service. Since the NULL "probe" shares its connection with the probable port probe, this allows

service detection to be done with only one brief connection in most cases. With UDP only one packet is usually required. But should the NULL probe and probable port probe(s) fail, Nmap goes through all of the existing probes sequentially. In the case of TCP, Nmap must make a new connection for each probe to avoid having previous probes corrupt the results. This worst-case scenario can take a bit of time, although the pain is limited by making most probes generic enough to match many services. For example, the GenericLines probe sends two blank lines ("r\nr\n") to the service. This matches daemons of 13 service types (so far), including ftp, ident, pop3, uucp, postgres, and whois. The GetRequest probe matches even more service types. Other examples include "help\r\n" and generic RPC and MS SMB probes. In addition, any softmatch reduces the number of tried probes dramatically.

5. One of the probes tests whether the target port is running SSL. If so (and if OpenSSL is available), Nmap connects back via SSL and restart the service scan to determine what is listening behind the encryption. A special directive allows different probable ports for normal and SSL tunneled connections. For example, Nmap should start against port 443 (https) with an SSL probe. But after SSL is detected and enabled, Nmap should try the GetRequest probe against port 443 because that port usually has a web server listening behind SSL encryption.
6. Another generic probe identifies RPC-based services. When these are found, the Nmap RPC Grinder (discussed later) is initiated to brute force the RPC program number/name and supported version numbers. Similarly, an SMB postprocessor for fingerprinting Windows services may be added eventually.
7. If at least one of the probes elicits some sort of response, yet Nmap is unable to recognize the service, the response content is printed to the user in the form of a "fingerprint" that can be submitted at a provided URL for the next version of Nmap.

## 7.4. Technique Demonstrated

If the English description above is not clear enough, you can see for yourself how it works by adding the `--version_trace` (and usually `-d` (debugging)) options to your Nmap command line. This shows all the connection and data read/write activity of the service scan. Example 7-4 is a real annotated example (output slightly modified for readability).

### Example 7-4. Detailed trace of version detection

```
# nmap -sSV -T4 -F -d --version_trace www.insecure.org

Starting nmap 3.48 ( http://www.insecure.org/nmap/ )
Host www.insecure.org (205.217.153.53) appears to be up ... good.
Initiating SYN Stealth Scan against www.insecure.org (205.217.153.53) at 19:53
Initiating service scan against 4 services on 1 host at 19:53
```

*The SYN scan has found 4 open ports - now we are beginning a service scan against each of them in parallel. We start with a TCP connection for the NULL probe:*

```
Starting probes against new service: 205.217.153.53:22 (tcp)
NSOCK (2.0750s) TCP connection requested to 205.217.153.53:22 (IOD #1) EID 8
Starting probes against new service: 205.217.153.53:25 (tcp)
NSOCK (2.0770s) TCP connection requested to 205.217.153.53:25 (IOD #2) EID 16
Starting probes against new service: 205.217.153.53:53 (tcp)
NSOCK (2.0830s) TCP connection requested to 205.217.153.53:53 (IOD #3) EID 24
```

```

Starting probes against new service: 205.217.153.53:80 (tcp)
NSOCK (2.0860s) TCP connection requested to 205.217.153.53:80 (IOD #4) EID 32
NSOCK (2.0870s) Callback: CONNECT SUCCESS for EID 32 [205.217.153.53:80]
NSOCK (2.0870s) Read request from IOD #4 [205.217.153.53:80] (timeout: 5000ms) EID 42
NSOCK (2.0870s) Callback: CONNECT SUCCESS for EID 24 [205.217.153.53:53]
NSOCK (2.0870s) Read request from IOD #3 [205.217.153.53:53] (timeout: 5000ms) EID 50
NSOCK (2.0870s) Callback: CONNECT SUCCESS for EID 16 [205.217.153.53:25]
NSOCK (2.0870s) Read request from IOD #2 [205.217.153.53:25] (timeout: 5000ms) EID 58
NSOCK (2.0870s) Callback: CONNECT SUCCESS for EID 8 [205.217.153.53:22]
NSOCK (2.0870s) Read request from IOD #1 [205.217.153.53:22] (timeout: 5000ms) EID 66

```

*At this point, "Null probe" connections have successfully been made to all four services. It starts at 2 seconds because that is how long the ping and SYN scans took.*

```

NSOCK (2.0880s) Callback: READ SUCCESS for EID 66 [205.217.153.53:22] (23 bytes): SSH-1.99-OpenSSH_3
Service scan match: www.insecure.org (205.217.153.53):22 is ssh. Version: |OpenSSH|3.1p1|protocol 1

```

*SSH was nice enough to fully identify itself immediately upon connection as OpenSSH 3.1p1. One down, three to go.*

```

NSOCK (2.0880s) Callback: READ SUCCESS for EID 58 [205.217.153.53:25] (27 bytes): 220 core.lnxnet.ne
Service scan soft match: www.insecure.org (205.217.153.53):25 is smtp

```

*The mail server on port 25 also gave us a useful banner. We do not know what type of mail server it is, but starting with "220 " and including the word "ESMTP" tells us it is a mail (SMTP) server. So Nmap softmatches smtp, meaning that only probes able to match SMTP servers are tried from now on. Note that non-printable characters are represented by dots -- so the ".." after ESMTP is really the "\r\n" line termination sequence.*

```

NSOCK (2.0880s) Read request from IOD #2 [205.217.153.53:25] (timeout: 4996ms) EID 74
NSOCK (7.0880s) Callback: READ TIMEOUT for EID 74 [205.217.153.53:25]
NSOCK (7.0880s) Write request for 6 bytes to IOD #2 EID 83 [205.217.153.53:25]: HELP..
NSOCK (7.0880s) Read request from IOD #2 [205.217.153.53:25] (timeout: 5000ms) EID 90

```

*Nmap listens a little longer on the SMTP connection, just in case the server has more to say. The read request times out after 5 seconds. Nmap then finds the next probe which is registered to port 25 and has smtp signatures. That probe simply consists of "HELP\r\n", which Nmap writes into the connection.*

```

NSOCK (7.0880s) Callback: READ TIMEOUT for EID 50 [205.217.153.53:53]
NSOCK (7.0880s) Write request for 32 bytes to IOD #3 EID 99 [205.217.153.53:53]: ....vers
NSOCK (7.0880s) Read request from IOD #3 [205.217.153.53:53] (timeout: 5000ms) EID 106

```

*The DNS server on port 53 does not return anything at all. The first probe registered to port 53 in nmap-service-probes is DNSVersionBindReq, which queries a DNS server for its version number. This is sent onto the wire.*

```

NSOCK (7.0880s) Callback: READ TIMEOUT for EID 42 [205.217.153.53:80]

```

NSOCK (7.0880s) Write request for 18 bytes to IOD #4 EID 115 [205.217.153.53:80]: GET / HTTP/1.0....  
NSOCK (7.0880s) Read request from IOD #4 [205.217.153.53:80] (timeout: 5000ms) EID 122

The port 80 NULL Probe also failed to return any data. An HTTP GET request is sent, since that probe is registered to port 80.

NSOCK (7.0920s) Callback: READ SUCCESS for EID 122 [205.217.153.53:80] [EOF](15858 bytes)  
Service scan match: www.insecure.org (205.217.153.53):80 is http. Version: |Apache httpd|2.0.39|(Un

*Apache returned a huge (15KB) response, so it is not printed. That response provided detailed configuration information, which Nmap picks out of the response. There are no other probes registered for port 80. So if this had failed, Nmap would have tried the first TCP probe in nmap-service-probes. That probe simply sends blank lines ("r\nr\n"). A new connection would have been made in case the GET probe confused the service.*

NSOCK (7.0920s) Callback: READ SUCCESS for EID 106 [205.217.153.53:53] (50 bytes): .0.....ve  
Service scan match: www.insecure.org (205.217.153.53):53 is domain. Version: |ISC Bind|9.2.1||

*Port 53 responded to our DNS version request. Most of the response (as with the probe) is binary, but you can clearly see the version 9.2.1 there. If this probe had failed, the next probe registered to port 53 is a DNS server status request (14 bytes: "\0\x0C\0\0\x10\0\0\0\0\0\0\0\0\0"). Having this backup probe helps because many more servers respond to a status request than a version number request.*

NSOCK (7.0920s) Callback: READ SUCCESS for EID 90 [205.217.153.53:25] (55 bytes): 214 qmail home pag Service scan match: www.insecure.org (205.217.153.53):25 is smtp. Version: |qmail smtpd|||

Port 25 gives a very helpful response to the "Help" probe. Other SMTP servers such as Postfix, Courier, and Exim can often be identified by this probe as well. If the response did not match, Nmap would have given up on this service because it had already softmatched smtp and there are no more smtp probes in nmap-service-probes.

The service scan took 5 seconds to scan 4 services on 1 host.

*This service scan run went pretty well. No service required more than one connection. It took five seconds because Qmail and Apache hit the 5-second NULL probe timeout before Nmap sent the first real probes. Here is the reward for these efforts:*

```
Interesting ports on www.insecure.org (205.217.153.53):
(The 1212 ports scanned but not shown below are in state: closed)

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.1p1 (protocol 1.99)
25/tcp    open  smtp    qmail smtpd
53/tcp    open  domain  ISC Bind 9.2.1
80/tcp    open  http    Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)
```

Nmap run completed -- 1 IP address (1 host up) scanned in 7.104 seconds

## 7.5. Post-processors

Nmap is usually finished working on a port once it has deduced the service and version information as demonstrated above. However, there are certain services for which Nmap performs additional work. These post-processors are presently available for RPC and SSL services, and Windows SMB interrogation is under consideration.

### 7.5.1. RPC Grinding

SunRPC (Sun Remote Procedure Call) is a common UNIX protocol used to implement many services including NFS. Nmap ships with an `nmap-rpc` database of almost 600 RPC programs. Many RPC services use high-numbered ports and/or the UDP transport protocol, making them available through many poorly configured firewalls. RPC programs (and the infrastructure libraries themselves) also have a long history of serious remotely exploitable security holes. So network admins and security auditors often wish to learn more about any RPC programs on their networks.

If the portmapper (`rpcbind`) service (UDP or TCP port 111) is available, RPC services can be enumerated with the UNIX `rpcinfo` command. Example 7-5 demonstrates this against a default Solaris 9 server.

#### Example 7-5. Enumerating RPC services with `rpcinfo`

```
> rpcinfo -p ultra
   program vers proto   port
    100000    4   tcp    111  rpcbind
    100000    4   udp    111  rpcbind
    100232   10   udp   32777  sadmind
    100083    1   tcp   32775  ttdbserverd
    100221    1   tcp   32777  kcms_server
    100068    5   udp   32778  cmsd
    100229    1   tcp   32779  metad
    100230    1   tcp   32781  metamhd
    100242    1   tcp   32783  rpc.metamedd
    100001    4   udp   32780  rstatd
    100002    3   udp   32782  rusersd
    100002    3   tcp   32785  rusersd
    100008    1   udp   32784  walld
    100012    1   udp   32786  sprayd
    100011    1   udp   32788  rquotad
    100024    1   udp   32790  status
    100024    1   tcp   32787  status
    100133    1   udp   32790  nsm_addrand
    100133    1   tcp   32787  nsm_addrand
[ Dozens of lines cut for brevity ]
```

This example shows that hosts frequently offer many RPC services, which increases the probability that one is exploitable. You should also notice that most of the services are on strange high-numbered ports (which may change for any number of reasons) and split between UDP and TCP transport protocols.

Because the RPC information is so sensitive, many administrators try to obscure this information by blocking the portmapper port (111). Unfortunately, this does not close the hole. Nmap can determine all of the same info by directly communicating with open RPC ports through a 3-step process

1. The TCP and/or UDP port scan finds all of the open ports

2. Version detection determines which of the open ports use the SunRPC protocol
3. The RPC brute force engine determines the program identity of each rpc port by trying a "NULL command" against each of the 600 programs numbers in `nmap-rpc`. Most of the time Nmap guesses wrong and receives an error message stating that the requested program number is not listening on the port. Nmap continues trying each number in its list until success is returned for one of them. Nmap gives up in the unlikely event that it exhausts all of its known program numbers or if the port sends malformed responses that suggest it is not really RPC.

\* Should I provide a diagram showing an actual RPC probe packet and the responses to expect?

The RPC program identification probes are done in parallel, and retransmissions are handled for UDP ports. This feature is automatically activated whenever version detection finds any RPC ports. Or it can be performed without version detection by specifying the `-sR` option. Example 7-6 demonstrates direct RPC scanning done as part of version detection.

#### **Example 7-6. Nmap direct RPC scan**

```
# nmap -F -A -sSU ultra

Starting nmap 3.48 ( http://www.insecure.org/nmap/ )
Interesting ports on ultra.yuma.net (192.168.0.50):
* I should change the domain name of my internal home network to
one I actually own, such as Nmap.Org

(The 2171 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE          VERSION
[A whole bunch of ports cut for brevity]
32776/tcp open  kcms_server      1 (rpc #100221)
32776/udp open  sadmind         10 (rpc #100232)
32777/tcp open  kcms_server      1 (rpc #100221)
32777/udp open  sadmind         10 (rpc #100232)
32778/tcp open  metad           1 (rpc #100229)
32778/udp open  cmsd            2-5 (rpc #100068)
32779/tcp open  metad           1 (rpc #100229)
32779/udp open  rstatd          2-4 (rpc #100001)
32780/tcp open  metamhd         1 (rpc #100230)
32780/udp open  rstatd          2-4 (rpc #100001)
32786/tcp open  status           1 (rpc #100024)
32786/udp open  sprayd          1 (rpc #100012)
32787/tcp open  status           1 (rpc #100024)
32787/udp open  rquotad         1 (rpc #100011)
Device type: general purpose
Running: Sun Solaris 9
OS details: Sun Solaris 9
Uptime 0.120 days (since Sun Nov 16 21:38:16 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 252.701 seconds
```

### 7.5.2. SSL Post-processor notes

As discussed in the technique section, Nmap has the ability to detect the SSL encryption protocol and then launch an encrypted session through which it executes normal version detection. As with the RPC grinder discussed previously, the SSL postprocessor is automatically executed whenever an appropriate (SSL) port is detected. This is demonstrated by Example 7-7.

#### **Example 7-7. Version scanning through SSL**

```
nmap -P0 -sSV -T4 -F www.amazon.com
```

```
Starting nmap 3.48 ( http://www.insecure.org/nmap/ )
Interesting ports on 207-171-184-16.amazon.com (207.171.184.16):
(The 1214 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache Stronghold httpd 2.4.2 (based on Apache 1.3.6)
443/tcp   open  ssl/http  Apache Stronghold httpd 2.4.2 (based on Apache 1.3.6)

Nmap run completed -- 1 IP address (1 host up) scanned in 35.038 seconds
```

Note that the version information is the same for each of the two open ports, but the service is `http` on port 80 and `ssl/http` on port 443. The common case of `https` on port 443 is not hardcoded - Nmap should be able to detect SSL on any port and determine the underlying protocol for any service that Nmap can detect in cleartext. If Nmap had not detected the server listening behind SSL, the service listed would be "ssl/unknown". If Nmap had not been built with SSL support, the service listed would have simply been "ssl". The "version" column would be blank in both of these cases.

The SSL support for Nmap depends on the free OpenSSL library (<http://www.openssl.org>) and has not been tested on Windows. Nor is it included in the Linux RPM binaries, to avoid breaking systems which lack these libraries. The Nmap source code distribution attempts to detect OpenSSL on a system and link to it when available. See chapter one for details on customizing the build process to include or exclude OpenSSL.

## 7.6. nmap-service-probes File Format

As with remote OS detection (-O), Nmap uses a flat file to store the version detection probes and match strings. While the version of `nmap-services` distributed with Nmap is sufficient for most users, understanding the file format allows advanced Nmap hackers to add their own services to the detection engine. Like many UNIX files, `nmap-service-probes` is line-oriented. Lines starting with a hash (#) are treated as comments and ignored by the parser. Blank lines are ignored as well. Other lines must contain one of the directives described below. Some readers prefer to peek at the examples in Section 7.6.6 before tackling the following dissection.

### 7.6.1. The `probe` directive

Syntax: Probe <protocol> <probename> <probesendstring>

Examples:

```
Probe TCP NULL q||
```

The probe directive tells Nmap what string to send to recognize various services. All of the directives discussed later operate on the most recent Probe statement. The arguments are as follows:

#### protocol

This must be either TCP or UDP. Nmap only uses probes that match the protocol of the service it is trying to scan.

#### probename

This is a plain English name for the probe. It is used in service fingerprints to describe which probes elicited responses.

#### probestring

Tells Nmap what to send. It must start with a q, then a delimiter character which begins and ends the string. Between the delimiter characters is the string that is actually sent. It is formatted similarly to a C or Perl string in that it allows the following standard escape characters: \\ \0, \a, \b, \f, \n, \r, \t, \v, \xHH. One Probe line in nmap-service-probes has an empty probestring, as shown in the third example above. This is the TCP NULL probe which just listens for the initial banners that many services send.

## 7.6.2. The match directive

Syntax: match <service> <pattern> [versioninfo]

Examples:

```
match ftp m/^220.*Welcome to PureFTPD (\d\S+)/ v/PureFTPD/$1//  
match ssh m/^SSH-(.\d+)-OpenSSH_(\S+)/ v/OpenSSH/$2/protocol $1/  
match mysql m/^.\0\0\0\n(4.[-\w]+)\0...0/s v/MySQL/$1//  
match ssc-agent m|^0\x1e0\x060\t0\$| v/Novell Netware ssc-agent///  
match chargen m@ABCDEFGHIJKLMNPQRSTUVWXYZ|  
match netbios-ssn m+^\0\0\0.\xffSMB\0.*([^\0]|([\^\w]\0))(([-\w]\0){2,50})+ v/Samba smbd/3.X/workgro
```

The match directive tells Nmap how to recognize services based on responses to the string sent by the previous Probe directive. A single Probe line may be followed by dozens or hundreds of match statements. If the given pattern matches, an optional version specifier builds the application name, version number, and additional info for Nmap to report. The arguments to this directive follow:

#### service

This is simply the service name that the pattern matches. Examples would be ssh, smtp, http, or snmp.

#### pattern

This pattern is used to determine whether the response received matches the service given in the previous parameter. The format is like Perl, with the syntax being "m/[regex]/[opts]". The "m" tells Nmap that a match string is beginning. The forward slash (/) is a delimiter, which can be substituted by almost any printable character as long as the second slash is also replaced to match. The regex is a Perl-style regular expression (<http://www.perldoc.com/perl5.8.0/pod/perlre.html>). This is made possible by the excellent Perl Compatible Regular Expressions (PCRE) library (<http://www.pcre.org>). The only options currently supported are 'i', which makes a match case-insensitive and 's' which includes newlines in the '.' specifier. As you might expect, these

two options have the same semantics as in Perl. Subexpressions to be captured (such as version numbers) are surrounded by parenthesis as shown in most of the examples above.

#### versioninfo

This field is of the form v/vendorproductname/version/info/ where the slash can be replaced by any delimiter character. Any of the 3 fields can be empty, and the whole argument can be omitted if no further information on the service is available. The vendorproductname includes the vendor and often service name when relevant and is of the form "Sun Solaris rexecd", "ISC Bind named", or "Apache httpd". The version string is the version "number" (may include non-numeric characters, and even multiple words), while "info" is miscellaneous further information that was immediately available and might be useful (like whether an X server is open, or the protocol number of ssh servers). Any of the version fields can include numbered strings such as \$1 or \$2, which are replaced (in a Perl-like fashion) with the corresponding parenthesized substring in the *pattern*. In rare cases, a helper function can be applied to the replacement text before insertion. The \$P(3) expression in the example netbios-ssn match string above is one such example. The P() function includes only printable characters from the captured string. For netbios-ssn, a string such as "W\00\0R\0K\0G\0R\0O\0U\0P\0" is decoded to simply "WORKGROUP".

### 7.6.3. The softmatch directive

Syntax: softmatch <service> <pattern>

Examples:

```
softmatch ftp m|^220 [-.\w ]+ftp.*\r\n$/i
softmatch smtp m|^220 [-.\w ]+SMTP.*\r\n|
softmatch pop3 m|^+OK [-[\[]\(\)! ,/+:<>@\.\w ]+\r\n$|
```

The softmatch directive is similar in format to the match directive discussed above. The main difference is that scanning continues after a softmatch, but it is limited to probes that are known to match the given service. This allows for a normal ("hard") match to be found later, which may provide useful version information. See Section 7.3 for more details on how this works. Arguments are not defined here because they are the same as for 'match' above, except that there is never a *versioninfo* argument. Also as with match, many softmatch statements can exist within a single Probe

### 7.6.4. The ports and sslports directives

Syntax: ports <portlist>

Examples:

```
ports 21,43,110,113,199,505,540,1248,5432,30444
ports 111,4045,32750-32810,38978
```

This line tells Nmap what ports the services identified by this Probe are commonly found on. It should only be used once within each Probe section. The syntax is a slightly simplified version of that taken by the Nmap -p option. See the examples above. More details on how this works are in Section 7.3

Syntax: sslports <portlist>

Example:

```
sslports 443
```

This is the same as 'ports' directive described above, except that these ports are often used to wrap a service in SSL. For example, the HTTP probe declares 'sslports 443' and SMTP-detecting probes have an 'sslports 465' line because those are the standard ports for https and smtps respectively. The *portlist* format is the same as with ports. This optional directive cannot appear more than once per Probe.

### 7.6.5. The `totalwaitms` directive

Syntax: `totalwaitms <milliseconds>`

Example:

```
totalwaitms 5000
```

This rarely necessary directive specifies the amount of time Nmap should wait before giving up on the most recently defined Probe against a particular service. The Nmap default is usually fine.

### 7.6.6. Putting it all together

Here are some examples from `nmap-service-probes` which put this all together (to save space many lines have been skipped). After reading this far into the section, the following should be understood.

```
# This is the NULL probe that just compares any banners given to us
#####
#NEXT PROBE#####
Probe TCP NULL q||

# Wait for at least 5 seconds for data. Otherwise an Nmap default is used.
totalwaitms 5000
# Windows 2003
match ftp m/^220[ -]Microsoft FTP Service\r\n/ v/Microsoft ftpd///
match ftp m/^220 ProFTPD (\d\S+) Server/ v/ProFTPD/$1///
softmatch ftp m/^220 [-.\w ]+ftp.*\r\n$/i
match ident m|^flock()\ on closed filehandle .*midentd| v/midentd//broken/
match imap m|^* OK Welcome to Binc IMAP v(\d[-.\w+])| v/Binc IMAPd/$1///
softmatch imap m|^* OK [-.\w ]+imap[-.\w ]+\r\n$/i
match lucent-fwadm m|^0001;2$| v/Lucent Secure Management Server///
match meetingmaker m/^xc1,$/ v/Meeting Maker calendaring///
# lopster 1.2.0.1 on Linux 1.1
match napster m|^1$| v/Lopster Napster P2P client///

Probe UDP Help q|help\r\n\r\n|
ports 7,13,37
match chargen m|@ABCDEFGHIJKLMNOPQRSTUVWXYZ|
match echo m|^help\r\n\r\n$|
# Will last until 0xC5FFFF, in April 2005 - need to shift in advance.
match time m|^[\xc0-\xc5]...$|
```

## 7.7. Community Contributions

No matter how technically advanced a service detection framework is, it would be nearly useless without a comprehensive database of services against which to match. This is where the open source nature of Nmap really shines. The Insecure.Org lab is pretty substantial by geek standards, but it can never hope to run more than a tiny percentage of machine types and services that are out there. Fortunately experience with OS detection fingerprints has shown that Nmap users together run all of the common stuff, plus a staggering array of bizarre equipment as well. The Nmap OS Fingerprint Database contains more than a thousand entries, including all sorts of switches, WAPs, VoIP phones, game consoles, UNIX boxes, Windows hosts, printers, routers, PDAs, firewalls, etc. Version detection also supports user submissions, and Nmap users have contributed thousands of services. There are three primary ways that the Nmap community helps to make this an exceptional database:

1. *Submit service fingerprints* -- If a service responds to one or more of Nmap's probes and yet Nmap is unable to identify that service, Nmap prints a "service fingerprint" like this one:

```
SF-Port21-TCP:V=3.40PVT16%D=9/6%Time=3F5A961C%r(NULL,3F,"220\x20stage\x20F
SF:TP\x20server\x20\Version\x202\.1WU\(1\)\+SCO-2\.6\.1\+-sec\)\x20ready\
SF:.\r\n")%r(GenericLines,81,"220\x20stage\x20FTP\x20server\x20\Version\x
SF:202\.1WU\(1\)\+SCO-2\.6\.1\+-sec\)\x20ready\.\r\n500\x20":\x20command\
SF:x20not\x20understood\.\r\n500\x20":\x20command\x20not\x20understood\.\
SF:r\n");
```

If you receive such a fingerprint, and are sure you know what daemon version is running on the target host, please submit the fingerprint at the URL Nmap gives you. The whole submission process is anonymous (unless you choose to provide identifying info) and should not take more than a couple minutes. If you are feeling particularly helpful, scan the system again using -d (Nmap sometimes gives longer fingerprints that way) and paste both fingerprints into the fingerprint box on the submission form. Sometimes people read the file format section and submit their own working match lines. This is OK, but please submit the service fingerprint(s) as well because existing scripts make integrating and testing them relatively easy.

For those who care, the information in the fingerprint above is port number (21), protocol (TCP), Nmap version (3.40PVT16), date (September 6), UNIX time in hex, and a sequence of probe responses in the form  
`r({probename}, {response length}, "{responsestring}")`

2. *Submit corrections* -- This is another easy way to help improve the database. When integrating a service fingerprint submitted for "chargen on Windows XP" or "FooBar FTP server 3.9.213", it is difficult to determine how general the match is. Will it also match chargen on Solaris or FooBar FTP 2.7? There is no good way to tell. So a very specific name is used in the hope that people will report when the match needs to be generalized. If you scan a host and the service fingerprint gives an incorrect OS, version number, application name, or even service type, please mail the full Nmap output and correct information to <fyodor@insecure.org> and Nmap will be updated appropriately.

3. *Submit new probes* -- Suppose Nmap fails to detect a service. If it received a response to any probes at all, it should provide a fingerprint that can be submitted as described in #1 above. But what if there is no response and thus a fingerprint is not available? Create and submit your own probe! These are very welcome. The following steps describe the process.

### Steps for creating a new version detection probe

- a. Download the latest version of Nmap from <http://www.insecure.org/nmap/> and try again. You would feel a bit silly spending time developing a new probe just to find out that it has already been added. Make sure no

- fingerprint is available, as it is better to recognize services using existing probes if possible than to create too many new ones. If the service does not respond to any of the existing probes, there is no other choice.
- b. Decide on a good probe string for recognizing the service. An ideal probe should elicit a response from as many instances of the service as possible, and ideally the responses should be unique enough to differentiate between them. This step is easiest if you understand the protocol very well, so consider reading the relevant RFCs and product documentation. One simple approach is to simply start a client for the given service and watch what initial handshaking is done by sniffing the network with Ethereal or Tcpdump, or connecting to a listening Netcat.
  - c. Once you have decided on the proper string, add the appropriate new Probe line to Nmap (see Section 7.3 and Section 7.6). Do not put in any match lines at first, although a ‘ports’ directive to make this new test go first against the registered ports is OK. Then scan the service with Nmap a few times. You should get a fingerprint back showing the service’s response to your new probe. Send the new probe line and the fingerprints (against different machines if possible, but even a few against the same daemon helps to note differences) to Fyodor at fyodor@insecure.org. It will likely then be integrated into future versions of Nmap. Any details you can provide on the nature of your probe string is helpful as well. For custom services that only appear on your network, it is better to simply add them to your own nmap-service-probes rather than the global Nmap

## 7.8. [RECIPE] Find all servers running an insecure or nonstandard version of an application

\* *I need to actually write this recipe*

## 7.9. [RECIPE] Hack version detection to suit custom needs, such as open proxy detection

\* *I need to actually write this recipe*

# **Chapter 8. OS Fingerprinting**

# Chapter 9. Detecting and Subverting Firewalls and Intrusion Detection Systems

## 9.1. Introduction

Many Internet pioneers envisioned a global open network with a universal IP address space allowing virtual connections between any two nodes. This allows hosts to act as true peers, serving and retrieving information from each other. People could access all of their home systems from work, changing the climate control settings or unlocking the doors for early guests. This vision of universal connectivity has been stifled by address space shortages and security concerns. In the early 1990s, organizations began deploying firewalls for the express purpose of reducing connectivity. Huge networks were cordoned off from the unfiltered Internet by application proxies, network address translation, and packet filters. The unrestricted flow of information gave way to tight regulation of approved communication channels and the content that passes over them.

Network obstructions such as firewalls can make mapping a network exceedingly difficult. It will not get any easier, as stifling casual reconnaissance is often a key goal of implementing the devices. Nevertheless, Nmap offers many features to help understand these complex networks, and to verify that filters are working as intended. It even supports mechanisms for bypassing poorly implemented defenses. One of the best methods of understanding your network security posture is to try to defeat it. Place yourself in the mindset of an attacker, and deploy techniques from this chapter against your networks. Launch an FTP bounce scan, Idle scan, fragmentation attack, or try to tunnel through one of your own proxies.

In addition to restricting network activity, companies are increasingly monitoring traffic with intrusion detection systems (IDS). All of the major IDSs ship with rules designed to detect Nmap scans because scans are sometimes a precursor to attacks. Many of these products have recently morphed into intrusion *prevention* systems (IPS) that actively block traffic deemed malicious. Unfortunately for network administrators and IDS vendors, reliably detecting bad intentions by analyzing packet data is a tough problem. Attackers with patience, skill, and the help of certain Nmap options can usually pass by IDSs undetected. Meanwhile, administrators must cope with large numbers of "false positive" results where innocent activity is misdiagnosed and alerted on or blocked.

## 9.2. Why would whitehats ever do this?

Some of you whitehat readers may be tempted to skip this chapter. For authorized use against your own networks, why would you ever want to evade your own security systems? Because it helps in understanding the danger of real attackers. If you can sneak around a blocked portmapper port using Nmap direct RPC scanning, then so can the bad guys. It is easy to make a mistake in configuring complex firewalls and other devices. Many of them even come with glaring security holes which conscientious users must find and close. Regular network scanning can help find the dangerous implicit rules of your Checkpoint Firewall-1 or Windows IPsec filters before attackers do.

There are good reasons for evading IDSs as well. The most common is to evaluate IDS performance. If attackers can slide under the radar by simply adding an Nmap flag or two, the system is not offering much protection. It may still catch the script kiddies and worms, but they are usually blazingly obvious anyway.

Occasionally people suggest that Nmap should not offer features for evading firewall rules or sneaking past IDSs. They argue that these features are just as likely to be misused by attackers as used by administrators to enhance security. The problem with this logic is that these methods would still be used by attackers, who would just find other tools or patch the functionality into Nmap. Meanwhile, administrators would find it that much harder to do their jobs.

Deploying only modern, patched FTP servers is a far more powerful defense than trying to prevent the distribution of tools implementing the FTP bounce attack.

## **9.3. Determining Firewall Rules**

The first step toward bypassing firewall rules is to understand them. Where possible, Nmap distinguishes between ports that are reachable but closed, and those that are actively filtered. An effective technique is to start with a normal SYN port scan, then move on to more exotic techniques such as ACK scan and IPID sequencing to gain a better understanding of the network.

### **9.3.1. Standard SYN scan**

One helpful feature of the TCP protocol is that systems are required by RFC 793 (<http://www.rfc-editor.org/rfc/rfc793.txt>) to send a negative response to unexpected connection requests in the form of a TCP RST (reset) packet. The RST packet makes closed ports easy for Nmap to recognize. Filtering devices such as firewalls, on the other hand, tend to drop packets destined for disallowed ports. In some cases they send ICMP error messages (usually port unreachable) instead. Because dropped packets and ICMP errors are easily distinguishable from RST packets, Nmap can reliably detect filtered TCP ports from open or closed ones, and it does so automatically. This is shown in Example 9-1.

#### **Example 9-1. Detection of closed and filtered TCP ports**

```
# nmap -sS -T4 scanme.nmap.org

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 1655 ports scanned but not shown below are in state: filtered)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    open     smtp
53/tcp    open     domain
80/tcp    open     http
113/tcp   closed   auth

Nmap run completed -- 1 IP address (1 host up) scanned in 31.669 seconds
```

One of the most important lines in Example 9-1 is the parenthetical note that “the 1655 ports scanned but not shown below are in state: filtered”. In other words, this host has a proper deny-by-default firewall policy. Only those ports the administrator explicitly allowed are reachable, while the default action is to deny (filter) them. Four of the enumerated ports are in the open state, while the auth port (113) is closed. 1655 out of 1660 tested ports are unreachable by this standard scan. Leaving port 113 closed but unfiltered is a common practice on the Internet due to widespread use of the auth (often called ident) protocol. If that port is filtered instead of open or closed, some mail and IRC servers will spend a long time trying to connect back to their client’s ident port until the connection times out. A forged RST packet from the firewall causes the server to give up on ident quickly.

#### **9.3.1.1. Sneaky firewalls that return RST**

While the Nmap distinction between closed ports (which return a RST packet) and filtered ports (returning nothing or an ICMP error) is usually accurate, many firewall devices are now capable of forging RST packets as though they

are coming from the destination host and claiming that the port is closed. One example of this capability is the Linux iptables system, which offers many methods for rejecting undesired packets. The iptables man page documents this feature as follows:

--reject-with *type*

The *type* given can be icmp-net-unreachable, icmp-host-unreachable, icmp-port-unreachable, icmp-proto-unreachable, icmp-net-prohibited or icmp-host-prohibited, which return the appropriate ICMP error message (port-unreachable is the default). The option tcp-reset can be used on rules which only match the TCP protocol: this causes a TCP RST packet to be sent back. This is mainly useful for blocking ident (113/tcp) probes which frequently occur when sending mail to broken mail hosts (which won't accept your mail otherwise).

Forging RST packets by firewalls and IDS/IPS is not particularly common outside of port 113, as it can be confusing to legitimate network operators and it also allows scanners to move on to the next port immediately without waiting on the timeout caused by dropped packets. Nevertheless, it does happen. Such forgery can usually be detected by careful analysis of the RST packet in comparison with other packets sent by the machine. Section 9.6 describes effective techniques for doing so.

### 9.3.2. ACK scan

As described in depth in Chapter 5, the ACK scan sends TCP packets with only the ACK bit set. Whether ports are open or closed, the target is required by RFC 793 (<http://www.rfc-editor.org/rfc/rfc793.txt>) to respond with a RST packet. Firewalls that block the probe, on the other hand, usually make no response or send back an ICMP destination unreachable error. This distinction allows Nmap to report whether the ACK packets are being filtered. The set of filtered ports reported by an Nmap ACK scan is often less than for a SYN scan against the same machine because ACK scans are more difficult to filter. Many networks allow nearly unrestricted outbound connections, but wish to block Internet hosts from initiating connections back to them. Blocking incoming SYN packets (without the ACK bit set) is an easy way to do this, but it still allows any ACK packets through. Blocking those ACK packets is more difficult, because they do not tell which side started the connection. To block unsolicited ACK packets (as sent by the Nmap ACK scan), while allowing ACK packets belonging to legitimate connections, firewalls must statefully watch every established connection to determine whether a given ACK is appropriate. These stateful firewalls are usually more secure because they can be more restrictive. Blocking ACK scans is one extra available restriction. The downsides are that they require more resources to function, and a stateful firewall reboot can cause a device to lose state and terminate all established connections passing through it.

While stateful firewalls are widespread and rising in popularity, the stateless approach is still quite common. For example, the Linux Netfilter/iptables system supports the --syn convenience option to make the stateless approach described above easy to implement.

In the previous section, a SYN scan showed that all but 5 of 1660 common ports on scanme.nmap.org were in the filtered state. Example 9-2 demonstrates an ACK scan against the same host to determine whether it is using a stateful firewall.

#### Example 9-2. ACK scan against Scanme

```
# nmap -sA -T4 scanme.nmap.org
Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
```

```
(The 1655 ports scanned but not shown below are in state: filtered)
PORT      STATE     SERVICE
22/tcp    UNfiltered ssh
25/tcp    UNfiltered smtp
53/tcp    UNfiltered domain
80/tcp    UNfiltered http
113/tcp   UNfiltered auth
```

Nmap run completed -- 1 IP address (1 host up) scanned in 31.389 seconds

The same five ports displayed in the SYN scan are shown here. The other 1655 are still filtered. This is because Scanme is protected by this stateful iptables directive: **iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT**. This only accepts packets that are part of or related to an established connection. Unsolicited ACK packets sent by Nmap are dropped, except to the five special ports shown. Special rules allow all packets to the open ports 22, 25, 53, and 80, as well as sending a RST packet in response to port 113 probes. Note that the five shown ports are in the unfiltered state, since the ACK scan cannot further divide them into open (22, 25, 53, and 80) or closed (113).

Now let us look at another example. A Linux host named Para on my local network uses the following (simplified to save space) firewall script:

```
#!/bin/sh
#
# A simple, stateless, host-based firewall script.

# First of all, flush & delete any existing tables
iptables -F
iptables -X

# Deny by default (input/forward)
iptables --policy INPUT DROP
iptables --policy OUTPUT ACCEPT
iptables --policy FORWARD DROP

# I want to make ssh and www accessible from outside
iptables -A INPUT -m multiport -p tcp --destination-port 22,80 -j ACCEPT

# Allow responses to outgoing TCP requests
iptables -A INPUT --proto tcp ! --syn -j ACCEPT
```

This firewall is stateless, as there is no sign of the --state option or the -m state module request. Example 9-3 shows SYN and ACK scans against this host.

### Example 9-3. Contrasting SYN and ACK scans against Para

```
# nmap -sS -p1-100 -T4 para

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on para (192.168.10.191):
(The 98 ports scanned but not shown below are in state: filtered)
PORT      STATE     SERVICE
22/tcp    open      ssh
```

```
80/tcp closed http
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap run completed -- 1 IP address (1 host up) scanned in 3.810 seconds

# nmap -sA -p1-100 -T4 para

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
All 100 scanned ports on para (192.168.10.191) are: UNfiltered
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap run completed -- 1 IP address (1 host up) scanned in 0.695 seconds
```

In the SYN scan, 98 of 100 ports are filtered. Yet the ACK scan shows every scanned port being unfiltered. In other words, all of the ACK packets are sneaking through unhindered and eliciting RST responses. These responses also make the scan more than five times as fast, since it does not have to wait on timeouts.

Now we know how to distinguish between stateful and stateless firewalls, but what good is that? The ACK scan of Para shows that some packets are probably reaching the destination host. I say probably because firewall forgery is always possible. While you may not be able to establish TCP connections to those ports, they can be useful for determining which IP addresses are in use, OS detection tests, certain IPID shenanigans, and as a channel for tunneling commands to rootkits installed on those machines. Other scan types, such as FIN scan, may even be able to determine which ports are open and thus infer the purpose of the hosts. Such hosts may be useful as zombies for an IPID idle scan.

This pair of scans also demonstrates that what we are calling a port state is not solely a property of the port itself. Here, the same port number is considered *filtered* by one scan type and *unfiltered* by another. What IP address you scan from, the rules of any filtering devices along the way, and which interface of the target machine you access can all affect how Nmap sees the ports. The port table only reflects what Nmap saw when running from a particular machine, with a defined set of options, at the given time.

### **9.3.3. IPID tricks**

The humble identification field within IP headers can divulge a surprising amount of information. Later in this chapter it will be used for port scanning (Idle scan technique) and to detect when firewall and intrusion detection systems are forging RST packets as though they come from protected hosts. Another neat trick is to discern what source addresses make it through the firewall. There is no point spending hours on a blind spoofing attack "from" 192.168.0.1 if some firewall along the way drops all such packets.

I usually test this condition with the free network probing tool hping2 (<http://www.hping.org>). This is a rather complex technique, but it can be valuable sometimes. Here are the steps I take.

1. Find at least one accessible (open or closed) port of one machine on the internal network. Routers, printers, and Windows boxes often work well. Recent releases of Linux, Solaris, and OpenBSD have largely resolved the issue of predictable IPID sequence numbers and will not work. The machine chosen should not be heavily trafficked.
2. Verify that the machine has predictable IPID sequences. The following command tests a Windows XP machine named playground. The hping2 options request that 5 SYN packets be sent to port 80, one second apart.

```
# hping2 -c 5 -i 1 -p 80 -S playground
HPING playground (eth0 192.168.0.40): S set, 40 headers + 0 data bytes
```

```

len=46 ip=192.168.0.40 ttl=128 id=64473 sport=80 flags=RA seq=0 rtt=0.7 ms
len=46 ip=192.168.0.40 ttl=128 id=64474 sport=80 flags=RA seq=1 rtt=0.3 ms
len=46 ip=192.168.0.40 ttl=128 id=64475 sport=80 flags=RA seq=2 rtt=0.3 ms
len=46 ip=192.168.0.40 ttl=128 id=64476 sport=80 flags=RA seq=3 rtt=0.3 ms
len=46 ip=192.168.0.40 ttl=128 id=64477 sport=80 flags=RA seq=4 rtt=0.3 ms

--- playground hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.3/0.7 ms

```

Since the IPID fields are perfectly sequential, we can move on to the next test. If they were random or very far apart, we would have to find a new accessible host.

3. Start a flood of probes to the target from a host near your own (just about any host will do). An example command is **hping2 --spoof scanme.nmap.org --fast -p 80 -c 10000 -S playground**. Replace scanme.nmap.org with some other host of your choosing, and playground with your target host. Getting replies back is not necessary, because the goal is simply to increment the IPID sequences. Do not use the real address of the machine you are running hping2 from. Using a machine nearby on the network is advised to reduce the probability that your own ISP will block the packets.

While this is going on, redo the test from the previous step against your target machine.

```

# hping2 -c 5 -i 1 -p 80 -S playground
HPING playground (eth0 192.168.0.40): S set, 40 headers + 0 data bytes
len=46 ip=192.168.0.40 ttl=128 id=64672 sport=80 flags=RA seq=0 rtt=0.6 ms
len=46 ip=192.168.0.40 ttl=128 id=64683 sport=80 flags=RA seq=1 rtt=0.2 ms
len=46 ip=192.168.0.40 ttl=128 id=64694 sport=80 flags=RA seq=2 rtt=0.2 ms
len=46 ip=192.168.0.40 ttl=128 id=64705 sport=80 flags=RA seq=3 rtt=0.2 ms
len=46 ip=192.168.0.40 ttl=128 id=64716 sport=80 flags=RA seq=4 rtt=0.2 ms

--- playground hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.3/0.6 ms

```

This time, the IPIDs are increasing by roughly 11 a second instead of one. The target is receiving our 10 forged packets per second, and responding to each. Each response increments the IPID. Some hosts use a unique IPID sequence for each IP address they communicate with. If that had been the case, we would not have seen the IPID leaping like this and we would have looked for a different target host on the network.

4. Repeat step 3 using spoofed addresses that you suspect may be allowed through the firewall or trusted. Try addresses from within their firewall, as well as the RFC 1918 (<http://www.rfc-editor.org/rfc/rfc1918.txt>) blessed private networks such as 10.0.0.0/8, 192.168.0.0/16, and 172.16.0.0/12. Also try localhost (127.0.0.1) and maybe another address from 127.0.0.0/8 to detect cases where 127.0.0.1 is hard coded in. There have been many security holes related to spoofed localhost packets, including the infamous Land denial of service attack. Misconfigured systems sometimes trust these addresses without checking whether they came in through the localhost interface. If a source address gets through to the end host, the IPID will jump as seen in step 3. If it continues to increment slowly as in step 2, the packets were likely dropped by a firewall or router.

The end result of this technique is a list of source address netblocks that are permitted through the firewall, and those that are blocked. This information is valuable for several reasons. The IP addresses a company chooses to block or allow may give clues as to what addresses are used internally or trusted. For example, machines on a company's

production network might trust IP addresses on the corporate network, or trust a system administrator's personal machine. Machines on the same production network also sometimes trust each other, or trust localhost. Common IP-based trust relationships are seen in nfs exports, host firewall rules, tcp wrappers, custom applications, rlogin, etc. Before spending substantial time trying to find and exploit these problems, use the test described here to determine whether the spoofed packets even get through.

A concrete example of this trusted-source-address problem is that I once found that a company's custom UDP service allowed users to skip authentication if they came from special netblocks entered into a configuration file. These netblocks corresponded to different corporate locations. Their internet-facing firewall smartly tried to block those addresses, as actual employees could access production from a private link. But by using the techniques described in this section, I found that the firewall was not perfectly synced with the config file. There were a few addresses from which I could successfully forge the UDP control messages and take over their application.

This technique of mapping out the firewall rules does not use Nmap, but the results are valuable for future runs. For example, this test can show whether to use certain decoys (-D). The best decoys will make it all the way to the target system. In addition, forged packets must get through for the IPID Idle scan (discussed later) to work. Testing potential source IPs with this technique is usually easier than finding and testing every potential Idle proxy machine on a network. Potential Idle proxies need only be tested if they pass step number two, above.

### **9.3.4. UDP version scanning**

The previous sections have all focused on the prevalent TCP protocol. Working with UDP is often more difficult, because the protocol does not provide acknowledgment of open ports like TCP does. Many UDP applications will simply ignore unexpected packets, leaving Nmap unsure whether the port is open or filtered. So Nmap places them in the open|filtered state, as shown in Example 9-4.

#### **Example 9-4. UDP scan against firewalled host**

```
# #nmap -sU -p50-59 scanme.nmap.org

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
PORT      STATE            SERVICE
50/udp    open|filtered   re-mail-ck
51/udp    open|filtered   la-maint
52/udp    open|filtered   xns-time
53/udp    open|filtered   domain
54/udp    open|filtered   xns-ch
55/udp    open|filtered   isi-gl
56/udp    open|filtered   xns-auth
57/udp    open|filtered   priv-term
58/udp    open|filtered   xns-mail
59/udp    open|filtered   priv-file

Nmap run completed -- 1 IP address (1 host up) scanned in 1.400 seconds
```

This 10-port scan was not very helpful. No port responded to the probe packets, and so they are all listed as open or filtered. One way to better understand which ports are actually open is to send a whole bunch of UDP probes for dozens of different known UDP services in the hope of eliciting a response from any open ports. Nmap version

detection (chapter 7) does exactly that. Example 9-5 shows the same scan with the addition of version detection (`-sV`).

**Example 9-5. UDP version scan against firewalled host**

```
# nmap -sV -sU -p50-59 scanme.nmap.org

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
PORT      STATE      SERVICE      VERSION
50/udp    open|filtered re-mail-ck
51/udp    open|filtered la-maint
52/udp    open|filtered xns-time
53/udp    open          domain      ISC Bind 9.2.1
54/udp    open|filtered xns-ch
55/udp    open|filtered isi-gl
56/udp    open|filtered xns-auth
57/udp    open|filtered priv-term
58/udp    open|filtered xns-mail
59/udp    open|filtered priv-file

Nmap run completed -- 1 IP address (1 host up) scanned in 31.380 seconds
```

Version detection shows beyond a doubt that port 53 (domain) is open, and even what it is running. The other are still in `open|filtered` because they did not respond to any of the probes. They are probably filtered, though this is not guaranteed. They could be running a service like SNMP, which only responds to packets with the correct community string. Or they could be running an obscure or custom UDP service for which no Nmap version detection probe exists. Also note that this scan took 15 times longer than the previous one. Sending all of those probes to each port is a relatively slow process.

## 9.4. Bypassing Firewall Rules

While mapping out firewall rules can be valuable, bypassing rules is often the primary goal. Nmap implements many techniques for doing this, though most are only effective against poorly configured networks. Unfortunately, those are common. Individual techniques may each have a low probability of success, so try as many different methods as possible. The attacker need only find one misconfiguration to succeed, while the network defenders must close every hole.

### 9.4.1. Exotic scan flags

The previous section discussed using an ACK scan to map out which target network ports are filtered. However, it could not determine which of the accessible ports were open or closed. Nmap offers several scan methods that are good at sneaking past firewalls while still providing the desired port state information. FIN scan is one such technique. In Section 9.3.2, SYN and ACK scans were run against a machine named Para. The SYN scan showed only 2 open ports, perhaps due to firewall restrictions. Meanwhile, the ACK scan is unable to recognize open ports from closed ones. Example 9-6 shows another scan attempt against this machine, this time using a FIN scan. Because a naked FIN packet is being set, this packet flies past the rules blocking SYN packets. While a SYN scan only found one open port below 100, the FIN scan finds both of them.

**Example 9-6. FIN scan against stateless firewall**

```
# nmap -sF -p1-100 -T4 para

Starting nmap 3.76 ( http://www.insecure.org/nmap/ )
Interesting ports on para (192.168.10.191):
(The 98 ports scanned but not shown below are in state: closed)
PORT      STATE      SERVICE
22/tcp    open|filtered ssh
53/tcp    open|filtered domain
MAC Address: 00:60:1D:38:32:90 (Lucent Technologies)

Nmap run completed -- 1 IP address (1 host up) scanned in 1.612 seconds
```

Many other scan types are worth trying, since the target firewall rules and target host type determine which techniques will work. Some particularly valuable scan types are FIN, Maimon, Window, SYN|FIN, and NULL scans. These are all described in Chapter 5.

#### **9.4.2. Source port manipulation**

One surprisingly common misconfiguration is to trust traffic based only on the source port number. It is easy to understand how this comes about. An administrator will set up a shiny new firewall, only to be flooded with complaints from ungrateful users whose applications stopped working. In particular, DNS may be broken because the UDP DNS replies from external servers can no longer enter the network. FTP is another common example. In active FTP transfers, the remote server tries to establish a connection back to the client to transfer the requested file.

Secure solutions to these problems exist, often in the form of application-level proxies or protocol-parsing firewall modules. Unfortunately there are also easier, insecure solutions. Noting that DNS replies come from port 53 and active ftp from port 20, many admins have fallen into the trap of simply allowing incoming traffic from those ports. They often assume that no attacker would notice and exploit such firewall holes. In other cases, admins consider this a short-term stop-gap measure until they can implement a more secure solution. Then they forget the security upgrade.

Overworked network administrators are not the only ones to fall into this trap. Numerous products have shipped with these insecure rules. Even Microsoft has been guilty. The IPsec filters that ship with Windows 2000 and Windows XP contain an implicit rule that allows all TCP or UDP traffic from port 88 (Kerberos). In another well-known case, versions of the Zone Alarm personal firewall up to 2.1.25 allowed incoming UDP packets with the source port 53 (DNS) or 67 (DHCP).

Nmap offers the `-g` option to exploit these weaknesses. Simply provide a port number, and Nmap will send packets from that port where possible. Nmap must use different port numbers for certain OS detection tests to work properly, and DNS requests ignore the `-g` flag because Nmap relies on system libraries to handle those. Most TCP scans, including SYN scan, support the option completely, as does UDP scan. In May 2004, JJ Gray posted example Nmap scans to Bugtraq that demonstrate exploitation of the Windows IPsec source port 88 bug against one of his clients. A normal scan, followed by a `-g 88` scan are shown in Example 9-7. Some output has been removed for brevity and clarity.

**Example 9-7. Bypassing Windows IPsec filter using source port 88**

```
# nmap -sS -v -v -P0 172.25.0.14
```

```
Starting nmap 3.50 ( http://www.insecure.org/nmap/ )
Interesting ports on 172.25.0.14:
(The 1658 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE
88/tcp    closed  kerberos-sec

Nmap run completed -- 1 IP address (1 host up) scanned in 7.017 seconds

# nmap -sS -v -v -P0 -g 88 172.25.0.14

Starting nmap 3.50 ( http://www.insecure.org/nmap/ )
Interesting ports on 172.25.0.14:
(The 1653 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
135/tcp   open   msrpc
139/tcp   open   netbios-ssn
445/tcp   open   microsoft-ds
1025/tcp  open   NFS-or-IIS
1027/tcp  open   IIS
1433/tcp  open   ms-sql-s

Nmap run completed -- 1 IP address (1 host up) scanned in 0.367 seconds
```

Note that the closed port 88 was the hint that led JJ to try using it as a source port. For further information on this vulnerability, see Microsoft Knowledge Base Article 811832  
(<http://support.microsoft.com/default.aspx?scid=kb;EN-US;811832>)

#### **9.4.3. IPv6 attacks**

While IPv6 has not exactly taken the world by storm, it is reasonably popular in Japan and certain other regions. When organizations adopt this protocol, they often forget to lock it down as they have instinctively learned to do with IPv4. Or they may try to, but find that their hardware does not support IPv6 filtering rules. Filtering IPv6 can sometimes be more critical than IPv4 because the expanded address space often allows the allocation of globally addressable IPv6 addresses to hosts that would normally have to use the RFC1918-blessed private IPv4 addresses.

Performing an IPv6 scan rather than the IPv4 default is often as easy as adding `-6` to the command line. Certain features such as OS detection and UDP scanning are not yet supported for this protocol, but the most popular features work. Example 9-8 demonstrates IPv4 and IPv6 scans, performed in 2002, of a well-known IPv6 development and advocacy organization.

#### **Example 9-8. Comparing IPv4 and IPv6 scans**

```
> nmap www.kame.net

Starting nmap V. 3.10ALPHA1 ( www.insecure.org/nmap/ )
Interesting ports on kame220.kame.net (203.178.141.220):
(The 1585 ports scanned but not shown below are in state: closed)
Port      State      Service
19/tcp    filtered  chargen
21/tcp    open       ftp
22/tcp    open       ssh
```

```

53/tcp      open     domain
80/tcp      open     http
111/tcp     filtered sunrpc
137/tcp     filtered netbios-ns
138/tcp     filtered netbios-dgm
139/tcp     filtered netbios-ssn
513/tcp     filtered login
514/tcp     filtered shell
2049/tcp    filtered nfs
2401/tcp    open     cvspserver
5999/tcp    open     ncd-conf
7597/tcp    filtered qaz
31337/tcp   filtered Elite

```

Nmap run completed -- 1 IP address (1 host up) scanned in 34 seconds

```
> nmap -6 www.kame.net
```

```

Starting nmap V. 3.10ALPHA1 ( www.insecure.org/nmap/ )
Interesting ports on 3ffe:501:4819:2000:210:f3ff:fe03:4d0:
(The 1595 ports scanned but not shown below are in state: closed)
Port      State       Service
21/tcp    open        ftp
22/tcp    open        ssh
53/tcp    open        domain
80/tcp    open        http
111/tcp   open        sunrpc
2401/tcp  open        cvspserver

```

Nmap run completed -- 1 IP address (1 host up) scanned in 19 seconds

The first scan shows numerous filtered ports, including frequently exploitable services such as sunrpc, Windows NetBIOS, and NFS. Yet scanning the same host with IPv6 shows no filtered ports! Suddenly SunRPC (port 111) is available, and waiting to be queried by an IPv6-enabled rpcinfo or by Nmap version detection, which supports IPv6. They fixed the issue shortly after I notified them of it.

In order to perform an IPv6 scan, a system must be configured for IPv6. It must have an IPv6 address and routing information. Since my ISPs do not provide an IPv6 address, I use a free ipv6 tunnel broker service. One of the better free tunnel brokers is run by BT Exact at <https://tb.ipv6.btexact.com/>. I have also used one that Hurricane Electric provides at <http://ipv6tb.he.net/>. 6to4 tunnels are another popular, free approach. Of course, this technique also requires that the target use IPv6.

#### 9.4.4. IPID Idle Scanning

The IPID Idle Scan has a reputation for being one of the most stealthy scan types, since no packets are sent to the target from your real address. Open ports are inferred from the IPID sequences of a chosen zombie machine. A less recognized feature of Idle scan is that the results obtained are actually those you would get if the zombie was to scan the target host directly. In a similar way that the `-g` option allows exploitation of trusted source ports, Idle Scan can sometimes exploit trusted source IP addresses. This ingenious scan type, which was originally conceived by security researcher Antirez, is described fully in Chapter 5.

### 9.4.5. Multiple ping probes

A common issue when trying to scan through firewalled networks is that dropped ping probes can lead to missed hosts. To reduce this problem, Nmap allows a very wide variety of probes to be sent in parallel. Hopefully at least one will get through. Chapter three discusses these techniques in depth, including empirical data on the best firewall-busting techniques.

### 9.4.6. Fragmentation

Some packet filters have trouble dealing with IP packet fragments. They could reassemble the packets themselves, but that requires extra resources. There is also the possibility that fragments will take different paths, preventing reassembly. Due to this complexity, some filters ignore all fragments, while others automatically pass all but the first fragment. Interesting things can happen if the first fragment is not long enough to contain the whole TCP header, or if the second packet partially overwrites it. The number of filtering devices vulnerable to these problems is shrinking, though it never hurts to try. An Nmap scan will use tiny IP fragments if the `-f` is specified. Run a sniffer like ethereal or tcpdump the first time you use this option, to ensure packets leave your machine fragmented. Some overly helpful hosts will defragment the packets before they even leave the device. Linux 2.4 kernels are particularly prone to this.

It might be nice if Nmap could send fragments out of order or with configurable length. The RFCs allow IP packets with only 8 bytes of data after the IP header. So a 20-byte TCP packet could be split into three packets (the final packet may be smaller still). Because certain Linux versions and other operating systems restrict sending tiny or out-of-order IP fragments over raw sockets, Nmap breaks the 20-byte TCP header into a 16-byte segment and a four-byte segment, which it then sends in order.

If a fragmented port scan gets through, a tool such as Fragroute (<http://www.monkey.org/~dugsong/fragroute/>) can be used to fragment other tools and exploits used to attack the host.

### 9.4.7. Proxies

Application-level proxies, particularly for the web, have become popular due to perceived security and network efficiency (through caching) benefits. Like firewalls and IDS, misconfigured proxies can cause far more security problems than they solve. The most frequent problem is a failure to set appropriate access controls. Hundreds of thousands of wide-open proxy machines exist on the Internet, allowing anyone to use them as an anonymous hopping points to other Internet sites. Dozens of organizations use automated scanners to find these open proxies and distribute the IP addresses. Occasionally the proxies are used for arguably positive things, such as escaping the draconian censorship imposed by the Chinese government on its residents. This "great firewall of China" has been known to block the New York Times website as well as other news, political, and spiritual sites that the government disagrees with. Unfortunately, the open proxies are more frequently abused by more sinister folks who want to anonymously crack into sites, commit credit card fraud, or flood the Internet with spam.

While hosting a wide-open proxy to Internet resources can cause numerous problems, a more serious condition is when the open proxies allow connections back into the protected network. Administrators who decide that internal hosts must use a proxy to access Internet resources often inadvertently allow traffic in the opposite direction as well. The hacker Adrian Lamo is famous for breaking into Microsoft, Excite, Yahoo, WorldCom, the New York Times, and other large networks, usually by exploiting this reverse-proxy technique.

Nmap does not presently offer a proxy scan-through option, though it is high on the priority list. Chapter 7 discusses a way to find open proxies using Nmap version detection.

\* I still need to add that section.

In addition, plenty of dedicated free proxy scanners are available on Internet sites such as Packet Storm (<http://packetstormsecurity.nl/>). Lists of thousands of open proxies are widespread as well.

#### **9.4.8. Source routing**

This old-school technique is still effective in some cases. If a particular router on the path is causing you trouble, try to find a route around it. Effectiveness of this technique is limited because packet filtering problems usually occur on or near the target network. Those machines are likely to either drop all source routed packets or to be the only way into the network. Nmap does not presently support source routing, so I use Hobbit's Netcat ([http://www.atstake.com/research/tools/network\\_utilities/](http://www.atstake.com/research/tools/network_utilities/)), with the `-g` option, when I find it necessary.

#### **9.4.9. FTP Bounce Scan**

While only a small percentage of FTP servers are still vulnerable, it is worth checking whether all of your clients' systems for this problem. At a minimum, it allows outside attackers to utilize vulnerable systems to scan other parties. Worse configurations even allow attackers to bypass the organization's firewalls. Details and examples of this technique are provided in Section 5.12. Example 9-9 shows an HP printer being used to relay a port scan. If this printer is behind the organization's firewall, it can be used to scan normally inaccessible (to the attacker) internal addresses as well.

##### **Example 9-9. Exploiting a printer with the FTP bounce scan**

```
felix~> nmap -p 22,25,135 -P0 -v -b XXX.YY.111.2 scanme.nmap.org

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Attempting connection to ftp://anonymous:-wwwuser@XXX.YY.111.2:21
Connected:220 JD FTP Server Ready
Login credentials accepted by ftp server!
Initiating TCP ftp bounce scan against scanme.nmap.org (205.217.153.55)
Adding open port 22/tcp
Adding open port 25/tcp
Scanned 3 ports in 12 seconds via the Bounce scan.
Interesting ports on scanme.nmap.org (205.217.153.55):
PORT      STATE     SERVICE
22/tcp    open      ssh
25/tcp    open      smtp
135/tcp   filtered msrpc

Nmap run completed -- 1 IP address (1 host up) scanned in 21.790 seconds
```

#### **9.4.10. Take an alternative path**

I hate to overuse the “think outside the box” cliche, but continually banging on the front door of a well-secured network is not always the best approach. Look for other ways in. Wardial their phone lines, attack subsidiaries who may have special network access, or show up at their offices with Wi-Fi sniffing equipment, or even sneak in and plug into a convenient ethernet jack. Nmap works well through all of these connections. Just make sure that your

penetration-testing contract covers these methods before your client catches you in a ninja suit grappling onto their datacenter rooftop.

## **9.5. Subverting Intrusion Detection Systems**

Firewalls are not the only obstacle that modern attackers face. Intrusion detection and prevention systems can be problematic as well. Network administration staff do not always take well to a flood of 2 A.M. intrusion alert pages from the IDS. Considerate hackers take pains to prevent their actions from causing all of these alerts in the first place. A first step is to detect whether an IDS is even present -- many small companies do not use them. If an IDS is suspected or detected, there are many effective techniques for subverting it. They fall into three categories that vary by intrusiveness: avoiding the IDS as if the attacker is not there, confusing the IDS with misleading data, and exploiting the IDS to gain further network privilege or just to shut it down. Alternatively, attackers who are not concerned with stealth can ignore the IDS completely as they pound away at the target network.

### **9.5.1. Intrusion detection system detection**

Early the never-ending battle between network administrators and malicious hackers, admins defended their turf by hardening systems and even installing firewalls to act as a perimeter barrier. Hackers developed new tools to penetrate or sneak around the firewalls and exploit vulnerable hosts. The arms race escalated with admins introducing intrusion detection systems that constantly watch for devious activity. Attackers responded, of course, by devising systems for detecting and deceiving the IDS. While intrusion detection systems are meant to be passive devices, many can be detected by attackers over the network.

The least conspicuous IDS is one that passively listens to network traffic without ever transmitting. Special network tap hardware devices are available to ensure that the IDS *cannot* transmit, even if it is compromised by attackers. Despite the security advantages of such a setup, it is not widely deployed due to practical considerations. Modern IDSs expect to be able send alerts to central management controls and the like. If this was all the IDS transmitted, the risk would be minimal. But to provide more extensive data on the alert, they often initiate probes that may be seen by attackers.

#### **9.5.1.1. Reverse probes**

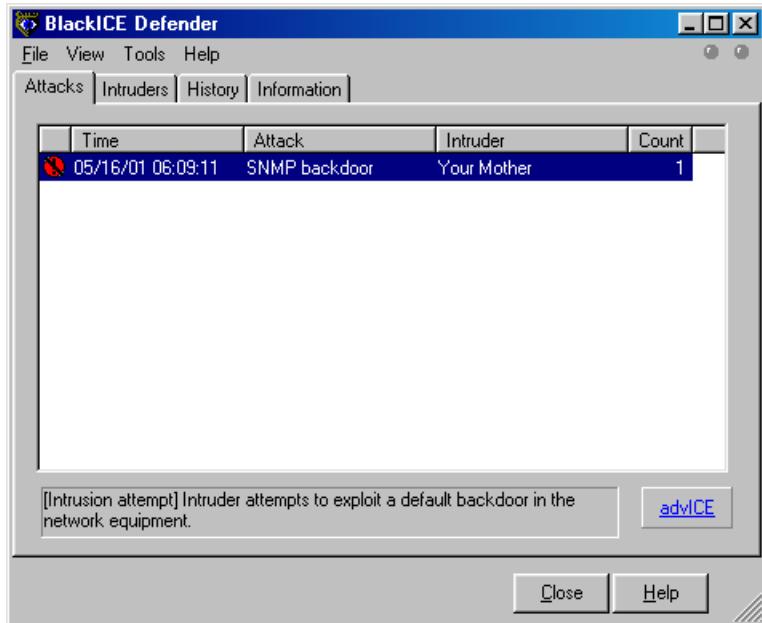
One probe commonly initiated by IDSs is reverse DNS query of the attacker's IP address. A domain name in an alert is more valuable than just an IP address, after all. Unfortunately, attackers who control their own rDNS (quite common) can watch the logs in real time and learn that they have been detected. This is a good time for attackers to feed misinformation, such as bogus names and cache entries to the requesting IDS.

Some IDSs go much further, and send more intrusive probes to the apparent attackers. When an attacker sees his target port scan him back, there is no question that he has set off alarms. Some IDSs send Windows NetBIOS information requests back to the attacker. ISS BlackIce Defender is one vendor that does (or at least did) this by default. I wrote a small tool called icepick which sends a simple packet that generates an alert from listening BlackIce instances. Then it watches for telltale NetBIOS queries and reports any BlackIce installations found. One could easily scan large networks looking for this IDS and then attempt to exploit them using holes discussed later in this chapter.

Not content with simply locating BlackIce installations or detecting them during penetration tests, I wrote a simple UNIX program called windentd which replies to the probe with misinformation. Figure 9-1 shows a BlackIce

console where the Intruder is listed as "Your Mother" thanks to windentd and icepick. Those simple tools are available from <http://www.insecure.org/presentations/CanSecWest01/>, though they are not supported.

**Figure 9-1. BlackIce discovers an unusual intruder**



### 9.5.1.2. Sudden firewall changes and suspicious packets

Many intrusion detection systems have lately morphed into what marketing departments label intrusion prevention systems. The best of these systems are inline on the network so that they can restrict packet flow when suspicious activity is detected. For example, they may block any further traffic from an IP address that they believe has port scanned them, or that has attempted a buffer overflow exploit. Attackers are likely to notice this if they port scan a system, then are unable to connect to the reported open ports. Attackers can confirm that they are blocked by trying to connect from another IP address.

Suspicious response packets can also be a tip-off that an attacker's actions have been flagged by an IDS. In particular, many IDSs that are *not* inline on the network will forge RST packets in an attempt to tear down connections. Ways to determine that these packets are forged are covered in Section 9.6.

### 9.5.1.3. Naming conventions

Naming conventions can be another giveaway of IDS presence. If an Nmap list scan returns host names such as realsecure, ids-monitor, or dragon-ids, you may have found an intrusion detection system. The admins might have given away that information inadvertently, or they may think of it like the alarm stickers on house and car windows. Perhaps they think that the script kiddies will be scared away by IDS-related names. It could also be misinformation. You can never fully trust DNS names. For example, you might assume that bugzilla.securityfocus.com is a web server running the popular Bugzilla web-based bug tracking software. Not so. The Nmap scan in Example 9-10 shows that it is probably a Symantec Raptor firewall instead. No web server is accessible.

**Example 9-10. Host names can be deceiving**

```
# nmap -sS -sV -T4 -p1-24 bugzilla.securityfocus.com

Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Interesting ports on 205.206.231.82:
(The 21 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp-proxy   Symantec Enterprise Firewall FTP proxy
22/tcp    open  ssh?        Symantec Raptor firewall secure gateway telnetd
23/tcp    open  telnet     Symantec Raptor firewall secure gateway telnetd

Nmap run completed -- 1 IP address (1 host up) scanned in 0.935 seconds
```

**9.5.1.4. Unexplained TTL jumps**

One more way to detect certain IDSs is to watch for unexplained gaps (or suspicious machines) in traceroutes. In Example 9-11, which was contrived for simplicity, traceroute locates nothing at hop 5. That may be an inline IDS or firewall protecting the target company. Of course, this can only detect inline IDSs. Even some of the inline devices may fail to decrement the TTL or may refuse to pass ICMP ttl-exceeded messages back from the protected network.

**Example 9-11. Noting TTL gaps with traceroute**

```
# traceroute www.target.com
traceroute to orestes.red.target.com (10.0.0.6), 30 hops max, 38 byte packets
 1 gw (205.217.153.49)  0.694 ms  0.641 ms  0.587 ms
 2 metrol-ge-152.pa.meer.net (205.217.152.1)  1.972 ms  1.413 ms  1.947 ms
 3 208.185.168.171 (208.185.168.171)  1.294 ms  1.853 ms  1.325 ms
 4 p4-2-0-0.r06.plalca01.us.bb.verio.net (129.250.9.129)  1.596 ms  1.779 ms  1.467 ms
 5 * * *
 6 orestes.red.target.com (10.0.0.6)  76.200 ms  76.180 ms  76.747 ms
#
```

**9.5.2. Avoiding intrusion detection systems**

The most subtle way to defeat intrusion detection systems is to avoid their watchful gaze entirely. The reality is that rules governing IDSs are pretty brittle in that they can often be defeated by manipulating the attack slightly. Attackers have dozens of techniques, from URL encoding to polymorphic shellcode generators for escaping IDS detection of their exploits. This section focuses on stealthy port scanning, which is even easier than stealthily exploiting vulnerabilities.

**9.5.2.1. Slow down**

When it comes to avoiding IDS alerts, patience is a virtue. Port scan detection is usually threshold based. The system watches for a given number of probes in a certain timeframe. This helps prevent false positives from innocent users. It is also essential to save resources -- saving connection probes forever would consume memory and make realtime list searching too slow. The downside to this threshold approach is that attackers can evade it by keeping their scan rate just below the threshold. Nmap offers several canned timing modes that can be selected with the `-T` option to

accomplish this. For example, the `-T paranoid` option causes Nmap to send just one probe at a time, waiting five minutes between them. A large scan may take weeks, but at least it probably will not be detected. The `-T sneaky` option is similar, but it only waits 15 seconds between probes.

Rather than specify canned timing modes such as `sneaky`, timing variables can be customized precisely with options such as `--max_parallelism`, `--min_rtt_timeout`, and `--scan_delay`. Chapter 6 describes these in depth.

#### 9.5.2.1.1. A practical example: bypassing default Snort 2.2.0 rules

Examining the handy open-source IDS Snort provides a lesson on sneaking under the radar. Snort has had several generations of port scan detectors. The latest, Flow-portscan, is quite formidable. A scan that slips by this is likely to escape detection by many other IDSs as well.

Flow-portscan is made up of two detection systems that can work in concert (or be enabled individually) to detect port scanners. The system and its dozens of configuration variables are documented in `docs/README.flow-portscan` (<http://cvs.snort.org/viewcvs.cgi/snort/doc/README.flow-portscan?rev=HEAD>) in the Snort distribution, but I'll provide a quick summary.

The simpler detection method in Flow-portscan is known as the *fixed time scale*. This simply watches for scanner-fixed-threshold probe packets in scanner-fixed-window seconds. Those two variables, which are set in `snort.conf`, each default to 15. Note that the counter includes any probes sent from a single machine to any host on the protected network. So quickly scanning a single port on each of 15 protected machines will generate an alert just as surely as scanning 15 ports on a single machine.

If this were the only detection method, the solution would be pretty easy. Pass the `--scan_delay 1075` option to ensure that Nmap waits 1.075 seconds between sending probes. The intuitive choice might be a one second wait between packets to avoid 15 packets in 15 seconds, but that is not enough. There are only 14 weights between sending the first packet and the fifteenth, so the wait must be at least  $15/14$ , or 1.07143 seconds. Some poor sap who chooses `--scan_delay 1000` would slow the scan down dramatically, while still triggering the alarm. If multiple hosts on the network are being probed, they must be scanned separately to avoid triggering the alarm. The option `--max_hostgroup 1` would insure that only one host at a time is scanned, but is not completely safe because it will not enforce the `--scan_delay` between the last probe sent to one host, and the first sent to the next. As long as at least 15 ports per host are being scanned, you could compensate by making the `--scan_delay` at least 1155ms, or simply start single-target Nmap instances from a shell script, waiting 1075ms between them. Example 9-12 shows such a stealthy scan of several machines on a network. Multiple Nmap instances are handled using the tcsh shell syntax. Here the IPs are specified manually. If many targets were desired, they could be enumerated into a file with the `-iL` (list scan) option, then Nmap started against each using a normal shell loop. The reason these scans took more than 1.075 seconds per port is that retransmissions were required for the filtered ports to ensure that they were not dropped due to network congestion.

#### Example 9-12. Slow scan to bypass the default Snort 2.2.0 Flow-portscan fixed time scan detection method

```

felix~# foreach target (205.217.153.53 205.217.153.54 205.217.153.55)
foreach? nmap --scan_delay 1075 -p21,22,23,25,53 $target
foreach? usleep 1075000
foreach? end

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Interesting ports on www.insecure.org (205.217.153.53):
PORT      STATE      SERVICE
21/tcp     filtered  ftp

```

```

22/tcp open      ssh
23/tcp filtered telnet
25/tcp open      smtp
53/tcp open      domain

```

Nmap run completed -- 1 IP address (1 host up) scanned in 10.746 seconds

```

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Interesting ports on lists.insecure.org (205.217.153.54):
PORT      STATE      SERVICE
21/tcp     filtered  ftp
22/tcp     open       ssh
23/tcp     filtered  telnet
25/tcp     open       smtp
53/tcp     open       domain

```

Nmap run completed -- 1 IP address (1 host up) scanned in 10.781 seconds

```

Starting nmap 3.70 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
PORT      STATE      SERVICE
21/tcp     filtered  ftp
22/tcp     open       ssh
23/tcp     filtered  telnet
25/tcp     open       smtp
53/tcp     open       domain

```

Nmap run completed -- 1 IP address (1 host up) scanned in 10.804 seconds

Unfortunately for port scanning enthusiasts, defeating Snort is not so simple. It has another method, known as *sliding time scale*. This method is similar to the fixed-window method just discussed, except that it increases the window whenever a new probe from a host is detected. An alarm is raised if scanner-sliding-threshold probes are detected during the window. The window starts at scanner-sliding-window seconds, and increases for each probe detected by the amount of time elapsed so far in the window times scanner-sliding-scale-factor. Those three variables default to 40 probes, 20 seconds, and a factor of 0.5 in snort.conf.

The sliding scale is rather insidious in the way it grows continually as new packets come in. The simplest (if slow) solution would be to send one probe every 20.1 seconds. This would evade both the default fixed and sliding scales. This could be done just as in Example 9-12, but using a higher value. You could speed this up by an order of magnitude by sending 14 packets really fast, waiting 20 seconds for the window to expire, then repeating with another 14 probes. You may be able to do this with a shell script controlling Nmap, but writing your own simple SYN scanning program for this custom job may be preferable.

### 9.5.2.2. Fragment packets

IP fragments can be a major problem for intrusion detection systems, particularly because the handling of oddities such as overlapping fragments and fragmentation assembly timeouts are ambiguous and differ substantially between platforms. So the IDS often has to guess at how the remote system will interpret a packet. Fragment assembly can also be resource intensive. For these reasons, many intrusion detection systems still do not support fragmentation very well. An Nmap scan will use tiny IP fragments if the `-f` is specified. Because some hosts do not handle

fragmented packets properly, run a sniffer like ethereal or tcpdump the first time you use this option to verify that packets leave your machine fragmented. Some overly helpful hosts will defragment the packets before they even leave the device.

### **9.5.2.3. Evade specific rules**

Most IDS vendors brag about how many alerts they support, but many (if not most) are easy to bypass. The most popular IDS among Nmap users is the open source Snort (<http://www.snort.org>). Example 9-13 shows all of the default rules in Snort 2.0.0 that reference Nmap.

#### **Example 9-13. Default Snort rules referencing Nmap**

```
felix~/src/snort-2.0.0/rules>grep -i nmap *
icmp.rules:alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICMP PING NMAP";
  dsize:0;itype: 8;reference:arachnids,162;classtype:attempted-recon;sid:469;rev:1;)
scan.rules:alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN nmap XMAS";
  flags:FPU; reference:arachnids,30; classtype:attempted-recon; sid:1228;rev:1;)
scan.rules:alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN nmap TCP";
  flags:A;ack:0; reference:arachnids,28; classtype:attempted-recon; sid:628;rev:1;)
scan.rules:alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN nmap fingerprint attempt";
  flags:SFP; reference:arachnids,05; classtype:attempted-recon; sid:629; rev:1;)
web-attacks.rules:alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
  (msg:"WEB-ATTACKS nmap command attempt"; flow:to_server,established;content:"nmap%20";
  nocase;sid:1361;classtype:web-application-attack; rev:4;)
```

Now let us look at these rules through the eyes of an attacker. The first rule looks for an ICMP ping packet without any payload (dsize:0). Simply specifying a non-zero --data\_length option, as discussed in Chapter 3, will defeat that rule. Or the user could specify a different type of ping scan entirely, such as TCP SYN ping.

The next rule searches for TCP packets with the FIN, PSH, and URG flags set (flags:FPU) and signals an Nmap XMAS scan alert. Adding the option --scanflags FINPSH to the XMAS scan flag will remove the URG flag. The scan will still work as expected, but the rule will fail to trigger.

The third rule in the list looks for TCP packets with the ACK bit set but an acknowledgment number of zero (flags:A;ack:0). Ancient versions of Nmap did this, but it was fixed in 1999 in response to the Snort rule.

Rule number four looks for TCP packets with the SYN, FIN, PSH, and URG flags set (flags:SFP). It then declares an Nmap OS Fingerprinting attempt. An attacker can avoid flagging this by omitting the -o flag. If he really wishes to do OS detection, that single test can be commented out in `osscan.cc`. The OS detection will still be quite accurate, but the IDS alert will not flag.

The final rule looks for people sending the string "nmap " to web servers. They are looking for attempts to execute commands through the web server. An attacker could defeat this by renaming Nmap, using a tab character instead of a space, or connecting with SSL encryption if available.

Of course there are other relevant rules that do not have Nmap in the name but could still be flagged by intrusive port scans. Advanced attackers install the IDS they are concerned with on their own network, then alter and test scans in advance to ensure that they do not trigger alarms.

Snort was only chosen for this example because its rules database is public and it is a fellow open source network security tool. Commercial IDSs suffer from similar issues.

#### **9.5.2.4. Avoid easily detected Nmap features**

Some features of Nmap are more conspicuous than others. In particular, version detection connects to many different services, which will often leave logs on those machines and set off alarms on intrusion detection systems. OS detection is also easy to spot by intrusion detection systems, because a few of the tests use rather unusual packets and packet sequences. The Snort rules shown in Example 9-13 demonstrate a typical Nmap OS detection signature.

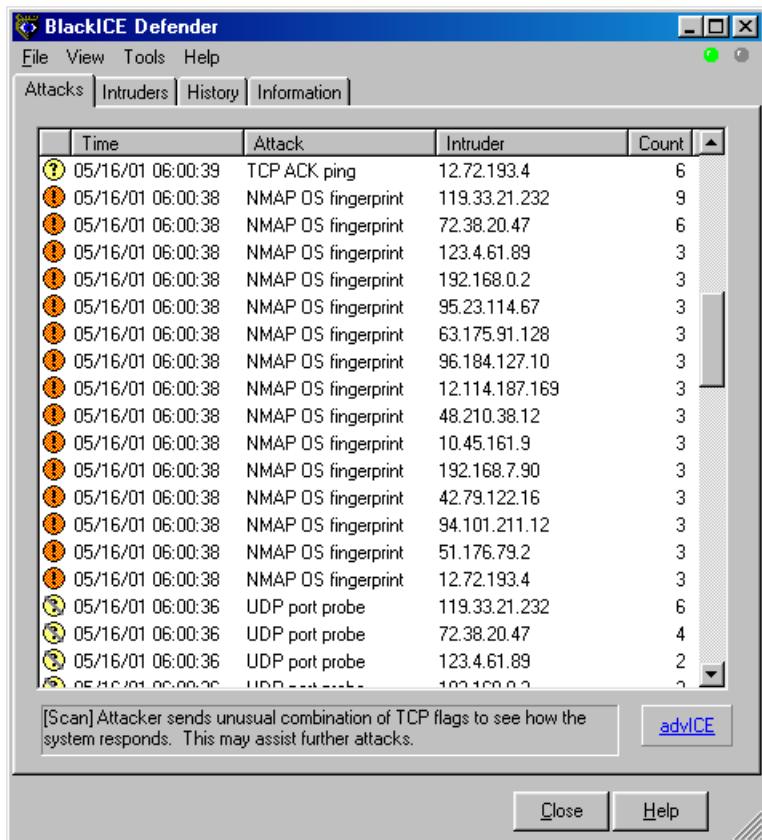
One solution for pen-testers who wish to remain stealthy is to skip these conspicuous probes entirely. Service and OS detection are valuable, but not essential for a successful attack. They can also be used on a case-by-case basis against machines or ports that look interesting, rather than flooding the whole target network with them.

### **9.5.3. Misleading intrusion detection systems**

The previous section discussed using subtlety to avoid the watchful eye of intrusion detection systems. An alternative approach is to actively mislead or confuse the IDS with packet forgery. Nmap offers numerous options for effecting this.

#### **9.5.3.1. Decoys**

Street criminals know that one effective means for avoiding authorities after a crime is to melt into any nearby crowds. The cops may not be able to tell the purse snatcher from all of the innocent passersby. In the network realm, Nmap can construct a scan that appears to be coming from dozens of hosts across the world. The target will have trouble determining which host represents the attackers, and which ones are innocent decoys. While this can be defeated through router path tracing, response-dropping, and other "active" mechanisms, it is generally an extremely effective technique for hiding the scan source. Figure 9-2 shows a BlackICE report screen that is inundated with decoys. The administrator cannot complain to the providers for every ISP on the list. It would take a long time, and all but one of the hosts are innocent.

**Figure 9-2.** An attacker masked by dozens of decoys

Decoys are added with the `-D` option. The argument is a list of hosts, separated by commas. The string `ME` can be used as one of the decoys to represent where the true source host should appear in the scan order. Otherwise it will be a random position. Including `ME` in the 6th position or further in the list prevents some common port scan detectors from reporting the activity. For example, Solar Designer's excellent Scanlogd only reports the first five scan sources to avoid flooding its logs with decoys.

Note that the hosts used as decoys should be up and running. It would be pretty easy to determine which host is scanning if only one is actually up on the network. Using too many down decoys can also cause target ports to become temporarily unresponsive, due to a condition known as a SYN flood. Using IP addresses instead of names is advised to avoid appearing in the decoy networks' nameserver logs. The targets themselves should ideally be expressed by IP addresses too.

Decoys are used both in the initial ping scan (using ICMP, SYN, ACK, or whatever) and during the actual port scanning phase. Decoys are also used during remote OS detection. They are not used for DNS queries or service/version detection. Using too many decoys can slow a scan dramatically, and sometimes even make it less accurate. Many retail (dialup, cable modem, DSL, etc.) ISPs filter out most spoofed packets, though spoofed packets from the same network range as yours may get through. Do some tests first against some machine you control across the Internet, or you could even test this against 3rd party servers using IPID tricks similar to those discussed in Section 9.3.3.

### 9.5.3.2. Port scan spoofing

While a huge group of decoys is quite effective at hiding the true source of a port scan, the IDS alerts will make it obvious that someone is using decoys. A more subtle, but limited, approach is to spoof a port scan from a single address. Specify the `-s` followed by a source IP, and Nmap will launch the requested port scan from that given source. No useful Nmap results will be available, since the target will respond to the spoofed IP, which Nmap will not see. IDS alarms at the target will blame the spoofed source for the scan. You may have to specify `-e interfacename` to select the proper interface name (such as `eth0`, `ppp0`, etc.) for Nmap to send the spoofed packets through. This can be useful for framing innocent parties, casting doubt in the administrator's mind about the accuracy of his IDS, and denial of service attacks that will be discussed in Section 9.5.3.4.

### 9.5.3.3. Idlescan

Idlescan is a clever technique that allows for spoofing the source IP address, as discussed in the previous section, while still obtaining accurate TCP port scan results. This is done by abusing properties of the IP identification field as implemented by many systems. It is described in much more depth in Chapter 5.

### 9.5.3.4. DOS attacks against reactive systems

Many vendors are pushing what they call intrusion *prevention* systems. These are basically IDSs that can actively block traffic and reset established connections that are deemed malicious. These are usually inline on the network or host-based, for greater control over network activity. Other (non-inline) systems listen promiscuously and try to deal with suspicious connections by forging TCP RST packets. In addition to the traditional IPS vendors that try to block a wide range of suspicious activity, many popular small programs such as Port Sentry (<http://sourceforge.net/projects/sentrytools/>) are designed specifically to block port scanners.

While blocking port scanners may at first seem like a good idea, there are many problems with this approach. The most obvious one is that port scans are usually quite easy to forge, as previous sections have demonstrated. It is often easy for attackers to tell when this sort of software is in place, because they will not be able to connect to purportedly open ports after doing a port scan. They will try again from another system and successfully connect, confirming that the original IP was blocked. Attackers can then use the host spoofing techniques discussed previously (`-s` option) to cause the target host to block any systems the attacker desires. This may include important DNS servers, major web sites, software update archives, mail servers, and the like. It probably would not take long to annoy the legitimate administrator enough to disable reactive blocking. While most such products offer a whitelist option to prevent blocking certain important hosts, enumerating them all is extraordinarily difficult. Attackers can usually find a new commonly used host to block, annoying users until the admin determines the problem and adjusts the whitelist accordingly.

## 9.5.4. Exploiting intrusion detection systems

The most audacious way to subvert intrusion detection systems is to hack them. Many commercial and open source vendors have pitiful security records of product exploitability. Internet Security System's flagship RealSecure and BlackICE IDS products had a vulnerability which allowed the Witty worm to compromise more than ten thousand installations, then attempted to disable them by random filesystem corruption. Other IDS and firewall vendors such as Cisco, Checkpoint, Netgear, and Symantec have suffered serious remotely exploitable vulnerabilities as well. Open source sniffers have not done much better, with exploitable bugs found in Snort, Ethereal, TCPdump, fakebo,

and many others. Denial of service attacks that crash the IDS (often with a single packet) are even more common than these privilege escalation vulnerabilities. A crashed IDS will not detect any Nmap scans.

Given all of these vulnerabilities, exploiting the IDS may be the most viable way into the target network. A nice aspect of this approach is that you do not even have to find the IDS. Sending a rogue packet to any "protected" machine on the network is usually enough to trigger these IDS bugs.

### **9.5.5. Ignoring intrusion detection systems**

While advanced attackers will often employ IDS subversion techniques described in this chapter, the much more common novice attackers (script kiddies) rarely concern themselves with IDSs. Many companies do not even deploy an IDS, and those that do often have them misconfigured or pay little attention to the alerts. An Internet-facing IDS will see so many attacks from script kiddies and worms that a few Nmap scans to locate a vulnerable service are unlikely to raise any flags.

Even if such an attacker compromises the network, is detected by a monitored IDS, and then kicked out of the systems, that is a small loss. Hacking is often a numbers game for them, so losing one compromised network out of thousands is inconsequential. Such a well-patrolled network would have likely quickly noticed their planned usage (such as denial of service attacks, mass scanning, or spam sending) quickly and shut them down anyway. They want to compromise negligently administered and poorly monitored networks that will long-lasting nodes of criminal activity.

Being tracked down and prosecuted is rarely a concern of the IDS-ignoring set. They usually launch attacks from other compromised networks, which are often several globe-spanning hops away from their true location. Or they may use anonymous connectivity such as provided by some Internet cafes, school computer labs, or the prevalent open wireless access points. Throwaway dialup accounts are also commonly used. Even if they get kicked off, signing up again with another (or the same) provider takes only minutes. Many attackers come from Romania, China, South Korea, and other countries where prosecution is highly unlikely.

Internet worms are another class of attack that rarely bothers with IDS evasion. As with script kiddies, the brute force and shameless scanning of millions of IP addresses often leads to more compromises per hour than a careful, targeted approach that emphasizes stealth.

While most attacks make no effort at stealth, the fact that most intrusion detection systems are so easily subverted is a major concern. Skilled attackers are a small minority, but are often the greatest threat. Do not be lulled into complacency by the large number of alerts spewed from IDSs. They cannot detect everything, and often miss what is most important.

Even skilled hackers sometimes ignore IDS concerns for initial reconnaissance. They simply scan away from some untraceable IP address, hoping to blend in with all of the other attackers and probe traffic on the Internet. After analyzing the results, they may launch more careful, stealthy attacks from other systems.

## **9.6. Detecting packet forgery by firewall and intrusion detection systems**

Previous sections mentioned that some firewall and intrusion detection systems can be configured to forge packets as if they came from one of the protected systems behind the device. TCP RST packets are a frequent example. Load balancers, SSL accelerators, network address translation, and certain honeynets can also lead to confusing or inconsistent results. Understanding how Nmap interprets responses helps a great deal in piecing together complex

remote network topologies. When Nmap reports unusual or unexpected results, you can add the `--packet_trace` option to see the raw packets upon which Nmap based its conclusions. In perplexing situations, you may have to go even further and launch custom probes and analyze packets with other tools such as hping2 and ethereal. The goal is often to find inconsistencies that help you understand the actual network setup. The following sections describe several useful techniques for doing so. While most of these tests do not involve Nmap directly, they can be useful for interpreting unexpected Nmap results.

### 9.6.1. Look for TTL consistency

Firewalls, load balancers, NAT gateways, and similar devices are usually located one or more hops in front of the machines they are protecting. In this case, packets can be created with a TTL such that they reach the network device but not the end host. If a RST is received from such a probe, it must have been sent by the device.

During one informal assessment, I scanned the network of a large magazine publisher over the Internet. Almost every IP address showed port 113 closed. Suspecting RST forgery by a firewall, I dug a bit deeper. Because it contained open, closed, and filtered ports, I decided to focus on this host in particular<sup>1</sup>:

```
# nmap -sS -P0 -T4 -F mx.chi.example.com
Starting nmap 3.51-TEST3 ( http://www.insecure.org/nmap/ )
Interesting ports on mx.chi.example.com (xx.yy.143.4):
(The 1216 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE
25/tcp    open  smtp
113/tcp   closed auth

Nmap run completed -- 1 IP address (1 host up) scanned in 53.196 seconds
```

Is port 113 really closed, or is the firewall spoofing RST packets? I counted the distance (in network hops) to ports 25 and 113 using the custom traceroute mode of the free hping2 utility, as shown in Example 9-14. I could have used the Nmap `--ttl` option to do this, but hping2 is designed for this exact purpose.

#### Example 9-14. Detection of closed and filtered TCP ports

```
# hping2 -t 5 --traceroute -p 25 -S mx.chi.example.com
[ combined with results from hping2 -i 1 --ttl \* -p 25 -S mx.chi.example.com ]
5->TTL 0 during transit from 64.159.2.97 (ae0-54.mp2.SanJose1.Level3.net)
6->TTL 0 during transit from 64.159.1.34 (so-3-0-0.mp2.Chicago1.Level3.net)
7->TTL 0 during transit from 200.247.10.170 (pos9-0.core1.Chicago1.level3.net)
8->TTL 0 during transit from 200.244.8.42 (gige6-0.ipcolo1.Chicago1.Level3.net)
9->TTL 0 during transit from XX.YY.73.205 (ge1-0.br1.ord.example.net)
10->TTL 0 during transit from XX.YY.228.247 (f0-0.bl.chi.example.com)
11->No response
12->TTL 0 during transit from XX.YY.143.130 (fw.chi.example.com)
13->46 bytes from XX.YY.143.4: flags=SA seq=0 ttl=52 id=48957 rtt=75.8 ms

# hping2 -t 5 --traceroute -p 113 -S mx.chi.example.com
[ results augmented again ]
5->TTL 0 during transit from 64.159.2.97 (ae0-54.mp2.SanJose1.Level3.net)
6->TTL 0 during transit from 64.159.1.34 (so-3-0-0.mp2.Chicago1.Level3.net)
7->TTL 0 during transit from 200.247.10.170 (pos9-0.core1.Chicago1.level3.net)
8->TTL 0 during transit from 200.244.8.42 (gige6-0.ipcolo1.Chicago1.Level3.net)
9->TTL 0 during transit from XX.YY.73.205 (ge1-0.br1.ord.example.net)
```

```
10->TTL 0 during transit from XX.YY.228.247 (f0-0.b1.chi.example.com)
11->Nothing
12->46 bytes from XX.YY.143.4: flags=RA seq=0 ttl=48 id=53414 rtt=75.0 ms
```

This custom traceroute shows that reaching open port 25 requires 13 hops. 12 hops away is a firewall in Chicago, helpfully named fw.chi.example.com. One would expect different ports on the same machine to be the same hop-distance away. Yet port 113 responds with a RST after only 12 hops. That RST is being forged by fw.chi.example.com. Since the firewall is known to forge port 113 responses, those packets should not be taken as an indicator that a host is available at a given IP address. I found available hosts by ping scanning the network again, using common probe types such as ICMP echo requests (-PE) and SYN packets to ports 22 and 80 (-PS22,80), but omitting any ping probes involving TCP port 113.

### **9.6.2. Look for IPID and sequence number consistency**

Every IP packet contains a 16-bit identification field that is used for defragmentation. It can also be exploited to gain a surprising amount of information on remote hosts. This includes port scanning using the Nmap Idle Scan technique, traffic estimation, host alias detection, and much more. It can also help to detect many network devices, such as load balancers. I once noticed strange OS detection results when scanning beta.search.microsoft.com. So I launched hping2 SYN probes against TCP port 80 to learn what was going on. Example 9-15 shows the results.

#### **Example 9-15. Testing IPID sequence number consistency**

```
hping2 -c 10 -i 1 -p 80 -S beta.search.microsoft.com.
HPING beta.search.microsoft.com. (eth0 207.46.197.115): S set, 40 headers
46 bytes from 207.46.197.115: flags=SA seq=0 ttl=56 id=57645 win=16616 rtt=21.2 ms
46 bytes from 207.46.197.115: flags=SA seq=1 ttl=56 id=57650 win=16616 rtt=21.4 ms
46 bytes from 207.46.197.115: flags=RA seq=2 ttl=56 id=18574 win=0 rtt=21.3 ms
46 bytes from 207.46.197.115: flags=RA seq=3 ttl=56 id=18587 win=0 rtt=21.1 ms
46 bytes from 207.46.197.115: flags=RA seq=4 ttl=56 id=18588 win=0 rtt=21.2 ms
46 bytes from 207.46.197.115: flags=SA seq=5 ttl=56 id=57741 win=16616 rtt=21.2 ms
46 bytes from 207.46.197.115: flags=RA seq=6 ttl=56 id=18589 win=0 rtt=21.2 ms
46 bytes from 207.46.197.115: flags=SA seq=7 ttl=56 id=57742 win=16616 rtt=21.7 ms
46 bytes from 207.46.197.115: flags=SA seq=8 ttl=56 id=57743 win=16616 rtt=21.6 ms
46 bytes from 207.46.197.115: flags=SA seq=9 ttl=56 id=57744 win=16616 rtt=21.3 ms
```

Looking at the sequence of IPID numbers (in bold), it is clear that there are really 2 machines sharing this IP address through some sort of load balancer. One has IPID sequences in the range of 57K, while the other is using 18K. Given this information, it is no wonder that Nmap had trouble settling on a single operating system guess. They may be running on very different systems.

Similar tests can be performed on other numeric fields, such as the TCP timestamp option or the initial sequence number returned by open ports.

### **9.6.3. The Bogus Checksum trick**

Another handy trick for determining whether an IDS or Firewall is spoofing response packets is to send probes with a bogus checksum. Essentially all end hosts check the checksum before further processing and will not respond to these corrupt packets. Firewalls, on the other hand, often omit this check. Packets returned from corrupt-checksum

probes can be assumed spoofed. This technique is further described in Phrack 60, article 12 (<http://www.phrack.org/phrack/60/p60-0x0c.txt>).

#### **9.6.4. Close Analysis of packet headers and contents**

It is surprising how many elements can differ in even a small TCP header. Refer to Chapter 8 for dozens of subtle details that can be indicative of a different OS. For example, different systems respond with different TCP options, RST packet text, type of service, etc. If there are several systems behind a load balancer, or the packets are being sent by firewall or intrusion detection systems, the packets will rarely match exactly.

#### **9.6.5. Unusual network uniformity**

When response packets are sent by a firewall, they are often more uniform than would be expected from clusters of individual machines. While scanning the large magazine company discussed in the previous TTL-checking section, I found that hundreds of sequential-IP machines responded with a RST to port 113. In a real cluster of machines, you would expect at least a couple to be out at a given time. Additionally, I was unable to elicit any other type of response from most of these addresses. This suspicious result led me to do the TTL tests which showed that fw.chi.example.com was actually spoofing the RST packets.

## **Notes**

1. Host names and IPs have been disguised slightly

# Chapter 10. Defenses against Nmap

## 10.1. Introduction

Chapter 9 discussed the myriad ways that Nmap (along with a few other open source security tools) can be used to slip through firewalls and outsmart intrusion detection systems. Now we look at the situation from the other side of the fence. How technology such as firewalls and IDSs can defend against Nmap. Possible defenses include blocking the probes, restricting information returned, slowing down the Nmap scan, and returning misleading information. The dangers of some defenses are covered as well. Obfuscating your network to the extent that attackers cannot understand what is going on is not a net win if your administrators no longer understand it either. Similarly, defensive software meant to confuse or block port scanners is not beneficial if it opens up more serious vulnerabilities itself. Many of the techniques described herein protect against active probes in general, not just those produced with Nmap.

## 10.2. Proactive Scanning

It is often said that the best defense is a good offense. An excellent way to defend against attackers is to think like them. Scan your networks regularly, and carefully analyze the output for vulnerabilities. Use crontab on UNIX, or the Task Scheduler on Windows, with a system such as NDiff or Nmap-report (see Section 1.2.3)

- \* Consider changing reference to section on automating scans and tracking differences between them, if and when available to notify you of any changes.

Proactive scanning provides the opportunity to find and fix vulnerabilities before attackers do. It also makes you better aware of what information attackers can obtain. When you have reviewed the results yourself for weaknesses and are comfortable with your security posture, port scanners become much less threatening. The people who are most paranoid about port scanners and employ the most defensive and detection software are often those with the least confidence in their network security. I do not want to dissuade anyone from using the techniques described throughout this chapter, but only to suggest that they first seek out and fix any existing network vulnerabilities. Fixing a hole is far more effective than trying to hide it. That approach is also less stressful than constantly worrying that attackers may find the vulnerabilities. Once known holes are patched and proactive scanning is in place, further defensive technology may be warranted to protect against zero-day exploits, internal threats, and any holes that your vulnerability analysis system may miss.

Remember that some poorly implemented and tested systems may react adversely to port scans, OS detection, or version detection. This is rarely a problem when scanning over the Internet, because machines that crash when scanned do not last long in the hostile Internet. Internal machines are often more fragile. When beginning a proactive scanning program, ensure that it is approved and communicated to affected parties in advance. Start with a relatively small part of the network and insure there are no problems, then take it further in stages. You may want to start with simple port scanning, then move on to OS detection or version detection later as desired.

## 10.3. Blocking and Slowing Nmap with Firewalls

One of the best defensive measures against scanning is a well-configured firewall. Rather than simply obfuscate the network configuration, as some techniques described later do, well-configured firewalls can effectively block many avenues of attack.

Any decent firewall book emphasizes this cardinal rule: deny by default. Rather than trying to block suspected malicious traffic, block everything first, then specifically override that to allow essential traffic. It is much easier to overlook blocking something malicious than to accidentally explicitly allow the same. Additionally, failing to block bad traffic may not be noticed until it is exploited by an attacker, while failing to allow legitimate traffic is usually quickly discovered by the affected users. And they will keep reminding you until it is fixed.

The two preceding reasons should be enough to convince anyone to go with deny-by-default, but there are other benefits as well. One is to slow down large scale reconnaissance from tools like Nmap. When an Nmap TCP SYN scan encounters a closed port, the target machine sends back a RST packet and that port status is determined in only one round-trip-time. That is under a quarter of a second even across the world from my webserver in California to an ISP in Moscow. If a firewall filters the port, on the other hand, Nmap has to wait for a worst-case timeout before giving up. Nmap then makes several retransmissions just in case the packet was dropped by some router due to overcapacity rather than by a firewall rule. In large-scale scans, the difference can be quite significant. For example, a 1660-port TCP SYN scan against a machine on my wireless network (**nmap -sS -T4 para**) takes only 5 seconds when all ports are open or closed. Filtering a dozen or so commonly exploited ports increases the scan time to 12 seconds. Moving to default-deny (filtering all ports except the 5 open ones) nearly triples the scan time to 33 seconds. A 28-second difference may not sound meaningful, but it can add up to extra days for large-scale scans.

Filtered ports are even more frustrating to attackers when the UDP protocol is used. When firewalling is not involved, virtually all systems respond with an ICMP port unreachable when Nmap probes a closed port. Open ports usually do not respond at all. So if a deny-by-default firewall drops a probe packet, Nmap cannot tell if the port is open or filtered. Retransmissions do not help here, as the port will never respond. Attackers must then resort to slower and much more conspicuous techniques such as Nmap version detection and SNMP community string brute forcing to make sense of the UDP ports.

To actually slow Nmap down, make sure the firewall is dropping the packets rather than responding with an ICMP error. Otherwise Nmap will run just as fast and accurately as if the ports were closed, though you still reap the benefit of blocking the probes. As an example of this distinction, the Linux iptables firewall offers the target actions DROP and REJECT. As the names imply, DROP does nothing beyond blocking the packet, while REJECT sends an error message back. The former is better for slowing down reconnaissance and is usually recommended, though REJECT can ease network trouble diagnosis by making it crystal clear that the firewall is blocking certain traffic.

Another tenet of firewalls is *defense in depth*. Even though ports are blocked by the firewall, make sure they are closed (no application is listening) anyway. Assume that a determined attacker will eventually breach the firewall. Even if they get through using a technique from Chapter 9, the individual machines should be locked down to present a strong defense. This leaves more room for mistakes, which everyone makes on occasion. Attackers will need to find weaknesses in both the firewall and individual machines. A port scanner is pretty impotent against ports that are both closed and filtered. Using private address space (such as with network address translation) and additional firewalls provide even more protection.

## 10.4. Detecting Nmap Scans

Some people believe that detecting port scans is a waste of time. They are so common that any organization connected to the Internet will be regularly scanned. Very few of these represent targeted attacks. Many are Internet worms endlessly pounding away seeking some Windows vulnerability or another. Some scans come from Internet research projects, others from curious or bored individuals exploring the Internet. I scanned tens of thousands of IPs seeking good examples and empirical data for this book. Other scans actually are malicious. Script kiddies regularly scan huge ranges for systems susceptible to their exploit du jour. While these folks have bad intentions, they are likely to move along on their own after finding no vulnerable services on your network. The biggest threat are

attackers specifically targeting your organization, though those represent such a small percentage of detected scans that they are extremely tough to distinguish. So many admins do not even bother recording port scans.

Other administrators take a different view. They contend that port scans are often precursors to attacks, and should at least be logged if not responded to. They often place detection systems on internal networks to reduce the flood of Internet port scan activity. The logs are sometimes analyzed for trends, or submitted to 3rd parties such as Dshield for world-wide correlation and analysis. Sometimes extensive logs and scary graphs measuring attacks are submitted to management to justify adequate budgets.

System logs alone are rarely sufficient for detecting port scans. Usually only scan types that establish full TCP connections are logged, while the default Nmap SYN scan sneaks through. Even full TCP connections are only logged if the particular application explicitly does so. Such error messages, when available, are often cryptic. However, a bunch of different services spouting error messages at the same time is a common indicator of scanning activity. Intrusive scans, particularly those using Nmap version detection, can often be detected by this means. But only if the administrators actually read the system logs regularly. The vast majority of log messages go forever unread. Log monitoring tools such as Logwatch (<http://www.logwatch.org>) and Swatch (<http://swatch.sourceforge.net/>) can certainly help, but the reality is that system logs are only marginally effective at detecting Nmap activity.

Special purpose port scan detectors are a more effective approach to detecting Nmap activity. Two common examples are PortSentry (<http://sourceforge.net/projects/sentrytools/>) and Scanlogd (<http://www.openwall.com/scanlogd/>). Scanlogd has been around since 1998 and was carefully designed for security. No vulnerabilities have been reported during its lifetime. PortSentry offers similar features, as well as a reactive capability that blocks the source IP of suspected scanners. Note that this reactive technique can be dangerous, as demonstrated in Section 10.5.6.

Despite being subject to threshold-based attacks discussed in Chapter 9, these port scan detection tools work pretty well. Yet the type of administrator who cares enough to keep tabs on port scans will also want to know about more serious attacks such as exploit attempts and installed backdoors. For this reason, intrusion detection systems that alert on a wide range of suspicious behavior are more popular than these special-purpose tools.

Many vendors now sell intrusion detection systems, but Nmap users gravitate to an open source lightweight IDS named Snort. It ranked as the third most popular security tool among a survey group of 1800 Nmap users.

\* *Note favorite tools appendix if I decide to add it.*

Like Nmap, Snort is improved by a global community of developers. It supports more than two thousand rules for detecting all sorts of suspicious activity, including port scans.

A properly installed and monitored IDS can be a tremendous security asset, but do not forget the risks discussed in Chapter 9. Snort has had multiple remotely exploitable vulnerabilities, and so have many of its commercial competitors. Additionally, a skilled attacker can defeat most IDS rules, so do not let your guard down. IDSs too often lead to a false sense of security.

## 10.5. Clever Trickery

Nmap, like other active probing tools, obtains its information by sending out packets to target systems and then trying to interpret and organize any responses into useful reports. Nmap must rely on information from systems and networks that may be downright hostile environments. Some administrators take offense at being scanned, and a small percentage try to confuse or slow Nmap with active measures beyond the firewall and IDS techniques discussed previously.

Many of these active response methods are quite clever. I would argue that many are too clever, causing more problems than they solve. One such problem is exploitability. Much of this custom active response software is just a

quick hack, written without careful security consideration. For example, an administrator friend of mine named Paul was quite proud of installing FakeBO on his machine. He laughed at the prospect of fooling script kiddies into thinking they found a Back Orifice infected machine to commandeer, when Paul was really just logging their attempts. The joke was on Paul when a FakeBO buffer overflow was discovered and an attacker used it to compromise his box and install a real backdoor.

The other major risk common to these technologies is displacement of time that is better spent elsewhere. Confusing attackers can be fun and gratifying, and in some cases even hampers attacks. But in the end, these techniques are mostly security by obscurity. That can still be beneficial, but is not as important as more resilient technologies such as firewalls and vulnerability patching. Advanced attackers will likely see through the obfuscation anyway, and the script kiddies and worms rarely bother with reconnaissance. The daily attempted ISS exploits against my Apache webserver are testament to that. These techniques should be considered only when you are already highly confident of your security posture. Too many people use them as a substitute to truly securing their networks.

### 10.5.1. Hiding Services on Obscure Ports

Occasionally administrators advocate running services on unusual ports to make it harder for attackers to find them. In particular, they note the frequency of single-port sweeps across their address space from attackers seeking out a vulnerable version of some software. Autonomous worms frequently do the same thing.

It is true that this sort of obfuscation may prevent some worms and script kiddies from finding services, but they are rarely more than a marginal threat to companies that quickly patch vulnerabilities. And companies who do not patch quickly will not be saved by this simple port obfuscation. Proponents often argue that even more skillful attackers will fall for this. Some have even posted to security lists that scanning all 65,536 TCP ports is inconceivable. They are wrong. Attackers can and do scan all TCP ports. In addition, techniques such as Nmap version detection make it easy to determine what service is listening on an unusual port. Example 10-1 shows such a scan. Notable is that it only takes 8 minutes, and this is from a slow residential aDSL line in another state. From a faster machine, the same scan takes only 3 minutes. If the default state had been filtered, the scan would have been slower but not unreasonably so. Even if a scan takes 10 or 20 minutes, an attacker does not have to sit around watching. A targeted attack against a company can easily be left overnight, and mass attackers may leave a scanner running for weeks, periodically downloading the latest data files.

#### Example 10-1. An all-tcp-port version scan

```
# nmap -sSV -T4 -O -p0-65535 apollo.sco.com

Starting nmap 3.50 ( http://www.insecure.org/nmap/ )
Interesting ports on apollo.sco.com (216.250.128.35):
(The 65524 ports scanned but not shown below are in state: closed)
PORT      STATE     SERVICE      VERSION
0/tcp      filtered  unknown
21/tcp     open      ftp          WU-FTPD 2.1WU(1)+SCO-2.6.1+-sec
22/tcp     open      ssh          SSH 1.2.22 (protocol 1.5)
199/tcp    open      smux?
457/tcp    open      http         NCSA httpd 1.3
615/tcp    open      http         NCSA httpd 1.5
1035/tcp   filtered unknown
1521/tcp   open      oracle-tns Oracle DB Listener 2.3.4.0.0 (for SCO System V/386)
13722/tcp  open      inetd        inetd (failed exec /usr/openv/netbackup/bin/bpjjava-msvc)
13782/tcp  open      inetd        inetd (failed exec /usr/openv/netbackup/bin/bpcd)
13783/tcp  open      inetd        inetd (failed exec /usr/openv/bin/vopied)
```

```

64206/tcp open    unknown
Device type: general purpose
Running: SCO UnixWare
OS details: SCO UnixWare 7.0.0 or OpenServer 5.0.4-5.0.6

Nmap run completed -- 1 IP address (1 host up) scanned in 501.897 seconds
#

```

The biggest downside to this approach is a major inconvenience to legitimate users. Some services, such as smtp and dns, almost always have to run on their well-known ports for practical reasons. Even for services such as http and ssh that can be more easily changed, doing so means that all users must remember an unusual port number such as 52,147 whenever they connect to the service. When there are several "hidden" services, it is particularly difficult to remember which is which. Using different ports on each machine becomes even more confusing, but standardizing on unusual port mappings across the organization reduces the purported benefit of this scheme. Attackers may notice that ssh is always at 52,147. The end result is that all-port Nmap scans against your servers may increase, as frustrated legitimate users try to find where essential services are hidden. Less savvy users may flood you with phone calls instead.

### 10.5.2. Port knocking

A technique called port knocking has recently become popular as a way to hide services from potential attackers. The method is well described on the front page of <http://www.portknocking.org/>:

Port knocking is a method of establishing a connection to a networked computer that has no open ports. Before a connection is established, ports are opened using a port knock sequence, which is a series of connection attempts to closed ports. A remote host generates and sends an authentic knock sequence in order to manipulate the server's firewall rules to open one or more specific ports. These manipulations are mediated by a port knock daemon, running on the server, which monitors the firewall log file for connection attempts that can be translated into authentic knock sequences. Once the desired ports are opened, the remote host can establish a connection and begin a session. Another knock sequence may be used to trigger the closing of the port.

This method is not brand new, but it exploded in popularity in 2003 when Martin Krzywinski coined the name port knocking, wrote an implementation, created the extensive web site, and wrote articles about it for Sys Admin and Linux Journal magazines. Port Knocking adds a second layer of protection to services, though authentication is usually weaker than that provided by primary services such as ssh. Implementations are usually subject to sniffing and replay attacks, and often suffer from brute force and denial of service threats as well.

The upside is a service concealment which is much stronger than the simple and ineffective obscure ports technique described previously. A port competently hidden through port knocking is nearly impossible to discover using active probes such as those sent by Nmap. On the other hand, sniffer-based systems such as intrusion detection systems and passive network mappers trivially detect this scheme.

Deciding whether to implement port knocking requires an analysis of the benefits and costs applicable to the proposed implementation. Service concealment is only beneficial for a small set of applications. The white-hat motivation is to prevent attackers from connecting to (and exploiting) vulnerable services, while still allowing connections from authorized users all over the world. If only certain IP addresses need to connect, firewall restrictions limiting connections to those specific IPs are usually a better approach. In an ideal world, applications would securely handle authentication themselves and there would be no need to hide them to prevent exploitation. Unfortunately, even security-conscious programs such as ssh have suffered numerous remotely exploitable

pre-authentication flaws. While these bugs should be fixed as soon as possible in any case, port knocking may provide an extra window of time before a new bug is exploited. After all, some ssh exploits spread underground long before official patches were available. Then when a bug is announced, even the most conscientious administrator may require several hours or days to learn about the bug, test the fix, and locate and patch all vulnerable instances. The response time of a home computer owner may be even longer. After all, the vast majority of computer users do not subscribe to Bugtraq.

The good guys are not the only ones who benefit from service concealment. It is at least as popular (if not more so) for gray hat and downright criminal uses. Many ISPs restrict users from running any server daemons such as web or ssh services. Customers could hide a personal sshd or web server (only for very limited use, as the public could not easily connect) using port knocking technology. Similarly, my friend Tom's employer only permitted connections from home using a Windows-only VPN client. Tom responded by setting up a port knocking system (before it was called that) which, upon receiving the appropriate probes, set up a reverse ssh tunnel from his work server back to his home Linux box. This allowed him to work from home with full access to the work network and without having to suffer the indignities of using Windows. It is worth re-iterating that the service provider in both the ISP and employer examples could have detected the subterfuge using a sniffer. Segueing into even darker uses, computer criminals frequently use techniques like these to hide backdoors in systems that they have compromised. Script kiddies may just leave a blatant ssh daemon or even raw root shell listening on some high port, vulnerable to detection by the next Nmap scan. More cautious attackers use concealment techniques including port knocking in their backdoors and rootkits.

While the service concealment provided by this system can be valuable, it comes with many limitations. Services intended for public use are inappropriate, since no one is going to install a special knock client just to visit your web site. In addition, publicizing the access instructions would defeat the system's primary purpose. Non-public service should usually be blocked by a firewall rather than shielded with port knocking. When a group of people need access, VPNs are often a better solution as they offer encryption and user-level access control. VPNs are also built to handle real-world networks, where packets can be dropped, duplicated, and re-ordered. A relatively simple probe using the Portknocking.Org implementation can require more than 30 port probes, all of which must arrive at the destination in order. For this many probes, you will need a special client. Using **telnet** or a web browser is too tedious. Additionally, all firewalls in the path must allow you to connect to these unusual ports. Given these restrictions and hassles, using a VPN may be just as convenient.

An additional risk is that port knocking implementations are still immature. The best-known one, written by Martin Krzywinski, warns on the download page that "this is a prototype and includes the bare minimum to get started. Do not use this for production environments." Also remember that proactive scanning to inventory your own network will be more difficult with programs such as this installed.

Do not let this long list of limitations dissuade you from even considering port knocking. It may be appropriate for specific circumstances, particularly those related to hidden backdoors or remote administration of a personal machine.

### **10.5.3. Honeypots and Honeynets**

An increasingly popular method for confusing attackers is to place bait systems on a network and monitor them for attacks. These are known as honeypots. Your author is a member of the Honeynet Project (<http://www.honeynet.org>), which installs networks of these for research purposes. Many corporations have deployed these systems for corporate security purposes, though doing so is risky. The extensive monitoring required makes them high-maintenance and there is always a risk that attackers will break in and use the machines to commit serious crimes. Lower maintenance solutions, such as Honeyd described in the next section, or even an IDS, may be more appropriate. In any case, Honeypots are designed to catch more invasive attacks than simple Nmap scans, so they are not discussed further.

### 10.5.4. OS Spoofing

Several programs have been developed specifically to trick Nmap OS detection. They manipulate the host operating system to support custom responses to Nmap probes. In this way, a Linux PC can be made to resemble an Apple LaserWriter printer or even a webcam. IP Personality (<http://ippersonality.sourceforge.net/>), released in 2000, is one of the most popular systems. It extends the Linux Netfilter framework to support these shenanigans. Unfortunately, it has not been updated since April 2002 and may not work on kernel versions beyond 2.4.18.

Tool availability alone does not make OS spoofing a good idea. One has to justify the effort somehow. The IP Personality FAQ avoids the question “Why would you need this?” by responding that “If you ask this, then you don’t”. Nevertheless, some people find it valuable enough to write and use these tools. One reason is that specific OS information makes it easier for attackers to infer vulnerabilities on your network, and also helps decide what sort of exploit to run. Of course the vulnerability itself is the real problem there, and should be fixed. Other people run this sort of tool because they are embarrassed about the OS they run, or they are extremely privacy conscious. If your operating system is in a legal gray area because some company is claiming IP infringement and filing suits against users, OS spoofing might protect against such a nuisance suit.

One serious problem with masking a host OS this way is that it can cause security and functionality problems. Nmap tests for several important security properties, such as TCP initial sequence number and IP identification number predictability. Emulating a different system, such as a printer, may require weakening these number sequences so that they are predictable and vulnerable to all the attacks that implies. The obscurity gained by spoofing your operating system fingerprint is not worth sacrificing valuable security mechanisms. This sort of spoofing can also cripple functionality. Many Nmap OS detection tests involve asking the system what TCP options are supported. Pretending not to support certain options such as timestamps and window scaling will remove the efficiency benefits of those options. Pretending to support unavailable options can be disasterous.

In Example 10-2, Nmap is fooled by IP Personality into believing a Linux box is really a Sega Dreamcast game console. It is from a paper entitled *A practical approach for defeating Nmap OS-Fingerprinting* (<http://voodoo.somoslopeor.com/papers/nmap.html>) by David Barroso Berrueta. That excellent paper includes far more examples, as well as detailed configuration instructions. It also describes many similar systems, with handy warnings such as “the code is not very stable. I loaded the module and in a few moments my Linux box got frozen.”

#### Example 10-2. Deceiving Nmap with IP Personality

```
# nmap -sS -O -oN nmap2.log 192.168.0.19

Interesting ports on 192.168.0.19:
(The 1597 ports scanned but not shown below are in state: closed)
Port      State       Service
22/tcp    open        ssh
25/tcp    open        smtp
80/tcp    open        http
143/tcp   open        imap2
Remote operating system guess: Sega Dreamcast
Nmap run completed -- 1 IP address (1 host up) scanned in 5.886 seconds
```

A newer and more popular program for operating system spoofing (among other features) is Honeyd (<http://www.honeyd.org>). It is actively maintained by author Niels Provos and offers several major benefits over IP Personality. One is that it is much easier to configure. Almost 100 configuration lines were required for the Dreamcast spoofing above. Honeyd, on the other hand, simply reads the Nmap OS detection database (`nmap-os-fingerprints`) and emulates any OS the user chooses. Honeyd also solves the security and functionality problems of OS spoofing by creating synthetic hosts for the emulation. You can ask Honeyd to take over

hundreds of unused IP addresses in an organization. It responds to probes sent to those IPs based on its configuration. This eliminates the security and functionality risks of trying to mask a host's own TCP stack. You are creating a bunch of synthetic hosts instead, so this does not help obscure the OS of existing hosts. The synthetic hosts basically constitute a low-maintenance honeynet that can be watched for attacks. It is mostly intended for research purposes, such as using the worldwide network of Honeyd installations to identify new worms and track spammer activity.

As with other techniques in this section, I recommend experimenting with OS spoofing only when completely satisfied by your security posture. Spoofing a single OS, or even adding hundreds of decoy Honeyd instances, is no substitute for patching vulnerable systems. Many attackers (and especially worms) do not even bother with OS detection before sending exploit code.

It is also worth noting that these systems are easy to detect by skilled attackers. It is extraordinarily hard to present a convincing facade, given all of application and tcp stack differences between operating systems. Nobody will believe that the system in Example 10-2 offering imap, smtp, and ssh is really a Dreamcast running its native OS. In addition, a bug in all versions up to 0.8 allowed for simple Honeyd identification with a single probe packet. There are also many TCP characteristics that Honeyd cannot yet handle. Those can be used to detect Honeyd, though Nmap does not automate this work. If Honeyd becomes widespread, detection functionality will likely be added to Nmap.

Deception programs such as Honeyd are just one reason that Nmap users should interpret Nmap results carefully and watch for inconsistencies, particularly when scanning networks that you do not control.

### **10.5.5. Tar pits**

Rather than trick attackers, some people aim for just slowing them down. Tar pits have long been popular methods for slowing Internet worms and spammers. Some administrators use TCP techniques such as zero-sized receive windows or slowly trickling data back byte by byte. LaBrea (<http://labrea.sourceforge.net/>) is a popular implementation of this. Others use applications-level techniques such as long delays before responding to each SMTP commands. While these are mostly used by anti-spammers, similar techniques can be used to slow Nmap scans. For example, limiting the rate of RST packets sent by closed ports can dramatically slow scanners down.

### **10.5.6. Reactive port scan detection**

We previously discussed scan detection using tools such as Scanlogd. Other tools go much further than that, and actually respond to the scans. Some people propose attacking back by launching exploits or denial of service attacks against the scan source. This is a terrible idea for many reasons. For one, scans are often forged. If the source address is accurate, it may be a previous victim that the attacker is using as a scapegoat. Or the scan may be part of an Internet research survey or come from a legitimate employee or customer. Even if the source address is a computer belonging to an actual attacker, striking back may disrupt innocent systems and routers along the path. It may also be illegal.

While the idea of attacking back is widely shunned in the security community, there is much more interest in responding to detected attacks by adjusting firewall rules to block the offending IP address. The idea is to prevent them from following up on the scan with an actual attack. There are several risks in this approach. One is that you show your hand. It will be obvious to attackers that they have been blocked, and most have plenty of other IP addresses they can use to continue probing. They will then know about your reactive system, and could escalate their own attacks. A more important problem is that scans are so easily forged. Chapter nine describes several methods for doing so. When an attacker notices the block, he may spoof scans from important systems, such as major web sites and DNS servers. A target network which then blocks those IPs will be committing a denial of service attack on itself. Restricting firewall blocks to scans that initiate a full TCP connection reduces the spoofing problem, but that fails to stop even the default Nmap SYN scan.

### **10.5.7. Escalating arms race**

While the primary focus of this book is on open source tools, a number of commercial vendors have introduced products that attempt to deceive Nmap. One example is the Cisco Security Agent. The evaluation guide claims the following protections against Nmap.

Network Mapper (Nmap) identifies which devices are present on a network and what operating system and services they are running by sending out a series of network probes. The presence of a device on the network and the ports it is running are both announced by its response to Nmap probes. The pattern of error messages returned identifies the operating system. Nmap is surprisingly accurate. It is frequently used at the initial stage of an attack or investigation to determine which systems might respond to an attacker's exploits.

Expected outcome of Nmap scan against Cisco Security Agent protected systems: Nmap is unable to identify the target operating system of systems running the default server or default desktop policies. Nmap scans appear to hang while its security tests timeout. Nmap scans against systems not protected by Cisco Security Agent report results very quickly

I am investigating how CSA works, and whether Nmap can automatically detect and adjust for it. Scanning technology is an arms race. Open source and commercial companies will continue to create products designed to slow down, block, or deceive Nmap and other tools. Meanwhile, Nmap continually improves, developing resiliency in the face of these challenges.

# Chapter 11. Nmap Output Formats

## 11.1. Introduction

A common problem with open source security tools is confusing and disorganized output. They often spew out many lines of irrelevant debugging information, forcing users to dig through pages of output trying to discern important results from the noise. Program authors often devote little effort to organizing and presenting results effectively. The output messages can be difficult to understand and poorly documented. This shouldn't be too surprising -- writing clever code to exploit some TCP/IP weakness is usually more gratifying than documentation or UI work. Since open source authors are rarely paid, they do what they enjoy.

At the risk of offending my friend Dan Kaminsky, I'll name his scanrand (<http://www.doxpara.com/>) port scanner as an example of a program that was clearly developed with far more emphasis on neat technical tricks than a user friendly UI. The sample output in Example 11-1 is from the Scanrand documentation page.

### Example 11-1. Scanrand output against a local network

```
bash-2.05a# scanrand 10.0.1.1-254:quick
UP:      10.0.1.38:80      [01]  0.003s
UP:      10.0.1.110:443    [01]  0.017s
UP:      10.0.1.254:443    [01]  0.021s
UP:      10.0.1.57:445     [01]  0.024s
UP:      10.0.1.59:445     [01]  0.024s
UP:      10.0.1.38:22      [01]  0.047s
UP:      10.0.1.110:22      [01]  0.058s
UP:      10.0.1.110:23      [01]  0.058s
UP:      10.0.1.254:22      [01]  0.077s
UP:      10.0.1.254:23      [01]  0.077s
UP:      10.0.1.25:135     [01]  0.088s
UP:      10.0.1.57:135     [01]  0.089s
UP:      10.0.1.59:135     [01]  0.090s
UP:      10.0.1.25:139     [01]  0.097s
UP:      10.0.1.27:139     [01]  0.098s
UP:      10.0.1.57:139     [01]  0.099s
UP:      10.0.1.59:139     [01]  0.099s
UP:      10.0.1.38:111     [01]  0.127s
UP:      10.0.1.57:1025    [01]  0.147s
UP:      10.0.1.59:1025    [01]  0.147s
UP:      10.0.1.57:5000    [01]  0.156s
UP:      10.0.1.59:5000    [01]  0.157s
UP:      10.0.1.53:111     [01]  0.182s
bash-2.05a#
```

While this does get the job done, it is difficult to interpret. Output is printed based on when the response was received, without any option for sorting the port numbers or even grouping all open ports on a target host together. A bunch of space is wasted near the beginning of each line and no summary of results is provided.

Nmap's output is also far from perfect, though I do try pretty hard to make it readable, well-organized, and flexible. Given the number of ways Nmap is used by people and other software, no single format can please everyone. So

Nmap offers several formats, including the interactive mode for humans to read directly and XML for easy parsing by software.

In addition to offering different output formats, Nmap offers options for controlling the verbosity of output as well as debugging messages. Output types may be sent to standard output or to named files, which Nmap can append to or clobber. Output files may also be used to resume aborted scans. This chapter includes full details on these options and every output format. chapter.

## 11.2. Command-line flags

As with almost all other Nmap capabilities, output behavior is controlled by command-line flags. These flags are grouped by category and described in the following sections.

### 11.2.1. Controlling output type

The most fundamental output control is designating the format(s) of output you would like. Nmap offers five types, as summarized in the following list and fully described in later sections.

#### Output formats supported by Nmap

##### Interactive output

This is the output that Nmap sends to the standard output stream (stdout) by default. So it has no special command-line option. Interactive mode caters to human users reading the results directly and it is characterized by a table of interesting ports that is shown in dozens of examples throughout this book.

##### Normal output (-oN)

This is very similar to interactive output, and is sent to the file you choose. It does differ from interactive output in several ways, which derive from the expectation that this output will be analyzed after the scan completes rather than interactively. So interactive output includes messages (depending on verbosity level specified with -v) such as scan completion time estimates and open port alerts. Normal output omits those as unnecessary once the scan completes and the final interesting ports table is printed. This output type prints the nmap command-line used and execution time and date on its first line.

##### XML output (-ox)

XML offers a stable format that is easily parsed by software. Free XML parsers are available for all major computer languages, including C/C++, Perl, Python, and Java. In almost all cases that a non-trivial application interfaces with Nmap, XML is the preferred format. This chapter also discusses how XML results can be transformed into other formats, such as HTML reports and database tables.

##### Grepable output (-oG)

This simple format is easy to manipulate on the command line with simple UNIX tools such as grep, awk, cut, and diff. Each host is listed on one line, with the tab, slash, and comma characters used to delimit output fields. While this can be handy for quickly grokking results, the XML format is preferred for more significant tasks as it is more stable and contains more information.

### sCRiPt KiDDi3 0utPU+ (-oS)

This format is provided for the 'l33t haXXorZ!'

While interactive output is the default and has no associated command-line options, the other four format options use the same syntax. They take one argument, which is the filename that results should be stored in. Multiple formats may be specified, but each format may only be specified once. For example, you may wish to save normal output for your own review while saving XML of the same scan for programmatic analysis. You might do this with the options `-oX myscan.xml -oN myscan.nmap`. While this chapter uses the simple names like `myscan.xml` for brevity, more descriptive names are generally recommended. The names chosen are a matter of personal preference, though I use long ones that incorporate the scan date and a word or two describing the scan, placed in a directory named after the company I'm scanning. As a convenience, you may specify `-oA basename` to store scan results in normal, XML, and grepable formats at once. They are stored in `basename.nmap`, `basename.xml`, and `basename.gnmap`, respectively. As with most programs, you can prefix the filenames with a directory path, such as `~/nmaplogs/foocorp/` on UNIX or `c:\hacking\sco` on Windows.

While these options save results to files, Nmap still prints interactive output to `stdout` as usual. For example, the command **nmap -oX myscan.xml target** prints XML to `myscan.xml` and fills standard output with the same interactive results it would have printed if `-oX` wasn't specified at all. You can change this by passing a hyphen character as the argument to one of the format types. This causes Nmap to deactivate interactive output, and instead print results in the format you specified to the standard output stream. So the command `nmap -oX - target` will send only XML output to `stdout`. Serious errors may still be printed to the normal error stream, `stderr`.

When you specify a filename to an output format flag such as `-oX` or `-oN`, that file is overwritten by default. If you prefer to keep the existing content of the file and append the new results, specify the `--append_output` option. All output filenames specified in that Nmap execution will then be appended to rather than clobbered.

Unlike some Nmap arguments, the space between the logfile option flag (such as `-oX`) and the filename or hyphen is mandatory. If you omit the flags and give arguments such as `-oG-` or `-oXscan.xml`, a backwards compatibility feature of Nmap will cause the creation of *normal format* output files named `G-` and `Xscan.xml` respectively.

## 11.2.2. Controlling verbosity of output

After deciding which format(s) you wish results to be saved in, you can decide how detailed those results should be. The first `-v` option enables verbosity with a level of one. Specify `-v` twice for a slightly greater effect. Verbosity levels greater than two aren't useful. Most changes only effect interactive output, and some also affect normal and script kiddie output. The other output types are meant to be processed by machines, so Nmap can give substantial detail by default in those formats without fatiguing a human user. However, there are a few changes in other modes where output size can be reduced substantially by omitting some detail. For example, a comment line in the grepable output that provides a list of all ports scanned is only printed in verbose mode because it can be quite long. The following list describes the major changes you get with at least one `-v` option.

### Scan completion time estimates

On scans that take more than a minute or two, you will see occasional updates like this in interactive output mode:

```
SYN Stealth Scan Timing: About 30.01% done; ETC: 16:04 (0:01:09 remaining)
```

New updates are given if the estimates change significantly. All port scanning techniques except for Idle scan and FTP bounce scan support completion time estimation, and so does version scanning.

#### Open ports reported when discovered

When verbosity is enabled, open ports are printed in interactive mode as they are discovered. They are still reported in the final interesting ports table as well. This allows users to begin investigating open ports before Nmap even completes. Open port alerts look like this:

```
Discovered open port 53/tcp on 205.217.153.55
```

#### Additional warnings

Nmap always prints warnings about obvious mistakes and critical problems. That standard is lowered when verbosity is enabled, allowing more warnings to be printed. There are dozens of these warnings, covering topics from targets experiencing excessive drops or extraordinarily long latency, to ports which respond to probes in unexpected ways. Rate limiting prevents these warnings from flooding the screen.

#### Additional notes

Nmap prints many extra informational notes when in verbose mode. For example, it prints out the time when each port scan is started along with the number of hosts and ports scanned. It later prints out a concluding line disclosing how long the scan took and briefly summarizing the results.

#### Extra OS detection information

With verbosity, results of the TCP ISN and IPID sequence number predictability tests are shown. These are done as a byproduct of OS detection. With verbosity greater than one, the actual OS detection fingerprint is shown in more cases.

#### Down hosts are printed in ping scan

During a ping scan with verbosity enabled, down hosts will be printed, rather than just up ones.

#### Birthday wishes

Nmap wishes itself a happy birthday when run in verbose mode on September 1.

The changes that are usually only useful until Nmap finishes and prints its report are only sent to interactive output mode. If you send normal output to a file with `-oN`, that file won't contain open port alerts or completion time estimates, though they are still printed to stdout. The assumption is that you will review the file when Nmap is done and don't want a lot of extra cruft, while you might watch Nmap's execution progress on standard output and care about runtime progress. If you really want everything printed to stdout sent to a file, use the output stream redirection provided by your shell (e.g. `nmap -v scanme.nmap.org > scanoutput.nmap`).

The dozens of small changes contingent on verbosity (mostly extra messages) are too numerous to cover here. They are also always subject to change. An effective way to see them all is to unpack the latest Nmap tarball and grep for them with a command such as `grep -A1 o.verbose *.cc`. Representative excerpts from the output are shown in Example 11-2.

**Example 11-2. Greping for verbosity conditionals**

```

felix~> grep -A1 o.verbose *.cc
idle_scan.cc: if (o.debugging || o.verbose) {
idle_scan.cc-   log_write(LOG_STDOUT, "Initiating Idlescan against %s\n", target->NameIP());
--
nmap.cc: if (o.verbose)
nmap.cc-   output_ports_to_machine_parseable_output(ports, o.TCPScan(), o.udpscan, o.ipprotscan);
--
nmap_rpc.cc: if (o.debugging || o.verbose)
nmap_rpc.cc-   gh_perror("recvfrom in get_rpc_results");
--
osscan.cc: if (o.verbose && openport != (unsigned long) -1)
osscan.cc-   log_write(LOG_STDOUT, "For OSScan assuming port %d is open, %d is closed...");
--
output.cc: if (o.verbose)
output.cc-   log_write(LOG_NORMAL|LOG_SKID|LOG_STDOUT, "IPID Sequence Generation: %s\n")

```

Example 11-3 puts all of this together by showing a normal scan followed by the same scan with verbosity enabled. Features such as the extra OS identification data, completion time estimates, open port alerts, and extra informational messages are easily identified in the latter output. This extra info is often helpful during interactive scanning, so I always specify `-v` when scanning a single machine unless I have a good reason not to.

**Example 11-3. A comparison of interactive output with and without verbosity enabled.**

```

# nmap -T4 -A -p- scanme.nmap.org

Starting nmap 3.77 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 65530 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.1p1 (protocol 1.99)
25/tcp    open  smtp     qmail smtpd
53/tcp    open  domain   ISC Bind 9.2.1
80/tcp    open  http     Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.4.20
Uptime 4.945 days (since Fri Nov 12 15:34:34 2004)

Nmap run completed -- 1 IP address (1 host up) scanned in 684.774 seconds

# nmap -v -T4 -A -p- scanme.nmap.org

Starting nmap 3.77 ( http://www.insecure.org/nmap/ )
Initiating SYN Stealth Scan against scanme.nmap.org (205.217.153.55) [65535 ports] at 3:22
Discovered open port 22/tcp on 205.217.153.55
Discovered open port 53/tcp on 205.217.153.55
Discovered open port 80/tcp on 205.217.153.55
Discovered open port 25/tcp on 205.217.153.55
SYN Stealth Scan Timing: About 4.58% done; ETC: 3:33 (0:10:24 remaining)
The SYN Stealth Scan took 679.55s to scan 65535 total ports.

```

```

Initiating service scan against 4 services on scanme.nmap.org (205.217.153.55) at 3:33
The service scan took 5.10s to scan 4 services on 1 host.
For OSScan assuming port 22 is open, 113 is closed, and neither are firewalled
Host scanme.nmap.org (205.217.153.55) appears to be up ... good.
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 65530 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.1p1 (protocol 1.99)
25/tcp    open  smtp     qmail smtpd
53/tcp    open  domain   ISC Bind 9.2.1
80/tcp    open  http     Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.4.20
Uptime 4.916 days (since Fri Nov 12 15:34:34 2004)
TCP Sequence Prediction: Class=random positive increments
                           Difficulty=3048990 (Good luck!)
IPID Sequence Generation: All zeros

Nmap run completed -- 1 IP address (1 host up) scanned in 687.967 seconds

```

### 11.2.3. Enabling debugging output

When even verbose mode doesn't provide sufficient data for you, debugging is available to flood you with much more! As with the verbosity option (-v), debugging is enabled with a command-line flag (-d) and the debug level can be increased by specifying it multiple times. Alternatively, you can set a debug level by giving an argument to -d. For example, -d9 sets level nine. That is the highest effective level and will produce thousands of lines unless you run a very simple scan with very few ports and targets.

Debugging output is useful when a bug is suspected in Nmap, or if you are simply confused as to what Nmap is doing and why. As this feature is mostly intended for developers, debug lines aren't always self-explanatory. If you don't understand a line, your only recourse is to ignore it, look it up in the source code, or request help from the development list (nmap-dev). Other lines are self explanatory. The messages often become more obscure as the debug level is increased. Example 11-4 shows a few different debugging lines that resulted from a -d5 scan of Scanme.

#### Example 11-4. Some representative debugging lines

```

Timeout vals: srtt: 30256 rttvar: 30256 to: 151280 delta 15699
              ==> srtt: 32218 rttvar: 26616 to: 138682
RCVD (1.0710s) TCP 205.217.153.55:113 > 63.205.186.56:34538 RA ttl=241 id=0 ack=1188628258
**TIMING STATS**: IP, probes active/freshportsleft/outstanding/retranwait/onbench,
                  cwnd/ccthresh/delay, timeout/srtt/rttvar/
Groupstats (1/1 incomplete): 10/*/*/*/* 15.00/50/* 128805/49393/19853
205.217.153.55: 10/65515/15/5/0 15.00/50/0 125924/41340/21146
Discovered filtered port 38281/tcp on 205.217.153.55
Packet capture filter (device ppp0): dst host [ip] and
                                      (icmp or (tcp and src host 205.217.153.55))
The avg TCP TS HZ is: 100.624257

```

No full example is given here because debug logs are so long. In Example 11-3, a scan against Scanme used 14 lines of text without verbosity, and 28 with it. The same scan with `-d` instead of `-v` took 74 lines. With `-d2` it ballooned to 65,768 lines, and `-d5` output 242,650 lines! The debug option implicitly enables verbosity, so there is no need to specify them both.

Determining the best output level for a certain debug task is a matter of trial and error. I try a low level first to understand what is going on, then increase it as necessary. As I learn more, I may be able to better isolate the problem or question. I then try to simplify the command in order to offset some increased verbiage of the higher debug level.

Just as grep can be useful to identify the changes and levels associated with verbosity, it also helps with investigating debug output. I recommend running this command from the `nmap-VERSION` directory in the Nmap source tarball:

```
grep -A1 o.debugging *.cc
```

## 11.2.4. Enabling packet tracing

The `--packet_trace` option causes Nmap to print a summary of every packet it sends and receives. This can be extremely useful for debugging or understanding Nmap's behavior, as examples throughout this book demonstrate. Example 11-5 shows a simple ping scan of Scanme with packet tracing enabled.

### Example 11-5. Using `--packet_trace` to detail a ping scan of Scanme

```
# nmap --packet_trace -sP scanme.nmap.org

Starting nmap 3.77 ( http://www.insecure.org/nmap/ ) at 2004-11-18 15:59 PST
SENT (0.0110s) ICMP 63.205.186.56 > 205.217.153.55 Echo request (type=8/code=0)
    ttl=47 id=12401 ipLen=28
SENT (0.0130s) TCP 63.205.186.56:45425 > 205.217.153.55:80 A ttl=39 id=22911
    ipLen=40 seq=2336084894 win=4096 ack=826135454
RCVD (0.0420s) ICMP 205.217.153.55 > 63.205.186.56 Echo reply (type=0/code=0)
    ttl=50 id=56265 ipLen=28
Host scanme.nmap.org (205.217.153.55) appears to be up.
Nmap run completed -- 1 IP address (1 host up) scanned in 0.171 seconds
```

This Nmap execution shows three extra lines caused by packet tracing (each have been wrapped for readability). Each line contains several fields. The first is whether a packet is sent or received by Nmap, as abbreviated to `SENT` and `RCVD`. The next field is a time counter, providing the elapsed time since Nmap started. The time is in seconds, and in this case Nmap only required a tiny fraction of one. The next field is the protocol: TCP, UDP, or ICMP. Next comes the source and destination IP addresses, separated with a directional arrow. For TCP or UDP packets, each IP is followed by a colon and the source or destination port number.

The remainder of each line is protocol specific. As you can see, ICMP provides a human-readable type if available (`Echo request` in this case) followed by the ICMP type and code values. The ICMP packet logs end with the IP TTL, ID, and packet length field. TCP packets use a slightly different format after the destination IP and port number. First comes a list of characters representing the set TCP flags. The flag characters are SFRPUEC, which stand for SYN, FIN, RST, PSH, URG, ECE, and CWR, respectively. The latter two flags are part of TCP explicit congestion notification, described in RFC 3168 (<http://www.rfc-editor.org/rfc/rfc3168.txt>).

Because packet tracing can lead to thousands of output lines, it helps to limit scan intensity to the minimum that still serves your purpose. A scan of a single port on a single machine won't bury you in data, while the output of a

--packet\_trace scan of a whole network can be overwhelming. Packet tracing is automatically enabled when the debug level (-d) is at least three.

Sometimes --packet\_trace provides specialized data that Nmap never shows otherwise. For example, Example 11-5 shows ICMP and TCP ping packets sent to the target host. The target responds to the ICMP echo request, which can be valuable information that Nmap doesn't otherwise show. It is possible that the target host replied to the TCP packet as well -- Nmap stops listening once it receives one response to a ping scan since that is all it takes to determine that a host is online.

### 11.2.5. Resuming canceled scans

Some extensive Nmap runs take a very long time -- on the order of days. Such scans don't always run to completion. Restrictions may prevent Nmap from being run during working hours, the network could go down, the machine Nmap is running on might suffer a planned or unplanned reboot, or Nmap itself could crash. The admin running Nmap could cancel it for any other reason as well, by specifying control-C. Restarting the whole scan from the beginning may be undesirable. Fortunately, if normal (-oN) or grepable (-oG) logs were kept, the user can ask Nmap to resume scanning with the target it was working on when execution ceased. Simply specify the --resume option and pass the normal/grepable output file as its argument. No other arguments are permitted, as Nmap parses the output file to use the same ones specified previously. Simply call Nmap as **nmap --resume logfilename**. Resumption does not support the XML output format combining the two runs into one valid XML file would be difficult.

## 11.3. Interactive output

Interactive output is what Nmap prints to the stdout stream, which usually appears on the terminal window you executed Nmap from. In other circumstances, you might have redirected stdout to a file or another application such as Nessus or an Nmap GUI may be reading the results. If a larger application is interpreting the results rather than printing Nmap output directly to the user (as the Nmap X-Window frontend NmapFE does), then using the XML output discussed in Section 11.6 would be more appropriate.

This format has but one goal: to present results that will be valuable to a human reading over them. No effort is made to make these easily machine parseable or to maintain a stable format between Nmap versions. Better formats exist for these things. The toughest challenge is deciding which information is valuable enough to print. Omitting data that a user wants is a shame, though flooding the user with pages of mostly irrelevant output can be even worse. The verbosity, debugging, and packet tracing flags are available to shift this balance based on individual users' preferences.

This output format needs no extensive description here, as most Nmap examples in this book already show it. To understand Nmap's interactive output for a certain feature, see the section of this book dedicated to that feature. Typical examples of interactive output are given in Example 11-3.

## 11.4. Normal output (-oN)

Normal output is printed to a file when the -oN option is specified with a filename argument. It is similar to interactive output, except that notes which lose relevance once a scan completes are removed. It is assumed that the file will be read after Nmap completes, so estimated completion times and new open port alerts are redundant to the

actual completion time and the ordered port table. Since output may be saved a long while and reviewed among many other logs, Nmap prints the execution time, command-line arguments, and Nmap version number on the first line. A similar line at the end of a scan divulges final timing and a host count. Those two lines begin with a pound character to identify them as comments. If your application must parse normal output rather than XML/Grepable formats, ensure that it ignores comments that it doesn't recognize rather than treating them as an error and aborting. Example 11-6 is a typical example of normal output. Note that `-oN -` was used to prevent interactive output and send normal output straight to stdout.

#### **Example 11-6. A typical example of normal output**

```
# nmap -T4 -A -p- -oN - scanme.nmap.org
# nmap 3.77 scan initiated Sun Nov 21 7:55:07 2004 as: nmap -T4 -A -p- -oN - scanme.nmap.org
Interesting ports on scanme.nmap.org (205.217.153.55):
(The 65530 ports scanned but not shown below are in state: filtered)
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh      OpenSSH 3.1p1 (protocol 1.99)
25/tcp    open     smtp     qmail smtplib
53/tcp    open     domain   ISC Bind 9.2.1
80/tcp    open     http     Apache httpd 2.0.39 ((Unix) mod_perl/1.99_07-dev Perl/v5.6.1)
113/tcp   closed   auth
Device type: general purpose
Running: Linux 2.4.x|2.5.X
OS details: Linux 2.4.0 - 2.5.20, Linux 2.4.18 - 2.4.20
Uptime 9.105 days (since Fri Nov 12 5:34:59 2004)

# Nmap run completed at Sun Nov 21 8:06:07 2004 -- 1 IP address (1 host up) scanned in 660.397 seconds
```

## **11.5. \$crIpT kLddI3 OuTPut (-oS)**

Script kiddie output is like interactive output, except that it is post-processed to better suit the 'l33t HaXXorZ! They previously looked down on Nmap due to its consistent capitalization and spelling. It is best understood by example, as given in Example 11-7.

#### **Example 11-7. A typical example of \$crIpT KiDDi3 OuTPut**

```
# nmap -T4 -A -oS - scanme.nmap.org

$TArTIng nmap 3.77 ( Http://wWw.!nS3cur3.0rG/nmap/ )
|nter3st|ng poRtz on $canm3.nmap.org (205.217.153.55):
(ThE 1658 porTz scannEd but not sh0wn below ar3 in $tat3: f|lTerEd)
P0rT      $TATE    $3RV1cE v3R$ION
22/tcp    0p3n    Ssh      0p3n$$H 3.1p1 (pr0tocol 1.99)
25/tcp    0p3n    $Mtp    Qmail smTPd
53/tcp    open     d0maIn  1SC bind 9.2.1
80/tCp   0p3n    http    4pacH3 httpd 2.0.39 ((Unlx) mOd_p3rl/1.99_07-dEv P3Rl/v5.6.1)
113/tcp   CLO$eD aUth
dEv|Ce typ3: g3nEral pUrp0$e
RUnNIng: L|nux 2.4.x|2.5.X
oS dEtalz: LInux 2.4.0 - 2.5.20, L!nux 2.4.18 - 2.4.20
uptIme 9.113 Dayz (sinc3 Fr1 Nov 12 15:34:59 2004)
```

```
Nmap rUn completeD -- 1 IP addre$z (1 h0$T up) $cann3d !n 27.119 $3cONds
```

Some humor-impaired people take this option far too seriously, and scold me for catering to script kiddies. It is simply a joke *making fun* of the script kiddies. They don't actually use this mode, as far as I know.

## 11.6. XML output (-oX)

XML, the *extensible markup language*, has its share of critics as well as plenty of zealous proponents. I was long in the former group, and only grudgingly incorporated XML into Nmap after volunteers performed most of the work. Since then, I have learned to appreciate the power and flexibility that XML offers, and even wrote this book in the DocBook XML format. I strongly recommend that programmers interact with Nmap through the XML interface rather than trying to parse the normal, interactive, or grepable output. That format includes more information than the others and is extensible enough that new features can be added without breaking existing programs that use it. It can be parsed by standard XML parsers, which are available for all popular programming languages, usually for free. Editors, validators, transformation systems, and many other applications already know how to handle the format. Normal and interactive output, on the other hand, are custom to Nmap and subject to regular changes as I strive for a clearer presentation to end users. Grepable output is also Nmap-specific and tougher to extend than XML. It is considered deprecated, and many Nmap features such as MAC address detection are not presented in this output format.

An example of Nmap XML output is shown in Example 11-8. Whitespace has been adjusted for readability. In this case, XML was sent to stdout thanks to the `-oX -` construct. Some programs executing Nmap opt to read the output that way, while others specify that output be sent to a filename and then they read that file after Nmap completes.

### Example 11-8. An example of Nmap XML output

```
# nmap -T4 -A -oX - -p1-1024 scanme.nmap.org
<?xml version="1.0" ?>
<!-- nmap 3.78 scan initiated Fri Dec 10 21:40:13 2004 as:
   nmap -T4 -A -oX - -p1-1024 scanme.nmap.org -->
<nmaprun scanner="nmap" args="nmap -T4 -A -oX - -p1-1024 scanme.nmap.org"
   start="1102743613" startstr="Fri Dec 10 21:40:13 2004"
   version="3.78" xmloutputversion="1.01">
<scaninfo type="syn" protocol="tcp" numservices="1024" services="1-1024" />
<verbose level="0" />
<debugging level="0" />
<host><status state="up" />
<address addr="205.217.153.55" addrtype="ipv4" />
<hostnames><hostname name="scanme.nmap.org" type="PTR" /></hostnames>
<ports><extraports state="filtered" count="1019" />
<port protocol="tcp" portid="22"><state state="open" />
  <service name="ssh" product="OpenSSH" version="3.1p1"
    extrainfo="protocol 1.99" method="probed" conf="10" />
</port>
<port protocol="tcp" portid="25"><state state="open" />
  <service name="smtp" product="qmail smtpd" method="probed" conf="10" />
</port>
<port protocol="tcp" portid="53"><state state="open" />
```

```

<service name="domain" product="ISC Bind" version="9.2.1" method="probed"
    conf="10" />
</port>
<port protocol="tcp" portid="80"><state state="open" />
    <service name="http" product="Apache httpd" version="2.0.39"
        extrainfo="(Unix) mod_perl/1.99_07-dev" method="probed" conf="10" />
</port>
<port protocol="tcp" portid="113"><state state="closed" />
    <service name="auth" method="table" conf="3" />
</port>
</ports>
<os>
    <portused state="open" proto="tcp" portid="22" />
    <portused state="closed" proto="tcp" portid="113" />
    <osclass type="general purpose" vendor="Linux" osfamily="Linux" osgen="2.4.X" accuracy="100" />
    <osclass type="general purpose" vendor="Linux" osfamily="Linux" osgen="2.5.X" accuracy="100" />
    <osmatch name="Linux 2.4.0 - 2.5.20" accuracy="100" />
    <osmatch name="Linux 2.4.18 - 2.4.20" accuracy="100" />
</os>
<uptime seconds="813079" lastboot="Fri Nov 12 15:35:00 2004" />
<tcpsequence index="1972182" class="random positive increments" difficulty="Good luck!"
    values="E2E6D835,E32B1CB7,E3203691,E3740715,E36B40C8,E33B1621" />
<ipidsequence class="All zeros" values="0,0,0,0,0,0" />
<tcptssequence class="100HZ" values="4D8A8C7,4D8A8D3,4D8A8DF,4D8A8EB,4D8A8F7,4D8A903" />
</host>
<runstats>
    <finished time="1102743614" timestr="Fri Dec 10 21:40:14 2004" />
    <hosts up="1" down="0" total="1" />
    <!-- Nmap run completed at Fri Dec 10 21:40:14 2004;
        1 IP address (1 host up) scanned in 21.142 seconds -->
</runstats>
</nmaprun>

```

Another advantage of XML is that its verbose nature makes it easier to read and understand than other formats. Readers familiar with Nmap in general can likely understand most of the XML output in Example 11-8 without further documentation. The grepable output format, on the other hand, is tough to decipher without its own reference guide.

There are a few aspects of the example XML output which may not be self-explanatory. For example, look at the two `port` elements in Example 11-9

### Example 11-9. Nmap XML port elements

```

<port protocol="tcp" portid="22"><state state="open" />
    <service name="ssh" product="OpenSSH" version="3.1p1"
        extrainfo="protocol 1.99" method="probed" conf="10" />
</port>
<port protocol="tcp" portid="113"><state state="closed" />
    <service name="auth" method="table" conf="3" />
</port>

```

The port protocol, id (port number), state, and service name are the same as would be shown in the interactive output port table. The service product, version, and extrainfo come from version detection and are combined together into one field of the interactive output port table. The `method` and `conf` attributes aren't present in any other output types. The method can be `table`, meaning the service name was simply looked up in `nmap-services` based on the port number and protocol, or it can be `probed`, meaning that it was determined through the version detection system. The `conf` attribute measures the confidence Nmap has that the service name is correct. The values range from one (least confident) to ten. Nmap only has a confidence level of three for ports determined by table lookup, while it is highly confident (level 10) that port 22 of Example 11-9 is ssh, because Nmap connected to the port and found a server exhibiting the ssh protocol.

One other aspect that some users find confusing is that the attributes `nmaprun/start` and `finished/end` hold timestamps given in UNIX time, the number of seconds January 1, 1970. This is often easier for programs to handle. For the convenience of human readers, versions 3.78 and newer include the equivalent calendar time written out in the attributes `nmaprun/startstr` and `finished/endstr`.

\* *If anyone finds other portions of the XML output confusing, let me know and I can cover them here.*

Nmap includes a document type definition (DTD) which allows XML parsers to validate Nmap XML output. While it is primarily intended for programmatic use, it can also help humans interpret Nmap XML output. The DTD defines the legal elements of the format, and often enumerates the attributes and values they can take on. It is reproduced in Appendix A.

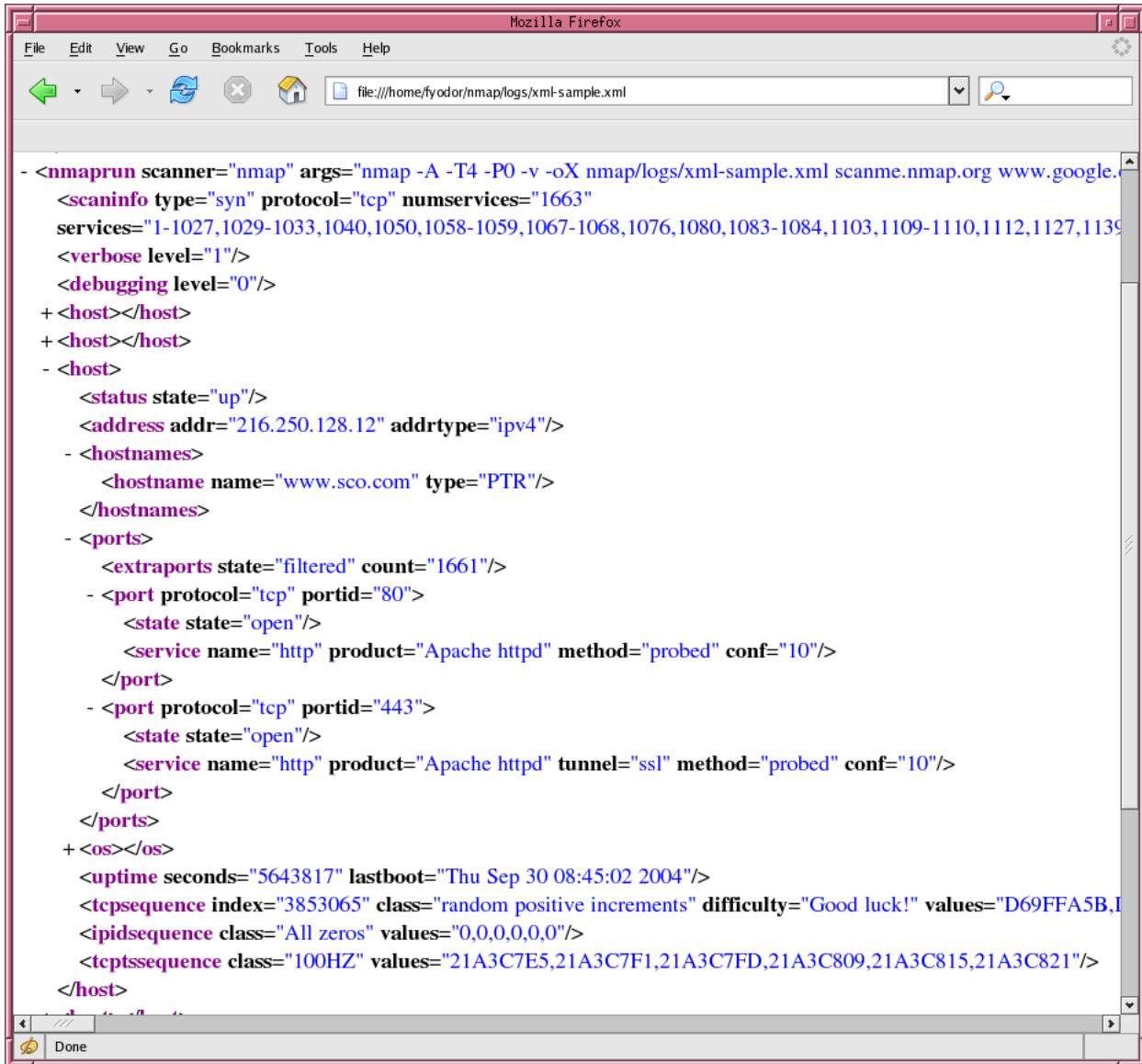
### 11.6.1. Using XML Output

The Nmap XML format can be used in many powerful ways, though few users actually take any advantage of it. I believe this is due to inexperience of many users with XML, combined with a lack of practical, solution-oriented documentation on using the Nmap XML format. This chapter provides several practical examples, including Section 11.7, Section 11.8, and Section 11.9.

A key advantage of XML is that you do not need to write your own parser as you do for specialized Nmap output types such as grepable and interactive output. Any general XML parser should do. The XML parser that people are most familiar with is the one in your web browser. Both IE and Mozilla/Firefox include capable parsers that can be used to view Nmap XML data. Using them is as simple as typing the XML filename or URL into the address bar. A document tree-view is shown, allowing you to expand and reduce elements as desired. It also provides syntax highlighting to quickly recognize key elements. If you know you'll be reading Nmap output, saving normal or interactive output as well as XML is advisable as most people find them the easiest to read and interpret. But if you only have XML output because you lost or didn't create the other forms, or because you are debugging a program that uses the XML, then reading the XML in a web browser is often preferable to using a text editor. Figure 11-1 shows Firefox rendering a tree view of Nmap XML.

\* *TODO: I may need to change this when I insert XSLT stylesheets into Nmap XML output. When that happens, you will get a pretty, rendered view automatically. Will need to change text after the figure then too.*

**Figure 11-1. Reading XML in a web browser**



Similarly, spreadsheet programs, including Microsoft Excel, are often able to import Nmap XML data directly for viewing.

A major problem with browsing Nmap XML logs directly through a web browser or spreadsheet is that the logs are treated in a generic way, just like any other XML file. The browser doesn't understand the relative importance of elements, nor how to organize the data for a more useful presentation. With the help of a stylesheet specific to Nmap, the logs can be rendered in a much more useful fashion. This is demonstrated in Section 11.9.

## 11.7. Manipulating XML output with Perl

Generic XML parsers are available for all popular programming languages, often for free. Examples are the libxml C library and the Apache Xerces parser for Java and C++ (with Perl and COM bindings). While these parsers are sufficient for handling Nmap XML output, developers have created custom modules for several languages which can make the task of interoperating with Nmap XML even easier.

The language with the best custom Nmap XML support is Perl. Max Schubert (affectionately known as Perldork) has created a module named Nmap::Scanner (<http://sourceforge.net/projects/nmap-scanner/>) and Anthony Persaud created one called Nmap::Parser (<http://www.nmapparser.com>). These two modules have many similarities: they can execute Nmap themselves or read from an output file, are well documented, come with numerous example scripts, are part of the Comprehensive Perl Archive Network (CPAN), and are popular with users. They each offer both a callback based parser for interpreting data as Nmap runs as well as an all-at-once parser for obtaining a fully parsed document once Nmap finishes executing. Their API is a bit different, as Nmap::Scanner relies on typesafe classes while Nmap::Parser relies on lighter-weight native Perl arrays. I recommend looking at each to decide which best meets your needs and preferences.

Example 11-10 is a simple demonstration of Nmap::Parser. It comes from the documentation (which contains many other examples) and performs a quick scan, then prints overall scan statistics as well as information on each available target host. Notice how readable it is compared to scripts using other Nmap output formats that are dominated by parsing logic and regular expressions. Even people with poor Perl skills could use this as a starting point to create simple programs to automate their Nmap scanning needs.

### Example 11-10. Nmap::Parser sample code

```
use Nmap::Parser;

#PARSING
my $np = new Nmap::Parser;

$nmap_exe = '/usr/bin/nmap';
$np->parsescan($nmap_exe,'-sT -p1-1023', @ips);

#or

$np->parsefile('nmap_output.xml') #using filenames

#GETTING SCAN INFORMATION

print "Scan Information:\n";
$si = $np->get_scaninfo();
#get scan information by calling methods
print
'Number of services scanned: '.$si->num_of_services()."\\n",
'Start Time: '.$si->start_time()."\\n",
'Scan Types: ',(join ' ', $si->scan_types())."\n";

#GETTING HOST INFORMATION

print "Hosts scanned:\\n";
for my $host_obj ($np->get_host_objects()){
    print
```

```
'Hostname  : '.$host_obj->hostname()."\n",
'Address   : '.$host_obj->ipv4_addr()."\n",
'OS match  : '.$host_obj->os_match()."\\n",
'Open Ports: '(join ',', $host_obj->tcp_ports('open'))."\n";
    #... you get the idea...
}

#frees memory - helpful when dealing with memory intensive scripts
$np->clean();
```

For comparison, Example 11-11 is a sample Perl script using Nmap::Scanner from its documentation. This one uses an event-driven callback approach, registering the functions `scan_started` and `port_found` to print real-time alerts when a host is found up and when each open port is discovered on the host.

### Example 11-11. Nmap::Scanner sample code

```
my $scanner = new Nmap::Scanner;
$scanner->register_scan_started_event(\&scan_started);
$scanner->register_port_found_event(\&port_found);
$scanner->scan(-ss -p 1-1024 -O --max-rtt-timeout 200 somehost.org.net.it);

sub scan_started {
    my $self      = shift;
    my $host      = shift;

    my $hostname = $host->name();
    my $addresses = join( , , map {$_->address()} $host->addresses());
    my $status   = $host->status();

    print "$hostname ($addresses) is $status\\n";
}

sub port_found {
    my $self      = shift;
    my $host      = shift;
    my $port      = shift;

    my $name = $host->name();
    my $addresses = join( , , map {$_->addr()} $host->addresses());

    print "On host $name ($addresses), found ",
        $port->state()," port ",
        join( /,$port->protocol(),$port->portid()), "\\n";
}
```

## 11.8. Output to a database

A common desire is to output Nmap results to a database for easier queries and tracking. This allows users from an individual penetration tester to an international enterprise to store all of their scan results and easily compare them. The enterprise might run large scans daily and schedule queries to mail administrators of newly open ports or available machines. The penetration tester might learn of a new vulnerability and search all of his old scan results for the affected application so that he can warn the relevant clients. Researchers may scan millions of IP addresses and keep the results in a database for easy real-time queries.

While these goals are laudable, Nmap offers no direct database output functionality. Not only are there too many different database types for me to support them all, but user's needs vary so dramatically that no single database schema is suitable. The needs of the enterprise, pen-tester, and researcher all call for different table structures.

For projects large enough to require a database, I recommend deciding on an optimal DB schema first, then writing a simple program or script to import Nmap XML data appropriately. Such scripts often take only minutes, thanks to the wide availability of XML parsers and database access modules. Perl often makes a good choice, as it offers a powerful database abstraction layer and also custom Nmap XML support. Section 11.7 shows how easily Perl scripts can make use of Nmap XML data.

Another option is to use a custom Nmap database support patch. The most popular of these is nmap-sql (<http://sourceforge.net/projects/nmssql>), which adds MySQL logging functionality into Nmap itself. The downsides are that it currently only supports the MySQL database and it must be frequently ported to new Nmap versions. An XML-based approach, on the other hand, is less likely to break when new Nmap versions are released.

## 11.9. Creating HTML reports

\* *TODO: I need to add this section once I finish deciding what to do about adding XSLT stylesheet to default XML output.*

## 11.10. Grepable output (-oG)

This output format is covered last because it is deprecated. The XML output format is far more powerful, and is nearly as convenient for experienced users. XML is a standard for which dozens of excellent parsers are available, while grepable output is my own simple hack. XML is extensible to support new Nmap features as they are released, while I often must omit those features from grepable output for lack of a place to put them.

Nevertheless, grepable output is still quite popular. It is a simple format that lists each host on one line and can be trivially searched and parsed with standard UNIX tools such as grep, awk, cut, sed, diff, and Perl. Even I usually use it for one-off tests done at the command line. Finding all the hosts with the ssh port open or that are running Solaris takes only a simple grep to identify the hosts, piped to an awk or cut command to print the desired fields. One grepable output aficionado is MadHat ([madhat@unspecific.com](mailto:madhat@unspecific.com)), who contributed to this section.

Example 11-12 shows a typical example of grepable output. Normally each host takes only one line, but I split this entry into seven lines to fit on the page. There are also three lines starting with a hash prompt (not counting the Nmap command line). Those are comments describing when Nmap started, the command line options used, and completion time and statistics. One of the comment lines enumerates the port numbers that were scanned. I shortened it to avoid wasting dozens of lines. That particular comment is only printed in verbose (-v) mode. Increasing the verbosity level beyond one -v will not further change the grepable output. The times and dates have been replaced with [time] to reduce line length.

**Example 11-12. A typical example of grepable output**

```
# nmap -oG - -T4 -A scanme.nmap.org
# nmap 3.77 scan initiated [time] as: nmap -oG - -T4 -A scanme.nmap.org
# Ports scanned: TCP(1663;1-1027,1029-1033,1040,...,65301) UDP(0;) PROTOCOLS(0;)
Host: 205.217.153.55 (scanme.nmap.org)
  Ports: 22/open/tcp//ssh//OpenSSH 3.1p1 (protocol 1.99)/,
          25/open/tcp//smtp//qmail smtpd/, 53/open/tcp//domain//ISC Bind 9.2.1/,
          80/open/tcp//http//Apache httpd 2.0.39 ((Unix) mod_perl|1.99_07-dev Perl|v5.6.1)/,
          113/closed/tcp//auth/// Ignored State: filtered (1658)
          OS: Linux 2.4.0 - 2.5.20|Linux 2.4.18 - 2.4.20 Seq Index: 3004446
          IPID Seq: All zeros
# Nmap run completed at [time] -- 1 IP address (1 host up) scanned in 27.177 seconds
```

The command-line here requested that grepable output be sent to standard output with the `-oG` argument to `-oG`. Aggressive timing (`-T4`) as well as OS and version detection (`-A`) were requested. The comment lines are self-explanatory, leaving the meat of grepable output in the `Host` line. Had I scanned more hosts, each of the available ones would have its own `Host` line.

**11.10.1. Grepable output fields**

The host line is split into fields, each of which consist of a field name followed by a colon and space, then the field content. The fields are separated by tab characters (ASCII number 9, '\t'). Example 11-12 shows six fields: Host, Ports, Ignored State, OS, Seq Index, and IPID. A Status section is included in list (`-sL`) and ping (`-sP`) scans, and a Protocols section is included in IP protocol (`-sO`) scans. The exact fields given depend on Nmap options used. For example, OS detection triggers the OS, Seq Index, and IPID fields. Because they are tab delimited, you might split up the fields with a Perl line such as:

```
@fields = split("\t", $host_line);
```

In the case of Example 11-12, the array `@fields` would contain six members. `$fields[0]` would contain “`Host : 205.217.153.55 (scanme.nmap.org)`”, and `$fields[1]` would contain the long Ports field. Scripts that parse grepable output should ignore fields they don’t recognize, as new fields may be added to support Nmap enhancements.

The eight possible fields are described in the following sections.

**11.10.1.1. Host field**

**Example:** Host: 205.217.153.55 (scanme.nmap.org)

The Host field always comes first and is included no matter what Nmap options are chosen. The contents are the IP address (an IPv6 address if `-6` was specified), a space, and then the reverse DNS name in parenthesis. If no reverse name is available, the parenthesis will be empty.

**11.10.1.2. Ports field**

**Example:** Ports: 111/open/tcp//rpcbind (rpcbind V2)/(rpcbind:100000\*2-2)/2 (rpc #100000)/, 113/closed/tcp//auth///

The Ports field is by far the most complex, as can be seen in Example 11-12. It includes entries for every interesting port (the ones which would be included in the port table in normal Nmap output). The port entries are separated with a comma and a space character. Each port entry consists of seven subfields, separated by a forward slash (/). The

subfields are: port number, state, protocol, owner, service, SunRPC info, and version info. Some subfields may be empty, particularly for basic port scans without OS or version detection. The consecutive slashes in Example 11-12 reveal empty subfields. In Perl, you might split them up as so:

```
($port, $state, $protocol, $owner, $service, $rpc_info, $version) = split('/', $ports);
```

Alternatively, you could grab the information from the command line using commands such as these:

```
cut -d/ -f<fieldnumbers>
awk -F/ '{print $<fieldnumber>}';
```

Certain subfields can contain a slash in other output modes. For example, an SSL-enabled web server would show up as `ssl/http` and the version info might contain strings such as `mod_ssl/2.8.12`. Since a slash is the subfield delimiter, this would screw up parsing. To avoid this problem, slashes are changed into the pipe character (`|`) when they would appear anywhere in the Port field.

Parsers should be written to allow more than seven slash-delimited subfields and to simply ignore the extras because future Nmap enhancements may call for new ones. The following list describes each of the seven currently defined Port subfields.

#### Port number

This is simply the numeric TCP or UDP port number.

#### State

The same port state which would appear in the normal output port table is shown here.

#### Protocol

This is `tcp` or `udp`.

#### Owner

Specifies the username that the remote service is running under if ident scan (`-I`) was requested and succeeded.

#### Service

The service name, as obtained from an `nmap-services` lookup, or (more reliably) through version detection (`-sv`) if it was requested and succeeded. With version detection enabled, compound entries such as `ssl|http` and entries with a trailing question mark may be seen. The meaning is the same as for normal output, as discussed in Chapter 7.

#### SunRPC info

If version detection (`-sv`) or RPC scan (`-sR`) were requested and the port was found to use the SunRPC protocol, the RPC program number and accepted version numbers are included here. A typical example is `"(rpcbind:100000*2-2)"`. The data is always returned inside parenthesis. It starts with the program name, then a colon and the program number, then an asterisk followed by the low and high supported version numbers separated by a hyphen. So in this example, `rpcbind` (program number 100,000) is listening on the port for `rpcbind` version 2 requests.

## Version info

If version detection is requested and succeeds, the results are provided here in the same format used in interactive output. For SunRPC ports, the RPC data is printed here too. The format for RPC results in this column is <low version number>-<high version number> (rpc #<rpc program number>). When only one version number is supported, it is printed by itself rather than as a range. A port which shows (rpcbind:100000\*2-2) in the SunRPC info subfield would show 2 (rpc #100000) in the version info subfield.

### 11.10.1.3. Protocols field

**Example:** Protocols: 1/open|icmp/, 2/open|filtered/igmp/

The IP protocol scan (-sO) has a Protocols field rather than Ports. Its contents are quite similar to the Ports field, but it has only three subfields rather than seven. They are delimited with slashes, just as with the Ports field. Any slashes that would appear in a subfield are changed into pipes (|), also as done in the Ports field. The subfields are protocol number, state, and protocol name. These correspond to the three fields shown in interactive output for a protocol scan. An example of IP protocol scan grepable output is shown in Example 11-13. The Host line is wrapped for readability.

#### Example 11-13. Grepable output for IP protocol scan

```
# nmap -v -oG - -sO localhost
# nmap 3.75 scan initiated [time] as: nmap -oG - -sO -v localhost
# Ports scanned: TCP(0;) UDP(0;) PROTOCOLS(256;0-255)
Host: 127.0.0.1 (felix) Protocols: 1/open|filtered/icmp/, 2/open|filtered/igmp/,
                                6/open|filtered/tcp/, 17/open|filtered/udp/,
                                255/open|filtered// Ignored State: closed (251)
# Nmap run completed at [time] -- 1 IP address (1 host up) scanned in 1.340 seconds
```

### 11.10.1.4. Ignored State field

**Example:** Ignored State: filtered (1658)

To save space, Nmap may omit ports in one non-open state from the list in the Ports field. Nmap does this in interactive output too. Regular Nmap users are familiar with the lines such as “The 1658 ports scanned but not shown below are in state: filtered”. For grepable mode, that state is given in the Ignored State field. Following the state name is a space, then in parenthesis is the number of ports found in that state.

### 11.10.1.5. OS field

**Example:** OS: Linux 2.4.0 - 2.5.20

Any perfect OS matches are listed here. If there are multiple matches, they are separated by a pipe character as shown in Example 11-12. Only the free-text descriptions are provided. Grepable mode does not provide the vendor, OS family, and device type classification shown in other output modes.

### 11.10.1.6. Seq Index field

**Example:** Seq Index: 3004446

This number is an estimate of the difficulty of performing TCP initial sequence number sequence prediction attacks against the remote host. These are also known as blind spoofing attacks, and they allow an attacker to forge a full TCP connection to a remote host as if it was coming from some other IP address. This can always help an attacker hide his or her tracks, and it can lead to privilege escalation against services such as rlogin that commonly grant extra privileges to trusted IP addresses. The seq index value is only available when OS detection (-O) is requested and succeeds in probing for this. It is reported in interactive output when verbosity (-v) is requested. More details on the computation and meaning of this value are provided in Chapter 8.

### 11.10.1.7. IPID field

**Example:** IPID Seq: All zeros

This simply describes the remote host's IPID generation algorithm. It is only available when OS detection (-O) is requested and succeeds in probing for it. Interactive mode reports this as well, and it is discussed in Chapter 8.

### 11.10.1.8. Status field

**Example:** Status: Up

Ping and list scans contain only two fields in grepable mode: Host and Status. Status describes the target host as either Up, Down, Smurf, or Unknown. List scan always categorizes targets as Unknown because it does not perform any tests. Ping scan lists a host as up if it responds to at least one ping probe, down if no responses are received, and smurf if ping probes sent to the target resulted in one or more responses from other hosts. In the special case of a Smurf status, the number of unique hosts responding to the ping probes is provided in parenthesis. A format example is: "Status: Smurf (72 responses)". Down hosts are only shown when verbosity is enabled with -v. Example 11-14 demonstrates a ping scan of 100 random hosts, while Example 11-15 demonstrates a list scan of five hosts.

#### Example 11-14. Ping scan grepable output

```
# nmap -sP -oG - -iR 100
# nmap 3.75 scan initiated [time] as: nmap -sP -oG - -iR 100
Host: 67.101.77.102 (h-67-101-77-102.nycmny83.covad.net)           Status: Up
Host: 219.93.164.197 () Status: Up
Host: 222.113.158.200 ()          Status: Up
Host: 66.130.155.190 (modemcable190.155-130-66.mc.videotron.ca) Status: Up
# Nmap run completed at [time] -- 100 IP addresses (4 hosts up) scanned in 13.226 seconds
```

#### Example 11-15. List scan grepable output

```
# nmap -sL -oG - -iR 5
# nmap 3.75 scan initiated [time] as: nmap -sL -oG - -iR 5
Host: 199.223.2.1 ()      Status: Unknown
Host: 191.222.112.87 ()    Status: Unknown
Host: 62.23.21.157 (host.157.21.23.62.rev.coltfrance.com)        Status: Unknown
Host: 138.217.47.127 (CPE-138-217-47-127.vic.bigpond.net.au)       Status: Unknown
Host: 8.118.0.91 ()        Status: Unknown
# Nmap run completed at [time] -- 5 IP addresses (0 hosts up) scanned in 1.797 seconds
```

## 11.10.2. Parsing grepable output on the command line

Grepable output really shines when you want to gather information quickly without the overhead of writing a script to parse XML output. Example 11-16 shows a typical example of this. The goal is to find all hosts on a class C sized network with port 80 open. Nmap is told to scan just that port of each host (skipping the ping stage) and to output a grepable report to stdout. The results are piped to a trivial awk command which finds lines containing /open/ and outputs fields two and three for each matching line. Those fields are the IP address and hostname (or empty parenthesis if the hostname is unavailable).

### Example 11-16. Parsing grepable output on the command line

```
> nmap -p80 -P0 -oG - 10.1.1.0/24 | awk '/open/{print $2 " " $3}'  
10.1.1.72 (userA.corp.foocompany.biz)  
10.1.1.73 (userB.corp.foocompany.biz)  
10.1.1.75 (userC.corp.foocompany.biz)  
10.1.1.149 (admin.corp.foocompany.biz)  
10.1.1.152 (printer.corp.foocompany.biz)  
10.1.1.160 (10-1-1-160.foocompany.biz)  
10.1.1.161 (10-1-1-161.foocompany.biz)  
10.1.1.201 (10-1-1-201.foocompany.biz)  
10.1.1.254 (10-1-1-254.foocompany.biz)
```

# Chapter 12. Understanding and Customizing Nmap Data Files

## 12.1. Introduction

Nmap relies for port scanning and other operations on six data files, all of which have names beginning with `nmap-`. One example is `nmap-services`, a registry of port names to their corresponding port number and protocol. The others, which this chapter describes one by one, are `nmap-service-probes` (version detection probe database), `nmap-rpc` (SunRPC program name to number database for direct RPC scanning), `nmap-os-fingerprints` (OS detection database), `nmap-mac-prefixes` (ethernet MAC address prefix (OUI) to vendor lookup table), and `nmap-protocols` (list of IP protocols for protocol scan). The source distribution installs these files in `/usr/local/share/nmap/` and the official Linux RPMs put them in `/usr/share/nmap/`. Other distributions may install them elsewhere.

The latest versions of these files are kept at <http://www.insecure.org/nmap/data/>, though it is strongly recommended that users upgrade to the most recent Nmap version rather than grabbing newer data files a la carte. There are no guarantees that newer files will work with older versions of Nmap (though they almost always do), and the resulting Frankenstein versions of Nmap can confuse the operating system and service fingerprint submission process.

Most users never change the data files, but it can be handy for advanced users who might want to add a version fingerprint or port assignment for a custom daemon running at their company. This section provides a description of each file and how they are commonly changed. The general mechanism for replacing Nmap data files with custom versions is then discussed. A couple of the files don't relate to port scanning directly, but they are all discussed here for convenience.

## 12.2. nmap-services

The `nmap-services` file is a registry of port names to their corresponding number and protocol. Most lines have a comment as well. Nmap ignores the comments, but users sometimes grep for them in the file when Nmap reports an open service of a type that the user does not recognize. Example 12-1 shows a typical excerpt from the file.

**Example 12-1. Excerpt from nmap-services**

```
qotd      17/tcp    # Quote of the Day
qotd      17/udp    # Quote of the Day
msp       18/tcp    # Message Send Protocol
msp       18/udp    # Message Send Protocol
chargen   19/tcp    # ttyst source Character Generator
chargen   19/udp    # ttyst source Character Generator
ftp-data  20/tcp    # File Transfer [Default Data]
ftp-data  20/udp    # File Transfer [Default Data]
ftp       21/tcp    # File Transfer [Control]
ftp       21/udp    # File Transfer [Control]
ssh       22/tcp    # Secure Shell Login
ssh       22/udp    # Secure Shell Login
telnet   23/tcp    #
telnet   23/udp    #
```

```

priv-mail      24/tcp      # any private mail system
priv-mail      24/udp      # any private mail system
smtp          25/tcp      # Simple Mail Transfer
smtp          25/udp      # Simple Mail Transfer

```

This file was originally based off the IANA assigned ports list at <http://www.iana.org/assignments/port-numbers>, though many other ports have been added over the years. The IANA does not track trojans, worms and the like, yet discovering them is important for many Nmap users.

This excerpt shows that UDP ports are often registered for tcp-only services such as ssh and ftp. This was inherited from the IANA, who tend to always register services for both protocols. Because Nmap scans ports listed in `nmap-services` by default, this aspect slows Nmap down by bloating the port list size. The `nmap-services` list will be cleaned up eventually to remove these redundant entries.

The grammar of this file is pretty simple. There are two whitespace-separated columns. The first is the service name or abbreviation, as seen in the `SERVICE` column of Nmap output. The second column gives the port number and protocol, separated by a slash. That syntax is seen in the `PORT` column of Nmap output. Nmap disregards anything beyond the second column, but most lines continue with whitespace then and a pound ('#') character, followed by a comment. Lines may be blank or contain just a pound character followed by comments.

Astute readers notice the similarity in structure between `nmap-services` and `/etc/services` (usually found at `c:\winnt\system\drivers\etc\services` on Windows). This is no coincidence. The format was kept to allow systems administrators to copy in any custom entries from their own `/etc/services`, or even to substitute their own version of that file entirely. The `/etc/services` format allows a third column providing alias names for a service. Nmap allows (but ignores) these in `nmap-services`.

Admins sometimes change this file to reflect custom services running on their network. For example, an online services company I once consulted for had dozens of different custom daemons running on high-numbered ports. Adding these port numbers to `nmap-services` ensures that they are scanned by default. If `-p1-65535` is used to scan all ports, the open ports will show up anyway. Adding them to the file is still helpful because Nmap will then print the proper names rather than `unknown`. Services specific to a single organization should generally stay in their own `nmap-services`, but other port registrations can benefit everyone. If you find that the default port for a major worm, trojan, filesharing application, or other service is missing from the latest `nmap-services`, please send it to me (`fyodor@insecure.org`) for inclusion in the next release. This helps all users while preventing you from having to maintain and update your own custom version of `nmap-services`.

Similarly, a certain registered port may be frequently wrong for a certain organization. `nmap-services` can only handle one service name per port number and protocol combination, yet sometimes several different types of applications end up using the same default port number. In that case, I try to choose the most popular one for `nmap-services`. Organizations which commonly use another service on such a port number may change the file accordingly.

Another common customization is to strip `nmap-services` down to only the most common, essential services for an organization. Then the Nmap `-F` option will scan only those ports and be much faster than with the original file. The file should normally be placed in a custom location accessible with the `--datadir` option rather than where Nmap will use it by default. Section 12.8 provides advice for customizing these files, including ways to prevent Nmap upgrades from wiping out your modified versions.

### 12.3. nmap-service-probes

This file contains the probes that the Nmap service/version detection system (`-sv` or `-A` options) uses during port

interrogation to determine what program is listening on a port. Example 12-2 offers a typical excerpt.

#### **Example 12-2. Excerpt from nmap-service-probes**

```
#####
# DNS Server status request: http://www.crynw.r.com/crynw/rfc1035/rfc1035.html
Probe UDP DNSStatusRequest q|\0\0\x10\0\0\0\0\0\0\0\0|
ports 53,135
match domain m|^00x90x04000000000000|
# This one below came from 2 tested Windows XP boxes
match msrpc m|^x04x060000x100000000000|
[...]
#####
# DNS Server status request: http://www.crynw.r.com/crynw/rfc1035/rfc1035.html
Probe UDP Help q|help\r\n\r\n|
ports 7,13,37
match chargen m|@ABCDEFGHIJKLMNPQRSTUVWXYZ|
match echo m|^help\r\n\r\n$|
match time m|^[\xc0-\xc5]...$|
```

The grammar of this file is fully described in Chapter 7. While `nmap-service-probes` is more complex than `nmap-services`, the benefits of improving it can also be greater. Nmap can be taught to actually recognize a company's custom services, rather than simply guessed based on `nmap-services` port registration.

Additionally, some admins have been using version detection for tasks well beyond its original intended purpose. A short probe can cause Nmap to print the title of web pages, recognize worm-infected machines, locate open proxies, and more. A recipe describing how to do this can be found in Section 7.9.

## **12.4. nmap-rpc**

As with `nmap-services`, `nmap-rpc` simply maps numbers to names. In this case, SunRPC program numbers are mapped to the program name which uses them. Example 12-3 offers a typical excerpt.

#### **Example 12-3. Excerpt from nmap-rpc**

```
rpcbind      100000  portmap sunrpc rpcbind
rstatd       100001  rstat rup perfmeter rstat_svc
rusersd      100002  rusers
nfs          100003  nfsprog nfsd
ypserv        100004  ypprog
mountd       100005  mount showmount
rpc.operd    100080  opermsg      # Sun Online-Backup
# DMFE/DAWS (Defense Automated Warning System)
#
GqsrV       200034  gqsrV
Ppt          200035  ppt
Pmt          200036  pmt
```

Nmap only cares about the first two whitespace-separated columns -- the program name and number. It doesn't look at any aliases or comments that may appear beyond that. Blank lines and those starting with pound comments are permitted. This format is the same as used by `/etc/rpc` on UNIX, so admins may use that file instead if they desire.

`nmap-rpc` is only used by the RPC grinding feature of Nmap version descriptions. That feature is covered in Section 7.5.1.

Users rarely change `nmap-rpc`. When they do, it is usually to add a custom service or a public one that is missing from the latest `nmap-rpc`. In the latter case, please send a note to me at [fyodor@insecure.org](mailto:fyodor@insecure.org) so that I can add it to the next version. As with `nmap-services`, some admins strip the file down, removing obscure RPC programs to save scan time. The same warning applies: specify your stripped `nmap-rpc` with the `--datadir` option rather than installing it where it will be used implicitly.

## 12.5. nmap-os-fingerprints

This file contains extensive data on how hundreds of different systems respond to specialized TCP and UDP queries. The data is grouped into more than a thousand structures, known as OS Fingerprints, that each contain response data for a known class of systems. When remote OS detection is requested with the `-o` option, responses received from the target system are compared with the `nmap-os-fingerprints` database. If a match is found, the corresponding description and classification likely describe the target OS as well. Example 12-4 is a typical excerpt, showing a couple fingerprints from the file.

### Example 12-4. Excerpt from `nmap-os-fingerprints`

```
Fingerprint Sega Dreamcast game console
Class Sega | embedded || game console
TSeq(Class=TD%gcd=<780%SI=<14)
T1 (DF=N%W=1D4C%ACK=S++%Flags=AS%Ops=M)
T2 (Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
T3 (Resp=Y%DF=N%W=1D4C%ACK=S++%Flags=AS%Ops=M)
T4 (DF=N%W=0%ACK=S%Flags=R%Ops=)
T5 (DF=N%W=0%ACK=S%Flags=AR%Ops=)
T6 (DF=N%W=0%ACK=S%Flags=R%Ops=)
T7 (DF=N%W=0%ACK=S++%Flags=AR%Ops=)
PU(Resp=N)

Fingerprint Linux 2.6.0 (x86)
Class Linux | Linux | 2.6.X | general purpose
TSeq(Class=RI%gcd=<6%SI=<269E81A&>62D97%IPID=Z%TS=1000HZ)
T1 (DF=Y%W=7FFF%ACK=S++%Flags=AS%Ops=MNNTNW)
T2 (Resp=N)
T3 (Resp=Y%DF=Y%W=7FFF%ACK=S++%Flags=AS%Ops=MNNTNW)
T4 (DF=Y%W=0%ACK=O%Flags=R%Ops=)
T5 (DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
T6 (DF=Y%W=0%ACK=O%Flags=R%Ops=)
T7 (DF=Y%W=0%ACK=S++%Flags=AR%Ops=)
PU(DF=N%TOS=D0%IPLen=164%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)
```

The process of OS fingerprinting, as well as the format of this file, are fully described in Chapter 8.

`nmap-os-fingerprints` is rarely changed by users because removing fingerprints offers few advantages and creating a new fingerprint to add is a moderately complex process. When Nmap finds an unrecognized machine that appears suitable for inclusion in the DB, it prints out a fingerprint and a URL where the user may submit it for incorporation into future versions of Nmap. Some users tweak the fingerprint names if a match is not quite right (for example Linux 2.6.9 is reported as “Linux 2.6.5 - 2.6.8”). Please also notify me of such problems -- Chapter 8

describes how to do so. Global changes help everyone, and prevent you from having to maintain your own fork of the file.

## **12.6. nmap-mac-prefixes**

Users rarely modify this file, which maps MAC address prefixes to vendor names. Read on for the complete treatment.

Ethernet devices, which have become the dominant network interface type, are each programmed with a unique 42-bit identifier known as a MAC address. This address is placed in ethernet headers to identify which machine on a local network sent a packet, and which machine the packet is destined for. Humans usually represent it as a hex string, such as 00:60:1D:38:32:90.

To assure that MAC addresses are unique in a world with thousands of vendors, the IEEE assigns an Organizationally Unique Identifier (OUI) to each company manufacturing ethernet devices. The company must use its own OUI for the first three bytes of MAC addresses for equipment it produces. For example, the OUI of 00:60:1D:38:32:90 is 00601D. It can choose the remaining three bytes however it wishes, as long as they are unique. A counter is the simple approach. Companies that assign all 24 million possible values can obtain more OUIs. `nmap-mac-prefixes` maps each assigned OUI to the name of the vendor that sells them. Example 12-5 is a typical excerpt.

### **Example 12-5. Excerpt from `nmap-mac-prefixes`**

```
006017 Tokimec
006018 Stellar ONE
006019 Roche Diagnostics
00601A Keithley Instruments
00601B Mesa Electronics
00601C Telxon
00601D Lucent Technologies
00601E Softlab
00601F Stallion Technologies
006020 Pivotal Networking
006021 DSC
006022 Vicom Systems
006023 Pericom Semiconductor
006024 Gradient Technologies
006025 Active Imaging PLC
006026 Viking Components
```

The first value is the 3-byte OUI as 6 hex digits. It is followed by the company name. This file is created, using a simple perl script, from the complete list of OUIs available from <http://standards.ieee.org/regauth/oui/oui.txt>. The IEEE also offers an OUI FAQ at <http://standards.ieee.org/faqs/OUI.html>.

Nmap can determine the MAC address of hosts on a local ethernet LAN by reading the headers off the wire. It uses this table to look up and report the manufacturer name based on the OUI. This can be useful for roughly identifying the type of machine you are dealing with. A device with a Cisco, Hewlett Packard, or Sun OUI probably identifies a router, printer, or SPARCstation, respectively. Example 12-5 shows that the device at 00:60:1D:38:32:90 was made by Lucent. It is in fact the Lucent Orinoco wireless card in my laptop.

## 12.7. nmap-protocols

This file maps the 1-byte IP Protocol number in the IP header into the corresponding protocol name. Example 12-6 is a typical excerpt.

### Example 12-6. Excerpt from nmap-protocols

```

hopopt      0    HOPOPT      # IPv6 Hop-by-Hop Option
icmp        1    ICMP       # Internet Control Message
igmp        2    IGMP       # Internet Group Management
ggp         3    GGP        # Gateway-to-Gateway
ip          4    IP         # IP in IP (encapsulation)
st          5    ST         # Stream
tcp         6    TCP        # Transmission Control
cbt         7    CBT        # CBT
egp         8    EGP        # Exterior Gateway Protocol
[ ... ]
chaos       16   CHAOS      # Chaos
udp         17   UDP        # User Datagram

```

The first two fields are the protocol name or abbreviation and the number in decimal format. Nmap doesn't care about anything after the protocol number. It is used for IP protocol scanning, as described at Section 5.11. Less than 140 protocols are defined and users almost never modify this file. The raw data is made available by the IANA at <http://www.iana.org/assignments/protocol-numbers>

## 12.8. Using Customized Data Files

Any or all of the Nmap data files may be replaced with versions customized to the user's liking. They can only be replaced in whole -- you can not specify changes that will be merged with the original files at runtime. When Nmap looks for each file, it searches by name in many directories and selects the first one found. This is the analogous to the way your UNIX shell finds programs you ask to execute by searching through the directories in your \$PATH one at a time in order. The following list gives the Nmap directory search order. It shows that an `nmap-services` found in the directory specified by `--datadir` will be used in preference to one found in `~/nmap/` because the former is searched first.

### Nmap data file directory search order

1. If `--datadir` option was specified, check the directory given as its argument.
2. If the `NMAPDIR` environmental variable is set, check that directory.
3. If Nmap is not running on Windows, search in `~/nmap` of the user running Nmap. It tries the real user ID's home directory, and then the effective UID's if they differ.
4. If Nmap *is* running on Windows, check the directory in which the Nmap binary resides.
5. Check the compiled in `NMAPDATADIR` directory. That value is defined to `c:\nmap` on Windows, and `$prefix/share/nmap` on UNIX. `$prefix` is `/usr/local` for the default source build and `/usr` for the Linux RPMs. The `$prefix` can be changed by giving `./configure` the `--prefix` option when compiling the source.
6. As a last resort, the current working directory of your shell (.) is tried. This is done last for the same security reasons that . should not appear first on your shell execution \$PATH. On a shared system, a malicious user could place bogus data files in a shared directory such as `/tmp`. Those files could be malformed, causing Nmap

to complain and exit, or they could cause Nmap to skip important ports. If Nmap tried . first, other users who happened to run Nmap in that shared directory would get the bogus versions. This could also happen by accident if you inadvertently ran Nmap in a directory that happened to have a file named `nmap-services` (or one of the other ones). Users who really want Nmap to try the current directory early may set `$NMAPDIR` to . at their own risk.

This list shows the many choices users have when deciding how to replace a file with their own customized version. The option I usually recommend is to place the customized files in a special directory named appropriately for the change. For example, an `nmap-services` stripped to contain just the hundred most common ports could be placed in `~/nmap-fewports`. Then specify this directory with the `--datadir` option. This ensures that the customized files are only used intentionally. Since the Nmap output-to-file formats include the Nmap command-line used, you will know which files were used when reviewing the logs later.

Another option is to simply edit the original in `NMAPDATADIR`. This is rarely recommended, as the edited file will likely be overwritten the next time Nmap is upgraded. Additionally, this makes it hard to use the original files if you suspect that your replacements are causing a problem. This also makes it difficult to compare your version with the original to recall what you changed.

A third option is to place the customized files in your UNIX `~/nmap` directory. Of course you should only insert files that you have changed. The others will still be retrieved from `NMAPDATADIR` as usual. This is very convenient, as Nmap will use the customized files implicitly whenever you run it. That can be a disadvantage as well. Users sometimes forget the files exist. When they upgrade Nmap to a version with newer data files, the old copies in `~/nmap` will still be used, reducing the quality of results.

Setting the `$NMAPDIR` to the directory with files is another alternative. This can be useful when testing a new version of Nmap. Suppose you obtain Nmap version 3.70, notice the huge list of changes, and decide to test it out before replacing your current known-working version. You might compile it in `~/src/nmap-3.70`, but execute it there and Nmap tries to read the data files from `/usr/local/share/nmap`. Those are the old versions, since Nmap 3.70 has not yet been installed. Simply set `$NMAPDIR` to `~/src/nmap-3.70`, test to your heart's content, and then perform the **make install**. A disadvantage to using `$NMAPDIR` regularly is that the directory name is not recorded in Nmap output files like it is when `--datadir` is used instead.

## **Chapter 13. Nmap Cookbook**

## **Chapter 14. The History and Future of Nmap**

# **Chapter 15. Nmap Reference Guide**

# Appendix A. Nmap XML Output DTD

## A.1.

This document type definition (DTD) is used by XML parsers to validate Nmap XML output. The latest version is always available at <http://www.insecure.org/nmap/data/nmap.dtd>. While it is primarily intended for programmatic use, it is included here due to its value in helping humans interpret Nmap XML output. The DTD defines the legal elements of the format, and often enumerates the attributes and values they can take on. Using the DTD is discussed further in Section 11.6.

\* *TODO: Must include the most recent version before book goes to press.*

```
<!--
nmap.dtd
This is the DTD for nmap's XML output (-oX) format.
$Id: nmap.dtd,v 1.8 2004/11/24 20:13:01 fyodor Exp $
```

Originally written by:  
William McVey <[wam@cisco.com](mailto:wam@cisco.com)> <[wam+nmap@wamber.net](mailto:wam+nmap@wamber.net)>

Now maintained by Fyodor <[fyodor@insecure.org](mailto:fyodor@insecure.org)> as part of Nmap.

To validate using this file, simply add a DOCTYPE line similar to:

```
<!DOCTYPE nmaprun SYSTEM "nmap.dtd">
to the nmap output immediately below the prologue (the first line). This
should allow you to run a validating parser against the output (so long
as the dtd is in your parser's dtd search path).
```

Bugs:

Most of the elements are "locked" into the specific order that nmap generates, when there really is no need for a specific ordering.

This is primarily because I don't know the xml DTD construct to specify "one each of this list of elements, in any order". If there is a construct similar to SGML's '&' operator, please let me know.

Since the work to write this DTD was done as part of WAM's job duties for the Cisco Secure Consulting Services group (<http://www.cisco.com/go/securityconsulting>), the following copyright needs to be included in this and any other derived works.

```
# Copyright (c) 2001 by Cisco systems, Inc.
#
# Permission to use, copy, modify, and distribute modified and
# unmodified copies of this software for any purpose and without fee is
# hereby granted, provided that (a) this copyright and permission notice
# appear on all copies of the software and supporting documentation, (b)
```

```

# the name of Cisco Systems, Inc. not be used in advertising or
# publicity pertaining to distribution of the program without specific
# prior permission, and (c) notice be given in supporting documentation
# that use, modification, copying and distribution is by permission of
# Cisco Systems, Inc.
#
# Cisco Systems, Inc. makes no representations about the suitability
# of this software for any purpose. THIS SOFTWARE IS PROVIDED "AS
# IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING,
# WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND
# FITNESS FOR A PARTICULAR PURPOSE.
#
-->

<!-- parameter entities to specify common "types" used elsewhere in the DTD -->
<!ENTITY % attr_numeric "CDATA" >
<!ENTITY % attr_ipaddr "CDATA" >
<!ENTITY % attr_numeric "CDATA" >
<!ENTITY % attr_type "(ipv4 | ipv6 | mac)" >

<!ENTITY % host_states "(up|down|unknown|skipped)" >

<!-- see: nmap.c:statenum2str for list of port states -->
<!-- Maybe they should be enumerated as in scan_types below , but I -->
<!-- don't know how to escape states like open|filtered -->
<!ENTITY % port_states "CDATA" >

<!ENTITY % hostname_types "(PTR)" >

<!-- see output.c:output_xml_scaninfo_records for scan types -->
<!ENTITY % scan_types "(syn|ack|bounce|connect|null|xmas|window|maimon|fin|udp|ipproto)" >

<!-- <!ENTITY % ip_versions "(ipv4)" > -->

<!ENTITY % port_protocols "(ip|tcp|udp)" >

<!-- I don't know exactly what these are, but the values were enumerated via:
     grep "conf=" *
-->
<!ENTITY % service_confs "( 3 | 5 | 10)" >

<!-- This element was started in nmap.c:nmap_main().
     It represents to the topmost element of the output document.
-->
<!ELEMENT nmaprun (scaninfo?, verbose, debugging, host*, runstats?) >
<!ATTLIST nmaprun
    scanner (nmap) #REQUIRED

```

```

args CDATA #IMPLIED
start %attr_numeric; #IMPLIED
version CDATA #REQUIRED
xmloutputversion (1.01) #REQUIRED
>

<!-- this element is written in output.c:doscaninfo() -->
<!ELEMENT scaninfo EMPTY >
<!ATTLIST scaninfo
  type %scan_types; #REQUIRED
  protocol %port_protocols; #REQUIRED
  numservices %attr_numeric; #REQUIRED
  services CDATA #REQUIRED
>

<!-- these elements are written in nmap.c:nmap_main() -->
<!ELEMENT verbose EMPTY >
<!ATTLIST verbose level %attr_numeric; #IMPLIED >

<!ELEMENT debugging EMPTY >
<!ATTLIST debugging level %attr_numeric; #IMPLIED >

<!--
this element is started in nmap.c:nmap_main() and filled by
output.c:write_host_status(), output.c:printportoutput(), and
output.c:printosscanoutput()
-->
<!ELEMENT host ( status, address , (address | hostnames |
  smurf | ports | addport | os | uptime |
  tcpsequence | ipidsequence | tcptssequence )* ) >

<!-- these elements are written by output.c:write_xml_initial_hostinfo() -->
<!ELEMENT status EMPTY >
<!ATTLIST status state %host_states; #REQUIRED >

<!ELEMENT address EMPTY >
<!ATTLIST address
  addr %attr_ipaddr; #REQUIRED
  addrtype %attr_type; "ipv4"
  vendor CDATA #IMPLIED
>

<!ELEMENT hostnames (hostname)* >
<!ELEMENT hostname EMPTY >
<!ATTLIST hostname
  name CDATA #IMPLIED

```

```

type %hostname_types; #IMPLIED
>

<!-- this element is written by output.c:write_host_status() -->
<!ELEMENT smurf EMPTY >
<!ATTLIST smurf responses %attr_numeric; #REQUIRED >

<!-- this element is written by portlist.cc:addport() -->
<!ELEMENT addport      EMPTY >
<!ATTLIST addport
    state      %port_states;  #REQUIRED
    owner      CDATA          #IMPLIED
    portid     %attr_numeric; #REQUIRED
    protocol   %port_protocols; #REQUIRED
>

<!-- these elements are written by output.c:printportoutput() -->

<!ELEMENT ports (extraports? , port*) >

<!ELEMENT extraports EMPTY >
<!ATTLIST extraports
    state  %port_states; #REQUIRED
    count  %attr_numeric; "closed"
>

<!ELEMENT port (state , owner? , service? ) >
<!ATTLIST port
    protocol %port_protocols; #REQUIRED
    portid  %attr_numeric; #REQUIRED
>

<!ELEMENT state EMPTY >
<!ATTLIST state state %port_states; #REQUIRED >

<!ELEMENT owner EMPTY >
<!ATTLIST owner name CDATA #REQUIRED >

<!ELEMENT service EMPTY >
<!ATTLIST service
    name CDATA #REQUIRED
    conf %service_confs; #REQUIRED
        method      (table|detection|probed) #REQUIRED
        version    CDATA          #IMPLIED
        product    CDATA          #IMPLIED
        extrainfo  CDATA          #IMPLIED

```

```

proto (rpc) #IMPLIED
rpcnum %attr_numeric; #IMPLIED
lowver %attr_numeric; #IMPLIED
highver %attr_numeric; #IMPLIED
>

<!-- these elements are written by output.c: printosscanoutput() -->

<!ELEMENT os ( portused*, osclass*, osmatch* ) >

<!ELEMENT portused EMPTY >
<!ATTLIST portused
  state %port_states; #REQUIRED
  proto %port_protocols; #REQUIRED
  portid %attr_numeric; #REQUIRED
>
<!ELEMENT osclass EMPTY >
<!ATTLIST osclass
  vendor      CDATA      #REQUIRED
  osgen       CDATA      #IMPLIED
  type        CDATA      #IMPLIED
  accuracy    CDATA      #REQUIRED
  osfamily   CDATA      #REQUIRED
>

<!ELEMENT osmatch EMPTY >
<!ATTLIST osmatch
  name        CDATA      #REQUIRED
  accuracy   %attr_numeric; #REQUIRED
>

<!ELEMENT uptime EMPTY >
<!ATTLIST uptime
  seconds    %attr_numeric; #REQUIRED
  lastboot   CDATA      #IMPLIED
>

<!ELEMENT tcpsequence EMPTY >
<!ATTLIST tcpsequence
  index     %attr_numeric; #REQUIRED
  class     CDATA      #REQUIRED
  difficulty CDATA      #REQUIRED
  values    CDATA      #REQUIRED
>

<!ELEMENT ipidsequence EMPTY >

```

```
<!ATTLIST ipidsequence
  class CDATA #REQUIRED
  values CDATA #REQUIRED
>

<!ELEMENT tcptssequence EMPTY >
<!ATTLIST tcptssequence
  class CDATA #REQUIRED
  values CDATA #IMPLIED
>

<!-- these elements are generated in output.c:printfinaloutput() -->
<!ELEMENT runstats (finished, hosts) >

<!ELEMENT finished EMPTY >
<!ATTLIST finished time %attr_numeric; #REQUIRED >

<!ELEMENT hosts EMPTY >
<!ATTLIST hosts
  up %attr_numeric; "0"
  down %attr_numeric; "0"
  skipped %attr_numeric; "0"
  total %attr_numeric; #REQUIRED
>
```

## **Appendix B. Appendix A: Complementary Tools**

## FUTURE PEN TESTING EVENTS

**SANS**  
**Pen Test Austin**  
MAY 18-23, 2015 | AUSTIN, TX

Courses offered:  
 • SEC401 • SEC560  
 • SEC504 • SEC617  
 • SEC542 • SEC660

2 Nights of NetWars Tournaments  
 An Evening of CyberCity Missions  
 Coin-a-palooza: A chance to earn up to 4 SANS Pen Test Challenge Coins

[sans.org/event/pentest2015](http://sans.org/event/pentest2015)



**SANS**  
**Penetration Testing**

**Attack Surfaces, Tools, and Techniques**

**POSTER - SPRING 2015**  
35TH EDITION

**On this poster:**

- Tools and techniques that every security professional should know to maximize the value of your pen testing and vulnerability assessment work
- In-depth network diagrams with various attack surfaces every enterprise must defend, as well as world-class pen test techniques to assess each vector
- A detailed mind map of sites and distributions you can use to practice your skills and keep them sharp
- A list of awesome resources for keeping your skills current
- A description of the SANS Pen Test Challenge Coins for our Capture the Flag winners
- An overview of the in-depth, hands-on, skill-driven courses in the SANS PenTest Curriculum

## COIN-A-PALOOZA

Each SANS Pen Test Course includes a final full day (Day 6) of hands-on computer security challenges that hammer home the lessons taught throughout the entire course. The top winners in each course of this full-day Capture-the-Flag event receive the much-coveted challenge coin associated with the course. Each coin is unique for its associated course, with a custom logo, a special tag line, and a theme. Coins are available for the 504, 542, 560, 561, 573, 575, 617, 642, 660, and 760 courses, as well as the SANS NetWars challenge. The prize coin congratulates the victors on their great accomplishment and challenges them further to use their amazing skills to make a positive difference in their workplace and career.



## RESOURCES

### Website

[pen-testing.sans.org](http://pen-testing.sans.org)

### GPWN Mailing List

[lists.sans.org/mailman/listinfo/gpwn-list](mailto:lists.sans.org/mailman/listinfo/gpwn-list)

### Twitter

@pentesttips

### Pen Test Blog

[pen-testing.sans.org/blog](http://pen-testing.sans.org/blog)

### Webcasts

[pen-testing.sans.org/resources/webcasts](http://pen-testing.sans.org/resources/webcasts)

### Poster & Cheat Sheets

[pen-testing.sans.org/resources/downloads](http://pen-testing.sans.org/resources/downloads)

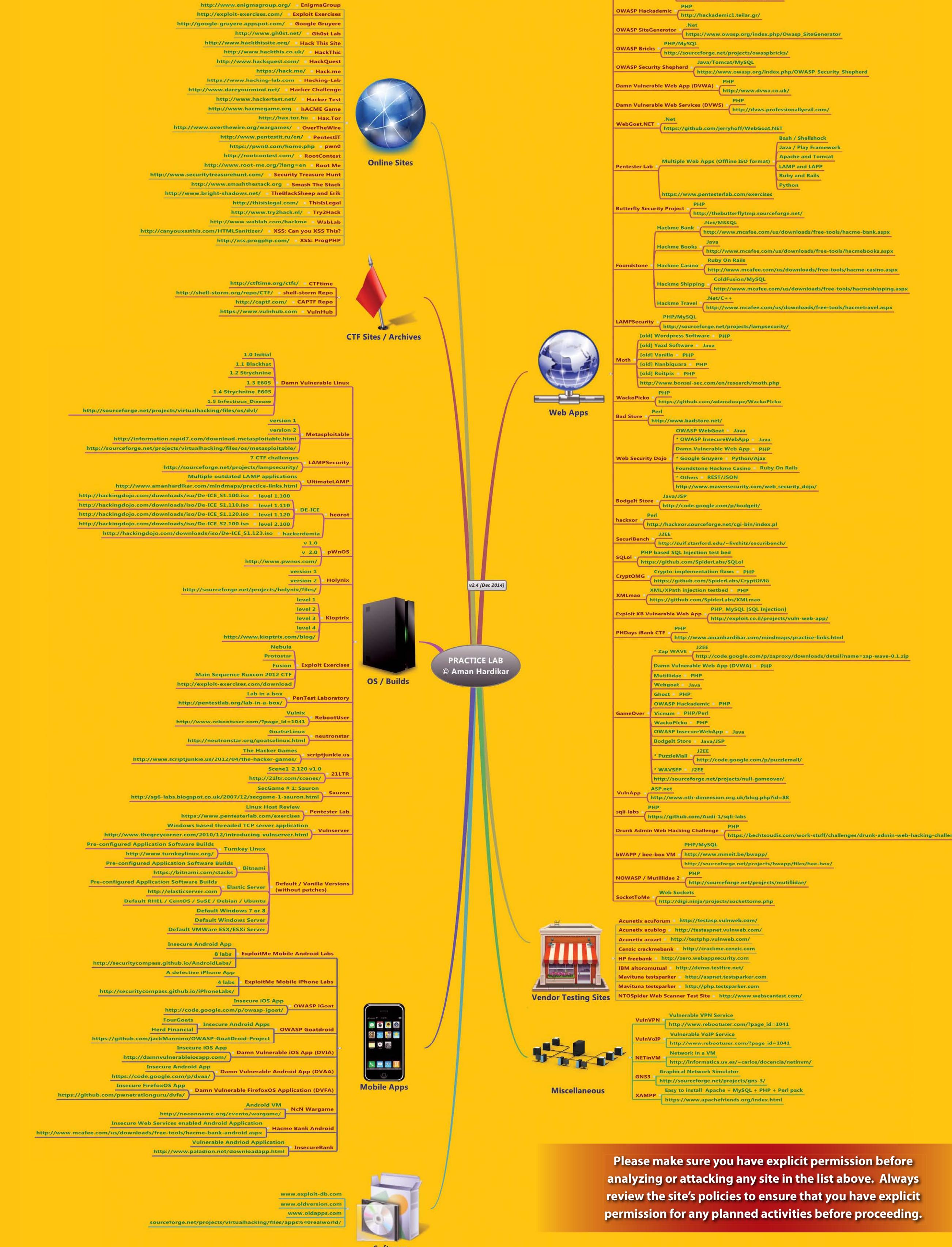
## PENETRATION TESTING PRACTICE LABS

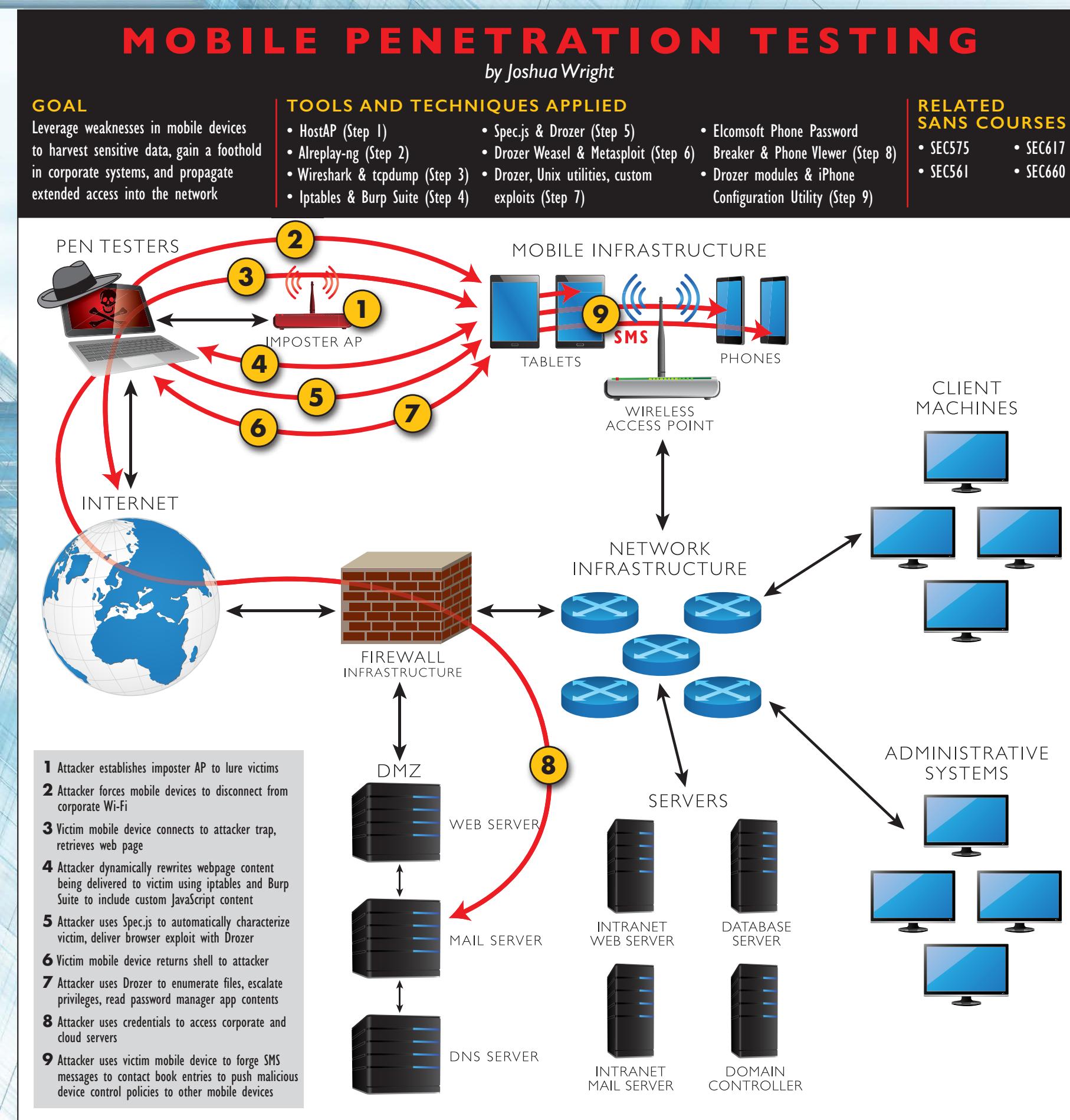
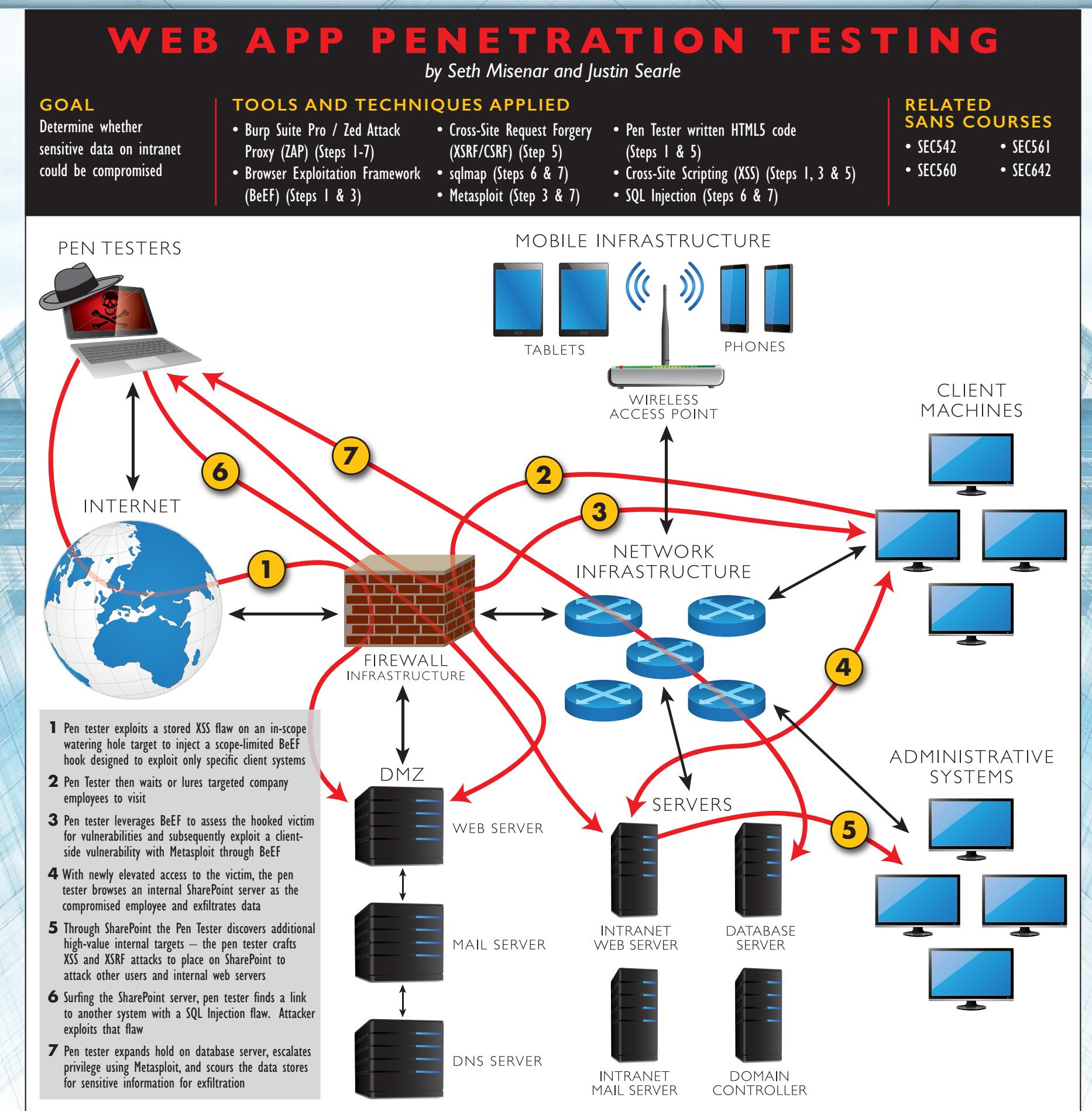
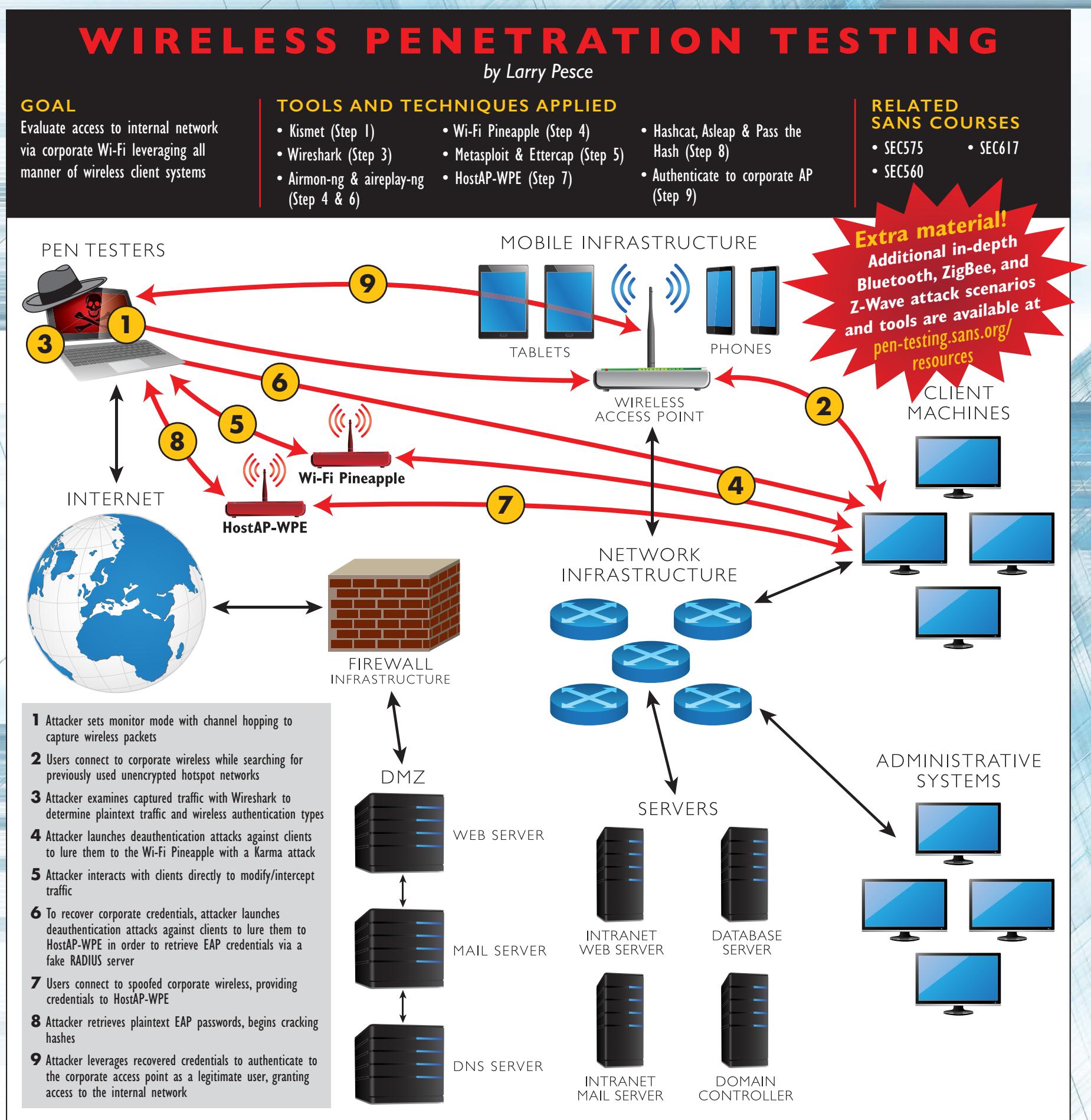
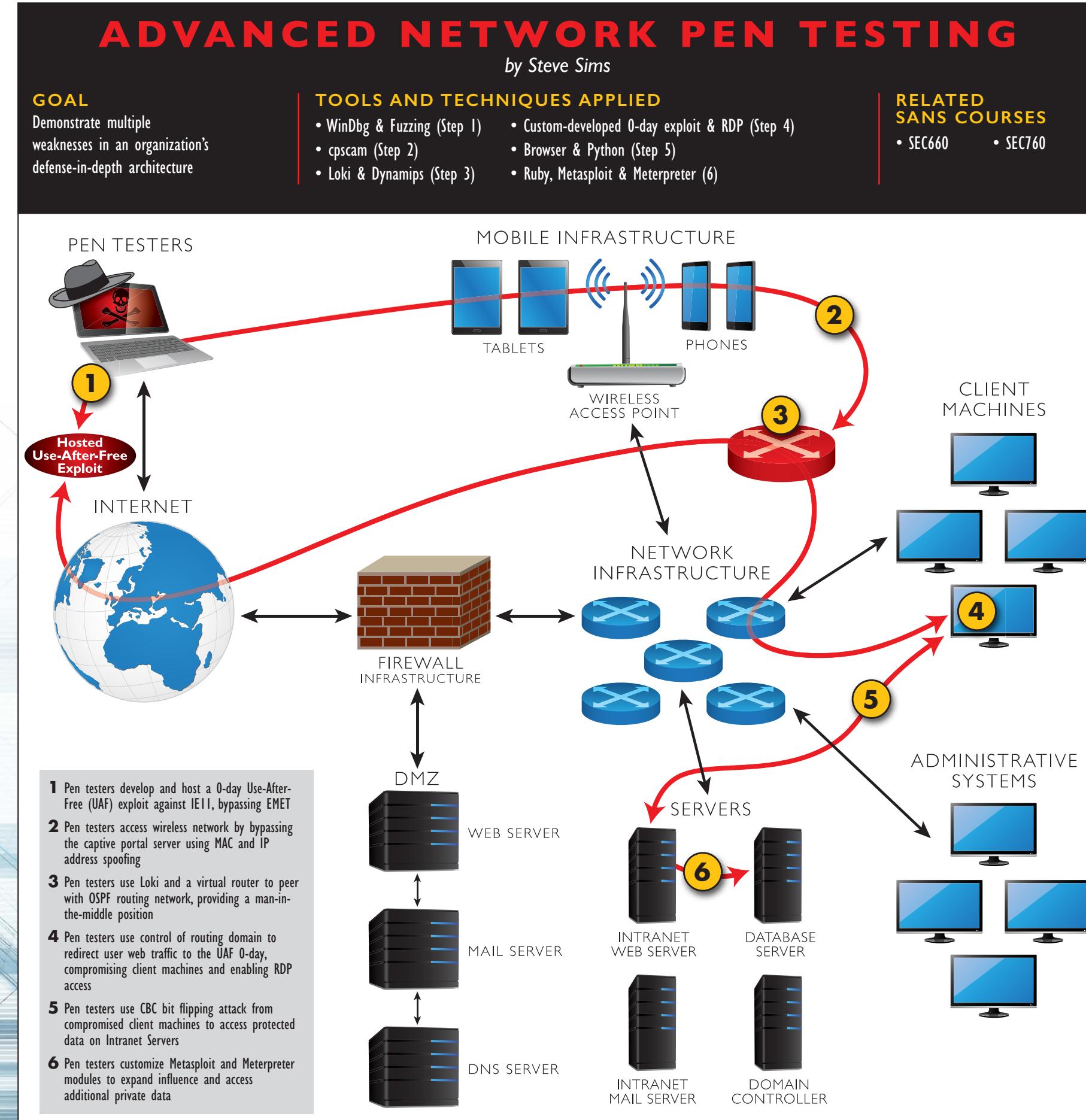
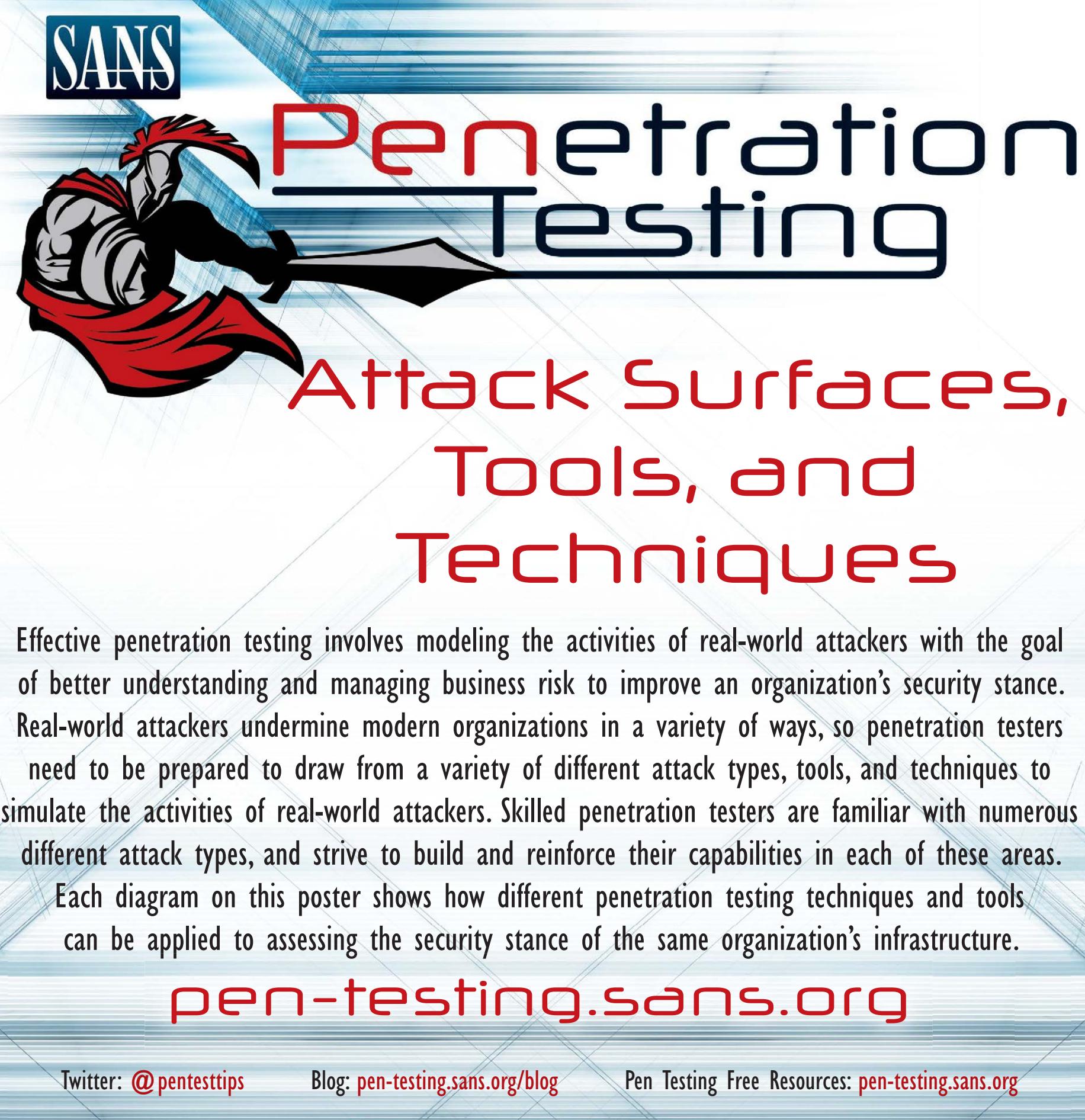
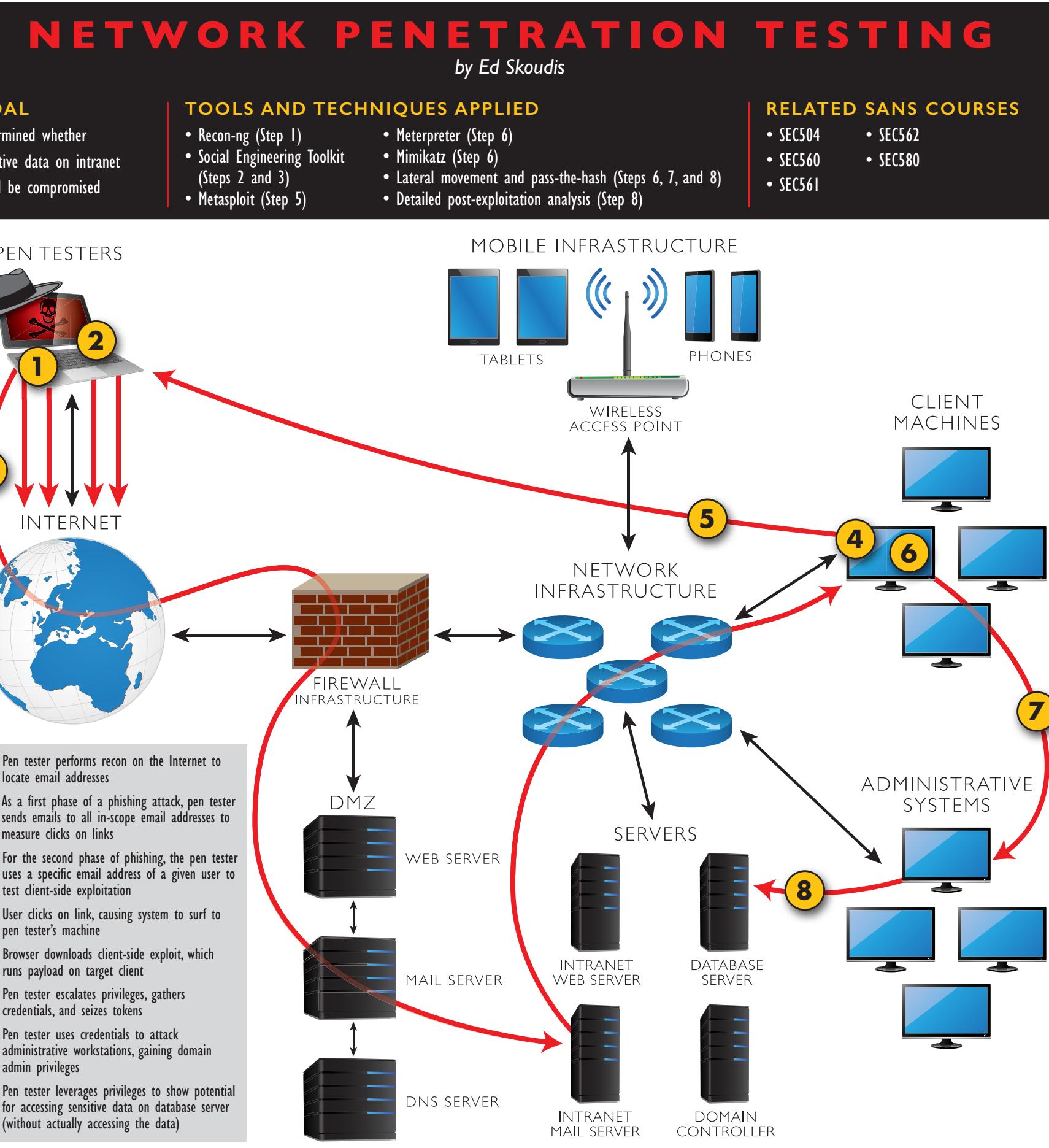
# Vulnerable Apps/Systems

New & Updated!  
JANUARY 2015

Created by Aman Hardikar .M

Building your skills through hands-on lab experimentation is vital in the life of a penetration tester. Aman Hardikar .M built a hugely useful mind map showing various free, publicly available distributions, challenges, and other resources for practicing your skills. The mind map is available on-line at [amanhardikar.com/mindmaps/Practice.html](http://amanhardikar.com/mindmaps/Practice.html), but feel free to use this poster version to check off the ones you've visited and beat. Thank you, Aman, for letting us include the mind map in this poster:





# Treasure Island

Robert Louis Stevenson



This eBook was designed and published by Planet PDF. For more free eBooks visit our Web site at <http://www.planetpdf.com/>. To hear about our latest releases subscribe to the [Planet PDF Newsletter](#).

## TREASURE ISLAND

To  
S.L.O.,  
an American gentleman  
in accordance with whose classic taste  
the following narrative has been designed,  
it is now, in return for numerous delightful hours,  
and with the kindest wishes,  
dedicated  
by his affectionate friend, the author.

## TO THE HESITATING PURCHASER

If sailor tales to sailor tunes,  
Storm and adventure, heat and cold,  
If schooners, islands, and maroons,  
And buccaneers, and buried gold,  
And all the old romance, retold  
Exactly in the ancient way,  
Can please, as me they pleased of old,  
The wiser youngsters of today:

—So be it, and fall on! If not,  
If studious youth no longer crave,  
His ancient appetites forgot,  
Kingston, or Ballantyne the brave,

*Treasure Island*

Or Cooper of the wood and wave:  
So be it, also! And may I  
And all my pirates share the grave  
Where these and their creations lie!

## PART ONE

### The Old Buccaneer

1

## **The Old Sea-dog at the Admiral Benbow**

SQUIRE TRELAWNEY, Dr. Livesey, and the rest of these gentlemen having asked me to write down the whole particulars about Treasure Island, from the beginning to the end, keeping nothing back but the bearings of the island, and that only because there is still treasure not yet lifted, I take up my pen in the year of grace 17 and go back to the time when my father kept the Admiral Benbow inn and the brown old seaman with the sabre cut first took up his lodging under our roof.

I remember him as if it were yesterday, as he came plodding to the inn door, his sea-chest following behind him in a hand-barrow—a tall, strong, heavy, nut-brown man, his tarry pigtail falling over the shoulder of his soiled blue coat, his hands ragged and scarred, with black, broken nails, and the sabre cut across one cheek, a dirty, livid white. I remember him looking round the cover and whistling to himself as he did so, and then breaking out in that old sea-song that he sang so often afterwards:

‘Fifteen men on the dead man’s chest—  
Yo-ho-ho, and a bottle of rum!’

in the high, old tottering voice that seemed to have been tuned and broken at the capstan bars. Then he rapped on the door with a bit of stick like a handspike that he carried, and when my father appeared, called roughly for a glass of rum. This, when it was brought to him, he drank slowly, like a connoisseur, lingering on the taste and still looking about him at the cliffs and up at our signboard.

‘This is a handy cove,’ says he at length; ‘and a pleasant sittyated grog-shop. Much company, mate?’

My father told him no, very little company, the more was the pity.

‘Well, then,’ said he, ‘this is the berth for me. Here you, matey,’ he cried to the man who trundled the barrow; ‘bring up alongside and help up my chest. I’ll stay here a bit,’ he continued. ‘I’m a plain man; rum and bacon and eggs is what I want, and that head up there for to watch ships off. What you mought call me? You mought call me captain. Oh, I see what you’re at— there”; and he threw down three or four gold pieces on the threshold. ‘You can tell me when I’ve worked through that,’ says he, looking as fierce as a commander.

And indeed bad as his clothes were and coarsely as he spoke, he had none of the appearance of a man who sailed

before the mast, but seemed like a mate or skipper accustomed to be obeyed or to strike. The man who came with the barrow told us the mail had set him down the morning before at the Royal George, that he had inquired what inns there were along the coast, and hearing ours well spoken of, I suppose, and described as lonely, had chosen it from the others for his place of residence. And that was all we could learn of our guest.

He was a very silent man by custom. All day he hung round the cove or upon the cliffs with a brass telescope; all evening he sat in a corner of the parlour next the fire and drank rum and water very strong. Mostly he would not speak when spoken to, only look up sudden and fierce and blow through his nose like a fog-horn; and we and the people who came about our house soon learned to let him be. Every day when he came back from his stroll he would ask if any seafaring men had gone by along the road. At first we thought it was the want of company of his own kind that made him ask this question, but at last we began to see he was desirous to avoid them. When a seaman did put up at the Admiral Benbow (as now and then some did, making by the coast road for Bristol) he would look in at him through the curtained door before he entered the parlour; and he was always sure to be as silent

as a mouse when any such was present. For me, at least, there was no secret about the matter, for I was, in a way, a sharer in his alarms. He had taken me aside one day and promised me a silver fourpenny on the first of every month if I would only keep my ‘weather-eye open for a seafaring man with one leg’ and let him know the moment he appeared. Often enough when the first of the month came round and I applied to him for my wage, he would only blow through his nose at me and stare me down, but before the week was out he was sure to think better of it, bring me my four-penny piece, and repeat his orders to look out for ‘the seafaring man with one leg.’

How that personage haunted my dreams, I need scarcely tell you. On stormy nights, when the wind shook the four corners of the house and the surf roared along the cove and up the cliffs, I would see him in a thousand forms, and with a thousand diabolical expressions. Now the leg would be cut off at the knee, now at the hip; now he was a monstrous kind of a creature who had never had but the one leg, and that in the middle of his body. To see him leap and run and pursue me over hedge and ditch was the worst of nightmares. And altogether I paid pretty dear for my monthly fourpenny piece, in the shape of these abominable fancies.

But though I was so terrified by the idea of the seafaring man with one leg, I was far less afraid of the captain himself than anybody else who knew him. There were nights when he took a deal more rum and water than his head would carry; and then he would sometimes sit and sing his wicked, old, wild sea-songs, minding nobody; but sometimes he would call for glasses round and force all the trembling company to listen to his stories or bear a chorus to his singing. Often I have heard the house shaking with ‘Yo-ho-ho, and a bottle of rum,’ all the neighbours joining in for dear life, with the fear of death upon them, and each singing louder than the other to avoid remark. For in these fits he was the most overriding companion ever known; he would slap his hand on the table for silence all round; he would fly up in a passion of anger at a question, or sometimes because none was put, and so he judged the company was not following his story. Nor would he allow anyone to leave the inn till he had drunk himself sleepy and reeled off to bed.

His stories were what frightened people worst of all. Dreadful stories they were—about hanging, and walking the plank, and storms at sea, and the Dry Tortugas, and wild deeds and places on the Spanish Main. By his own

account he must have lived his life among some of the wickedest men that God ever allowed upon the sea, and the language in which he told these stories shocked our plain country people almost as much as the crimes that he described. My father was always saying the inn would be ruined, for people would soon cease coming there to be tyrannized over and put down, and sent shivering to their beds; but I really believe his presence did us good. People were frightened at the time, but on looking back they rather liked it; it was a fine excitement in a quiet country life, and there was even a party of the younger men who pretended to admire him, calling him a ‘true sea-dog’ and a ‘real old salt’ and such like names, and saying there was the sort of man that made England terrible at sea.

In one way, indeed, he bade fair to ruin us, for he kept on staying week after week, and at last month after month, so that all the money had been long exhausted, and still my father never plucked up the heart to insist on having more. If ever he mentioned it, the captain blew through his nose so loudly that you might say he roared, and stared my poor father out of the room. I have seen him wringing his hands after such a rebuff, and I am sure the annoyance and the terror he lived in must have greatly hastened his early and unhappy death.

All the time he lived with us the captain made no change whatever in his dress but to buy some stockings from a hawker. One of the cocks of his hat having fallen down, he let it hang from that day forth, though it was a great annoyance when it blew. I remember the appearance of his coat, which he patched himself upstairs in his room, and which, before the end, was nothing but patches. He never wrote or received a letter, and he never spoke with any but the neighbours, and with these, for the most part, only when drunk on rum. The great sea-chest none of us had ever seen open.

He was only once crossed, and that was towards the end, when my poor father was far gone in a decline that took him off. Dr. Livesey came late one afternoon to see the patient, took a bit of dinner from my mother, and went into the parlour to smoke a pipe until his horse should come down from the hamlet, for we had no stabling at the old Benbow. I followed him in, and I remember observing the contrast the neat, bright doctor, with his powder as white as snow and his bright, black eyes and pleasant manners, made with the coltish country folk, and above all, with that filthy, heavy, bleared scarecrow of a pirate of ours, sitting, far gone in rum, with his arms on the

table. Suddenly he—the captain, that is—began to pipe up his eternal song:

‘Fifteen men on the dead man’s chest—  
Yo-ho-ho, and a bottle of rum!  
Drink and the devil had done for the rest—  
Yo-ho-ho, and a bottle of rum!’

At first I had supposed ‘the dead man’s chest’ to be that identical big box of his upstairs in the front room, and the thought had been mingled in my nightmares with that of the one-legged seafaring man. But by this time we had all long ceased to pay any particular notice to the song; it was new, that night, to nobody but Dr. Livesey, and on him I observed it did not produce an agreeable effect, for he looked up for a moment quite angrily before he went on with his talk to old Taylor, the gardener, on a new cure for the rheumatics. In the meantime, the captain gradually brightened up at his own music, and at last flapped his hand upon the table before him in a way we all knew to mean silence. The voices stopped at once, all but Dr. Livesey’s; he went on as before speaking clear and kind and drawing briskly at his pipe between every word or two. The captain glared at him for a while, flapped his hand again, glared still harder, and at last broke out with a villainous, low oath, ‘Silence, there, between decks!’

‘Were you addressing me, sir?’ says the doctor; and when the ruffian had told him, with another oath, that this was so, ‘I have only one thing to say to you, sir,’ replies the doctor, ‘that if you keep on drinking rum, the world will soon be quit of a very dirty scoundrel!’

The old fellow’s fury was awful. He sprang to his feet, drew and opened a sailor’s clasp-knife, and balancing it open on the palm of his hand, threatened to pin the doctor to the wall.

The doctor never so much as moved. He spoke to him as before, over his shoulder and in the same tone of voice, rather high, so that all the room might hear, but perfectly calm and steady: ‘If you do not put that knife this instant in your pocket, I promise, upon my honour, you shall hang at the next assizes.’

Then followed a battle of looks between them, but the captain soon knuckled under, put up his weapon, and resumed his seat, grumbling like a beaten dog.

‘And now, sir,’ continued the doctor, ‘since I now know there’s such a fellow in my district, you may count I’ll have an eye upon you day and night. I’m not a doctor only; I’m a magistrate; and if I catch a breath of complaint against you, if it’s only for a piece of incivility

like tonight's, I'll take effectual means to have you hunted down and routed out of this. Let that suffice.'

Soon after, Dr. Livesey's horse came to the door and he rode away, but the captain held his peace that evening, and for many evenings to come.

2

## **Black Dog Appears and Disappears**

IT was not very long after this that there occurred the first of the mysterious events that rid us at last of the captain, though not, as you will see, of his affairs. It was a bitter cold winter, with long, hard frosts and heavy gales; and it was plain from the first that my poor father was little likely to see the spring. He sank daily, and my mother and I had all the inn upon our hands, and were kept busy enough without paying much regard to our unpleasant guest.

It was one January morning, very early—a pinching, frosty morning—the cove all grey with hoar-frost, the ripple lapping softly on the stones, the sun still low and only touching the hilltops and shining far to seaward. The captain had risen earlier than usual and set out down the beach, his cutlass swinging under the broad skirts of the old blue coat, his brass telescope under his arm, his hat tilted back upon his head. I remember his breath hanging like smoke in his wake as he strode off, and the last sound I heard of him as he turned the big rock was a loud snort

of indignation, as though his mind was still running upon Dr. Livesey.

Well, mother was upstairs with father and I was laying the breakfast-table against the captain's return when the parlour door opened and a man stepped in on whom I had never set my eyes before. He was a pale, tallowy creature, wanting two fingers of the left hand, and though he wore a cutlass, he did not look much like a fighter. I had always my eye open for seafaring men, with one leg or two, and I remember this one puzzled me. He was not sailorly, and yet he had a smack of the sea about him too.

I asked him what was for his service, and he said he would take rum; but as I was going out of the room to fetch it, he sat down upon a table and motioned me to draw near. I paused where I was, with my napkin in my hand.

‘Come here, sonny,’ says he. ‘Come nearer here.’

I took a step nearer.

‘Is this here table for my mate Bill?’ he asked with a kind of leer.

I told him I did not know his mate Bill, and this was for a person who stayed in our house whom we called the captain.

‘Well,’ said he, ‘my mate Bill would be called the captain, as like as not. He has a cut on one cheek and a mighty pleasant way with him, particularly in drink, has my mate Bill. We’ll put it, for argument like, that your captain has a cut on one cheek—and we’ll put it, if you like, that that cheek’s the right one. Ah, well! I told you. Now, is my mate Bill in this here house?’

I told him he was out walking.

‘Which way, sonny? Which way is he gone?’

And when I had pointed out the rock and told him how the captain was likely to return, and how soon, and answered a few other questions, ‘Ah,’ said he, ‘this’ll be as good as drink to my mate Bill.’

The expression of his face as he said these words was not at all pleasant, and I had my own reasons for thinking that the stranger was mistaken, even supposing he meant what he said. But it was no affair of mine, I thought; and besides, it was difficult to know what to do. The stranger kept hanging about just inside the inn door, peering round the corner like a cat waiting for a mouse. Once I stepped out myself into the road, but he immediately called me back, and as I did not obey quick enough for his fancy, a most horrible change came over his tallowy face, and he ordered me in with an oath that made me jump. As soon

as I was back again he returned to his former manner, half fawning, half sneering, patted me on the shoulder, told me I was a good boy and he had taken quite a fancy to me. ‘I have a son of my own,’ said he, ‘as like you as two blocks, and he’s all the pride of my ‘art. But the great thing for boys is discipline, sonny—discipline. Now, if you had sailed along of Bill, you wouldn’t have stood there to be spoke to twice—not you. That was never Bill’s way, nor the way of sich as sailed with him. And here, sure enough, is my mate Bill, with a spy-glass under his arm, bless his old ‘art, to be sure. You and me’ll just go back into the parlour, sonny, and get behind the door, and we’ll give Bill a little surprise—bless his ‘art, I say again.

So saying, the stranger backed along with me into the parlour and put me behind him in the corner so that we were both hidden by the open door. I was very uneasy and alarmed, as you may fancy, and it rather added to my fears to observe that the stranger was certainly frightened himself. He cleared the hilt of his cutlass and loosened the blade in the sheath; and all the time we were waiting there he kept swallowing as if he felt what we used to call a lump in the throat.

At last in strode the captain, slammed the door behind him, without looking to the right or left, and marched

straight across the room to where his breakfast awaited him.

‘Bill,’ said the stranger in a voice that I thought he had tried to make bold and big.

The captain spun round on his heel and fronted us; all the brown had gone out of his face, and even his nose was blue; he had the look of a man who sees a ghost, or the evil one, or something worse, if anything can be; and upon my word, I felt sorry to see him all in a moment turn so old and sick.

‘Come, Bill, you know me; you know an old shipmate, Bill, surely,’ said the stranger.

The captain made a sort of gasp.

‘Black Dog!’ said he.

‘And who else?’ returned the other, getting more at his ease. ‘Black Dog as ever was, come for to see his old shipmate Billy, at the Admiral Benbow inn. Ah, Bill, Bill, we have seen a sight of times, us two, since I lost them two talons,’ holding up his mutilated hand.

‘Now, look here,’ said the captain; ‘you’ve run me down; here I am; well, then, speak up; what is it?’

‘That’s you, Bill,’ returned Black Dog, ‘you’re in the right of it, Billy. I’ll have a glass of rum from this dear

child here, as I've took such a liking to; and we'll sit down, if you please, and talk square, like old shipmates.'

When I returned with the rum, they were already seated on either side of the captain's breakfast-table—Black Dog next to the door and sitting sideways so as to have one eye on his old shipmate and one, as I thought, on his retreat.

He bade me go and leave the door wide open. 'None of your keyholes for me, sonny,' he said; and I left them together and retired into the bar.

'For a long time, though I certainly did my best to listen, I could hear nothing but a low gattling; but at last the voices began to grow higher, and I could pick up a word or two, mostly oaths, from the captain.

'No, no, no, no; and an end of it!' he cried once. And again, 'If it comes to swinging, swing all, say I.'

Then all of a sudden there was a tremendous explosion of oaths and other noises—the chair and table went over in a lump, a clash of steel followed, and then a cry of pain, and the next instant I saw Black Dog in full flight, and the captain hotly pursuing, both with drawn cutlasses, and the former streaming blood from the left shoulder. Just at the door the captain aimed at the fugitive one last tremendous cut, which would certainly have split him to

the chine had it not been intercepted by our big signboard of Admiral Benbow. You may see the notch on the lower side of the frame to this day.

That blow was the last of the battle. Once out upon the road, Black Dog, in spite of his wound, showed a wonderful clean pair of heels and disappeared over the edge of the hill in half a minute. The captain, for his part, stood staring at the signboard like a bewildered man. Then he passed his hand over his eyes several times and at last turned back into the house.

'Jim,' says he, 'rum"; and as he spoke, he reeled a little, and caught himself with one hand against the wall.

'Are you hurt?' cried I.

'Rum,' he repeated. 'I must get away from here. Rum! Rum!'

I ran to fetch it, but I was quite unsteady by all that had fallen out, and I broke one glass and fouled the tap, and while I was still getting in my own way, I heard a loud fall in the parlour, and running in, beheld the captain lying full length upon the floor. At the same instant my mother, alarmed by the cries and fighting, came running downstairs to help me. Between us we raised his head. He was breathing very loud and hard, but his eyes were closed and his face a horrible colour.

‘Dear, deary me,’ cried my mother, ‘what a disgrace upon the house! And your poor father sick!’

In the meantime, we had no idea what to do to help the captain, nor any other thought but that he had got his death-hurt in the scuffle with the stranger. I got the rum, to be sure, and tried to put it down his throat, but his teeth were tightly shut and his jaws as strong as iron. It was a happy relief for us when the door opened and Doctor Livesey came in, on his visit to my father.

‘Oh, doctor,’ we cried, ‘what shall we do? Where is he wounded?’

‘Wounded? A fiddle-stick’s end!’ said the doctor. ‘No more wounded than you or I. The man has had a stroke, as I warned him. Now, Mrs. Hawkins, just you run upstairs to your husband and tell him, if possible, nothing about it. For my part, I must do my best to save this fellow’s trebly worthless life; Jim, you get me a basin.’

When I got back with the basin, the doctor had already ripped up the captain’s sleeve and exposed his great sinewy arm. It was tattooed in several places. ‘Here’s luck,’ ‘A fair wind,’ and ‘Billy Bones his fancy,’ were very neatly and clearly executed on the forearm; and up near the shoulder there was a sketch of a gallows and a

man hanging from it—done, as I thought, with great spirit.

‘Prophetic,’ said the doctor, touching this picture with his finger. ‘And now, Master Billy Bones, if that be your name, we’ll have a look at the colour of your blood. Jim,’ he said, ‘are you afraid of blood?’

‘No, sir,’ said I.

‘Well, then,’ said he, ‘you hold the basin’; and with that he took his lancet and opened a vein.

A great deal of blood was taken before the captain opened his eyes and looked mistily about him. First he recognized the doctor with an unmistakable frown; then his glance fell upon me, and he looked relieved. But suddenly his colour changed, and he tried to raise himself, crying, ‘Where’s Black Dog?’

‘There is no Black Dog here,’ said the doctor, ‘except what you have on your own back. You have been drinking rum; you have had a stroke, precisely as I told you; and I have just, very much against my own will, dragged you headforemost out of the grave. Now, Mr. Bones—’

‘That’s not my name,’ he interrupted.

‘Much I care,’ returned the doctor. ‘It’s the name of a buccaneer of my acquaintance; and I call you by it for the

sake of shortness, and what I have to say to you is this; one glass of rum won't kill you, but if you take one you'll take another and another, and I stake my wig if you don't break off short, you'll die— do you understand that?— die, and go to your own place, like the man in the Bible. Come, now, make an effort. I'll help you to your bed for once.'

Between us, with much trouble, we managed to hoist him upstairs, and laid him on his bed, where his head fell back on the pillow as if he were almost fainting.

'Now, mind you,' said the doctor, 'I clear my conscience—the name of rum for you is death.'

And with that he went off to see my father, taking me with him by the arm.

'This is nothing,' he said as soon as he had closed the door. 'I have drawn blood enough to keep him quiet awhile; he should lie for a week where he is—that is the best thing for him and you; but another stroke would settle him.'

3

## The Black Spot

ABOUT noon I stopped at the captain's door with some cooling drinks and medicines. He was lying very much as we had left him, only a little higher, and he seemed both weak and excited.

'Jim,' he said, 'you're the only one here that's worth anything, and you know I've been always good to you. Never a month but I've given you a silver fourpenny for yourself. And now you see, mate, I'm pretty low, and deserted by all; and Jim, you'll bring me one noggin of rum, now, won't you, matey?'

'The doctor—' I began.

But he broke in cursing the doctor, in a feeble voice but heartily. 'Doctors is all swabs,' he said; 'and that doctor there, why, what do he know about seafaring men? I been in places hot as pitch, and mates dropping round with Yellow Jack, and the blessed land a-heaving like the sea with earthquakes—what to the doctor know of lands like that?—and I lived on rum, I tell you. It's been meat and drink, and man and wife, to me; and if I'm not to

have my rum now I'm a poor old hulk on a lee shore, my blood'll be on you, Jim, and that doctor swab"; and he ran on again for a while with curses. 'Look, Jim, how my fingers fidgets,' he continued in the pleading tone. 'I can't keep 'em still, not I. I haven't had a drop this blessed day. That doctor's a fool, I tell you. If I don't have a drain o' rum, Jim, I'll have the horrors; I seen some on 'em already. I seen old Flint in the corner there, behind you; as plain as print, I seen him; and if I get the horrors, I'm a man that has lived rough, and I'll raise Cain. Your doctor hisself said one glass wouldn't hurt me. I'll give you a golden guinea for a noggin, Jim.'

He was growing more and more excited, and this alarmed me for my father, who was very low that day and needed quiet; besides, I was reassured by the doctor's words, now quoted to me, and rather offended by the offer of a bribe.

'I want none of your money,' said I, 'but what you owe my father. I'll get you one glass, and no more.'

When I brought it to him, he seized it greedily and drank it out.

'Aye, aye,' said he, 'that's some better, sure enough. And now, matey, did that doctor say how long I was to lie here in this old berth?'

## Treasure Island

‘A week at least,’ said I.

‘Thunder!’ he cried. ‘A week! I can’t do that; they’d have the black spot on me by then. The lubbers is going about to get the wind of me this blessed moment; lubbers as couldn’t keep what they got, and want to nail what is another’s. Is that seamanly behaviour, now, I want to know? But I’m a saving soul. I never wasted good money of mine, nor lost it neither; and I’ll trick ‘em again. I’m not afraid on ‘em. I’ll shake out another reef, matey, and daddle ‘em again.’

As he was thus speaking, he had risen from bed with great difficulty, holding to my shoulder with a grip that almost made me cry out, and moving his legs like so much dead weight. His words, spirited as they were in meaning, contrasted sadly with the weakness of the voice in which they were uttered. He paused when he had got into a sitting position on the edge.

‘That doctor’s done me,’ he murmured. ‘My ears is singing. Lay me back.’

Before I could do much to help him he had fallen back again to his former place, where he lay for a while silent.

‘Jim,’ he said at length, ‘you saw that seafaring man today?’

‘Black Dog?’ I asked.

‘Ah! Black Dog,’ says he. ‘HE’S a bad un; but there’s worse that put him on. Now, if I can’t get away nohow, and they tip me the black spot, mind you, it’s my old sea-chest they’re after; you get on a horse—you can, can’t you? Well, then, you get on a horse, and go to— well, yes, I will!—to that eternal doctor swab, and tell him to pipe all hands—magistrates and sich—and he’ll lay ‘em aboard at the Admiral Benbow—all old Flint’s crew, man and boy, all on ‘em that’s left. I was first mate, I was, old Flint’s first mate, and I’m the on’y one as knows the place. He gave it me at Savannah, when he lay a-dying, like as if I was to now, you see. But you won’t peach unless they get the black spot on me, or unless you see that Black Dog again or a seafaring man with one leg, Jim—him above all.’

‘But what is the black spot, captain?’ I asked.

‘That’s a summons, mate. I’ll tell you if they get that. But you keep your weather-eye open, Jim, and I’ll share with you equals, upon my honour.’

He wandered a little longer, his voice growing weaker; but soon after I had given him his medicine, which he took like a child, with the remark, ‘If ever a seaman wanted drugs, it’s me,’ he fell at last into a heavy, swoon-like sleep, in which I left him. What I should have done

had all gone well I do not know. Probably I should have told the whole story to the doctor, for I was in mortal fear lest the captain should repent of his confessions and make an end of me. But as things fell out, my poor father died quite suddenly that evening, which put all other matters on one side. Our natural distress, the visits of the neighbours, the arranging of the funeral, and all the work of the inn to be carried on in the meanwhile kept me so busy that I had scarcely time to think of the captain, far less to be afraid of him.

He got downstairs next morning, to be sure, and had his meals as usual, though he ate little and had more, I am afraid, than his usual supply of rum, for he helped himself out of the bar, scowling and blowing through his nose, and no one dared to cross him. On the night before the funeral he was as drunk as ever; and it was shocking, in that house of mourning, to hear him singing away at his ugly old sea-song; but weak as he was, we were all in the fear of death for him, and the doctor was suddenly taken up with a case many miles away and was never near the house after my father's death. I have said the captain was weak, and indeed he seemed rather to grow weaker than regain his strength. He clambered up and down stairs, and went from the parlour to the bar and back again, and

sometimes put his nose out of doors to smell the sea, holding on to the walls as he went for support and breathing hard and fast like a man on a steep mountain. He never particularly addressed me, and it is my belief he had as good as forgotten his confidences; but his temper was more flighty, and allowing for his bodily weakness, more violent than ever. He had an alarming way now when he was drunk of drawing his cutlass and laying it bare before him on the table. But with all that, he minded people less and seemed shut up in his own thoughts and rather wandering. Once, for instance, to our extreme wonder, he piped up to a different air, a kind of country love-song that he must have learned in his youth before he had begun to follow the sea.

So things passed until, the day after the funeral, and about three o'clock of a bitter, foggy, frosty afternoon, I was standing at the door for a moment, full of sad thoughts about my father, when I saw someone drawing slowly near along the road. He was plainly blind, for he tapped before him with a stick and wore a great green shade over his eyes and nose; and he was hunched, as if with age or weakness, and wore a huge old tattered sea-cloak with a hood that made him appear positively deformed. I never saw in my life a more dreadful-looking

figure. He stopped a little from the inn, and raising his voice in an odd sing-song, addressed the air in front of him, ‘Will any kind friend inform a poor blind man, who has lost the precious sight of his eyes in the gracious defence of his native country, England—and God bless King George!—where or in what part of this country he may now be?’

‘You are at the Admiral Benbow, Black Hill Cove, my good man,’ said I.

‘I hear a voice,’ said he, ‘a young voice. Will you give me your hand, my kind young friend, and lead me in?’

I held out my hand, and the horrible, soft-spoken, eyeless creature gripped it in a moment like a vise. I was so much startled that I struggled to withdraw, but the blind man pulled me close up to him with a single action of his arm.

‘Now, boy,’ he said, ‘take me in to the captain.’

‘Sir,’ said I, ‘upon my word I dare not.’

‘Oh,’ he sneered, ‘that’s it! Take me in straight or I’ll break your arm.’

And he gave it, as he spoke, a wrench that made me cry out.

‘Sir,’ said I, ‘it is for yourself I mean. The captain is not what he used to be. He sits with a drawn cutlass. Another gentleman—’

‘Come, now, march,’ interrupted he; and I never heard a voice so cruel, and cold, and ugly as that blind man’s. It cowed me more than the pain, and I began to obey him at once, walking straight in at the door and towards the parlour, where our sick old buccaneer was sitting, dazed with rum. The blind man clung close to me, holding me in one iron fist and leaning almost more of his weight on me than I could carry. ‘Lead me straight up to him, and when I’m in view, cry out, ‘Here’s a friend for you, Bill.’ If you don’t, I’ll do this,’ and with that he gave me a twitch that I thought would have made me faint. Between this and that, I was so utterly terrified of the blind beggar that I forgot my terror of the captain, and as I opened the parlour door, cried out the words he had ordered in a trembling voice.

The poor captain raised his eyes, and at one look the rum went out of him and left him staring sober. The expression of his face was not so much of terror as of mortal sickness. He made a movement to rise, but I do not believe he had enough force left in his body.

‘Now, Bill, sit where you are,’ said the beggar. ‘If I can’t see, I can hear a finger stirring. Business is business. Hold out your left hand. Boy, take his left hand by the wrist and bring it near to my right.’

We both obeyed him to the letter, and I saw him pass something from the hollow of the hand that held his stick into the palm of the captain’s, which closed upon it instantly.

‘And now that’s done,’ said the blind man; and at the words he suddenly left hold of me, and with incredible accuracy and nimbleness, skipped out of the parlour and into the road, where, as I still stood motionless, I could hear his stick go tap-tap-tapping into the distance.

It was some time before either I or the captain seemed to gather our senses, but at length, and about at the same moment, I released his wrist, which I was still holding, and he drew in his hand and looked sharply into the palm.

‘Ten o’clock!’ he cried. ‘Six hours. We’ll do them yet,’ and he sprang to his feet.

Even as he did so, he reeled, put his hand to his throat, stood swaying for a moment, and then, with a peculiar sound, fell from his whole height face foremost to the floor.

I ran to him at once, calling to my mother. But haste was all in vain. The captain had been struck dead by thundering apoplexy. It is a curious thing to understand, for I had certainly never liked the man, though of late I had begun to pity him, but as soon as I saw that he was dead, I burst into a flood of tears. It was the second death I had known, and the sorrow of the first was still fresh in my heart.

## The Sea-chest

I LOST no time, of course, in telling my mother all that I knew, and perhaps should have told her long before, and we saw ourselves at once in a difficult and dangerous position. Some of the man's money—if he had any—was certainly due to us, but it was not likely that our captain's shipmates, above all the two specimens seen by me, Black Dog and the blind beggar, would be inclined to give up their booty in payment of the dead man's debts. The captain's order to mount at once and ride for Doctor Livesey would have left my mother alone and unprotected, which was not to be thought of. Indeed, it seemed impossible for either of us to remain much longer in the house; the fall of coals in the kitchen grate, the very ticking of the clock, filled us with alarms. The neighbourhood, to our ears, seemed haunted by approaching footsteps; and what between the dead body of the captain on the parlour floor and the thought of that detestable blind beggar hovering near at hand and ready to return, there were moments when, as the saying goes, I

jumped in my skin for terror. Something must speedily be resolved upon, and it occurred to us at last to go forth together and seek help in the neighbouring hamlet. No sooner said than done. Bare-headed as we were, we ran out at once in the gathering evening and the frosty fog.

The hamlet lay not many hundred yards away, though out of view, on the other side of the next cove; and what greatly encouraged me, it was in an opposite direction from that whence the blind man had made his appearance and whither he had presumably returned. We were not many minutes on the road, though we sometimes stopped to lay hold of each other and hearken. But there was no unusual sound—nothing but the low wash of the ripple and the croaking of the inmates of the wood.

It was already candle-light when we reached the hamlet, and I shall never forget how much I was cheered to see the yellow shine in doors and windows; but that, as it proved, was the best of the help we were likely to get in that quarter. For—you would have thought men would have been ashamed of themselves—no soul would consent to return with us to the Admiral Benbow. The more we told of our troubles, the more—man, woman, and child—they clung to the shelter of their houses. The name of Captain Flint, though it was strange to me, was

well enough known to some there and carried a great weight of terror. Some of the men who had been to field-work on the far side of the Admiral Benbow remembered, besides, to have seen several strangers on the road, and taking them to be smugglers, to have bolted away; and one at least had seen a little lugger in what we called Kitt's Hole. For that matter, anyone who was a comrade of the captain's was enough to frighten them to death. And the short and the long of the matter was, that while we could get several who were willing enough to ride to Dr. Livesey's, which lay in another direction, not one would help us to defend the inn.

They say cowardice is infectious; but then argument is, on the other hand, a great emboldener; and so when each had said his say, my mother made them a speech. She would not, she declared, lose money that belonged to her fatherless boy; 'If none of the rest of you dare,' she said, 'Jim and I dare. Back we will go, the way we came, and small thanks to you big, hulking, chicken-hearted men. We'll have that chest open, if we die for it. And I'll thank you for that bag, Mrs. Crossley, to bring back our lawful money in.'

Of course I said I would go with my mother, and of course they all cried out at our foolhardiness, but even

then not a man would go along with us. All they would do was to give me a loaded pistol lest we were attacked, and to promise to have horses ready saddled in case we were pursued on our return, while one lad was to ride forward to the doctor's in search of armed assistance.

My heart was beating finely when we two set forth in the cold night upon this dangerous venture. A full moon was beginning to rise and peered redly through the upper edges of the fog, and this increased our haste, for it was plain, before we came forth again, that all would be as bright as day, and our departure exposed to the eyes of any watchers. We slipped along the hedges, noiseless and swift, nor did we see or hear anything to increase our terrors, till, to our relief, the door of the Admiral Benbow had closed behind us.

I slipped the bolt at once, and we stood and panted for a moment in the dark, alone in the house with the dead captain's body. Then my mother got a candle in the bar, and holding each other's hands, we advanced into the parlour. He lay as we had left him, on his back, with his eyes open and one arm stretched out.

'Draw down the blind, Jim,' whispered my mother; 'they might come and watch outside. And now,' said she when I had done so, 'we have to get the key off THAT;

## Treasure Island

and who's to touch it, I should like to know!" and she gave a kind of sob as she said the words.

I went down on my knees at once. On the floor close to his hand there was a little round of paper, blackened on the one side. I could not doubt that this was the BLACK SPOT; and taking it up, I found written on the other side, in a very good, clear hand, this short message: 'You have till ten tonight.'

'He had till ten, Mother,' said I; and just as I said it, our old clock began striking. This sudden noise startled us shockingly; but the news was good, for it was only six.

'Now, Jim,' she said, 'that key.'

I felt in his pockets, one after another. A few small coins, a thimble, and some thread and big needles, a piece of pigtail tobacco bitten away at the end, his gully with the crooked handle, a pocket compass, and a tinder box were all that they contained, and I began to despair.

'Perhaps it's round his neck,' suggested my mother.

Overcoming a strong repugnance, I tore open his shirt at the neck, and there, sure enough, hanging to a bit of tarry string, which I cut with his own gully, we found the key. At this triumph we were filled with hope and hurried upstairs without delay to the little room where he had

slept so long and where his box had stood since the day of his arrival.

It was like any other seaman's chest on the outside, the initial 'B' burned on the top of it with a hot iron, and the corners somewhat smashed and broken as by long, rough usage.

'Give me the key,' said my mother; and though the lock was very stiff, she had turned it and thrown back the lid in a twinkling.

A strong smell of tobacco and tar rose from the interior, but nothing was to be seen on the top except a suit of very good clothes, carefully brushed and folded. They had never been worn, my mother said. Under that, the miscellany began—a quadrant, a tin canikin, several sticks of tobacco, two brace of very handsome pistols, a piece of bar silver, an old Spanish watch and some other trinkets of little value and mostly of foreign make, a pair of compasses mounted with brass, and five or six curious West Indian shells. I have often wondered since why he should have carried about these shells with him in his wandering, guilty, and hunted life.

In the meantime, we had found nothing of any value but the silver and the trinkets, and neither of these were in our way. Underneath there was an old boat-cloak,

whitened with sea-salt on many a harbour-bar. My mother pulled it up with impatience, and there lay before us, the last things in the chest, a bundle tied up in oilcloth, and looking like papers, and a canvas bag that gave forth, at a touch, the jingle of gold.

'I'll show these rogues that I'm an honest woman,' said my mother. 'I'll have my dues, and not a farthing over. Hold Mrs. Crossley's bag.' And she began to count over the amount of the captain's score from the sailor's bag into the one that I was holding.

It was a long, difficult business, for the coins were of all countries and sizes—doubloons, and louis d'ors, and guineas, and pieces of eight, and I know not what besides, all shaken together at random. The guineas, too, were about the scarcest, and it was with these only that my mother knew how to make her count.

When we were about half-way through, I suddenly put my hand upon her arm, for I had heard in the silent frosty air a sound that brought my heart into my mouth—the tap-tapping of the blind man's stick upon the frozen road. It drew nearer and nearer, while we sat holding our breath. Then it struck sharp on the inn door, and then we could hear the handle being turned and the bolt rattling as the wretched being tried to enter; and then there was a

long time of silence both within and without. At last the tapping recommenced, and, to our indescribable joy and gratitude, died slowly away again until it ceased to be heard.

‘Mother,’ said I, ‘take the whole and let’s be going,’ for I was sure the bolted door must have seemed suspicious and would bring the whole hornet’s nest about our ears, though how thankful I was that I had bolted it, none could tell who had never met that terrible blind man.

But my mother, frightened as she was, would not consent to take a fraction more than was due to her and was obstinately unwilling to be content with less. It was not yet seven, she said, by a long way; she knew her rights and she would have them; and she was still arguing with me when a little low whistle sounded a good way off upon the hill. That was enough, and more than enough, for both of us.

‘I’ll take what I have,’ she said, jumping to her feet.

‘And I’ll take this to square the count,’ said I, picking up the oilskin packet.

Next moment we were both groping downstairs, leaving the candle by the empty chest; and the next we had opened the door and were in full retreat. We had not started a moment too soon. The fog was rapidly

dispersing; already the moon shone quite clear on the high ground on either side; and it was only in the exact bottom of the dell and round the tavern door that a thin veil still hung unbroken to conceal the first steps of our escape. Far less than half-way to the hamlet, very little beyond the bottom of the hill, we must come forth into the moonlight. Nor was this all, for the sound of several footsteps running came already to our ears, and as we looked back in their direction, a light tossing to and fro and still rapidly advancing showed that one of the newcomers carried a lantern.

‘My dear,’ said my mother suddenly, ‘take the money and run on. I am going to faint.’

This was certainly the end for both of us, I thought. How I cursed the cowardice of the neighbours; how I blamed my poor mother for her honesty and her greed, for her past foolhardiness and present weakness! We were just at the little bridge, by good fortune; and I helped her, tottering as she was, to the edge of the bank, where, sure enough, she gave a sigh and fell on my shoulder. I do not know how I found the strength to do it at all, and I am afraid it was roughly done, but I managed to drag her down the bank and a little way under the arch. Farther I could not move her, for the bridge was too low to let me

do more than crawl below it. So there we had to stay—my mother almost entirely exposed and both of us within earshot of the inn.

## The Last of the Blind Man

MY curiosity, in a sense, was stronger than my fear, for I could not remain where I was, but crept back to the bank again, whence, sheltering my head behind a bush of broom, I might command the road before our door. I was scarcely in position ere my enemies began to arrive, seven or eight of them, running hard, their feet beating out of time along the road and the man with the lantern some paces in front. Three men ran together, hand in hand; and I made out, even through the mist, that the middle man of this trio was the blind beggar. The next moment his voice showed me that I was right.

‘Down with the door!’ he cried.

‘Aye, aye, sir!’ answered two or three; and a rush was made upon the Admiral Benbow, the lantern-bearer following; and then I could see them pause, and hear speeches passed in a lower key, as if they were surprised to find the door open. But the pause was brief, for the blind man again issued his commands. His voice sounded

louder and higher, as if he were afire with eagerness and rage.

‘In, in, in!’ he shouted, and cursed them for their delay.

Four or five of them obeyed at once, two remaining on the road with the formidable beggar. There was a pause, then a cry of surprise, and then a voice shouting from the house, ‘Bill’s dead.’

But the blind man swore at them again for their delay.

‘Search him, some of you shirking lubbers, and the rest of you aloft and get the chest,’ he cried.

I could hear their feet rattling up our old stairs, so that the house must have shook with it. Promptly afterwards, fresh sounds of astonishment arose; the window of the captain’s room was thrown open with a slam and a jingle of broken glass, and a man leaned out into the moonlight, head and shoulders, and addressed the blind beggar on the road below him.

‘Pew,’ he cried, ‘they’ve been before us. Someone’s turned the chest out alow and aloft.’

‘Is it there?’ roared Pew.

‘The money’s there.’

The blind man cursed the money.

‘Flint’s fist, I mean,’ he cried.

‘We don’t see it here nohow,’ returned the man.

‘Here, you below there, is it on Bill?’ cried the blind man again.

At that another fellow, probably him who had remained below to search the captain’s body, came to the door of the inn. ‘Bill’s been overhauled a’ready,’ said he; ‘nothin’ left.’

‘It’s these people of the inn—it’s that boy. I wish I had put his eyes out!’ cried the blind man, Pew. ‘There were no time ago—they had the door bolted when I tried it. Scatter, lads, and find ‘em.’

‘Sure enough, they left their glim here,’ said the fellow from the window.

‘Scatter and find ‘em! Rout the house out!’ reiterated Pew, striking with his stick upon the road.

Then there followed a great to-do through all our old inn, heavy feet pounding to and fro, furniture thrown over, doors kicked in, until the very rocks re-echoed and the men came out again, one after another, on the road and declared that we were nowhere to be found. And just the same whistle that had alarmed my mother and myself over the dead captain’s money was once more clearly audible through the night, but this time twice repeated. I had thought it to be the blind man’s trumpet, so to speak, summoning his crew to the assault, but I now found that it

was a signal from the hillside towards the hamlet, and from its effect upon the buccaneers, a signal to warn them of approaching danger.

‘There’s Dirk again,’ said one. ‘Twice! We’ll have to budge, mates.’

‘Budge, you skulk!’ cried Pew. ‘Dirk was a fool and a coward from the first—you wouldn’t mind him. They must be close by; they can’t be far; you have your hands on it. Scatter and look for them, dogs! Oh, shiver my soul,’ he cried, ‘if I had eyes!’

This appeal seemed to produce some effect, for two of the fellows began to look here and there among the lumber, but half-heartedly, I thought, and with half an eye to their own danger all the time, while the rest stood irresolute on the road.

‘You have your hands on thousands, you fools, and you hang a leg! You’d be as rich as kings if you could find it, and you know it’s here, and you stand there skulking. There wasn’t one of you dared face Bill, and I did it—a blind man! And I’m to lose my chance for you! I’m to be a poor, crawling beggar, sponging for rum, when I might be rolling in a coach! If you had the pluck of a weevil in a biscuit you would catch them still.’

‘Hang it, Pew, we’ve got the doubloons!’ grumbled one.

‘They might have hid the blessed thing,’ said another. ‘Take the Georges, Pew, and don’t stand here squalling.’

Squalling was the word for it; Pew’s anger rose so high at these objections till at last, his passion completely taking the upper hand, he struck at them right and left in his blindness and his stick sounded heavily on more than one.

These, in their turn, cursed back at the blind miscreant, threatened him in horrid terms, and tried in vain to catch the stick and wrest it from his grasp.

This quarrel was the saving of us, for while it was still raging, another sound came from the top of the hill on the side of the hamlet—the tramp of horses galloping. Almost at the same time a pistol-shot, flash and report, came from the hedge side. And that was plainly the last signal of danger, for the buccaneers turned at once and ran, separating in every direction, one seaward along the cove, one slant across the hill, and so on, so that in half a minute not a sign of them remained but Pew. Him they had deserted, whether in sheer panic or out of revenge for his ill words and blows I know not; but there he remained behind, tapping up and down the road in a frenzy, and

groping and calling for his comrades. Finally he took a wrong turn and ran a few steps past me, towards the hamlet, crying, ‘Johnny, Black Dog, Dirk,’ and other names, ‘you won’t leave old Pew, mates—not old Pew!’

Just then the noise of horses topped the rise, and four or five riders came in sight in the moonlight and swept at full gallop down the slope.

At this Pew saw his error, turned with a scream, and ran straight for the ditch, into which he rolled. But he was on his feet again in a second and made another dash, now utterly bewildered, right under the nearest of the coming horses.

The rider tried to save him, but in vain. Down went Pew with a cry that rang high into the night; and the four hoofs trampled and spurned him and passed by. He fell on his side, then gently collapsed upon his face and moved no more.

I leaped to my feet and hailed the riders. They were pulling up, at any rate, horrified at the accident; and I soon saw what they were. One, tailing out behind the rest, was a lad that had gone from the hamlet to Dr. Livesey’s; the rest were revenue officers, whom he had met by the way, and with whom he had had the intelligence to return at once. Some news of the lugger in Kitt’s Hole had found

## Treasure Island

its way to Supervisor Dance and set him forth that night in our direction, and to that circumstance my mother and I owed our preservation from death.

Pew was dead, stone dead. As for my mother, when we had carried her up to the hamlet, a little cold water and salts and that soon brought her back again, and she was none the worse for her terror, though she still continued to deplore the balance of the money. In the meantime the supervisor rode on, as fast as he could, to Kitt's Hole; but his men had to dismount and grope down the dingle, leading, and sometimes supporting, their horses, and in continual fear of ambushes; so it was no great matter for surprise that when they got down to the Hole the lugger was already under way, though still close in. He hailed her. A voice replied, telling him to keep out of the moonlight or he would get some lead in him, and at the same time a bullet whistled close by his arm. Soon after, the lugger doubled the point and disappeared. Mr. Dance stood there, as he said, 'like a fish out of water,' and all he could do was to dispatch a man to B—— to warn the cutter. 'And that,' said he, 'is just about as good as nothing. They've got off clean, and there's an end. 'Only,' he added, 'I'm glad I trod on Master Pew's corns,' for by this time he had heard my story.

I went back with him to the Admiral Benbow, and you cannot imagine a house in such a state of smash; the very clock had been thrown down by these fellows in their furious hunt after my mother and myself; and though nothing had actually been taken away except the captain's money-bag and a little silver from the till, I could see at once that we were ruined. Mr. Dance could make nothing of the scene.

'They got the money, you say? Well, then, Hawkins, what in fortune were they after? More money, I suppose?'

'No, sir; not money, I think,' replied I. 'In fact, sir, I believe I have the thing in my breast pocket; and to tell you the truth, I should like to get it put in safety.'

'To be sure, boy; quite right,' said he. 'I'll take it, if you like.'

'I thought perhaps Dr. Livesey—' I began.

'Perfectly right,' he interrupted very cheerily, 'perfectly right—a gentleman and a magistrate. And, now I come to think of it, I might as well ride round there myself and report to him or squire. Master Pew's dead, when all's done; not that I regret it, but he's dead, you see, and people will make it out against an officer of his Majesty's revenue, if make it out they can. Now, I'll tell you, Hawkins, if you like, I'll take you along.'

I thanked him heartily for the offer, and we walked back to the hamlet where the horses were. By the time I had told mother of my purpose they were all in the saddle.

‘Dogger,’ said Mr. Dance, ‘you have a good horse; take up this lad behind you.’

As soon as I was mounted, holding on to Dogger’s belt, the supervisor gave the word, and the party struck out at a bouncing trot on the road to Dr. Livesey’s house.

## 6

## The Captain's Papers

WE rode hard all the way till we drew up before Dr. Livesey's door. The house was all dark to the front.

Mr. Dance told me to jump down and knock, and Dogger gave me a stirrup to descend by. The door was opened almost at once by the maid.

'Is Dr. Livesey in?' I asked.

No, she said, he had come home in the afternoon but had gone up to the hall to dine and pass the evening with the squire.

'So there we go, boys,' said Mr. Dance.

This time, as the distance was short, I did not mount, but ran with Dogger's stirrup-leather to the lodge gates and up the long, leafless, moonlit avenue to where the white line of the hall buildings looked on either hand on great old gardens. Here Mr. Dance dismounted, and taking me along with him, was admitted at a word into the house.

The servant led us down a matted passage and showed us at the end into a great library, all lined with bookcases

and busts upon the top of them, where the squire and Dr. Livesey sat, pipe in hand, on either side of a bright fire.

I had never seen the squire so near at hand. He was a tall man, over six feet high, and broad in proportion, and he had a bluff, rough-and-ready face, all roughened and reddened and lined in his long travels. His eyebrows were very black, and moved readily, and this gave him a look of some temper, not bad, you would say, but quick and high.

‘Come in, Mr. Dance,’ says he, very stately and condescending.

‘Good evening, Dance,’ says the doctor with a nod. ‘And good evening to you, friend Jim. What good wind brings you here?’

The supervisor stood up straight and stiff and told his story like a lesson; and you should have seen how the two gentlemen leaned forward and looked at each other, and forgot to smoke in their surprise and interest. When they heard how my mother went back to the inn, Dr. Livesey fairly slapped his thigh, and the squire cried ‘Bravo!’ and broke his long pipe against the grate. Long before it was done, Mr. Trelawney (that, you will remember, was the squire’s name) had got up from his seat and was striding about the room, and the doctor, as if to hear the better,

had taken off his powdered wig and sat there looking very strange indeed with his own close-cropped black poll.'

At last Mr. Dance finished the story.

'Mr. Dance,' said the squire, 'you are a very noble fellow. And as for riding down that black, atrocious miscreant, I regard it as an act of virtue, sir, like stamping on a cockroach. This lad Hawkins is a trump, I perceive. Hawkins, will you ring that bell? Mr. Dance must have some ale.'

'And so, Jim,' said the doctor, 'you have the thing that they were after, have you?'

'Here it is, sir,' said I, and gave him the oilskin packet.

The doctor looked it all over, as if his fingers were itching to open it; but instead of doing that, he put it quietly in the pocket of his coat.

'Squire,' said he, 'when Dance has had his ale he must, of course, be off on his Majesty's service; but I mean to keep Jim Hawkins here to sleep at my house, and with your permission, I propose we should have up the cold pie and let him sup.'

'As you will, Livesey,' said the squire; 'Hawkins has earned better than cold pie.'

So a big pigeon pie was brought in and put on a sidetable, and I made a hearty supper, for I was as hungry

as a hawk, while Mr. Dance was further complimented and at last dismissed.

‘And now, squire,’ said the doctor.

‘And now, Livesey,’ said the squire in the same breath.

‘One at a time, one at a time,’ laughed Dr. Livesey.  
‘You have heard of this Flint, I suppose?’

‘Heard of him!’ cried the squire. ‘Heard of him, you say! He was the bloodthirstiest buccaneer that sailed. Blackbeard was a child to Flint. The Spaniards were so prodigiously afraid of him that, I tell you, sir, I was sometimes proud he was an Englishman. I’ve seen his top-sails with these eyes, off Trinidad, and the cowardly son of a rum-puncheon that I sailed with put back—put back, sir, into Port of Spain.’

‘Well, I’ve heard of him myself, in England,’ said the doctor. ‘But the point is, had he money?’

‘Money!’ cried the squire. ‘Have you heard the story? What were these villains after but money? What do they care for but money? For what would they risk their rascal carcasses but money?’

‘That we shall soon know,’ replied the doctor. ‘But you are so confoundedly hot-headed and exclamatory that I cannot get a word in. What I want to know is this: Supposing that I have here in my pocket some clue to

where Flint buried his treasure, will that treasure amount to much?"

'Amount, sir!' cried the squire. 'It will amount to this: If we have the clue you talk about, I fit out a ship in Bristol dock, and take you and Hawkins here along, and I'll have that treasure if I search a year.'

'Very well,' said the doctor. 'Now, then, if Jim is agreeable, we'll open the packet"; and he laid it before him on the table.

The bundle was sewn together, and the doctor had to get out his instrument case and cut the stitches with his medical scissors. It contained two things—a book and a sealed paper.

'First of all we'll try the book,' observed the doctor.

The squire and I were both peering over his shoulder as he opened it, for Dr. Livesey had kindly motioned me to come round from the side-table, where I had been eating, to enjoy the sport of the search. On the first page there were only some scraps of writing, such as a man with a pen in his hand might make for idleness or practice. One was the same as the tattoo mark, 'Billy Bones his fancy"; then there was 'Mr. W. Bones, mate,' 'No more rum,' 'Off Palm Key he got itt,' and some other snatches, mostly single words and unintelligible. I could

not help wondering who it was that had ‘got itt,’ and what ‘itt’ was that he got. A knife in his back as like as not.

‘Not much instruction there,’ said Dr. Livesey as he passed on.

The next ten or twelve pages were filled with a curious series of entries. There was a date at one end of the line and at the other a sum of money, as in common account-books, but instead of explanatory writing, only a varying number of crosses between the two. On the 12th of June, 1745, for instance, a sum of seventy pounds had plainly become due to someone, and there was nothing but six crosses to explain the cause. In a few cases, to be sure, the name of a place would be added, as ‘Offe Caraccas,’ or a mere entry of latitude and longitude, as ‘62° 17' 20”, 19° 2' 40”.’

The record lasted over nearly twenty years, the amount of the separate entries growing larger as time went on, and at the end a grand total had been made out after five or six wrong additions, and these words appended, ‘Bones, his pile.’

‘I can’t make head or tail of this,’ said Dr. Livesey.

‘The thing is as clear as noonday,’ cried the squire. ‘This is the black-hearted hound’s account-book. These crosses stand for the names of ships or towns that they

sank or plundered. The sums are the scoundrel's share, and where he feared an ambiguity, you see he added something clearer. 'Offe Caraccas,' now; you see, here was some unhappy vessel boarded off that coast. God help the poor souls that manned her—coral long ago.'

'Right!' said the doctor. 'See what it is to be a traveller. Right! And the amounts increase, you see, as he rose in rank.'

There was little else in the volume but a few bearings of places noted in the blank leaves towards the end and a table for reducing French, English, and Spanish moneys to a common value.

'Thrifty man!' cried the doctor. 'He wasn't the one to be cheated.'

'And now,' said the squire, 'for the other.'

The paper had been sealed in several places with a thimble by way of seal; the very thimble, perhaps, that I had found in the captain's pocket. The doctor opened the seals with great care, and there fell out the map of an island, with latitude and longitude, soundings, names of hills and bays and inlets, and every particular that would be needed to bring a ship to a safe anchorage upon its shores. It was about nine miles long and five across, shaped, you might say, like a fat dragon standing up, and

had two fine land-locked harbours, and a hill in the centre part marked ‘The Spy-glass.’ There were several additions of a later date, but above all, three crosses of red ink—two on the north part of the island, one in the southwest—and beside this last, in the same red ink, and in a small, neat hand, very different from the captain’s tottery characters, these words: ‘Bulk of treasure here.’

Over on the back the same hand had written this further information:

Tall tree, Spy-glass shoulder, bearing a point to the N. of N.N.E.

Skeleton Island E.S.E. and by E.

Ten feet.

The bar silver is in the north cache; you can find it by the trend of the east hummock, ten fathoms south of the black crag with the face on it.

The arms are easy found, in the sand-hill, N. point of north inlet cape, bearing E. and a quarter N. J.F.

That was all; but brief as it was, and to me incomprehensible, it filled the squire and Dr. Livesey with delight.

‘Livesey,’ said the squire, ‘you will give up this wretched practice at once. Tomorrow I start for Bristol. In three weeks’ time—three weeks!—two weeks—ten

days—we'll have the best ship, sir, and the choicest crew in England. Hawkins shall come as cabin-boy. You'll make a famous cabin-boy, Hawkins. You, Livesey, are ship's doctor; I am admiral. We'll take Redruth, Joyce, and Hunter. We'll have favourable winds, a quick passage, and not the least difficulty in finding the spot, and money to eat, to roll in, to play duck and drake with ever after.'

'Trelawney,' said the doctor, 'I'll go with you; and I'll go bail for it, so will Jim, and be a credit to the undertaking. There's only one man I'm afraid of.'

'And who's that?' cried the squire. 'Name the dog, sir!'

'You,' replied the doctor; 'for you cannot hold your tongue. We are not the only men who know of this paper. These fellows who attacked the inn tonight—bold, desperate blades, for sure—and the rest who stayed aboard that lugger, and more, I dare say, not far off, are, one and all, through thick and thin, bound that they'll get that money. We must none of us go alone till we get to sea. Jim and I shall stick together in the meanwhile; you'll take Joyce and Hunter when you ride to Bristol, and from first to last, not one of us must breathe a word of what we've found.'

*Treasure Island*

‘Livesey,’ returned the squire, ‘you are always in the right of it. I’ll be as silent as the grave.’

## PART TWO

### The Sea-cook

## I Go to Bristol

IT was longer than the squire imagined ere we were ready for the sea, and none of our first plans—not even Dr. Livesey's, of keeping me beside him—could be carried out as we intended. The doctor had to go to London for a physician to take charge of his practice; the squire was hard at work at Bristol; and I lived on at the hall under the charge of old Redruth, the gamekeeper, almost a prisoner, but full of sea-dreams and the most charming anticipations of strange islands and adventures. I brooded by the hour together over the map, all the details of which I well remembered. Sitting by the fire in the housekeeper's room, I approached that island in my fancy from every possible direction; I explored every acre of its surface; I climbed a thousand times to that tall hill they call the Spy-glass, and from the top enjoyed the most wonderful and changing prospects. Sometimes the isle was thick with savages, with whom we fought, sometimes full of dangerous animals that hunted us, but in all my fancies nothing occurred to me so strange and tragic as our actual adventures.

So the weeks passed on, till one fine day there came a letter addressed to Dr. Livesey, with this addition, ‘To be opened, in the case of his absence, by Tom Redruth or young Hawkins.’ Obeying this order, we found, or rather I found—for the gamekeeper was a poor hand at reading anything but print—the following important news:

Old Anchor Inn, Bristol, March 1, 17—

Dear Livesey—As I do not know whether you are at the hall or still in London, I send this in double to both places. The ship is bought and fitted. She lies at anchor, ready for sea. You never imagined a sweeter schooner—a child might sail her—two hundred tons; name, HISPANIOLA. I got her through my old friend, Blandly, who has proved himself throughout the most surprising trump. The admirable fellow literally slaved in my interest, and so, I may say, did everyone in Bristol, as soon as they got wind of the port we sailed for—treasure, I mean.

‘Redruth,’ said I, interrupting the letter, ‘Dr. Livesey will not like that. The squire has been talking, after all.’

‘Well, who’s a better right?’ growled the gamekeeper. ‘A pretty rum go if squire ain’t to talk for Dr. Livesey, I should think.’

At that I gave up all attempts at commentary and read straight on:

Blandly himself found the HISPANIOLA, and by the most admirable management got her for the merest trifle. There is a class of men in Bristol monstrously prejudiced against Blandly. They go the length of declaring that this honest creature would do anything for money, that the HISPANIOLA belonged to him, and that he sold it me absurdly high—the most transparent calumnies. None of them dare, however, to deny the merits of the ship. Wo far there was not a hitch. The workpeople, to be sure—riggers and what not—were most annoyingly slow; but time cured that. It was the crew that troubled me. I wished a round score of men—in case of natives, buccaneers, or the odious French—and I had the worry of the deuce itself to find so much as half a dozen, till the most remarkable stroke of fortune brought me the very man that I required. I was standing on the dock, when, by the merest accident, I fell in talk with him. I found he was an old sailor, kept a public-house, knew all the seafaring men in Bristol, had lost his health ashore, and wanted a good berth as cook to get to sea again. He had hobbled down there that morning, he said, to get a smell of the salt. I was monstrously touched—so would you have been—and, out of pure pity,

I engaged him on the spot to be ship's cook. Long John Silver, he is called, and has lost a leg; but that I regarded as a recommendation, since he lost it in his country's service, under the immortal Hawke. He has no pension, Livesey. Imagine the abominable age we live in! Well, sir, I thought I had only found a cook, but it was a crew I had discovered. Between Silver and myself we got together in a few days a company of the toughest old salts imaginable—not pretty to look at, but fellows, by their faces, of the most indomitable spirit. I declare we could fight a frigate. Long John even got rid of two out of the six or seven I had already engaged. He showed me in a moment that they were just the sort of fresh-water swabs we had to fear in an adventure of importance. I am in the most magnificent health and spirits, eating like a bull, sleeping like a tree, yet I shall not enjoy a moment till I hear my old tarpaulins tramping round the capstan. Seaward, ho! Hang the treasure! It's the glory of the sea that has turned my head. So now, Livesey, come post; do not lose an hour, if you respect me. Let young Hawkins go at once to see his mother, with Redruth for a guard; and then both come full speed to Bristol. John Trelawney

Postscript—I did not tell you that Blandly, who, by the way, is to send a consort after us if we don't turn up by

the end of August, had found an admirable fellow for sailing master—a stiff man, which I regret, but in all other respects a treasure. Long John Silver unearthed a very competent man for a mate, a man named Arrow. I have a boatswain who pipes, Livesey; so things shall go man-o'-war fashion on board the good ship HISPANIOLA. I forgot to tell you that Silver is a man of substance; I know of my own knowledge that he has a banker's account, which has never been overdrawn. He leaves his wife to manage the inn; and as she is a woman of colour, a pair of old bachelors like you and I may be excused for guessing that it is the wife, quite as much as the health, that sends him back to roving. J. T.

P.P.S.—Hawkins may stay one night with his mother.  
J. T.

You can fancy the excitement into which that letter put me. I was half beside myself with glee; and if ever I despised a man, it was old Tom Redruth, who could do nothing but grumble and lament. Any of the under-gamekeepers would gladly have changed places with him; but such was not the squire's pleasure, and the squire's pleasure was like law among them all. Nobody but old Redruth would have dared so much as even to grumble.

The next morning he and I set out on foot for the Admiral Benbow, and there I found my mother in good health and spirits. The captain, who had so long been a cause of so much discomfort, was gone where the wicked cease from troubling. The squire had had everything repaired, and the public rooms and the sign repainted, and had added some furniture—above all a beautiful armchair for mother in the bar. He had found her a boy as an apprentice also so that she should not want help while I was gone.

It was on seeing that boy that I understood, for the first time, my situation. I had thought up to that moment of the adventures before me, not at all of the home that I was leaving; and now, at sight of this clumsy stranger, who was to stay here in my place beside my mother, I had my first attack of tears. I am afraid I led that boy a dog's life, for as he was new to the work, I had a hundred opportunities of setting him right and putting him down, and I was not slow to profit by them.

The night passed, and the next day, after dinner, Redruth and I were afoot again and on the road. I said good-bye to Mother and the cove where I had lived since I was born, and the dear old Admiral Benbow—since he was repainted, no longer quite so dear. One of my last

thoughts was of the captain, who had so often strode along the beach with his cocked hat, his sabre-cut cheek, and his old brass telescope. Next moment we had turned the corner and my home was out of sight.

The mail picked us up about dusk at the Royal George on the heath. I was wedged in between Redruth and a stout old gentleman, and in spite of the swift motion and the cold night air, I must have dozed a great deal from the very first, and then slept like a log up hill and down dale through stage after stage, for when I was awakened at last it was by a punch in the ribs, and I opened my eyes to find that we were standing still before a large building in a city street and that the day had already broken a long time.

‘Where are we?’ I asked.

‘Bristol,’ said Tom. ‘Get down.’

Mr. Trelawney had taken up his residence at an inn far down the docks to superintend the work upon the schooner. Thither we had now to walk, and our way, to my great delight, lay along the quays and beside the great multitude of ships of all sizes and rigs and nations. In one, sailors were singing at their work, in another there were men aloft, high over my head, hanging to threads that seemed no thicker than a spider’s. Though I had lived by the shore all my life, I seemed never to have been near the

sea till then. The smell of tar and salt was something new. I saw the most wonderful figureheads, that had all been far over the ocean. I saw, besides, many old sailors, with rings in their ears, and whiskers curled in ringlets, and tarry pigtails, and their swaggering, clumsy sea-walk; and if I had seen as many kings or archbishops I could not have been more delighted.

And I was going to sea myself, to sea in a schooner, with a piping boatswain and pig-tailed singing seamen, to sea, bound for an unknown island, and to seek for buried treasure!

While I was still in this delightful dream, we came suddenly in front of a large inn and met Squire Trelawney, all dressed out like a sea-officer, in stout blue cloth, coming out of the door with a smile on his face and a capital imitation of a sailor's walk.

'Here you are,' he cried, 'and the doctor came last night from London. Bravo! The ship's company complete!'

'Oh, sir,' cried I, 'when do we sail?'

'Sail!' says he. 'We sail tomorrow!'

## At the Sign of the Spy-glass

WHEN I had done breakfasting the squire gave me a note addressed to John Silver, at the sign of the Spy-glass, and told me I should easily find the place by following the line of the docks and keeping a bright lookout for a little tavern with a large brass telescope for sign. I set off, overjoyed at this opportunity to see some more of the ships and seamen, and picked my way among a great crowd of people and carts and bales, for the dock was now at its busiest, until I found the tavern in question.

It was a bright enough little place of entertainment. The sign was newly painted; the windows had neat red curtains; the floor was cleanly sanded. There was a street on each side and an open door on both, which made the large, low room pretty clear to see in, in spite of clouds of tobacco smoke.

The customers were mostly seafaring men, and they talked so loudly that I hung at the door, almost afraid to enter.

As I was waiting, a man came out of a side room, and at a glance I was sure he must be Long John. His left leg was cut off close by the hip, and under the left shoulder he carried a crutch, which he managed with wonderful dexterity, hopping about upon it like a bird. He was very tall and strong, with a face as big as a ham—plain and pale, but intelligent and smiling. Indeed, he seemed in the most cheerful spirits, whistling as he moved about among the tables, with a merry word or a slap on the shoulder for the more favoured of his guests.

Now, to tell you the truth, from the very first mention of Long John in Squire Trelawney's letter I had taken a fear in my mind that he might prove to be the very one-legged sailor whom I had watched for so long at the old Benbow. But one look at the man before me was enough. I had seen the captain, and Black Dog, and the blind man, Pew, and I thought I knew what a buccaneer was like—a very different creature, according to me, from this clean and pleasant-tempered landlord.

I plucked up courage at once, crossed the threshold, and walked right up to the man where he stood, propped on his crutch, talking to a customer.

‘Mr. Silver, sir?’ I asked, holding out the note.

## Treasure Island

‘Yes, my lad,’ said he; ‘such is my name, to be sure. And who may you be?’ And then as he saw the squire’s letter, he seemed to me to give something almost like a start.

‘Oh!’ said he, quite loud, and offering his hand. ‘I see. You are our new cabin-boy; pleased I am to see you.’

And he took my hand in his large firm grasp.

Just then one of the customers at the far side rose suddenly and made for the door. It was close by him, and he was out in the street in a moment. But his hurry had attracted my notice, and I recognized him at glance. It was the tallow-faced man, wanting two fingers, who had come first to the Admiral Benbow.

‘Oh,’ I cried, ‘stop him! It’s Black Dog!’

‘I don’t care two coppers who he is,’ cried Silver. ‘But he hasn’t paid his score. Harry, run and catch him.’

One of the others who was nearest the door leaped up and started in pursuit.

‘If he were Admiral Hawke he shall pay his score,’ cried Silver; and then, relinquishing my hand, ‘Who did you say he was?’ he asked. ‘Black what?’

‘Dog, sir,’ said I. Has Mr. Trelawney not told you of the buccaneers? He was one of them.’

‘So?’ cried Silver. ‘In my house! Ben, run and help Harry. One of those swabs, was he? Was that you drinking with him, Morgan? Step up here.’

The man whom he called Morgan—an old, grey-haired, mahogany-faced sailor—came forward pretty sheepishly, rolling his quid.

‘Now, Morgan,’ said Long John very sternly, ‘you never clapped your eyes on that Black—Black Dog before, did you, now?’

‘Not I, sir,’ said Morgan with a salute.

‘You didn’t know his name, did you?’

‘No, sir.’

‘By the powers, Tom Morgan, it’s as good for you!’ exclaimed the landlord. ‘If you had been mixed up with the like of that, you would never have put another foot in my house, you may lay to that. And what was he saying to you?’

‘I don’t rightly know, sir,’ answered Morgan.

‘Do you call that a head on your shoulders, or a blessed dead-eye?’ cried Long John. ‘Don’t rightly know, don’t you! Perhaps you don’t happen to rightly know who you was speaking to, perhaps? Come, now, what was he jawing—v’yages, cap’ns, ships? Pipe up! What was it?’

‘We was a-talkin’ of keel-hauling,’ answered Morgan.

‘Keel-hauling, was you? And a mighty suitable thing, too, and you may lay to that. Get back to your place for a lubber, Tom.’

And then, as Morgan rolled back to his seat, Silver added to me in a confidential whisper that was very flattering, as I thought, ‘He’s quite an honest man, Tom Morgan, on’y stupid. And now,’ he ran on again, aloud, ‘let’s see—Black Dog? No, I don’t know the name, not I. Yet I kind of think I’ve—yes, I’ve seen the swab. He used to come here with a blind beggar, he used.’

‘That he did, you may be sure,’ said I. ‘I knew that blind man too. His name was Pew.’

‘It was!’ cried Silver, now quite excited. ‘Pew! That were his name for certain. Ah, he looked a shark, he did! If we run down this Black Dog, now, there’ll be news for Cap’n Trelawney! Ben’s a good runner; few seamen run better than Ben. He should run him down, hand over hand, by the powers! He talked o’ keel- hauling, did he? I’LL keel-haul him!’

All the time he was jerking out these phrases he was stumping up and down the tavern on his crutch, slapping tables with his hand, and giving such a show of excitement as would have convinced an Old Bailey judge or a Bow Street runner. My suspicions had been

thoroughly reawakened on finding Black Dog at the Spy-glass, and I watched the cook narrowly. But he was too deep, and too ready, and too clever for me, and by the time the two men had come back out of breath and confessed that they had lost the track in a crowd, and been scolded like thieves, I would have gone bail for the innocence of Long John Silver.

‘See here, now, Hawkins,’ said he, ‘here’s a blessed hard thing on a man like me, now, ain’t it? There’s Cap’n Trelawney—what’s he to think? Here I have this confounded son of a Dutchman sitting in my own house drinking of my own rum! Here you comes and tells me of it plain; and here I let him give us all the slip before my blessed deadlights! Now, Hawkins, you do me justice with the cap’n. You’re a lad, you are, but you’re as smart as paint. I see that when you first come in. Now, here it is: What could I do, with this old timber I hobble on? When I was an A B master mariner I’d have come up alongside of him, hand over hand, and broached him to in a brace of old shakes, I would; but now—‘

And then, all of a sudden, he stopped, and his jaw dropped as though he had remembered something.

‘The score!’ he burst out. ‘Three goes o’ rum! Why, shiver my timbers, if I hadn’t forgotten my score!’

And falling on a bench, he laughed until the tears ran down his cheeks. I could not help joining, and we laughed together, peal after peal, until the tavern rang again.

‘Why, what a precious old sea-calf I am!’ he said at last, wiping his cheeks. ‘You and me should get on well, Hawkins, for I’ll take my davy I should be rated ship’s boy. But come now, stand by to go about. This won’t do. Dooty is dooty, messmates. I’ll put on my old cockerel hat, and step along of you to Cap’n Trelawney, and report this here affair. For mind you, it’s serious, young Hawkins; and neither you nor me’s come out of it with what I should make so bold as to call credit. Nor you neither, says you; not smart— none of the pair of us smart. But dash my buttons! That was a good un about my score.’

And he began to laugh again, and that so heartily, that though I did not see the joke as he did, I was again obliged to join him in his mirth.

On our little walk along the quays, he made himself the most interesting companion, telling me about the different ships that we passed by, their rig, tonnage, and nationality, explaining the work that was going forward—how one was discharging, another taking in cargo, and a third making ready for sea—and every now and then

telling me some little anecdote of ships or seamen or repeating a nautical phrase till I had learned it perfectly. I began to see that here was one of the best of possible shipmates.

When we got to the inn, the squire and Dr. Livesey were seated together, finishing a quart of ale with a toast in it, before they should go aboard the schooner on a visit of inspection.

Long John told the story from first to last, with a great deal of spirit and the most perfect truth. ‘That was how it were, now, weren’t it, Hawkins?’ he would say, now and again, and I could always bear him entirely out.

The two gentlemen regretted that Black Dog had got away, but we all agreed there was nothing to be done, and after he had been complimented, Long John took up his crutch and departed.

‘All hands aboard by four this afternoon,’ shouted the squire after him.

‘Aye, aye, sir,’ cried the cook, in the passage.

‘Well, squire,’ said Dr. Livesey, ‘I don’t put much faith in your discoveries, as a general thing; but I will say this, John Silver suits me.’

‘The man’s a perfect trump,’ declared the squire.

‘And now,’ added the doctor, ‘Jim may come on board with us, may he not?’

‘To be sure he may,’ says squire. ‘Take your hat, Hawkins, and we’ll see the ship.’

## Powder and Arms

THE HISPANIOLA lay some way out, and we went under the figureheads and round the sterns of many other ships, and their cables sometimes grated underneath our keel, and sometimes swung above us. At last, however, we got alongside, and were met and saluted as we stepped aboard by the mate, Mr. Arrow, a brown old sailor with earrings in his ears and a squint. He and the squire were very thick and friendly, but I soon observed that things were not the same between Mr. Trelawney and the captain.

This last was a sharp-looking man who seemed angry with everything on board and was soon to tell us why, for we had hardly got down into the cabin when a sailor followed us.

‘Captain Smollett, sir, axing to speak with you,’ said he.

‘I am always at the captain’s orders. Show him in,’ said the squire.

The captain, who was close behind his messenger, entered at once and shut the door behind him.

‘Well, Captain Smollett, what have you to say? All well, I hope; all shipshape and seaworthy?’

‘Well, sir,’ said the captain, ‘better speak plain, I believe, even at the risk of offence. I don’t like this cruise; I don’t like the men; and I don’t like my officer. That’s short and sweet.’

‘Perhaps, sir, you don’t like the ship?’ inquired the squire, very angry, as I could see.

‘I can’t speak as to that, sir, not having seen her tried,’ said the captain. ‘She seems a clever craft; more I can’t say.’

‘Possibly, sir, you may not like your employer, either?’ says the squire.

But here Dr. Livesey cut in.

‘Stay a bit,’ said he, ‘stay a bit. No use of such questions as that but to produce ill feeling. The captain has said too much or he has said too little, and I’m bound to say that I require an explanation of his words. You don’t, you say, like this cruise. Now, why?’

‘I was engaged, sir, on what we call sealed orders, to sail this ship for that gentleman where he should bid me,’ said the captain. ‘So far so good. But now I find that

every man before the mast knows more than I do. I don't call that fair, now, do you?"

'No,' said Dr. Livesey, 'I don't.'

'Next,' said the captain, 'I learn we are going after treasure—hear it from my own hands, mind you. Now, treasure is ticklish work; I don't like treasure voyages on any account, and I don't like them, above all, when they are secret and when (begging your pardon, Mr. Trelawney) the secret has been told to the parrot.'

'Silver's parrot?' asked the squire.

'It's a way of speaking,' said the captain. 'Blabbed, I mean. It's my belief neither of you gentlemen know what you are about, but I'll tell you my way of it— life or death, and a close run.'

'That is all clear, and, I dare say, true enough,' replied Dr. Livesey. 'We take the risk, but we are not so ignorant as you believe us. Next, you say you don't like the crew. Are they not good seamen?'

'I don't like them, sir,' returned Captain Smollett. 'And I think I should have had the choosing of my own hands, if you go to that.'

'Perhaps you should,' replied the doctor. 'My friend should, perhaps, have taken you along with him; but the

slight, if there be one, was unintentional. And you don't like Mr. Arrow?"

"I don't, sir. I believe he's a good seaman, but he's too free with the crew to be a good officer. A mate should keep himself to himself—shouldn't drink with the men before the mast!"

"Do you mean he drinks?" cried the squire.

"No, sir," replied the captain, "only that he's too familiar."

"Well, now, and the short and long of it, captain?" asked the doctor. "Tell us what you want."

"Well, gentlemen, are you determined to go on this cruise?"

"Like iron," answered the squire.

"Very good," said the captain. "Then, as you've heard me very patiently, saying things that I could not prove, hear me a few words more. They are putting the powder and the arms in the fore hold. Now, you have a good place under the cabin; why not put them there?— first point. Then, you are bringing four of your own people with you, and they tell me some of them are to be berthed forward. Why not give them the berths here beside the cabin?— second point."

"Any more?" asked Mr. Trelawney.

‘One more,’ said the captain. ‘There’s been too much blabbing already.’

‘Far too much,’ agreed the doctor.

‘I’ll tell you what I’ve heard myself,’ continued Captain Smollett: ‘that you have a map of an island, that there’s crosses on the map to show where treasure is, and that the island lies—’ And then he named the latitude and longitude exactly.

‘I never told that,’ cried the squire, ‘to a soul!’

‘The hands know it, sir,’ returned the captain.

‘Livesey, that must have been you or Hawkins,’ cried the squire.

‘It doesn’t much matter who it was,’ replied the doctor. And I could see that neither he nor the captain paid much regard to Mr. Trelawney’s protestations. Neither did I, to be sure, he was so loose a talker; yet in this case I believe he was really right and that nobody had told the situation of the island.

‘Well, gentlemen,’ continued the captain, ‘I don’t know who has this map; but I make it a point, it shall be kept secret even from me and Mr. Arrow. Otherwise I would ask you to let me resign.’

‘I see,’ said the doctor. ‘You wish us to keep this matter dark and to make a garrison of the stern part of the

## Treasure Island

ship, manned with my friend's own people, and provided with all the arms and powder on board. In other words, you fear a mutiny.'

'Sir,' said Captain Smollett, 'with no intention to take offence, I deny your right to put words into my mouth. No captain, sir, would be justified in going to sea at all if he had ground enough to say that. As for Mr. Arrow, I believe him thoroughly honest; some of the men are the same; all may be for what I know. But I am responsible for the ship's safety and the life of every man Jack aboard of her. I see things going, as I think, not quite right. And I ask you to take certain precautions or let me resign my berth. And that's all.'

'Captain Smollett,' began the doctor with a smile, 'did ever you hear the fable of the mountain and the mouse? You'll excuse me, I dare say, but you remind me of that fable. When you came in here, I'll stake my wig, you meant more than this.'

'Doctor,' said the captain, 'you are smart. When I came in here I meant to get discharged. I had no thought that Mr. Trelawney would hear a word.'

'No more I would,' cried the squire. 'Had Livesey not been here I should have seen you to the deuce. As it is, I

have heard you. I will do as you desire, but I think the worse of you.'

'That's as you please, sir,' said the captain. 'You'll find I do my duty.'

And with that he took his leave.

'Trelawney,' said the doctor, 'contrary to all my notions, I believed you have managed to get two honest men on board with you—that man and John Silver.'

'Silver, if you like,' cried the squire; 'but as for that intolerable humbug, I declare I think his conduct unmanly, unsailorly, and downright un-English.'

'Well,' says the doctor, 'we shall see.'

When we came on deck, the men had begun already to take out the arms and powder, yo-ho-ing at their work, while the captain and Mr. Arrow stood by superintending.

The new arrangement was quite to my liking. The whole schooner had been overhauled; six berths had been made astern out of what had been the after-part of the main hold; and this set of cabins was only joined to the galley and forecastle by a sparred passage on the port side. It had been originally meant that the captain, Mr. Arrow, Hunter, Joyce, the doctor, and the squire were to occupy these six berths. Now Redruth and I were to get two of them and Mr. Arrow and the captain were to sleep

on deck in the companion, which had been enlarged on each side till you might almost have called it a round-house. Very low it was still, of course; but there was room to swing two hammocks, and even the mate seemed pleased with the arrangement. Even he, perhaps, had been doubtful as to the crew, but that is only guess, for as you shall hear, we had not long the benefit of his opinion.

We were all hard at work, changing the powder and the berths, when the last man or two, and Long John along with them, came off in a shore-boat.

The cook came up the side like a monkey for cleverness, and as soon as he saw what was doing, ‘So ho, mates!’ says he. ‘What’s this?’

‘We’re a-changing of the powder, Jack,’ answers one.

‘Why, by the powers,’ cried Long John, ‘if we do, we’ll miss the morning tide!’

‘My orders!’ said the captain shortly. ‘You may go below, my man. Hands will want supper.’

‘Aye, aye, sir,’ answered the cook, and touching his forelock, he disappeared at once in the direction of his galley.

‘That’s a good man, captain,’ said the doctor.

‘Very likely, sir,’ replied Captain Smollett. ‘Easy with that, men—easy,’ he ran on, to the fellows who were

shifting the powder; and then suddenly observing me examining the swivel we carried amidships, a long brass nine, ‘Here you, ship’s boy,’ he cried, ‘out o’ that! Off with you to the cook and get some work.’

And then as I was hurrying off I heard him say, quite loudly, to the doctor, ‘I’ll have no favourites on my ship.’

I assure you I was quite of the squire’s way of thinking, and hated the captain deeply.

# 10

## The Voyage

ALL that night we were in a great bustle getting things stowed in their place, and boatfuls of the squire's friends, Mr. Blandly and the like, coming off to wish him a good voyage and a safe return. We never had a night at the Admiral Benbow when I had half the work; and I was dog-tired when, a little before dawn, the boatswain sounded his pipe and the crew began to man the capstan-bars. I might have been twice as weary, yet I would not have left the deck, all was so new and interesting to me—the brief commands, the shrill note of the whistle, the men bustling to their places in the glimmer of the ship's lanterns.

‘Now, Barbecue, tip us a stave,’ cried one voice.

‘The old one,’ cried another.

‘Aye, aye, mates,’ said Long John, who was standing by, with his crutch under his arm, and at once broke out in the air and words I knew so well:

‘Fifteen men on the dead man’s chest—‘

And then the whole crew bore chorus:—

‘Yo-ho-ho, and a bottle of rum!’

And at the third ‘Ho!’ drove the bars before them with a will.

Even at that exciting moment it carried me back to the old Admiral Benbow in a second, and I seemed to hear the voice of the captain piping in the chorus. But soon the anchor was short up; soon it was hanging dripping at the bows; soon the sails began to draw, and the land and shipping to flit by on either side; and before I could lie down to snatch an hour of slumber the HISPANIOLA had begun her voyage to the Isle of Treasure.

I am not going to relate that voyage in detail. It was fairly prosperous. The ship proved to be a good ship, the crew were capable seamen, and the captain thoroughly understood his business. But before we came the length of Treasure Island, two or three things had happened which require to be known.

Mr. Arrow, first of all, turned out even worse than the captain had feared. He had no command among the men, and people did what they pleased with him. But that was by no means the worst of it, for after a day or two at sea he began to appear on deck with hazy eye, red cheeks, stuttering tongue, and other marks of drunkenness. Time after time he was ordered below in disgrace. Sometimes

he fell and cut himself; sometimes he lay all day long in his little bunk at one side of the companion; sometimes for a day or two he would be almost sober and attend to his work at least passably.

In the meantime, we could never make out where he got the drink. That was the ship's mystery. Watch him as we pleased, we could do nothing to solve it; and when we asked him to his face, he would only laugh if he were drunk, and if he were sober deny solemnly that he ever tasted anything but water.

He was not only useless as an officer and a bad influence amongst the men, but it was plain that at this rate he must soon kill himself outright, so nobody was much surprised, nor very sorry, when one dark night, with a head sea, he disappeared entirely and was seen no more.

'Overboard!' said the captain. 'Well, gentlemen, that saves the trouble of putting him in irons.'

But there we were, without a mate; and it was necessary, of course, to advance one of the men. The boatswain, Job Anderson, was the likeliest man aboard, and though he kept his old title, he served in a way as mate. Mr. Trelawney had followed the sea, and his knowledge made him very useful, for he often took a watch himself in easy weather. And the coxswain, Israel

Hands, was a careful, wily, old, experienced seaman who could be trusted at a pinch with almost anything.

He was a great confidant of Long John Silver, and so the mention of his name leads me on to speak of our ship's cook, Barbecue, as the men called him.

Aboard ship he carried his crutch by a lanyard round his neck, to have both hands as free as possible. It was something to see him wedge the foot of the crutch against a bulkhead, and propped against it, yielding to every movement of the ship, get on with his cooking like someone safe ashore. Still more strange was it to see him in the heaviest of weather cross the deck. He had a line or two rigged up to help him across the widest spaces—Long John's earrings, they were called; and he would hand himself from one place to another, now using the crutch, now trailing it alongside by the lanyard, as quickly as another man could walk. Yet some of the men who had sailed with him before expressed their pity to see him so reduced.

'He's no common man, Barbecue,' said the coxswain to me. 'He had good schooling in his young days and can speak like a book when so minded; and brave—a lion's nothing alongside of Long John! I seen him grapple four and knock their heads together—him unarmed.'

All the crew respected and even obeyed him. He had a way of talking to each and doing everybody some particular service. To me he was unweariedly kind, and always glad to see me in the galley, which he kept as clean as a new pin, the dishes hanging up burnished and his parrot in a cage in one corner.

‘Come away, Hawkins,’ he would say; ‘come and have a yarn with John. Nobody more welcome than yourself, my son. Sit you down and hear the news. Here’s Cap’n Flint—I calls my parrot Cap’n Flint, after the famous buccaneer—here’s Cap’n Flint predicting success to our v’yage. Wasn’t you, cap’n?’

And the parrot would say, with great rapidity, ‘Pieces of eight! Pieces of eight! Pieces of eight!’ till you wondered that it was not out of breath, or till John threw his handkerchief over the cage.

‘Now, that bird,’ he would say, ‘is, maybe, two hundred years old, Hawkins—they live forever mostly; and if anybody’s seen more wickedness, it must be the devil himself. She’s sailed with England, the great Cap’n England, the pirate. She’s been at Madagascar, and at Malabar, and Surinam, and Providence, and Portobello. She was at the fishing up of the wrecked plate ships. It’s there she learned ‘Pieces of eight,’ and little wonder; three

hundred and fifty thousand of ‘em, Hawkins! She was at the boarding of the viceroy of the Indies out of Goa, she was; and to look at her you would think she was a babby. But you smelt powder— didn’t you, cap’n?’

‘Stand by to go about,’ the parrot would scream.

‘Ah, she’s a handsome craft, she is,’ the cook would say, and give her sugar from his pocket, and then the bird would peck at the bars and swear straight on, passing belief for wickedness. ‘There,’ John would add, ‘you can’t touch pitch and not be mucked, lad. Here’s this poor old innocent bird o’ mine swearing blue fire, and none the wiser, you may lay to that. She would swear the same, in a manner of speaking, before chaplain.’ And John would touch his forelock with a solemn way he had that made me think he was the best of men.

In the meantime, the squire and Captain Smollett were still on pretty distant terms with one another. The squire made no bones about the matter; he despised the captain. The captain, on his part, never spoke but when he was spoken to, and then sharp and short and dry, and not a word wasted. He owned, when driven into a corner, that he seemed to have been wrong about the crew, that some of them were as brisk as he wanted to see and all had behaved fairly well. As for the ship, he had taken a

downright fancy to her. ‘She’ll lie a point nearer the wind than a man has a right to expect of his own married wife, sir. But,’ he would add, ‘all I say is, we’re not home again, and I don’t like the cruise.’

The squire, at this, would turn away and march up and down the deck, chin in air.

‘A trifle more of that man,’ he would say, ‘and I shall explode.’

We had some heavy weather, which only proved the qualities of the HISPANIOLA. Every man on board seemed well content, and they must have been hard to please if they had been otherwise, for it is my belief there was never a ship’s company so spoiled since Noah put to sea. Double grog was going on the least excuse; there was duff on odd days, as, for instance, if the squire heard it was any man’s birthday, and always a barrel of apples standing broached in the waist for anyone to help himself that had a fancy.

‘Never knew good come of it yet,’ the captain said to Dr. Livesey. ‘Spoil forecastle hands, make devils. That’s my belief.’

But good did come of the apple barrel, as you shall hear, for if it had not been for that, we should have had no

note of warning and might all have perished by the hand of treachery.

This was how it came about.

We had run up the trades to get the wind of the island we were after—I am not allowed to be more plain—and now we were running down for it with a bright lookout day and night. It was about the last day of our outward voyage by the largest computation; some time that night, or at latest before noon of the morrow, we should sight the Treasure Island. We were heading S.S.W. and had a steady breeze abeam and a quiet sea. The HISPANIOLA rolled steadily, dipping her bowsprit now and then with a whiff of spray. All was drawing alow and aloft; everyone was in the bravest spirits because we were now so near an end of the first part of our adventure.

Now, just after sundown, when all my work was over and I was on my way to my berth, it occurred to me that I should like an apple. I ran on deck. The watch was all forward looking out for the island. The man at the helm was watching the luff of the sail and whistling away gently to himself, and that was the only sound excepting the swish of the sea against the bows and around the sides of the ship.

## *Treasure Island*

In I got bodily into the apple barrel, and found there was scarce an apple left; but sitting down there in the dark, what with the sound of the waters and the rocking movement of the ship, I had either fallen asleep or was on the point of doing so when a heavy man sat down with rather a clash close by. The barrel shook as he leaned his shoulders against it, and I was just about to jump up when the man began to speak. It was Silver's voice, and before I had heard a dozen words, I would not have shown myself for all the world, but lay there, trembling and listening, in the extreme of fear and curiosity, for from these dozen words I understood that the lives of all the honest men aboard depended upon me alone.

## 11

## What I Heard in the Apple Barrel

‘NO, not I,’ said Silver. ‘Flint was cap’n; I was quartermaster, along of my timber leg. The same broadside I lost my leg, old Pew lost his deadlights. It was a master surgeon, him that amputated me—out of college and all—Latin by the bucket, and what not; but he was hanged like a dog, and sun-dried like the rest, at Corso Castle. That was Roberts’ men, that was, and comed of changing names to their ships—ROYAL FORTUNE and so on. Now, what a ship was christened, so let her stay, I says. So it was with the CASSANDRA, as brought us all safe home from Malabar, after England took the viceroy of the Indies; so it was with the old WALRUS, Flint’s old ship, as I’ve seen amuck with the red blood and fit to sink with gold.’

‘Ah!’ cried another voice, that of the youngest hand on board, and evidently full of admiration. ‘He was the flower of the flock, was Flint!’

‘Davis was a man too, by all accounts,’ said Silver. ‘I never sailed along of him; first with England, then with

Flint, that's my story; and now here on my own account, in a manner of speaking. I laid by nine hundred safe, from England, and two thousand after Flint. That ain't bad for a man before the mast—all safe in bank. ‘Tain’t earning now, it’s saving does it, you may lay to that. Where’s all England’s men now? I dunno. Where’s Flint’s? Why, most on ‘em aboard here, and glad to get the duff—been begging before that, some on ‘em. Old Pew, as had lost his sight, and might have thought shame, spends twelve hundred pound in a year, like a lord in Parliament. Where is he now? Well, he’s dead now and under hatches; but for two year before that, shiver my timbers, the man was starving! He begged, and he stole, and he cut throats, and starved at that, by the powers!’

‘Well, it ain’t much use, after all,’ said the young seaman.

“Tain’t much use for fools, you may lay to it—that, nor nothing,’ cried Silver. ‘But now, you look here: you’re young, you are, but you’re as smart as paint. I see that when I set my eyes on you, and I’ll talk to you like a man.’

You may imagine how I felt when I heard this abominable old rogue addressing another in the very same words of flattery as he had used to myself. I think, if I had

been able, that I would have killed him through the barrel. Meantime, he ran on, little supposing he was overheard.

‘Here it is about gentlemen of fortune. They lives rough, and they risk swinging, but they eat and drink like fighting-cocks, and when a cruise is done, why, it’s hundreds of pounds instead of hundreds of farthings in their pockets. Now, the most goes for rum and a good fling, and to sea again in their shirts. But that’s not the course I lay. I puts it all away, some here, some there, and none too much anywhere, by reason of suspicion. I’m fifty, mark you; once back from this cruise, I set up gentleman in earnest. Time enough too, says you. Ah, but I’ve lived easy in the meantime, never denied myself o’ nothing heart desires, and slep’ soft and ate dainty all my days but when at sea. And how did I begin? Before the mast, like you!’

‘Well,’ said the other, ‘but all the other money’s gone now, ain’t it? You daren’t show face in Bristol after this.’

‘Why, where might you suppose it was?’ asked Silver derisively.

‘At Bristol, in banks and places,’ answered his companion.

‘It were,’ said the cook; ‘it were when we weighed anchor. But my old missis has it all by now. And the Spy-

glass is sold, lease and goodwill and rigging; and the old girl's off to meet me. I would tell you where, for I trust you, but it'd make jealousy among the mates.'

'And can you trust your missis?' asked the other.

'Gentlemen of fortune,' returned the cook, 'usually trusts little among themselves, and right they are, you may lay to it. But I have a way with me, I have. When a mate brings a slip on his cable—one as knows me, I mean—it won't be in the same world with old John. There was some that was feared of Pew, and some that was feared of Flint; but Flint his own self was feared of me. Feared he was, and proud. They was the roughest crew afloat, was Flint's; the devil himself would have been feared to go to sea with them. Well now, I tell you, I'm not a boasting man, and you seen yourself how easy I keep company, but when I was quartermaster, LAMBS wasn't the word for Flint's old buccaneers. Ah, you may be sure of yourself in old John's ship.'

'Well, I tell you now,' replied the lad, 'I didn't half a quarter like the job till I had this talk with you, John; but there's my hand on it now.'

'And a brave lad you were, and smart too,' answered Silver, shaking hands so heartily that all the barrel shook,

‘and a finer figurehead for a gentleman of fortune I never clapped my eyes on.’

By this time I had begun to understand the meaning of their terms. By a ‘gentleman of fortune’ they plainly meant neither more nor less than a common pirate, and the little scene that I had overheard was the last act in the corruption of one of the honest hands—perhaps of the last one left aboard. But on this point I was soon to be relieved, for Silver giving a little whistle, a third man strolled up and sat down by the party.

‘Dick’s square,’ said Silver.

‘Oh, I know’d Dick was square,’ returned the voice of the coxswain, Israel Hands. ‘He’s no fool, is Dick.’ And he turned his quid and spat. ‘But look here,’ he went on, ‘here’s what I want to know, Barbecue: how long are we a-going to stand off and on like a blessed bumboat? I’ve had a’most enough o’ Cap’n Smollett; he’s hazed me long enough, by thunder! I want to go into that cabin, I do. I want their pickles and wines, and that.’

‘Israel,’ said Silver, ‘your head ain’t much account, nor ever was. But you’re able to hear, I reckon; leastways, your ears is big enough. Now, here’s what I say: you’ll berth forward, and you’ll live hard, and you’ll speak soft,

and you'll keep sober till I give the word; and you may lay to that, my son.'

'Well, I don't say no, do I?' growled the coxswain.  
'What I say is, when? That's what I say.'

'When! By the powers!' cried Silver. 'Well now, if you want to know, I'll tell you when. The last moment I can manage, and that's when. Here's a first-rate seaman, Cap'n Smollett, sails the blessed ship for us. Here's this squire and doctor with a map and such—I don't know where it is, do I? No more do you, says you. Well then, I mean this squire and doctor shall find the stuff, and help us to get it aboard, by the powers. Then we'll see. If I was sure of you all, sons of double Dutchmen, I'd have Cap'n Smollett navigate us half-way back again before I struck.'

'Why, we're all seamen aboard here, I should think,' said the lad Dick.

'We're all forecastle hands, you mean,' snapped Silver. 'We can steer a course, but who's to set one? That's what all you gentlemen split on, first and last. If I had my way, I'd have Cap'n Smollett work us back into the trades at least; then we'd have no blessed miscalculations and a spoonful of water a day. But I know the sort you are. I'll finish with 'em at the island, as soon's the blunt's on board, and a pity it is. But you're

never happy till you're drunk. Split my sides, I've a sick heart to sail with the likes of you!'

'Easy all, Long John,' cried Israel. 'Who's a-crossin' of you?'

'Why, how many tall ships, think ye, now, have I seen laid aboard? And how many brisk lads drying in the sun at Execution Dock?' cried Silver. 'And all for this same hurry and hurry and hurry. You hear me? I seen a thing or two at sea, I have. If you would on'y lay your course, and a p'int to windward, you would ride in carriages, you would. But not you! I know you. You'll have your mouthful of rum tomorrow, and go hang.'

'Everybody knowed you was a kind of a chapling, John; but there's others as could hand and steer as well as you,' said Israel. 'They liked a bit o' fun, they did. They wasn't so high and dry, nohow, but took their fling, like jolly companions every one.'

'So?' says Silver. 'Well, and where are they now? Pew was that sort, and he died a beggar-man. Flint was, and he died of rum at Savannah. Ah, they was a sweet crew, they was! On'y, where are they?'

'But,' asked Dick, 'when we do lay 'em athwart, what are we to do with 'em, anyhow?'

‘There’s the man for me!’ cried the cook admiringly. ‘That’s what I call business. Well, what would you think? Put ‘em ashore like maroons? That would have been England’s way. Or cut ‘em down like that much pork? That would have been Flint’s, or Billy Bones’s.’

‘Billy was the man for that,’ said Israel. ‘Dead men don’t bite,’ says he. Well, he’s dead now hisself; he knows the long and short on it now; and if ever a rough hand come to port, it was Billy.’

‘Right you are,’ said Silver; ‘rough and ready. But mark you here, I’m an easy man—I’m quite the gentleman, says you; but this time it’s serious. Dooty is dooty, mates. I give my vote—death. When I’m in Parlyment and riding in my coach, I don’t want none of these sea-lawyers in the cabin a-coming home, unlooked for, like the devil at prayers. Wait is what I say; but when the time comes, why, let her rip!’

‘John,’ cries the coxswain, ‘you’re a man!’

‘You’ll say so, Israel when you see,’ said Silver. ‘Only one thing I claim—I claim Trelawney. I’ll wring his calf’s head off his body with these hands, Dick!’ he added, breaking off. ‘You just jump up, like a sweet lad, and get me an apple, to wet my pipe like.’

You may fancy the terror I was in! I should have leaped out and run for it if I had found the strength, but my limbs and heart alike misgave me. I heard Dick begin to rise, and then someone seemingly stopped him, and the voice of Hands exclaimed, ‘Oh, stow that! Don’t you get sucking of that bilge, John. Let’s have a go of the rum.’

‘Dick,’ said Silver, ‘I trust you. I’ve a gauge on the keg, mind. There’s the key; you fill a pannikin and bring it up.’

Terrified as I was, I could not help thinking to myself that this must have been how Mr. Arrow got the strong waters that destroyed him.

Dick was gone but a little while, and during his absence Israel spoke straight on in the cook’s ear. It was but a word or two that I could catch, and yet I gathered some important news, for besides other scraps that tended to the same purpose, this whole clause was audible: ‘Not another man of them’ll jine.’ Hence there were still faithful men on board.

When Dick returned, one after another of the trio took the pannikin and drank—one ‘To luck,’ another with a ‘Here’s to old Flint,’ and Silver himself saying, in a kind of song, ‘Here’s to ourselves, and hold your luff, plenty of prizes and plenty of duff.’

Just then a sort of brightness fell upon me in the barrel, and looking up, I found the moon had risen and was silverying the mizzen-top and shining white on the luff of the fore-sail; and almost at the same time the voice of the lookout shouted, ‘Land ho!’

# 12

## Council of War

THERE was a great rush of feet across the deck. I could hear people tumbling up from the cabin and the forecastle, and slipping in an instant outside my barrel, I dived behind the fore-sail, made a double towards the stern, and came out upon the open deck in time to join Hunter and Dr. Livesey in the rush for the weather bow.

There all hands were already congregated. A belt of fog had lifted almost simultaneously with the appearance of the moon. Away to the south-west of us we saw two low hills, about a couple of miles apart, and rising behind one of them a third and higher hill, whose peak was still buried in the fog. All three seemed sharp and conical in figure.

So much I saw, almost in a dream, for I had not yet recovered from my horrid fear of a minute or two before. And then I heard the voice of Captain Smollett issuing orders. The HISPANIOLA was laid a couple of points nearer the wind and now sailed a course that would just clear the island on the east.

## Treasure Island

‘And now, men,’ said the captain, when all was sheeted home, ‘has any one of you ever seen that land ahead?’

‘I have, sir,’ said Silver. ‘I’ve watered there with a trader I was cook in.’

‘The anchorage is on the south, behind an islet, I fancy?’ asked the captain.

‘Yes, sir; Skeleton Island they calls it. It were a main place for pirates once, and a hand we had on board knowed all their names for it. That hill to the nor’ard they calls the Fore-mast Hill; there are three hills in a row running south’ard—fore, main, and mizzen, sir. But the main—that’s the big un, with the cloud on it—they usually calls the Spy-glass, by reason of a lookout they kept when they was in the anchorage cleaning, for it’s there they cleaned their ships, sir, asking your pardon.’

‘I have a chart here,’ says Captain Smollett. ‘See if that’s the place.’

Long John’s eyes burned in his head as he took the chart, but by the fresh look of the paper I knew he was doomed to disappointment. This was not the map we found in Billy Bones’s chest, but an accurate copy, complete in all things—names and heights and soundings—with the single exception of the red crosses

and the written notes. Sharp as must have been his annoyance, Silver had the strength of mind to hide it.

‘Yes, sir,’ said he, ‘this is the spot, to be sure, and very prettily drawed out. Who might have done that, I wonder? The pirates were too ignorant, I reckon. Aye, here it is: ‘Capt. Kidd’s Anchorage’—just the name my shipmate called it. There’s a strong current runs along the south, and then away nor’ard up the west coast. Right you was, sir,’ says he, ‘to haul your wind and keep the weather of the island. Leastways, if such was your intention as to enter and careen, and there ain’t no better place for that in these waters.’

‘Thank you, my man,’ says Captain Smollett. ‘I’ll ask you later on to give us a help. You may go.’

I was surprised at the coolness with which John avowed his knowledge of the island, and I own I was half-frightened when I saw him drawing nearer to myself. He did not know, to be sure, that I had overheard his council from the apple barrel, and yet I had by this time taken such a horror of his cruelty, duplicity, and power that I could scarce conceal a shudder when he laid his hand upon my arm.

‘Ah,’ says he, ‘this here is a sweet spot, this island—a sweet spot for a lad to get ashore on. You’ll bathe, and

you'll climb trees, and you'll hunt goats, you will; and you'll get aloft on them hills like a goat yourself. Why, it makes me young again. I was going to forget my timber leg, I was. It's a pleasant thing to be young and have ten toes, and you may lay to that. When you want to go a bit of exploring, you just ask old John, and he'll put up a snack for you to take along.'

And clapping me in the friendliest way upon the shoulder, he hobbled off forward and went below.

Captain Smollett, the squire, and Dr. Livesey were talking together on the quarter-deck, and anxious as I was to tell them my story, I durst not interrupt them openly. While I was still casting about in my thoughts to find some probable excuse, Dr. Livesey called me to his side. He had left his pipe below, and being a slave to tobacco, had meant that I should fetch it; but as soon as I was near enough to speak and not to be overheard, I broke immediately, 'Doctor, let me speak. Get the captain and squire down to the cabin, and then make some pretence to send for me. I have terrible news.'

The doctor changed countenance a little, but next moment he was master of himself.

'Thank you, Jim,' said he quite loudly, 'that was all I wanted to know,' as if he had asked me a question.

And with that he turned on his heel and rejoined the other two. They spoke together for a little, and though none of them started, or raised his voice, or so much as whistled, it was plain enough that Dr. Livesey had communicated my request, for the next thing that I heard was the captain giving an order to Job Anderson, and all hands were piped on deck.

‘My lads,’ said Captain Smollett, ‘I’ve a word to say to you. This land that we have sighted is the place we have been sailing for. Mr. Trelawney, being a very open-handed gentleman, as we all know, has just asked me a word or two, and as I was able to tell him that every man on board had done his duty, alow and aloft, as I never ask to see it done better, why, he and I and the doctor are going below to the cabin to drink YOUR health and luck, and you’ll have grog served out for you to drink OUR health and luck. I’ll tell you what I think of this: I think it handsome. And if you think as I do, you’ll give a good sea-cheer for the gentleman that does it.’

The cheer followed—that was a matter of course; but it rang out so full and hearty that I confess I could hardly believe these same men were plotting for our blood.

‘One more cheer for Cap’n Smollett,’ cried Long John when the first had subsided.

And this also was given with a will.

On the top of that the three gentlemen went below, and not long after, word was sent forward that Jim Hawkins was wanted in the cabin.

I found them all three seated round the table, a bottle of Spanish wine and some raisins before them, and the doctor smoking away, with his wig on his lap, and that, I knew, was a sign that he was agitated. The stern window was open, for it was a warm night, and you could see the moon shining behind on the ship's wake.

'Now, Hawkins,' said the squire, 'you have something to say. Speak up.'

I did as I was bid, and as short as I could make it, told the whole details of Silver's conversation. Nobody interrupted me till I was done, nor did any one of the three of them make so much as a movement, but they kept their eyes upon my face from first to last.

'Jim,' said Dr. Livesey, 'take a seat.'

And they made me sit down at table beside them, poured me out a glass of wine, filled my hands with raisins, and all three, one after the other, and each with a bow, drank my good health, and their service to me, for my luck and courage.

‘Now, captain,’ said the squire, ‘you were right, and I was wrong. I own myself an ass, and I await your orders.’

‘No more an ass than I, sir,’ returned the captain. ‘I never heard of a crew that meant to mutiny but what showed signs before, for any man that had an eye in his head to see the mischief and take steps according. But this crew,’ he added, ‘beats me.’

‘Captain,’ said the doctor, ‘with your permission, that’s Silver. A very remarkable man.’

‘He’d look remarkably well from a yard-arm, sir,’ returned the captain. ‘But this is talk; this don’t lead to anything. I see three or four points, and with Mr. Trelawney’s permission, I’ll name them.’

‘You, sir, are the captain. It is for you to speak,’ says Mr. Trelawney grandly.

‘First point,’ began Mr. Smollett. ‘We must go on, because we can’t turn back. If I gave the word to go about, they would rise at once. Second point, we have time before us—at least until this treasure’s found. Third point, there are faithful hands. Now, sir, it’s got to come to blows sooner or later, and what I propose is to take time by the forelock, as the saying is, and come to blows some fine day when they least expect it. We can count, I take it, on your own home servants, Mr. Trelawney?’

‘As upon myself,’ declared the squire.

‘Three,’ reckoned the captain; ‘ourselves make seven, counting Hawkins here. Now, about the honest hands?’

‘Most likely Trelawney’s own men,’ said the doctor; ‘those he had picked up for himself before he lit on Silver.’

‘Nay,’ replied the squire. ‘Hands was one of mine.’

‘I did think I could have trusted Hands,’ added the captain.

‘And to think that they’re all Englishmen!’ broke out the squire. ‘Sir, I could find it in my heart to blow the ship up.’

‘Well, gentlemen,’ said the captain, ‘the best that I can say is not much. We must lay to, if you please, and keep a bright lookout. It’s trying on a man, I know. It would be pleasanter to come to blows. But there’s no help for it till we know our men. Lay to, and whistle for a wind, that’s my view.’

‘Jim here,’ said the doctor, ‘can help us more than anyone. The men are not shy with him, and Jim is a noticing lad.’

‘Hawkins, I put prodigious faith in you,’ added the squire.

I began to feel pretty desperate at this, for I felt altogether helpless; and yet, by an odd train of circumstances, it was indeed through me that safety came. In the meantime, talk as we pleased, there were only seven out of the twenty-six on whom we knew we could rely; and out of these seven one was a boy, so that the grown men on our side were six to their nineteen.

## PART THREE

### My Shore Adventure

## 13

### How My Shore Adventure Began

THE appearance of the island when I came on deck next morning was altogether changed. Although the breeze had now utterly ceased, we had made a great deal of way during the night and were now lying becalmed about half a mile to the south-east of the low eastern coast. Grey-coloured woods covered a large part of the surface. This even tint was indeed broken up by streaks of yellow sand-break in the lower lands, and by many tall trees of the pine family, out-topping the others—some singly, some in clumps; but the general colouring was uniform and sad. The hills ran up clear above the vegetation in spires of naked rock. All were strangely shaped, and the Spy-glass, which was by three or four hundred feet the tallest on the island, was likewise the strangest in configuration, running up sheer from almost every side and then suddenly cut off at the top like a pedestal to put a statue on.

The HISPANIOLA was rolling scuppers under in the ocean swell. The booms were tearing at the blocks, the rudder was banging to and fro, and the whole ship

creaking, groaning, and jumping like a manufactory. I had to cling tight to the backstay, and the world turned giddily before my eyes, for though I was a good enough sailor when there was way on, this standing still and being rolled about like a bottle was a thing I never learned to stand without a qualm or so, above all in the morning, on an empty stomach.

Perhaps it was this—perhaps it was the look of the island, with its grey, melancholy woods, and wild stone spires, and the surf that we could both see and hear foaming and thundering on the steep beach—at least, although the sun shone bright and hot, and the shore birds were fishing and crying all around us, and you would have thought anyone would have been glad to get to land after being so long at sea, my heart sank, as the saying is, into my boots; and from the first look onward, I hated the very thought of Treasure Island.

We had a dreary morning's work before us, for there was no sign of any wind, and the boats had to be got out and manned, and the ship warped three or four miles round the corner of the island and up the narrow passage to the haven behind Skeleton Island. I volunteered for one of the boats, where I had, of course, no business. The heat was sweltering, and the men grumbled fiercely over their

work. Anderson was in command of my boat, and instead of keeping the crew in order, he grumbled as loud as the worst.

‘Well,’ he said with an oath, ‘it’s not forever.’

I thought this was a very bad sign, for up to that day the men had gone briskly and willingly about their business; but the very sight of the island had relaxed the cords of discipline.

All the way in, Long John stood by the steersman and conned the ship. He knew the passage like the palm of his hand, and though the man in the chains got everywhere more water than was down in the chart, John never hesitated once.

‘There’s a strong scour with the ebb,’ he said, ‘and this here passage has been dug out, in a manner of speaking, with a spade.’

We brought up just where the anchor was in the chart, about a third of a mile from each shore, the mainland on one side and Skeleton Island on the other. The bottom was clean sand. The plunge of our anchor sent up clouds of birds wheeling and crying over the woods, but in less than a minute they were down again and all was once more silent.

## Treasure Island

The place was entirely land-locked, buried in woods, the trees coming right down to high-water mark, the shores mostly flat, and the hilltops standing round at a distance in a sort of amphitheatre, one here, one there. Two little rivers, or rather two swamps, emptied out into this pond, as you might call it; and the foliage round that part of the shore had a kind of poisonous brightness. From the ship we could see nothing of the house or stockade, for they were quite buried among trees; and if it had not been for the chart on the companion, we might have been the first that had ever anchored there since the island arose out of the seas.

There was not a breath of air moving, nor a sound but that of the surf booming half a mile away along the beaches and against the rocks outside. A peculiar stagnant smell hung over the anchorage—a smell of sodden leaves and rotting tree trunks. I observed the doctor sniffing and sniffing, like someone tasting a bad egg.

‘I don’t know about treasure,’ he said, ‘but I’ll stake my wig there’s fever here.’

If the conduct of the men had been alarming in the boat, it became truly threatening when they had come aboard. They lay about the deck growling together in talk. The slightest order was received with a black look and

grudgingly and carelessly obeyed. Even the honest hands must have caught the infection, for there was not one man aboard to mend another. Mutiny, it was plain, hung over us like a thunder-cloud.

And it was not only we of the cabin party who perceived the danger. Long John was hard at work going from group to group, spending himself in good advice, and as for example no man could have shown a better. He fairly outstripped himself in willingness and civility; he was all smiles to everyone. If an order were given, John would be on his crutch in an instant, with the cheeriest ‘Aye, aye, sir!’ in the world; and when there was nothing else to do, he kept up one song after another, as if to conceal the discontent of the rest.

Of all the gloomy features of that gloomy afternoon, this obvious anxiety on the part of Long John appeared the worst.

We held a council in the cabin.

‘Sir,’ said the captain, ‘if I risk another order, the whole ship’ll come about our ears by the run. You see, sir, here it is. I get a rough answer, do I not? Well, if I speak back, pikes will be going in two shakes; if I don’t, Silver will see there’s something under that, and the game’s up. Now, we’ve only one man to rely on.’

‘And who is that?’ asked the squire.

‘Silver, sir,’ returned the captain; ‘he’s as anxious as you and I to smother things up. This is a tiff; he’d soon talk ‘em out of it if he had the chance, and what I propose to do is to give him the chance. Let’s allow the men an afternoon ashore. If they all go, why we’ll fight the ship. If they none of them go, well then, we hold the cabin, and God defend the right. If some go, you mark my words, sir, Silver’ll bring ‘em aboard again as mild as lambs.’

It was so decided; loaded pistols were served out to all the sure men; Hunter, Joyce, and Redruth were taken into our confidence and received the news with less surprise and a better spirit than we had looked for, and then the captain went on deck and addressed the crew.

‘My lads,’ said he, ‘we’ve had a hot day and are all tired and out of sorts. A turn ashore’ll hurt nobody—the boats are still in the water; you can take the gigs, and as many as please may go ashore for the afternoon. I’ll fire a gun half an hour before sundown.’

I believe the silly fellows must have thought they would break their shins over treasure as soon as they were landed, for they all came out of their sulks in a moment and gave a cheer that started the echo in a far-away hill

and sent the birds once more flying and squalling round the anchorage.

The captain was too bright to be in the way. He whipped out of sight in a moment, leaving Silver to arrange the party, and I fancy it was as well he did so. Had he been on deck, he could no longer so much as have pretended not to understand the situation. It was as plain as day. Silver was the captain, and a mighty rebellious crew he had of it. The honest hands—and I was soon to see it proved that there were such on board—must have been very stupid fellows. Or rather, I suppose the truth was this, that all hands were disaffected by the example of the ringleaders—only some more, some less; and a few, being good fellows in the main, could neither be led nor driven any further. It is one thing to be idle and skulk and quite another to take a ship and murder a number of innocent men.

At last, however, the party was made up. Six fellows were to stay on board, and the remaining thirteen, including Silver, began to embark.

Then it was that there came into my head the first of the mad notions that contributed so much to save our lives. If six men were left by Silver, it was plain our party could not take and fight the ship; and since only six were

left, it was equally plain that the cabin party had no present need of my assistance. It occurred to me at once to go ashore. In a jiffy I had slipped over the side and curled up in the fore-sheets of the nearest boat, and almost at the same moment she shoved off.

No one took notice of me, only the bow oar saying, ‘Is that you, Jim? Keep your head down.’ But Silver, from the other boat, looked sharply over and called out to know if that were me; and from that moment I began to regret what I had done.

The crews raced for the beach, but the boat I was in, having some start and being at once the lighter and the better manned, shot far ahead of her consort, and the bow had struck among the shore-side trees and I had caught a branch and swung myself out and plunged into the nearest thicket while Silver and the rest were still a hundred yards behind.

‘Jim, Jim!’ I heard him shouting.

But you may suppose I paid no heed; jumping, ducking, and breaking through, I ran straight before my nose till I could run no longer.

## The First Blow

I WAS so pleased at having given the slip to Long John that I began to enjoy myself and look around me with some interest on the strange land that I was in.

I had crossed a marshy tract full of willows, bulrushes, and odd, outlandish, swampy trees; and I had now come out upon the skirts of an open piece of undulating, sandy country, about a mile long, dotted with a few pines and a great number of contorted trees, not unlike the oak in growth, but pale in the foliage, like willows. On the far side of the open stood one of the hills, with two quaint, craggy peaks shining vividly in the sun.

I now felt for the first time the joy of exploration. The isle was uninhabited; my shipmates I had left behind, and nothing lived in front of me but dumb brutes and fowls. I turned hither and thither among the trees. Here and there were flowering plants, unknown to me; here and there I saw snakes, and one raised his head from a ledge of rock and hissed at me with a noise not unlike the spinning of a

top. Little did I suppose that he was a deadly enemy and that the noise was the famous rattle.

Then I came to a long thicket of these oaklike trees—live, or evergreen, oaks, I heard afterwards they should be called—which grew low along the sand like brambles, the boughs curiously twisted, the foliage compact, like thatch. The thicket stretched down from the top of one of the sandy knolls, spreading and growing taller as it went, until it reached the margin of the broad, reedy fen, through which the nearest of the little rivers soaked its way into the anchorage. The marsh was steaming in the strong sun, and the outline of the Spy-glass trembled through the haze.

All at once there began to go a sort of bustle among the bulrushes; a wild duck flew up with a quack, another followed, and soon over the whole surface of the marsh a great cloud of birds hung screaming and circling in the air. I judged at once that some of my shipmates must be drawing near along the borders of the fen. Nor was I deceived, for soon I heard the very distant and low tones of a human voice, which, as I continued to give ear, grew steadily louder and nearer.

This put me in a great fear, and I crawled under cover of the nearest live-oak and squatted there, hearkening, as silent as a mouse.

Another voice answered, and then the first voice, which I now recognized to be Silver's, once more took up the story and ran on for a long while in a stream, only now and again interrupted by the other. By the sound they must have been talking earnestly, and almost fiercely; but no distinct word came to my hearing.

At last the speakers seemed to have paused and perhaps to have sat down, for not only did they cease to draw any nearer, but the birds themselves began to grow more quiet and to settle again to their places in the swamp.

And now I began to feel that I was neglecting my business, that since I had been so foolhardy as to come ashore with these desperadoes, the least I could do was to overhear them at their councils, and that my plain and obvious duty was to draw as close as I could manage, under the favourable ambush of the crouching trees.

I could tell the direction of the speakers pretty exactly, not only by the sound of their voices but by the behaviour of the few birds that still hung in alarm above the heads of the intruders.

Crawling on all fours, I made steadily but slowly towards them, till at last, raising my head to an aperture among the leaves, I could see clear down into a little green dell beside the marsh, and closely set about with trees, where Long John Silver and another of the crew stood face to face in conversation.

The sun beat full upon them. Silver had thrown his hat beside him on the ground, and his great, smooth, blond face, all shining with heat, was lifted to the other man's in a kind of appeal.

'Mate,' he was saying, 'it's because I thinks gold dust of you—gold dust, and you may lay to that! If I hadn't took to you like pitch, do you think I'd have been here a-warning of you? All's up—you can't make nor mend; it's to save your neck that I'm a-speaking, and if one of the wild uns knew it, where'd I be, Tom— now, tell me, where'd I be?'

'Silver,' said the other man—and I observed he was not only red in the face, but spoke as hoarse as a crow, and his voice shook too, like a taut rope—'Silver,' says he, 'you're old, and you're honest, or has the name for it; and you've money too, which lots of poor sailors hasn't; and you're brave, or I'm mistook. And will you tell me you'll let yourself be led away with that kind of a mess of

swabs? Not you! As sure as God sees me, I'd sooner lose my hand. If I turn agin my dooty—‘

And then all of a sudden he was interrupted by a noise. I had found one of the honest hands—well, here, at that same moment, came news of another. Far away out in the marsh there arose, all of a sudden, a sound like the cry of anger, then another on the back of it; and then one horrid, long-drawn scream. The rocks of the Spy-glass re-echoed it a score of times; the whole troop of marsh-birds rose again, darkening heaven, with a simultaneous whirr; and long after that death yell was still ringing in my brain, silence had re-established its empire, and only the rustle of the redescending birds and the boom of the distant surges disturbed the languor of the afternoon.

Tom had leaped at the sound, like a horse at the spur, but Silver had not winked an eye. He stood where he was, resting lightly on his crutch, watching his companion like a snake about to spring.

‘John!’ said the sailor, stretching out his hand.

‘Hands off!’ cried Silver, leaping back a yard, as it seemed to me, with the speed and security of a trained gymnast.

‘Hands off, if you like, John Silver,’ said the other. ‘It’s a black conscience that can make you feared of me. But in heaven’s name, tell me, what was that?’

‘That?’ returned Silver, smiling away, but warier than ever, his eye a mere pin-point in his big face, but gleaming like a crumb of glass. ‘That?’ Oh, I reckon that’ll be Alan.’

And at this point Tom flashed out like a hero.

‘Alan!’ he cried. ‘Then rest his soul for a true seaman! And as for you, John Silver, long you’ve been a mate of mine, but you’re mate of mine no more. If I die like a dog, I’ll die in my dooty. You’ve killed Alan, have you? Kill me too, if you can. But I defies you.’

And with that, this brave fellow turned his back directly on the cook and set off walking for the beach. But he was not destined to go far. With a cry John seized the branch of a tree, whipped the crutch out of his armpit, and sent that uncouth missile hurtling through the air. It struck poor Tom, point foremost, and with stunning violence, right between the shoulders in the middle of his back. His hands flew up, he gave a sort of gasp, and fell.

Whether he were injured much or little, none could ever tell. Like enough, to judge from the sound, his back was broken on the spot. But he had no time given him to

recover. Silver, agile as a monkey even without leg or crutch, was on the top of him next moment and had twice buried his knife up to the hilt in that defenceless body. From my place of ambush, I could hear him pant aloud as he struck the blows.

I do not know what it rightly is to faint, but I do know that for the next little while the whole world swam away from before me in a whirling mist; Silver and the birds, and the tall Spy-glass hilltop, going round and round and topsy-turvy before my eyes, and all manner of bells ringing and distant voices shouting in my ear.

When I came again to myself the monster had pulled himself together, his crutch under his arm, his hat upon his head. Just before him Tom lay motionless upon the sward; but the murderer minded him not a whit, cleansing his blood-stained knife the while upon a wisp of grass. Everything else was unchanged, the sun still shining mercilessly on the steaming marsh and the tall pinnacle of the mountain, and I could scarce persuade myself that murder had been actually done and a human life cruelly cut short a moment since before my eyes.

But now John put his hand into his pocket, brought out a whistle, and blew upon it several modulated blasts that rang far across the heated air. I could not tell, of course,

## *Treasure Island*

the meaning of the signal, but it instantly awoke my fears. More men would be coming. I might be discovered. They had already slain two of the honest people; after Tom and Alan, might not I come next?

Instantly I began to extricate myself and crawl back again, with what speed and silence I could manage, to the more open portion of the wood. As I did so, I could hear hails coming and going between the old buccaneer and his comrades, and this sound of danger lent me wings. As soon as I was clear of the thicket, I ran as I never ran before, scarce minding the direction of my flight, so long as it led me from the murderers; and as I ran, fear grew and grew upon me until it turned into a kind of frenzy.

Indeed, could anyone be more entirely lost than I? When the gun fired, how should I dare to go down to the boats among those fiends, still smoking from their crime? Would not the first of them who saw me wring my neck like a snipe's? Would not my absence itself be an evidence to them of my alarm, and therefore of my fatal knowledge? It was all over, I thought. Good-bye to the HISPANIOLA; good-bye to the squire, the doctor, and the captain! There was nothing left for me but death by starvation or death by the hands of the mutineers.

All this while, as I say, I was still running, and without taking any notice, I had drawn near to the foot of the little hill with the two peaks and had got into a part of the island where the live-oaks grew more widely apart and seemed more like forest trees in their bearing and dimensions. Mingled with these were a few scattered pines, some fifty, some nearer seventy, feet high. The air too smelt more freshly than down beside the marsh.

And here a fresh alarm brought me to a standstill with a thumping heart.

## The Man of the Island

FROM the side of the hill, which was here steep and stony, a spout of gravel was dislodged and fell rattling and bounding through the trees. My eyes turned instinctively in that direction, and I saw a figure leap with great rapidity behind the trunk of a pine. What it was, whether bear or man or monkey, I could in no wise tell. It seemed dark and shaggy; more I knew not. But the terror of this new apparition brought me to a stand.

I was now, it seemed, cut off upon both sides; behind me the murderers, before me this lurking nondescript. And immediately I began to prefer the dangers that I knew to those I knew not. Silver himself appeared less terrible in contrast with this creature of the woods, and I turned on my heel, and looking sharply behind me over my shoulder, began to retrace my steps in the direction of the boats.

Instantly the figure reappeared, and making a wide circuit, began to head me off. I was tired, at any rate; but had I been as fresh as when I rose, I could see it was in

vain for me to contend in speed with such an adversary. From trunk to trunk the creature flitted like a deer, running manlike on two legs, but unlike any man that I had ever seen, stooping almost double as it ran. Yet a man it was, I could no longer be in doubt about that.

I began to recall what I had heard of cannibals. I was within an ace of calling for help. But the mere fact that he was a man, however wild, had somewhat reassured me, and my fear of Silver began to revive in proportion. I stood still, therefore, and cast about for some method of escape; and as I was so thinking, the recollection of my pistol flashed into my mind. As soon as I remembered I was not defenceless, courage glowed again in my heart and I set my face resolutely for this man of the island and walked briskly towards him.

He was concealed by this time behind another tree trunk; but he must have been watching me closely, for as soon as I began to move in his direction he reappeared and took a step to meet me. Then he hesitated, drew back, came forward again, and at last, to my wonder and confusion, threw himself on his knees and held out his clasped hands in supplication.

At that I once more stopped.

‘Who are you?’ I asked.

‘Ben Gunn,’ he answered, and his voice sounded hoarse and awkward, like a rusty lock. ‘I’m poor Ben Gunn, I am; and I haven’t spoke with a Christian these three years.’

I could now see that he was a white man like myself and that his features were even pleasing. His skin, wherever it was exposed, was burnt by the sun; even his lips were black, and his fair eyes looked quite startling in so dark a face. Of all the beggar-men that I had seen or fancied, he was the chief for raggedness. He was clothed with tatters of old ship’s canvas and old sea-cloth, and this extraordinary patchwork was all held together by a system of the most various and incongruous fastenings, brass buttons, bits of stick, and loops of tarry gaskin. About his waist he wore an old brass-buckled leather belt, which was the one thing solid in his whole accoutrement.

‘Three years!’ I cried. ‘Were you shipwrecked?’

‘Nay, mate,’ said he; ‘marooned.’

I had heard the word, and I knew it stood for a horrible kind of punishment common enough among the buccaneers, in which the offender is put ashore with a little powder and shot and left behind on some desolate and distant island.

‘Marooned three years agone,’ he continued, ‘and lived on goats since then, and berries, and oysters. Wherever a man is, says I, a man can do for himself. But, mate, my heart is sore for Christian diet. You mightn’t happen to have a piece of cheese about you, now? No? Well, many’s the long night I’ve dreamed of cheese—toasted, mostly—and woke up again, and here I were.’

‘If ever I can get aboard again,’ said I, ‘you shall have cheese by the stone.’

All this time he had been feeling the stuff of my jacket, smoothing my hands, looking at my boots, and generally, in the intervals of his speech, showing a childish pleasure in the presence of a fellow creature. But at my last words he perked up into a kind of startled slyness.

‘If ever you can get aboard again, says you?’ he repeated. ‘Why, now, who’s to hinder you?’

‘Not you, I know,’ was my reply.

‘And right you was,’ he cried. ‘Now you—what do you call yourself, mate?’

‘Jim,’ I told him.

‘Jim, Jim,’ says he, quite pleased apparently. ‘Well, now, Jim, I’ve lived that rough as you’d be ashamed to hear of. Now, for instance, you wouldn’t think I had had a pious mother—to look at me?’ he asked.

‘Why, no, not in particular,’ I answered.

‘Ah, well,’ said he, ‘but I had—remarkable pious. And I was a civil, pious boy, and could rattle off my catechism that fast, as you couldn’t tell one word from another. And here’s what it come to, Jim, and it begun with chuck-farthen on the blessed grave-stones! That’s what it begun with, but it went further’n that; and so my mother told me, and predicked the whole, she did, the pious woman! But it were Providence that put me here. I’ve thought it all out in this here lonely island, and I’m back on piety. You don’t catch me tasting rum so much, but just a thimbleful for luck, of course, the first chance I have. I’m bound I’ll be good, and I see the way to. And, Jim’—looking all round him and lowering his voice to a whisper—‘I’m rich.’

I now felt sure that the poor fellow had gone crazy in his solitude, and I suppose I must have shown the feeling in my face, for he repeated the statement hotly: ‘Rich! Rich! I says. And I’ll tell you what: I’ll make a man of you, Jim. Ah, Jim, you’ll bless your stars, you will, you was the first that found me!’

And at this there came suddenly a lowering shadow over his face, and he tightened his grasp upon my hand and raised a forefinger threateningly before my eyes.

‘Now, Jim, you tell me true: that ain’t Flint’s ship?’ he asked.

At this I had a happy inspiration. I began to believe that I had found an ally, and I answered him at once.

‘It’s not Flint’s ship, and Flint is dead; but I’ll tell you true, as you ask me—there are some of Flint’s hands aboard; worse luck for the rest of us.’

‘Not a man—with one—leg?’ he gasped.

‘Silver?’ I asked.

‘Ah, Silver!’ says he. ‘That were his name.’

‘He’s the cook, and the ringleader too.’

He was still holding me by the wrist, and at that he give it quite a wring.

‘If you was sent by Long John,’ he said, ‘I’m as good as pork, and I know it. But where was you, do you suppose?’

I had made my mind up in a moment, and by way of answer told him the whole story of our voyage and the predicament in which we found ourselves. He heard me with the keenest interest, and when I had done he patted me on the head.

‘You’re a good lad, Jim,’ he said; ‘and you’re all in a clove hitch, ain’t you? Well, you just put your trust in Ben Gunn—Ben Gunn’s the man to do it. Would you think it

likely, now, that your squire would prove a liberal-minded one in case of help—him being in a clove hitch, as you remark?’

I told him the squire was the most liberal of men.

‘Aye, but you see,’ returned Ben Gunn, ‘I didn’t mean giving me a gate to keep, and a suit of livery clothes, and such; that’s not my mark, Jim. What I mean is, would he be likely to come down to the toon of, say one thousand pounds out of money that’s as good as a man’s own already?’

‘I am sure he would,’ said I. ‘As it was, all hands were to share.’

‘AND a passage home?’ he added with a look of great shrewdness.

‘Why,’ I cried, ‘the squire’s a gentleman. And besides, if we got rid of the others, we should want you to help work the vessel home.’

‘Ah,’ said he, ‘so you would.’ And he seemed very much relieved.

‘Now, I’ll tell you what,’ he went on. ‘So much I’ll tell you, and no more. I were in Flint’s ship when he buried the treasure; he and six along—six strong seamen. They was ashore nigh on a week, and us standing off and on in the old WALRUS. One fine day up went the signal, and

here come Flint by himself in a little boat, and his head done up in a blue scarf. The sun was getting up, and mortal white he looked about the cutwater. But, there he was, you mind, and the six all dead—dead and buried. How he done it, not a man aboard us could make out. It was battle, murder, and sudden death, leastways—him against six. Billy Bones was the mate; Long John, he was quartermaster; and they asked him where the treasure was. ‘Ah,’ says he, ‘you can go ashore, if you like, and stay,’ he says; ‘but as for the ship, she’ll beat up for more, by thunder!’ That’s what he said.

‘Well, I was in another ship three years back, and we sighted this island. ‘Boys,’ said I, ‘here’s Flint’s treasure; let’s land and find it.’ The cap’n was displeased at that, but my messmates were all of a mind and landed. Twelve days they looked for it, and every day they had the worse word for me, until one fine morning all hands went aboard. ‘As for you, Benjamin Gunn,’ says they, ‘here’s a musket,’ they says, ‘and a spade, and pick-axe. You can stay here and find Flint’s money for yourself,’ they says.

‘Well, Jim, three years have I been here, and not a bite of Christian diet from that day to this. But now, you look here; look at me. Do I look like a man before the mast? No, says you. Nor I weren’t, neither, I says.’

And with that he winked and pinched me hard.

‘Just you mention them words to your squire, Jim,’ he went on. ‘Nor he weren’t, neither—that’s the words. Three years he were the man of this island, light and dark, fair and rain; and sometimes he would maybe think upon a prayer (says you), and sometimes he would maybe think of his old mother, so be as she’s alive (you’ll say); but the most part of Gunn’s time (this is what you’ll say)—the most part of his time was took up with another matter. And then you’ll give him a nip, like I do.’

And he pinched me again in the most confidential manner.

‘Then,’ he continued, ‘then you’ll up, and you’ll say this: Gunn is a good man (you’ll say), and he puts a precious sight more confidence—a precious sight, mind that—in a gen’leman born than in these gen’leman of fortune, having been one hisself.’

‘Well,’ I said, ‘I don’t understand one word that you’ve been saying. But that’s neither here nor there; for how am I to get on board?’

‘Ah,’ said he, ‘that’s the hitch, for sure. Well, there’s my boat, that I made with my two hands. I keep her under the white rock. If the worst come to the worst, we might try that after dark. Hi!’ he broke out. ‘What’s that?’

For just then, although the sun had still an hour or two to run, all the echoes of the island awoke and bellowed to the thunder of a cannon.

‘They have begun to fight!’ I cried. ‘Follow me.’

And I began to run towards the anchorage, my terrors all forgotten, while close at my side the marooned man in his goatskins trotted easily and lightly.

‘Left, left,’ says he; ‘keep to your left hand, mate Jim! Under the trees with you! Theer’s where I killed my first goat. They don’t come down here now; they’re all mastheaded on them mountings for the fear of Benjamin Gunn. Ah! And there’s the ceteemory’— cemetery, he must have meant. ‘You see the mounds? I come here and prayed, nows and thens, when I thought maybe a Sunday would be about doo. It weren’t quite a chapel, but it seemed more solemn like; and then, says you, Ben Gunn was short-handed—no chapling, nor so much as a Bible and a flag, you says.’

So he kept talking as I ran, neither expecting nor receiving any answer.

The cannon-shot was followed after a considerable interval by a volley of small arms.

*Treasure Island*

Another pause, and then, not a quarter of a mile in front of me, I beheld the Union Jack flutter in the air above a wood.

## PART FOUR

### The Stockade

## 16

### **Narrative Continued by the Doctor: How the Ship Was Abandoned**

IT was about half past one—three bells in the sea phrase—that the two boats went ashore from the HISPANIOLA. The captain, the squire, and I were talking matters over in the cabin. Had there been a breath of wind, we should have fallen on the six mutineers who were left aboard with us, slipped our cable, and away to sea. But the wind was wanting; and to complete our helplessness, down came Hunter with the news that Jim Hawkins had slipped into a boat and was gone ashore with the rest.

It never occurred to us to doubt Jim Hawkins, but we were alarmed for his safety. With the men in the temper they were in, it seemed an even chance if we should see the lad again. We ran on deck. The pitch was bubbling in the seams; the nasty stench of the place turned me sick; if ever a man smelt fever and dysentery, it was in that abominable anchorage. The six scoundrels were sitting grumbling under a sail in the forecastle; ashore we could see the gigs made fast and a man sitting in each, hard by

where the river runs in. One of them was whistling ‘Lillibullero.’

Waiting was a strain, and it was decided that Hunter and I should go ashore with the jolly-boat in quest of information.

The gigs had leaned to their right, but Hunter and I pulled straight in, in the direction of the stockade upon the chart. The two who were left guarding their boats seemed in a bustle at our appearance; ‘Lillibullero’ stopped off, and I could see the pair discussing what they ought to do. Had they gone and told Silver, all might have turned out differently; but they had their orders, I suppose, and decided to sit quietly where they were and hark back again to ‘Lillibullero.’

There was a slight bend in the coast, and I steered so as to put it between us; even before we landed we had thus lost sight of the gigs. I jumped out and came as near running as I durst, with a big silk handkerchief under my hat for coolness’ sake and a brace of pistols ready primed for safety.

I had not gone a hundred yards when I reached the stockade.

This was how it was: a spring of clear water rose almost at the top of a knoll. Well, on the knoll, and

enclosing the spring, they had clapped a stout log-house fit to hold two score of people on a pinch and loopholed for musketry on either side. All round this they had cleared a wide space, and then the thing was completed by a palisade six feet high, without door or opening, too strong to pull down without time and labour and too open to shelter the besiegers. The people in the log-house had them in every way; they stood quiet in shelter and shot the others like partridges. All they wanted was a good watch and food; for, short of a complete surprise, they might have held the place against a regiment.

What particularly took my fancy was the spring. For though we had a good enough place of it in the cabin of the HISPANIOLA, with plenty of arms and ammunition, and things to eat, and excellent wines, there had been one thing overlooked—we had no water. I was thinking this over when there came ringing over the island the cry of a man at the point of death. I was not new to violent death—I have served his Royal Highness the Duke of Cumberland, and got a wound myself at Fontenoy—but I know my pulse went dot and carry one. ‘Jim Hawkins is gone,’ was my first thought.

It is something to have been an old soldier, but more still to have been a doctor. There is no time to dilly-dally

in our work. And so now I made up my mind instantly, and with no time lost returned to the shore and jumped on board the jolly-boat.

By good fortune Hunter pulled a good oar. We made the water fly, and the boat was soon alongside and I aboard the schooner.

I found them all shaken, as was natural. The squire was sitting down, as white as a sheet, thinking of the harm he had led us to, the good soul! And one of the six forecastle hands was little better.

‘There’s a man,’ says Captain Smollett, nodding towards him, ‘new to this work. He came nigh-hand fainting, doctor, when he heard the cry. Another touch of the rudder and that man would join us.’

I told my plan to the captain, and between us we settled on the details of its accomplishment.

We put old Redruth in the gallery between the cabin and the forecastle, with three or four loaded muskets and a mattress for protection. Hunter brought the boat round under the stern-port, and Joyce and I set to work loading her with powder tins, muskets, bags of biscuits, kegs of pork, a cask of cognac, and my invaluable medicine chest.

In the meantime, the squire and the captain stayed on deck, and the latter hailed the coxswain, who was the principal man aboard.

‘Mr. Hands,’ he said, ‘here are two of us with a brace of pistols each. If any one of you six make a signal of any description, that man’s dead.’

They were a good deal taken aback, and after a little consultation one and all tumbled down the fore companion, thinking no doubt to take us on the rear. But when they saw Redruth waiting for them in the sparred galley, they went about ship at once, and a head popped out again on deck.

‘Down, dog!’ cries the captain.

And the head popped back again; and we heard no more, for the time, of these six very faint-hearted seamen.

By this time, tumbling things in as they came, we had the jolly-boat loaded as much as we dared. Joyce and I got out through the stern-port, and we made for shore again as fast as oars could take us.

This second trip fairly aroused the watchers along shore. ‘Lillibullero’ was dropped again; and just before we lost sight of them behind the little point, one of them whipped ashore and disappeared. I had half a mind to change my plan and destroy their boats, but I feared that

Silver and the others might be close at hand, and all might very well be lost by trying for too much.

We had soon touched land in the same place as before and set to provision the block house. All three made the first journey, heavily laden, and tossed our stores over the palisade. Then, leaving Joyce to guard them—one man, to be sure, but with half a dozen muskets—Hunter and I returned to the jolly-boat and loaded ourselves once more. So we proceeded without pausing to take breath, till the whole cargo was bestowed, when the two servants took up their position in the block house, and I, with all my power, sculled back to the HISPANIOLA.

That we should have risked a second boat load seems more daring than it really was. They had the advantage of numbers, of course, but we had the advantage of arms. Not one of the men ashore had a musket, and before they could get within range for pistol shooting, we flattered ourselves we should be able to give a good account of a half-dozen at least.

The squire was waiting for me at the stern window, all his faintness gone from him. He caught the painter and made it fast, and we fell to loading the boat for our very lives. Pork, powder, and biscuit was the cargo, with only a musket and a cutlass apiece for the squire and me and

Redruth and the captain. The rest of the arms and powder we dropped overboard in two fathoms and a half of water, so that we could see the bright steel shining far below us in the sun, on the clean, sandy bottom.

By this time the tide was beginning to ebb, and the ship was swinging round to her anchor. Voices were heard faintly hallooing in the direction of the two gigs; and though this reassured us for Joyce and Hunter, who were well to the eastward, it warned our party to be off.

Redruth retreated from his place in the gallery and dropped into the boat, which we then brought round to the ship's counter, to be handier for Captain Smollett.

'Now, men,' said he, 'do you hear me?'

There was no answer from the forecastle.

'It's to you, Abraham Gray—it's to you I am speaking.'

Still no reply.

'Gray,' resumed Mr. Smollett, a little louder, 'I am leaving this ship, and I order you to follow your captain. I know you are a good man at bottom, and I dare say not one of the lot of you's as bad as he makes out. I have my watch here in my hand; I give you thirty seconds to join me in.'

There was a pause.

‘Come, my fine fellow,’ continued the captain; ‘don’t hang so long in stays. I’m risking my life and the lives of these good gentlemen every second.’

There was a sudden scuffle, a sound of blows, and out burst Abraham Gray with a knife cut on the side of the cheek, and came running to the captain like a dog to the whistle.

‘I’m with you, sir,’ said he.

And the next moment he and the captain had dropped aboard of us, and we had shoved off and given way.

We were clear out of the ship, but not yet ashore in our stockade.

## **Narrative Continued by the Doctor: The Jolly-boat's Last Trip**

THIS fifth trip was quite different from any of the others. In the first place, the little gallipot of a boat that we were in was gravely overloaded. Five grown men, and three of them—Trelawney, Redruth, and the captain—over six feet high, was already more than she was meant to carry. Add to that the powder, pork, and bread-bags. The gunwale was lipping astern. Several times we shipped a little water, and my breeches and the tails of my coat were all soaking wet before we had gone a hundred yards.

The captain made us trim the boat, and we got her to lie a little more evenly. All the same, we were afraid to breathe.

In the second place, the ebb was now making—a strong rippling current running westward through the basin, and then south'ard and seaward down the straits by which we had entered in the morning. Even the ripples were a danger to our overloaded craft, but the worst of it

was that we were swept out of our true course and away from our proper landing-place behind the point. If we let the current have its way we should come ashore beside the gigs, where the pirates might appear at any moment.

‘I cannot keep her head for the stockade, sir,’ said I to the captain. I was steering, while he and Redruth, two fresh men, were at the oars. ‘The tide keeps washing her down. Could you pull a little stronger?’

‘Not without swamping the boat,’ said he. ‘You must bear up, sir, if you please—bear up until you see you’re gaining.’

I tried and found by experiment that the tide kept sweeping us westward until I had laid her head due east, or just about right angles to the way we ought to go.

‘We’ll never get ashore at this rate,’ said I.

‘If it’s the only course that we can lie, sir, we must even lie it,’ returned the captain. ‘We must keep upstream. You see, sir,’ he went on, ‘if once we dropped to leeward of the landing-place, it’s hard to say where we should get ashore, besides the chance of being boarded by the gigs; whereas, the way we go the current must slacken, and then we can dodge back along the shore.’

## Treasure Island

‘The current’s less a’ready, sir,’ said the man Gray, who was sitting in the fore-sheets; ‘you can ease her off a bit.’

‘Thank you, my man,’ said I, quite as if nothing had happened, for we had all quietly made up our minds to treat him like one of ourselves.

Suddenly the captain spoke up again, and I thought his voice was a little changed.

‘The gun!’ said he.

‘I have thought of that,’ said I, for I made sure he was thinking of a bombardment of the fort. ‘They could never get the gun ashore, and if they did, they could never haul it through the woods.’

‘Look astern, doctor,’ replied the captain.

We had entirely forgotten the long nine; and there, to our horror, were the five rogues busy about her, getting off her jacket, as they called the stout tarpaulin cover under which she sailed. Not only that, but it flashed into my mind at the same moment that the round-shot and the powder for the gun had been left behind, and a stroke with an axe would put it all into the possession of the evil ones abroad.

‘Israel was Flint’s gunner,’ said Gray hoarsely.

At any risk, we put the boat's head direct for the landing-place. By this time we had got so far out of the run of the current that we kept steerage way even at our necessarily gentle rate of rowing, and I could keep her steady for the goal. But the worst of it was that with the course I now held we turned our broadside instead of our stern to the HISPANIOLA and offered a target like a barn door.

I could hear as well as see that brandy-faced rascal Israel Hands plumping down a round-shot on the deck.

'Who's the best shot?' asked the captain.

'Mr. Trelawney, out and away,' said I.

'Mr. Trelawney, will you please pick me off one of these men, sir? Hands, if possible,' said the captain.

Trelawney was as cool as steel. He looked to the priming of his gun.

'Now,' cried the captain, 'easy with that gun, sir, or you'll swamp the boat. All hands stand by to trim her when he aims.'

The squire raised his gun, the rowing ceased, and we leaned over to the other side to keep the balance, and all was so nicely contrived that we did not ship a drop.

They had the gun, by this time, slewed round upon the swivel, and Hands, who was at the muzzle with the

rammer, was in consequence the most exposed. However, we had no luck, for just as Trelawney fired, down he stooped, the ball whistled over him, and it was one of the other four who fell.

The cry he gave was echoed not only by his companions on board but by a great number of voices from the shore, and looking in that direction I saw the other pirates trooping out from among the trees and tumbling into their places in the boats.

‘Here come the gigs, sir,’ said I.

‘Give way, then,’ cried the captain. ‘We mustn’t mind if we swamp her now. If we can’t get ashore, all’s up.’

‘Only one of the gigs is being manned, sir,’ I added; ‘the crew of the other most likely going round by shore to cut us off.’

‘They’ll have a hot run, sir,’ returned the captain. ‘Jack ashore, you know. It’s not them I mind; it’s the round-shot. Carpet bowls! My lady’s maid couldn’t miss. Tell us, squire, when you see the match, and we’ll hold water.’

In the meanwhile we had been making headway at a good pace for a boat so overloaded, and we had shipped but little water in the process. We were now close in; thirty or forty strokes and we should beach her, for the ebb had already disclosed a narrow belt of sand below the

clustering trees. The gig was no longer to be feared; the little point had already concealed it from our eyes. The ebb-tide, which had so cruelly delayed us, was now making reparation and delaying our assailants. The one source of danger was the gun.

‘If I durst,’ said the captain, ‘I’d stop and pick off another man.’

But it was plain that they meant nothing should delay their shot. They had never so much as looked at their fallen comrade, though he was not dead, and I could see him trying to crawl away.

‘Ready!’ cried the squire.

‘Hold!’ cried the captain, quick as an echo.

And he and Redruth backed with a great heave that sent her stern bodily under water. The report fell in at the same instant of time. This was the first that Jim heard, the sound of the squire’s shot not having reached him. Where the ball passed, not one of us precisely knew, but I fancy it must have been over our heads and that the wind of it may have contributed to our disaster.

At any rate, the boat sank by the stern, quite gently, in three feet of water, leaving the captain and myself, facing each other, on our feet. The other three took complete headers, and came up again drenched and bubbling.

So far there was no great harm. No lives were lost, and we could wade ashore in safety. But there were all our stores at the bottom, and to make things worse, only two guns out of five remained in a state for service. Mine I had snatched from my knees and held over my head, by a sort of instinct. As for the captain, he had carried his over his shoulder by a bandoleer, and like a wise man, lock uppermost. The other three had gone down with the boat.

To add to our concern, we heard voices already drawing near us in the woods along shore, and we had not only the danger of being cut off from the stockade in our half-crippled state but the fear before us whether, if Hunter and Joyce were attacked by half a dozen, they would have the sense and conduct to stand firm. Hunter was steady, that we knew; Joyce was a doubtful case—a pleasant, polite man for a valet and to brush one's clothes, but not entirely fitted for a man of war.

With all this in our minds, we waded ashore as fast as we could, leaving behind us the poor jolly-boat and a good half of all our powder and provisions.

## 18

### Narrative Continued by the Doctor: End of the First Day's Fighting

WE made our best speed across the strip of wood that now divided us from the stockade, and at every step we took the voices of the buccaneers rang nearer. Soon we could hear their footfalls as they ran and the cracking of the branches as they breasted across a bit of thicket.

I began to see we should have a brush for it in earnest and looked to my priming.

'Captain,' said I, 'Trelawney is the dead shot. Give him your gun; his own is useless.'

They exchanged guns, and Trelawney, silent and cool as he had been since the beginning of the bustle, hung a moment on his heel to see that all was fit for service. At the same time, observing Gray to be unarmed, I handed him my cutlass. It did all our hearts good to see him spit in his hand, knit his brows, and make the blade sing through the air. It was plain from every line of his body that our new hand was worth his salt.

Forty paces farther we came to the edge of the wood and saw the stockade in front of us. We struck the enclosure about the middle of the south side, and almost at the same time, seven mutineers—Job Anderson, the boatswain, at their head—appeared in full cry at the southwestern corner.

They paused as if taken aback, and before they recovered, not only the squire and I, but Hunter and Joyce from the block house, had time to fire. The four shots came in rather a scattering volley, but they did the business: one of the enemy actually fell, and the rest, without hesitation, turned and plunged into the trees.

After reloading, we walked down the outside of the palisade to see to the fallen enemy. He was stone dead—shot through the heart.

We began to rejoice over our good success when just at that moment a pistol cracked in the bush, a ball whistled close past my ear, and poor Tom Redruth stumbled and fell his length on the ground. Both the squire and I returned the shot, but as we had nothing to aim at, it is probable we only wasted powder. Then we reloaded and turned our attention to poor Tom.

The captain and Gray were already examining him, and I saw with half an eye that all was over.

I believe the readiness of our return volley had scattered the mutineers once more, for we were suffered without further molestation to get the poor old gamekeeper hoisted over the stockade and carried, groaning and bleeding, into the log-house.

Poor old fellow, he had not uttered one word of surprise, complaint, fear, or even acquiescence from the very beginning of our troubles till now, when we had laid him down in the log-house to die. He had lain like a Trojan behind his mattress in the gallery; he had followed every order silently, doggedly, and well; he was the oldest of our party by a score of years; and now, sullen, old, serviceable servant, it was he that was to die.

The squire dropped down beside him on his knees and kissed his hand, crying like a child.

‘Be I going, doctor?’ he asked.

‘Tom, my man,’ said I, ‘you’re going home.’

‘I wish I had had a lick at them with the gun first,’ he replied.

‘Tom,’ said the squire, ‘say you forgive me, won’t you?’

‘Would that be respectful like, from me to you, squire?’ was the answer. ‘Howsoever, so be it, amen!’

After a little while of silence, he said he thought somebody might read a prayer. ‘It’s the custom, sir,’ he added apologetically. And not long after, without another word, he passed away.

In the meantime the captain, whom I had observed to be wonderfully swollen about the chest and pockets, had turned out a great many various stores—the British colours, a Bible, a coil of stoutish rope, pen, ink, the log-book, and pounds of tobacco. He had found a longish fir-tree lying felled and trimmed in the enclosure, and with the help of Hunter he had set it up at the corner of the log-house where the trunks crossed and made an angle. Then, climbing on the roof, he had with his own hand bent and run up the colours.

This seemed mightily to relieve him. He re-entered the log-house and set about counting up the stores as if nothing else existed. But he had an eye on Tom’s passage for all that, and as soon as all was over, came forward with another flag and reverently spread it on the body.

‘Don’t you take on, sir,’ he said, shaking the squire’s hand. ‘All’s well with him; no fear for a hand that’s been shot down in his duty to captain and owner. It mayn’t be good divinity, but it’s a fact.’

Then he pulled me aside.

‘Dr. Livesey,’ he said, ‘in how many weeks do you and squire expect the consort?’

I told him it was a question not of weeks but of months, that if we were not back by the end of August Blandly was to send to find us, but neither sooner nor later. ‘You can calculate for yourself,’ I said.

‘Why, yes,’ returned the captain, scratching his head; ‘and making a large allowance, sir, for all the gifts of Providence, I should say we were pretty close hauled.’

‘How do you mean?’ I asked.

‘It’s a pity, sir, we lost that second load. That’s what I mean,’ replied the captain. ‘As for powder and shot, we’ll do. But the rations are short, very short— so short, Dr. Livesey, that we’re perhaps as well without that extra mouth.’

And he pointed to the dead body under the flag.

Just then, with a roar and a whistle, a round-shot passed high above the roof of the log-house and plumped far beyond us in the wood.

‘Oho!’ said the captain. ‘Blaze away! You’ve little enough powder already, my lads.’

At the second trial, the aim was better, and the ball descended inside the stockade, scattering a cloud of sand but doing no further damage.

‘Captain,’ said the squire, ‘the house is quite invisible from the ship. It must be the flag they are aiming at. Would it not be wiser to take it in?’

‘Strike my colours!’ cried the captain. ‘No, sir, not I’; and as soon as he had said the words, I think we all agreed with him. For it was not only a piece of stout, seamanly, good feeling; it was good policy besides and showed our enemies that we despised their cannonade.

All through the evening they kept thundering away. Ball after ball flew over or fell short or kicked up the sand in the enclosure, but they had to fire so high that the shot fell dead and buried itself in the soft sand. We had no ricochet to fear, and though one popped in through the roof of the log-house and out again through the floor, we soon got used to that sort of horse-play and minded it no more than cricket.

‘There is one good thing about all this,’ observed the captain; ‘the wood in front of us is likely clear. The ebb has made a good while; our stores should be uncovered. Volunteers to go and bring in pork.

Gray and hunter were the first to come forward. Well armed, they stole out of the stockade, but it proved a useless mission. The mutineers were bolder than we fancied or they put more trust in Israel’s gunnery. For

four or five of them were busy carrying off our stores and wading out with them to one of the gigs that lay close by, pulling an oar or so to hold her steady against the current. Silver was in the stern-sheets in command; and every man of them was now provided with a musket from some secret magazine of their own.

The captain sat down to his log, and here is the beginning of the entry:

Alexander Smollett, master; David Livesey, ship's doctor; Abraham Gray, carpenter's mate; John Trelawney, owner; John Hunter and Richard Joyce, owner's servants, landsmen—being all that is left faithful of the ship's company—with stores for ten days at short rations, came ashore this day and flew British colours on the log-house in Treasure Island. Thomas Redruth, owner's servant, landsman, shot by the mutineers; James Hawkins, cabin-boy—

And at the same time, I was wondering over poor Jim Hawkins' fate.

A hail on the land side.

'Somebody hailing us,' said Hunter, who was on guard.

'Doctor! Squire! Captain! Hullo, Hunter, is that you?' came the cries.

*Treasure Island*

And I ran to the door in time to see Jim Hawkins, safe and sound, come climbing over the stockade.

## Narrative Resumed by Jim Hawkins: The Garrison in the Stockade

AS soon as Ben Gunn saw the colours he came to a halt, stopped me by the arm, and sat down.

‘Now,’ said he, ‘there’s your friends, sure enough.’

‘Far more likely it’s the mutineers,’ I answered.

‘That!’ he cried. ‘Why, in a place like this, where nobody puts in but gen’lemen of fortune, Silver would fly the Jolly Roger, you don’t make no doubt of that. No, that’s your friends. There’s been blows too, and I reckon your friends has had the best of it; and here they are ashore in the old stockade, as was made years and years ago by Flint. Ah, he was the man to have a headpiece, was Flint! Barring rum, his match were never seen. He were afraid of none, not he; on’y Silver—Silver was that genteel.’

‘Well,’ said I, ‘that may be so, and so be it; all the more reason that I should hurry on and join my friends.’

‘Nay, mate,’ returned Ben, ‘not you. You’re a good boy, or I’m mistook; but you’re on’y a boy, all told. Now,

Ben Gunn is fly. Rum wouldn't bring me there, where you're going—not rum wouldn't, till I see your born gen'leman and gets it on his word of honour. And you won't forget my words; 'A precious sight (that's what you'll say), a precious sight more confidence'— and then nips him.

And he pinched me the third time with the same air of cleverness.

'And when Ben Gunn is wanted, you know where to find him, Jim. Just wheer you found him today. And him that comes is to have a white thing in his hand, and he's to come alone. Oh! And you'll say this: 'Ben Gunn,' says you, 'has reasons of his own.'

'Well,' said I, 'I believe I understand. You have something to propose, and you wish to see the squire or the doctor, and you're to be found where I found you. Is that all?'

'And when? says you,' he added. 'Why, from about noon observation to about six bells.'

'Good,' said I, 'and now may I go?'

'You won't forget?' he inquired anxiously. 'Precious sight, and reasons of his own, says you. Reasons of his own; that's the mainstay; as between man and man. Well, then'—still holding me—'I reckon you can go, Jim. And,

Jim, if you was to see Silver, you wouldn't go for to sell Ben Gunn? Wild horses wouldn't draw it from you? No, says you. And if them pirates camp ashore, Jim, what would you say but there'd be widders in the morning?"

Here he was interrupted by a loud report, and a cannonball came tearing through the trees and pitched in the sand not a hundred yards from where we two were talking. The next moment each of us had taken to his heels in a different direction.

For a good hour to come frequent reports shook the island, and balls kept crashing through the woods. I moved from hiding-place to hiding-place, always pursued, or so it seemed to me, by these terrifying missiles. But towards the end of the bombardment, though still I durst not venture in the direction of the stockade, where the balls fell oftenest, I had begun, in a manner, to pluck up my heart again, and after a long detour to the east, crept down among the shore-side trees.

The sun had just set, the sea breeze was rustling and tumbling in the woods and ruffling the grey surface of the anchorage; the tide, too, was far out, and great tracts of sand lay uncovered; the air, after the heat of the day, chilled me through my jacket.

The HISPANIOLA still lay where she had anchored; but, sure enough, there was the Jolly Roger—the black flag of piracy —flying from her peak. Even as I looked, there came another red flash and another report that sent the echoes clattering, and one more round-shot whistled through the air. It was the last of the cannonade.

I lay for some time watching the bustle which succeeded the attack. Men were demolishing something with axes on the beach near the stockade—the poor jolly-boat, I afterwards discovered. Away, near the mouth of the river, a great fire was glowing among the trees, and between that point and the ship one of the gigs kept coming and going, the men, whom I had seen so gloomy, shouting at the oars like children. But there was a sound in their voices which suggested rum.

At length I thought I might return towards the stockade. I was pretty far down on the low, sandy spit that encloses the anchorage to the east, and is joined at half-water to Skeleton Island; and now, as I rose to my feet, I saw, some distance further down the spit and rising from among low bushes, an isolated rock, pretty high, and peculiarly white in colour. It occurred to me that this might be the white rock of which Ben Gunn had spoken

and that some day or other a boat might be wanted and I should know where to look for one.

Then I skirted among the woods until I had regained the rear, or shoreward side, of the stockade, and was soon warmly welcomed by the faithful party.

I had soon told my story and began to look about me. The log-house was made of unsquared trunks of pine—roof, walls, and floor. The latter stood in several places as much as a foot or a foot and a half above the surface of the sand. There was a porch at the door, and under this porch the little spring welled up into an artificial basin of a rather odd kind—no other than a great ship's kettle of iron, with the bottom knocked out, and sunk ‘to her bearings,’ as the captain said, among the sand.

Little had been left besides the framework of the house, but in one corner there was a stone slab laid down by way of hearth and an old rusty iron basket to contain the fire.

The slopes of the knoll and all the inside of the stockade had been cleared of timber to build the house, and we could see by the stumps what a fine and lofty grove had been destroyed. Most of the soil had been washed away or buried in drift after the removal of the trees; only where the streamlet ran down from the kettle a

thick bed of moss and some ferns and little creeping bushes were still green among the sand. Very close around the stockade—too close for defence, they said—the wood still flourished high and dense, all of fir on the land side, but towards the sea with a large admixture of live-oaks.

The cold evening breeze, of which I have spoken, whistled through every chink of the rude building and sprinkled the floor with a continual rain of fine sand. There was sand in our eyes, sand in our teeth, sand in our suppers, sand dancing in the spring at the bottom of the kettle, for all the world like porridge beginning to boil. Our chimney was a square hole in the roof; it was but a little part of the smoke that found its way out, and the rest eddied about the house and kept us coughing and piping the eye.

Add to this that Gray, the new man, had his face tied up in a bandage for a cut he had got in breaking away from the mutineers and that poor old Tom Redruth, still unburied, lay along the wall, stiff and stark, under the Union Jack.

If we had been allowed to sit idle, we should all have fallen in the blues, but Captain Smollett was never the man for that. All hands were called up before him, and he

divided us into watches. The doctor and Gray and I for one; the squire, Hunter, and Joyce upon the other. Tired though we all were, two were sent out for firewood; two more were set to dig a grave for Redruth; the doctor was named cook; I was put sentry at the door; and the captain himself went from one to another, keeping up our spirits and lending a hand wherever it was wanted.

From time to time the doctor came to the door for a little air and to rest his eyes, which were almost smoked out of his head, and whenever he did so, he had a word for me.

‘That man Smollett,’ he said once, ‘is a better man than I am. And when I say that it means a deal, Jim.’

Another time he came and was silent for a while. Then he put his head on one side, and looked at me.

‘Is this Ben Gunn a man?’ he asked.

‘I do not know, sir,’ said I. ‘I am not very sure whether he’s sane.’

‘If there’s any doubt about the matter, he is,’ returned the doctor. ‘A man who has been three years biting his nails on a desert island, Jim, can’t expect to appear as sane as you or me. It doesn’t lie in human nature. Was it cheese you said he had a fancy for?’

‘Yes, sir, cheese,’ I answered.

‘Well, Jim,’ says he, ‘just see the good that comes of being dainty in your food. You’ve seen my snuff-box, haven’t you? And you never saw me take snuff, the reason being that in my snuff-box I carry a piece of Parmesan cheese—a cheese made in Italy, very nutritious. Well, that’s for Ben Gunn!’

Before supper was eaten we buried old Tom in the sand and stood round him for a while bare-headed in the breeze. A good deal of firewood had been got in, but not enough for the captain’s fancy, and he shook his head over it and told us we ‘must get back to this tomorrow rather livelier.’ Then, when we had eaten our pork and each had a good stiff glass of brandy grog, the three chiefs got together in a corner to discuss our prospects.

It appears they were at their wits’ end what to do, the stores being so low that we must have been starved into surrender long before help came. But our best hope, it was decided, was to kill off the buccaneers until they either hauled down their flag or ran away with the HISPANIOLA. From nineteen they were already reduced to fifteen, two others were wounded, and one at least—the man shot beside the gun—severely wounded, if he were not dead. Every time we had a crack at them, we were to take it, saving our own lives, with the extremest

care. And besides that, we had two able allies—rum and the climate.

As for the first, though we were about half a mile away, we could hear them roaring and singing late into the night; and as for the second, the doctor staked his wig that, camped where they were in the marsh and unprovided with remedies, the half of them would be on their backs before a week.

‘So,’ he added, ‘if we are not all shot down first they’ll be glad to be packing in the schooner. It’s always a ship, and they can get to buccaneering again, I suppose.’

‘First ship that ever I lost,’ said Captain Smollett.

I was dead tired, as you may fancy; and when I got to sleep, which was not till after a great deal of tossing, I slept like a log of wood.

The rest had long been up and had already breakfasted and increased the pile of firewood by about half as much again when I was wakened by a bustle and the sound of voices.

‘Flag of truce!’ I heard someone say; and then, immediately after, with a cry of surprise, ‘Silver himself!’

And at that, up I jumped, and rubbing my eyes, ran to a loophole in the wall.

## 20

### Silver's Embassy

SURE enough, there were two men just outside the stockade, one of them waving a white cloth, the other, no less a person than Silver himself, standing placidly by.

It was still quite early, and the coldest morning that I think I ever was abroad in—a chill that pierced into the marrow. The sky was bright and cloudless overhead, and the tops of the trees shone rosily in the sun. But where Silver stood with his lieutenant, all was still in shadow, and they waded knee-deep in a low white vapour that had crawled during the night out of the morass. The chill and the vapour taken together told a poor tale of the island. It was plainly a damp, feverish, unhealthy spot.

'Keep indoors, men,' said the captain. 'Ten to one this is a trick.'

Then he hailed the buccaneer.

'Who goes? Stand, or we fire.'

'Flag of truce,' cried Silver.

The captain was in the porch, keeping himself carefully out of the way of a treacherous shot, should any

be intended. He turned and spoke to us, ‘Doctor’s watch on the lookout. Dr. Livesey take the north side, if you please; Jim, the east; Gray, west. The watch below, all hands to load muskets. Lively, men, and careful.’

And then he turned again to the mutineers.

‘And what do you want with your flag of truce?’ he cried.

This time it was the other man who replied.

‘Cap’n Silver, sir, to come on board and make terms,’ he shouted.

‘Cap’n Silver! Don’t know him. Who’s he?’ cried the captain. And we could hear him adding to himself, ‘Cap’n, is it? My heart, and here’s promotion!’

Long John answered for himself. ‘Me, sir. These poor lads have chosen me cap’n, after your desertion, sir’— laying a particular emphasis upon the word ‘desertion.’ ‘We’re willing to submit, if we can come to terms, and no bones about it. All I ask is your word, Cap’n Smollett, to let me safe and sound out of this here stockade, and one minute to get out o’ shot before a gun is fired.’

‘My man,’ said Captain Smollett, ‘I have not the slightest desire to talk to you. If you wish to talk to me, you can come, that’s all. If there’s any treachery, it’ll be on your side, and the Lord help you.’

## Treasure Island

‘That’s enough, cap’n,’ shouted Long John cheerily. ‘A word from you’s enough. I know a gentleman, and you may lay to that.’

We could see the man who carried the flag of truce attempting to hold Silver back. Nor was that wonderful, seeing how cavalier had been the captain’s answer. But Silver laughed at him aloud and slapped him on the back as if the idea of alarm had been absurd. Then he advanced to the stockade, threw over his crutch, got a leg up, and with great vigour and skill succeeded in surmounting the fence and dropping safely to the other side.

I will confess that I was far too much taken up with what was going on to be of the slightest use as sentry; indeed, I had already deserted my eastern loophole and crept up behind the captain, who had now seated himself on the threshold, with his elbows on his knees, his head in his hands, and his eyes fixed on the water as it bubbled out of the old iron kettle in the sand. He was whistling ‘Come, Lasses and Lads.’

Silver had terrible hard work getting up the knoll. What with the steepness of the incline, the thick tree stumps, and the soft sand, he and his crutch were as helpless as a ship in stays. But he stuck to it like a man in silence, and at last arrived before the captain, whom he

saluted in the handsomest style. He was tricked out in his best; an immense blue coat, thick with brass buttons, hung as low as to his knees, and a fine laced hat was set on the back of his head.

‘Here you are, my man,’ said the captain, raising his head. ‘You had better sit down.’

‘You ain’t a-going to let me inside, cap’n?’ complained Long John. ‘It’s a main cold morning, to be sure, sir, to sit outside upon the sand.’

‘Why, Silver,’ said the captain, ‘if you had pleased to be an honest man, you might have been sitting in your galley. It’s your own doing. You’re either my ship’s cook—and then you were treated handsome—or Cap’n Silver, a common mutineer and pirate, and then you can go hang!’

‘Well, well, cap’n,’ returned the sea-cook, sitting down as he was bidden on the sand, ‘you’ll have to give me a hand up again, that’s all. A sweet pretty place you have of it here. Ah, there’s Jim! The top of the morning to you, Jim. Doctor, here’s my service. Why, there you all are together like a happy family, in a manner of speaking.’

‘If you have anything to say, my man, better say it,’ said the captain.

‘Right you were, Cap’n Smollett,’ replied Silver. ‘Dooty is dooty, to be sure. Well now, you look here, that was a good lay of yours last night. I don’t deny it was a good lay. Some of you pretty handy with a handspike-end. And I’ll not deny neither but what some of my people was shook—maybe all was shook; maybe I was shook myself; maybe that’s why I’m here for terms. But you mark me, cap’n, it won’t do twice, by thunder! We’ll have to do sentry-go and ease off a point or so on the rum. Maybe you think we were all a sheet in the wind’s eye. But I’ll tell you I was sober; I was on’y dog tired; and if I’d awoke a second sooner, I’d ‘a caught you at the act, I would. He wasn’t dead when I got round to him, not he.’

‘Well?’ says Captain Smollett as cool as can be.

All that Silver said was a riddle to him, but you would never have guessed it from his tone. As for me, I began to have an inkling. Ben Gunn’s last words came back to my mind. I began to suppose that he had paid the buccaneers a visit while they all lay drunk together round their fire, and I reckoned up with glee that we had only fourteen enemies to deal with.

‘Well, here it is,’ said Silver. ‘We want that treasure, and we’ll have it—that’s our point! You would just as

soon save your lives, I reckon; and that's yours. You have a chart, haven't you?"

"That's as may be," replied the captain.

"Oh, well, you have, I know that," returned Long John. "You needn't be so husky with a man; there ain't a particle of service in that, and you may lay to it. What I mean is, we want your chart. Now, I never meant you no harm, myself."

"That won't do with me, my man," interrupted the captain. "We know exactly what you meant to do, and we don't care, for now, you see, you can't do it."

And the captain looked at him calmly and proceeded to fill a pipe.

"If Abe Gray—" Silver broke out.

"Avast there!" cried Mr. Smollett. "Gray told me nothing, and I asked him nothing; and what's more, I would see you and him and this whole island blown clean out of the water into blazes first. So there's my mind for you, my man, on that."

This little whiff of temper seemed to cool Silver down. He had been growing nettled before, but now he pulled himself together.

"Like enough," said he. "I would set no limits to what gentlemen might consider shipshape, or might not, as the

case were. And seein' as how you are about to take a pipe, cap'n, I'll make so free as do likewise.'

And he filled a pipe and lighted it; and the two men sat silently smoking for quite a while, now looking each other in the face, now stopping their tobacco, now leaning forward to spit. It was as good as the play to see them.

'Now,' resumed Silver, 'here it is. You give us the chart to get the treasure by, and drop shooting poor seamen and stoving of their heads in while asleep. You do that, and we'll offer you a choice. Either you come aboard along of us, once the treasure shipped, and then I'll give you my affy-davy, upon my word of honour, to clap you somewhere safe ashore. Or if that ain't to your fancy, some of my hands being rough and having old scores on account of hazing, then you can stay here, you can. We'll divide stores with you, man for man; and I'll give my affy-davy, as before to speak the first ship I sight, and send 'em here to pick you up. Now, you'll own that's talking. Handsomer you couldn't look to get, now you. And I hope'—raising his voice—'that all hands in this here block house will overhaul my words, for what is spoke to one is spoke to all.'

Captain Smollett rose from his seat and knocked out the ashes of his pipe in the palm of his left hand.

‘Is that all?’ he asked.

‘Every last word, by thunder!’ answered John. ‘Refuse that, and you’ve seen the last of me but musket-balls.’

‘Very good,’ said the captain. ‘Now you’ll hear me. If you’ll come up one by one, unarmed, I’ll engage to clap you all in irons and take you home to a fair trial in England. If you won’t, my name is Alexander Smollett, I’ve flown my sovereign’s colours, and I’ll see you all to Davy Jones. You can’t find the treasure. You can’t sail the ship—there’s not a man among you fit to sail the ship. You can’t fight us— Gray, there, got away from five of you. Your ship’s in irons, Master Silver; you’re on a lee shore, and so you’ll find. I stand here and tell you so; and they’re the last good words you’ll get from me, for in the name of heaven, I’ll put a bullet in your back when next I meet you. Tramp, my lad. Bundle out of this, please, hand over hand, and double quick.’

Silver’s face was a picture; his eyes started in his head with wrath. He shook the fire out of his pipe.

‘Give me a hand up!’ he cried.

‘Not I,’ returned the captain.

‘Who’ll give me a hand up?’ he roared.

Not a man among us moved. Growling the foulest imprecations, he crawled along the sand till he got hold of

the porch and could hoist himself again upon his crutch. Then he spat into the spring.

‘There!’ he cried. ‘That’s what I think of ye. Before an hour’s out, I’ll stove in your old block house like a rum puncheon. Laugh, by thunder, laugh! Before an hour’s out, ye’ll laugh upon the other side. Them that die’ll be the lucky ones.’

And with a dreadful oath he stumbled off, ploughed down the sand, was helped across the stockade, after four or five failures, by the man with the flag of truce, and disappeared in an instant afterwards among the trees.

**21**

### The Attack

AS soon as Silver disappeared, the captain, who had been closely watching him, turned towards the interior of the house and found not a man of us at his post but Gray. It was the first time we had ever seen him angry.

‘Quarters!’ he roared. And then, as we all slunk back to our places, ‘Gray,’ he said, ‘I’ll put your name in the log; you’ve stood by your duty like a seaman. Mr. Trelawney, I’m surprised at you, sir. Doctor, I thought you had worn the king’s coat! If that was how you served at Fontenoy, sir, you’d have been better in your berth.’

The doctor’s watch were all back at their loopholes, the rest were busy loading the spare muskets, and everyone with a red face, you may be certain, and a flea in his ear, as the saying is.

The captain looked on for a while in silence. Then he spoke.

‘My lads,’ said he, ‘I’ve given Silver a broadside. I pitched it in red-hot on purpose; and before the hour’s out, as he said, we shall be boarded. We’re outnumbered,

I needn't tell you that, but we fight in shelter; and a minute ago I should have said we fought with discipline. I've no manner of doubt that we can drub them, if you choose.'

Then he went the rounds and saw, as he said, that all was clear.

On the two short sides of the house, east and west, there were only two loopholes; on the south side where the porch was, two again; and on the north side, five. There was a round score of muskets for the seven of us; the firewood had been built into four piles—tables, you might say—one about the middle of each side, and on each of these tables some ammunition and four loaded muskets were laid ready to the hand of the defenders. In the middle, the cutlasses lay ranged.

'Toss out the fire,' said the captain; 'the chill is past, and we mustn't have smoke in our eyes.'

The iron fire-basket was carried bodily out by Mr. Trelawney, and the embers smothered among sand.

'Hawkins hasn't had his breakfast. Hawkins, help yourself, and back to your post to eat it,' continued Captain Smollett. 'Lively, now, my lad; you'll want it before you've done. Hunter, serve out a round of brandy to all hands.'

And while this was going on, the captain completed, in his own mind, the plan of the defence.

‘Doctor, you will take the door,’ he resumed. ‘See, and don’t expose yourself; keep within, and fire through the porch. Hunter, take the east side, there. Joyce, you stand by the west, my man. Mr. Trelawney, you are the best shot—you and Gray will take this long north side, with the five loopholes; it’s there the danger is. If they can get up to it and fire in upon us through our own ports, things would begin to look dirty. Hawkins, neither you nor I are much account at the shooting; we’ll stand by to load and bear a hand.’

As the captain had said, the chill was past. As soon as the sun had climbed above our girdle of trees, it fell with all its force upon the clearing and drank up the vapours at a draught. Soon the sane was baking and the resin melting in the logs of the block house. Jackets and coats were flung aside, shirts thrown open at the neck and rolled up to the shoulders; and we stood there, each at his post, in a fever of heat and anxiety.

An hour passed away.

‘Hang them!’ said the captain. ‘This is as dull as the doldrums. Gray, whistle for a wind.’

And just at that moment came the first news of the attack.

'If you please, sir,' said Joyce, 'if I see anyone, am I to fire?'

'I told you so!' cried the captain.

'Thank you, sir,' returned Joyce with the same quiet civility.

Nothing followed for a time, but the remark had set us all on the alert, straining ears and eyes—the musketeers with their pieces balanced in their hands, the captain out in the middle of the block house with his mouth very tight and a frown on his face.

So some seconds passed, till suddenly Joyce whipped up his musket and fired. The report had scarcely died away ere it was repeated and repeated from without in a scattering volley, shot behind shot, like a string of geese, from every side of the enclosure. Several bullets struck the log-house, but not one entered; and as the smoke cleared away and vanished, the stockade and the woods around it looked as quiet and empty as before. Not a bough waved, not the gleam of a musket-barrel betrayed the presence of our foes.

'Did you hit your man?' asked the captain.

'No, sir,' replied Joyce. 'I believe not, sir.'

‘Next best thing to tell the truth,’ muttered Captain Smollett. ‘Load his gun, Hawkins. How many should say there were on your side, doctor?’

‘I know precisely,’ said Dr. Livesey. ‘Three shots were fired on this side. I saw the three flashes—two close together—one farther to the west.’

‘Three!’ repeated the captain. ‘And how many on yours, Mr. Trelawney?’

But this was not so easily answered. There had come many from the north—seven by the squire’s computation, eight or nine according to Gray. From the east and west only a single shot had been fired. It was plain, therefore, that the attack would be developed from the north and that on the other three sides we were only to be annoyed by a show of hostilities. But Captain Smollett made no change in his arrangements. If the mutineers succeeded in crossing the stockade, he argued, they would take possession of any unprotected loophole and shoot us down like rats in our own stronghold.

Nor had we much time left to us for thought. Suddenly, with a loud huzza, a little cloud of pirates leaped from the woods on the north side and ran straight on the stockade. At the same moment, the fire was once more opened from

## *Treasure Island*

the woods, and a rifle ball sang through the doorway and knocked the doctor's musket into bits.

The boarders swarmed over the fence like monkeys. Squire and Gray fired again and yet again; three men fell, one forwards into the enclosure, two back on the outside. But of these, one was evidently more frightened than hurt, for he was on his feet again in a crack and instantly disappeared among the trees.

Two had bit the dust, one had fled, four had made good their footing inside our defences, while from the shelter of the woods seven or eight men, each evidently supplied with several muskets, kept up a hot though useless fire on the log-house.

The four who had boarded made straight before them for the building, shouting as they ran, and the men among the trees shouted back to encourage them. Several shots were fired, but such was the hurry of the marksmen that not one appears to have taken effect. In a moment, the four pirates had swarmed up the mound and were upon us.

The head of Job Anderson, the boatswain, appeared at the middle loophole.

'At 'em, all hands—all hands!' he roared in a voice of thunder.

At the same moment, another pirate grasped Hunter's musket by the muzzle, wrenched it from his hands, plucked it through the loophole, and with one stunning blow, laid the poor fellow senseless on the floor. Meanwhile a third, running unharmed all around the house, appeared suddenly in the doorway and fell with his cutlass on the doctor.

Our position was utterly reversed. A moment since we were firing, under cover, at an exposed enemy; now it was we who lay uncovered and could not return a blow.

The log-house was full of smoke, to which we owed our comparative safety. Cries and confusion, the flashes and reports of pistol-shots, and one loud groan rang in my ears.

'Out, lads, out, and fight 'em in the open! Cutlasses!' cried the captain.

I snatched a cutlass from the pile, and someone, at the same time snatching another, gave me a cut across the knuckles which I hardly felt. I dashed out of the door into the clear sunlight. Someone was close behind, I knew not whom. Right in front, the doctor was pursuing his assailant down the hill, and just as my eyes fell upon him, beat down his guard and sent him sprawling on his back with a great slash across the face.

‘Round the house, lads! Round the house!’ cried the captain; and even in the hurly-burly, I perceived a change in his voice.

Mechanically, I obeyed, turned eastwards, and with my cutlass raised, ran round the corner of the house. Next moment I was face to face with Anderson. He roared aloud, and his hanger went up above his head, flashing in the sunlight. I had not time to be afraid, but as the blow still hung impending, leaped in a trice upon one side, and missing my foot in the soft sand, rolled headlong down the slope.

When I had first sallied from the door, the other mutineers had been already swarming up the palisade to make an end of us. One man, in a red night-cap, with his cutlass in his mouth, had even got upon the top and thrown a leg across. Well, so short had been the interval that when I found my feet again all was in the same posture, the fellow with the red night-cap still half-way over, another still just showing his head above the top of the stockade. And yet, in this breath of time, the fight was over and the victory was ours.

Gray, following close behind me, had cut down the big boatswain ere he had time to recover from his last blow. Another had been shot at a loophole in the very act of

firing into the house and now lay in agony, the pistol still smoking in his hand. A third, as I had seen, the doctor had disposed of at a blow. Of the four who had scaled the palisade, one only remained unaccounted for, and he, having left his cutlass on the field, was now clambering out again with the fear of death upon him.

‘Fire—fire from the house!’ cried the doctor. ‘And you, lads, back into cover.’

But his words were unheeded, no shot was fired, and the last boarder made good his escape and disappeared with the rest into the wood. In three seconds nothing remained of the attacking party but the five who had fallen, four on the inside and one on the outside of the palisade.

The doctor and Gray and I ran full speed for shelter. The survivors would soon be back where they had left their muskets, and at any moment the fire might recommence.

The house was by this time somewhat cleared of smoke, and we saw at a glance the price we had paid for victory. Hunter lay beside his loophole, stunned; Joyce by his, shot through the head, never to move again; while right in the centre, the squire was supporting the captain, one as pale as the other.

‘The captain’s wounded,’ said Mr. Trelawney.

‘Have they run?’ asked Mr. Smollett.

‘All that could, you may be bound,’ returned the doctor; ‘but there’s five of them will never run again.’

‘Five!’ cried the captain. ‘Come, that’s better. Five against three leaves us four to nine. That’s better odds than we had at starting. We were seven to nineteen then, or thought we were, and that’s as bad to bear.’\*

\*The mutineers were soon only eight in number, for the man shot by Mr. Trelawney on board the schooner died that same evening of his wound. But this was, of course, not known till after by the faithful party.

## PART FIVE

### My Sea Adventure

## How My Sea Adventure Began

THERE was no return of the mutineers—not so much as another shot out of the woods. They had ‘got their rations for that day,’ as the captain put it, and we had the place to ourselves and a quiet time to overhaul the wounded and get dinner. Squire and I cooked outside in spite of the danger, and even outside we could hardly tell what we were at, for horror of the loud groans that reached us from the doctor’s patients.

Out of the eight men who had fallen in the action, only three still breathed—that one of the pirates who had been shot at the loophole, Hunter, and Captain Smollett; and of these, the first two were as good as dead; the mutineer indeed died under the doctor’s knife, and Hunter, do what we could, never recovered consciousness in this world. He lingered all day, breathing loudly like the old buccaneer at home in his apoplectic fit, but the bones of his chest had been crushed by the blow and his skull fractured in falling, and some time in the following night, without sign or sound, he went to his Maker.

As for the captain, his wounds were grievous indeed, but not dangerous. No organ was fatally injured. Anderson's ball—for it was Job that shot him first—had broken his shoulder-blade and touched the lung, not badly; the second had only torn and displaced some muscles in the calf. He was sure to recover, the doctor said, but in the meantime, and for weeks to come, he must not walk nor move his arm, nor so much as speak when he could help it.

My own accidental cut across the knuckles was a flea-bite. Doctor Livesey patched it up with plaster and pulled my ears for me into the bargain.

After dinner the squire and the doctor sat by the captain's side awhile in consultation; and when they had talked to their hearts' content, it being then a little past noon, the doctor took up his hat and pistols, girt on a cutlass, put the chart in his pocket, and with a musket over his shoulder crossed the palisade on the north side and set off briskly through the trees.

Gray and I were sitting together at the far end of the block house, to be out of earshot of our officers consulting; and Gray took his pipe out of his mouth and fairly forgot to put it back again, so thunder-struck he was at this occurrence.

‘Why, in the name of Davy Jones,’ said he, ‘is Dr. Livesey mad?’

‘Why no,’ says I. ‘He’s about the last of this crew for that, I take it.’

‘Well, shipmate,’ said Gray, ‘mad he may not be; but if HE’S not, you mark my words, I am.’

‘I take it,’ replied I, ‘the doctor has his idea; and if I am right, he’s going now to see Ben Gunn.’

I was right, as appeared later; but in the meantime, the house being stifling hot and the little patch of sand inside the palisade ablaze with midday sun, I began to get another thought into my head, which was not by any means so right. What I began to do was to envy the doctor walking in the cool shadow of the woods with the birds about him and the pleasant smell of the pines, while I sat grilling, with my clothes stuck to the hot resin, and so much blood about me and so many poor dead bodies lying all around that I took a disgust of the place that was almost as strong as fear.

All the time I was washing out the block house, and then washing up the things from dinner, this disgust and envy kept growing stronger and stronger, till at last, being near a bread-bag, and no one then observing me, I took

the first step towards my escapade and filled both pockets of my coat with biscuit.

I was a fool, if you like, and certainly I was going to do a foolish, over-bold act; but I was determined to do it with all the precautions in my power. These biscuits, should anything befall me, would keep me, at least, from starving till far on in the next day.

The next thing I laid hold of was a brace of pistols, and as I already had a powder-horn and bullets, I felt myself well supplied with arms.

As for the scheme I had in my head, it was not a bad one in itself. I was to go down the sandy spit that divides the anchorage on the east from the open sea, find the white rock I had observed last evening, and ascertain whether it was there or not that Ben Gunn had hidden his boat, a thing quite worth doing, as I still believe. But as I was certain I should not be allowed to leave the enclosure, my only plan was to take French leave and slip out when nobody was watching, and that was so bad a way of doing it as made the thing itself wrong. But I was only a boy, and I had made my mind up.

Well, as things at last fell out, I found an admirable opportunity. The squire and Gray were busy helping the captain with his bandages, the coast was clear, I made a

bolt for it over the stockade and into the thickest of the trees, and before my absence was observed I was out of cry of my companions.

This was my second folly, far worse than the first, as I left but two sound men to guard the house; but like the first, it was a help towards saving all of us.

I took my way straight for the east coast of the island, for I was determined to go down the sea side of the spit to avoid all chance of observation from the anchorage. It was already late in the afternoon, although still warm and sunny. As I continued to thread the tall woods, I could hear from far before me not only the continuous thunder of the surf, but a certain tossing of foliage and grinding of boughs which showed me the sea breeze had set in higher than usual. Soon cool draughts of air began to reach me, and a few steps farther I came forth into the open borders of the grove, and saw the sea lying blue and sunny to the horizon and the surf tumbling and tossing its foam along the beach.

I have never seen the sea quiet round Treasure Island. The sun might blaze overhead, the air be without a breath, the surface smooth and blue, but still these great rollers would be running along all the external coast, thundering and thundering by day and night; and I scarce believe

there is one spot in the island where a man would be out of earshot of their noise.

I walked along beside the surf with great enjoyment, till, thinking I was now got far enough to the south, I took the cover of some thick bushes and crept warily up to the ridge of the spit.

Behind me was the sea, in front the anchorage. The sea breeze, as though it had the sooner blown itself out by its unusual violence, was already at an end; it had been succeeded by light, variable airs from the south and south-east, carrying great banks of fog; and the anchorage, under lee of Skeleton Island, lay still and leaden as when first we entered it. The HISPANIOLA, in that unbroken mirror, was exactly portrayed from the truck to the waterline, the Jolly Roger hanging from her peak.

Alongside lay one of the gigs, Silver in the stern-sheets—him I could always recognize—while a couple of men were leaning over the stern bulwarks, one of them with a red cap—the very rogue that I had seen some hours before stride-legs upon the palisade. Apparently they were talking and laughing, though at that distance—upwards of a mile—I could, of course, hear no word of what was said. All at once there began the most horrid, unearthly screaming, which at first startled me badly, though I had

## *Treasure Island*

soon remembered the voice of Captain Flint and even thought I could make out the bird by her bright plumage as she sat perched upon her master's wrist.

Soon after, the jolly-boat shoved off and pulled for shore, and the man with the red cap and his comrade went below by the cabin companion.

Just about the same time, the sun had gone down behind the Spy-glass, and as the fog was collecting rapidly, it began to grow dark in earnest. I saw I must lose no time if I were to find the boat that evening.

The white rock, visible enough above the brush, was still some eighth of a mile further down the spit, and it took me a goodish while to get up with it, crawling, often on all fours, among the scrub. Night had almost come when I laid my hand on its rough sides. Right below it there was an exceedingly small hollow of green turf, hidden by banks and a thick underwood about knee-deep, that grew there very plentifully; and in the centre of the dell, sure enough, a little tent of goat-skins, like what the gipsies carry about with them in England.

I dropped into the hollow, lifted the side of the tent, and there was Ben Gunn's boat—home-made if ever anything was home-made; a rude, lop-sided framework of tough wood, and stretched upon that a covering of goat-

skin, with the hair inside. The thing was extremely small, even for me, and I can hardly imagine that it could have floated with a full-sized man. There was one thwart set as low as possible, a kind of stretcher in the bows, and a double paddle for propulsion.

I had not then seen a coracle, such as the ancient Britons made, but I have seen one since, and I can give you no fairer idea of Ben Gunn's boat than by saying it was like the first and the worst coracle ever made by man. But the great advantage of the coracle it certainly possessed, for it was exceedingly light and portable.

Well, now that I had found the boat, you would have thought I had had enough of truancy for once, but in the meantime I had taken another notion and become so obstinately fond of it that I would have carried it out, I believe, in the teeth of Captain Smollett himself. This was to slip out under cover of the night, cut the HISPANIOLA adrift, and let her go ashore where she fancied. I had quite made up my mind that the mutineers, after their repulse of the morning, had nothing nearer their hearts than to up anchor and away to sea; this, I thought, it would be a fine thing to prevent, and now that I had seen how they left their watchmen unprovided with a boat, I thought it might be done with little risk.

Down I sat to wait for darkness, and made a hearty meal of biscuit. It was a night out of ten thousand for my purpose. The fog had now buried all heaven. As the last rays of daylight dwindled and disappeared, absolute blackness settled down on Treasure Island. And when, at last, I shouldered the coracle and groped my way stumblingly out of the hollow where I had supped, there were but two points visible on the whole anchorage.

One was the great fire on shore, by which the defeated pirates lay carousing in the swamp. The other, a mere blur of light upon the darkness, indicated the position of the anchored ship. She had swung round to the ebb—her bow was now towards me—the only lights on board were in the cabin, and what I saw was merely a reflection on the fog of the strong rays that flowed from the stern window.

The ebb had already run some time, and I had to wade through a long belt of swampy sand, where I sank several times above the ankle, before I came to the edge of the retreating water, and wading a little way in, with some strength and dexterity, set my coracle, keel downwards, on the surface.

## The Ebb-tide Runs

THE coracle—as I had ample reason to know before I was done with her—was a very safe boat for a person of my height and weight, both buoyant and clever in a sea-way; but she was the most cross-grained, lop-sided craft to manage. Do as you pleased, she always made more leeway than anything else, and turning round and round was the manoeuvre she was best at. Even Ben Gunn himself has admitted that she was ‘queer to handle till you knew her way.’

Certainly I did not know her way. She turned in every direction but the one I was bound to go; the most part of the time we were broadside on, and I am very sure I never should have made the ship at all but for the tide. By good fortune, paddle as I pleased, the tide was still sweeping me down; and there lay the HISPANIOLA right in the fairway, hardly to be missed.

First she loomed before me like a blot of something yet blacker than darkness, then her spars and hull began to take shape, and the next moment, as it seemed (for, the

farther I went, the brisker grew the current of the ebb), I was alongside of her hawser and had laid hold.

The hawser was as taut as a bowstring, and the current so strong she pulled upon her anchor. All round the hull, in the blackness, the rippling current bubbled and chattered like a little mountain stream. One cut with my sea-gully and the HISPANIOLA would go humming down the tide.

So far so good, but it next occurred to my recollection that a taut hawser, suddenly cut, is a thing as dangerous as a kicking horse. Ten to one, if I were so foolhardy as to cut the HISPANIOLA from her anchor, I and the coracle would be knocked clean out of the water.

This brought me to a full stop, and if fortune had not again particularly favoured me, I should have had to abandon my design. But the light airs which had begun blowing from the south-east and south had hauled round after nightfall into the south-west. Just while I was meditating, a puff came, caught the HISPANIOLA, and forced her up into the current; and to my great joy, I felt the hawser slacken in my grasp, and the hand by which I held it dip for a second under water.

With that I made my mind up, took out my gully, opened it with my teeth, and cut one strand after another,

till the vessel swung only by two. Then I lay quiet, waiting to sever these last when the strain should be once more lightened by a breath of wind.

All this time I had heard the sound of loud voices from the cabin, but to say truth, my mind had been so entirely taken up with other thoughts that I had scarcely given ear. Now, however, when I had nothing else to do, I began to pay more heed.

One I recognized for the coxswain's, Israel Hands, that had been Flint's gunner in former days. The other was, of course, my friend of the red night-cap. Both men were plainly the worse of drink, and they were still drinking, for even while I was listening, one of them, with a drunken cry, opened the stern window and threw out something, which I divined to be an empty bottle. But they were not only tipsy; it was plain that they were furiously angry. Oaths flew like hailstones, and every now and then there came forth such an explosion as I thought was sure to end in blows. But each time the quarrel passed off and the voices grumbled lower for a while, until the next crisis came and in its turn passed away without result.

On shore, I could see the glow of the great camp-fire burning warmly through the shore-side trees. Someone

was singing, a dull, old, droning sailor's song, with a droop and a quaver at the end of every verse, and seemingly no end to it at all but the patience of the singer. I had heard it on the voyage more than once and remembered these words:

'But one man of her crew alive,  
What put to sea with seventy-five.'

And I thought it was a ditty rather too dolefully appropriate for a company that had met such cruel losses in the morning. But, indeed, from what I saw, all these buccaneers were as callous as the sea they sailed on.

At last the breeze came; the schooner sidled and drew nearer in the dark; I felt the hawser slacken once more, and with a good, tough effort, cut the last fibres through.

The breeze had but little action on the coracle, and I was almost instantly swept against the bows of the HISPANIOLA. At the same time, the schooner began to turn upon her heel, spinning slowly, end for end, across the current.

I wrought like a fiend, for I expected every moment to be swamped; and since I found I could not push the coracle directly off, I now shoved straight astern. At length I was clear of my dangerous neighbour, and just as I gave the last impulsion, my hands came across a light

cord that was trailing overboard across the stern bulwarks. Instantly I grasped it.

Why I should have done so I can hardly say. It was at first mere instinct, but once I had it in my hands and found it fast, curiosity began to get the upper hand, and I determined I should have one look through the cabin window.

I pulled in hand over hand on the cord, and when I judged myself near enough, rose at infinite risk to about half my height and thus commanded the roof and a slice of the interior of the cabin.

By this time the schooner and her little consort were gliding pretty swiftly through the water; indeed, we had already fetched up level with the camp-fire. The ship was talking, as sailors say, loudly, treading the innumerable ripples with an incessant weltering splash; and until I got my eye above the window-sill I could not comprehend why the watchmen had taken no alarm. One glance, however, was sufficient; and it was only one glance that I durst take from that unsteady skiff. It showed me Hands and his companion locked together in deadly wrestle, each with a hand upon the other's throat.

I dropped upon the thwart again, none too soon, for I was near overboard. I could see nothing for the moment

but these two furious, encrimsoned faces swaying together under the smoky lamp, and I shut my eyes to let them grow once more familiar with the darkness.

The endless ballad had come to an end at last, and the whole diminished company about the camp-fire had broken into the chorus I had heard so often:

‘Fifteen men on the dead man’s chest—  
Yo-ho-ho, and a bottle of rum!  
Drink and the devil had done for the rest—  
Yo-ho-ho, and a bottle of rum!’

I was just thinking how busy drink and the devil were at that very moment in the cabin of the *HISPA NIOLA*, when I was surprised by a sudden lurch of the coracle. At the same moment, she yawed sharply and seemed to change her course. The speed in the meantime had strangely increased.

I opened my eyes at once. All round me were little ripples, combing over with a sharp, bristling sound and slightly phosphorescent. The *HISPA NIOLA* herself, a few yards in whose wake I was still being whirled along, seemed to stagger in her course, and I saw her spars toss a little against the blackness of the night; nay, as I looked longer, I made sure she also was wheeling to the southward.

I glanced over my shoulder, and my heart jumped against my ribs. There, right behind me, was the glow of the camp-fire. The current had turned at right angles, sweeping round along with it the tall schooner and the little dancing coracle; ever quickening, ever bubbling higher, ever muttering louder, it went spinning through the narrows for the open sea.

Suddenly the schooner in front of me gave a violent yaw, turning, perhaps, through twenty degrees; and almost at the same moment one shout followed another from on board; I could hear feet pounding on the companion ladder and I knew that the two drunkards had at last been interrupted in their quarrel and awakened to a sense of their disaster.

I lay down flat in the bottom of that wretched skiff and devoutly recommended my spirit to its Maker. At the end of the straits, I made sure we must fall into some bar of raging breakers, where all my troubles would be ended speedily; and though I could, perhaps, bear to die, I could not bear to look upon my fate as it approached.

So I must have lain for hours, continually beaten to and fro upon the billows, now and again wetted with flying sprays, and never ceasing to expect death at the next plunge. Gradually weariness grew upon me; a numbness,

an occasional stupor, fell upon my mind even in the midst of my terrors, until sleep at last supervened and in my sea-tossed coracle I lay and dreamed of home and the old Admiral Benbow.

## The Cruise of the Coracle

IT was broad day when I awoke and found myself tossing at the south-west end of Treasure Island. The sun was up but was still hid from me behind the great bulk of the Spy-glass, which on this side descended almost to the sea in formidable cliffs.

Haulbowline Head and Mizzen-mast Hill were at my elbow, the hill bare and dark, the head bound with cliffs forty or fifty feet high and fringed with great masses of fallen rock. I was scarce a quarter of a mile to seaward, and it was my first thought to paddle in and land.

That notion was soon given over. Among the fallen rocks the breakers spouted and bellowed; loud reverberations, heavy sprays flying and falling, succeeded one another from second to second; and I saw myself, if I ventured nearer, dashed to death upon the rough shore or spending my strength in vain to scale the beetling crags.

Nor was that all, for crawling together on flat tables of rock or letting themselves drop into the sea with loud reports I beheld huge slimy monsters—soft snails, as it

## Treasure Island

were, of incredible bigness—two or three score of them together, making the rocks to echo with their barkings.

I have understood since that they were sea lions, and entirely harmless. But the look of them, added to the difficulty of the shore and the high running of the surf, was more than enough to disgust me of that landing-place. I felt willing rather to starve at sea than to confront such perils.

In the meantime I had a better chance, as I supposed, before me. North of Haulbowline Head, the land runs in a long way, leaving at low tide a long stretch of yellow sand. To the north of that, again, there comes another cape—Cape of the Woods, as it was marked upon the chart—buried in tall green pines, which descended to the margin of the sea.

I remembered what Silver had said about the current that sets northward along the whole west coast of Treasure Island, and seeing from my position that I was already under its influence, I preferred to leave Haulbowline Head behind me and reserve my strength for an attempt to land upon the kindlier-looking Cape of the Woods.

There was a great, smooth swell upon the sea. The wind blowing steady and gentle from the south, there was

no contrariety between that and the current, and the billows rose and fell unbroken.

Had it been otherwise, I must long ago have perished; but as it was, it is surprising how easily and securely my little and light boat could ride. Often, as I still lay at the bottom and kept no more than an eye above the gunwale, I would see a big blue summit heaving close above me; yet the coracle would but bounce a little, dance as if on springs, and subside on the other side into the trough as lightly as a bird.

I began after a little to grow very bold and sat up to try my skill at paddling. But even a small change in the disposition of the weight will produce violent changes in the behaviour of a coracle. And I had hardly moved before the boat, giving up at once her gentle dancing movement, ran straight down a slope of water so steep that it made me giddy, and struck her nose, with a spout of spray, deep into the side of the next wave.

I was drenched and terrified, and fell instantly back into my old position, whereupon the coracle seemed to find her head again and led me as softly as before among the billows. It was plain she was not to be interfered with, and at that rate, since I could in no way influence her course, what hope had I left of reaching land?

I began to be horribly frightened, but I kept my head, for all that. First, moving with all care, I gradually baled out the coracle with my sea-cap; then, getting my eye once more above the gunwale, I set myself to study how it was she managed to slip so quietly through the rollers.

I found each wave, instead of the big, smooth glossy mountain it looks from shore or from a vessel's deck, was for all the world like any range of hills on dry land, full of peaks and smooth places and valleys. The coracle, left to herself, turning from side to side, threaded, so to speak, her way through these lower parts and avoided the steep slopes and higher, toppling summits of the wave.

'Well, now,' thought I to myself, 'it is plain I must lie where I am and not disturb the balance; but it is plain also that I can put the paddle over the side and from time to time, in smooth places, give her a shove or two towards land.' No sooner thought upon than done. There I lay on my elbows in the most trying attitude, and every now and again gave a weak stroke or two to turn her head to shore.

It was very tiring and slow work, yet I did visibly gain ground; and as we drew near the Cape of the Woods, though I saw I must infallibly miss that point, I had still made some hundred yards of easting. I was, indeed, close in. I could see the cool green tree-tops swaying together

in the breeze, and I felt sure I should make the next promontory without fail.

It was high time, for I now began to be tortured with thirst. The glow of the sun from above, its thousandfold reflection from the waves, the sea-water that fell and dried upon me, caking my very lips with salt, combined to make my throat burn and my brain ache. The sight of the trees so near at hand had almost made me sick with longing, but the current had soon carried me past the point, and as the next reach of sea opened out, I beheld a sight that changed the nature of my thoughts.

Right in front of me, not half a mile away, I beheld the HISPANIOLA under sail. I made sure, of course, that I should be taken; but I was so distressed for want of water that I scarce knew whether to be glad or sorry at the thought, and long before I had come to a conclusion, surprise had taken entire possession of my mind and I could do nothing but stare and wonder.

The HISPANIOLA was under her main-sail and two jibs, and the beautiful white canvas shone in the sun like snow or silver. When I first sighted her, all her sails were drawing; she was lying a course about north-west, and I presumed the men on board were going round the island on their way back to the anchorage. Presently she began

to fetch more and more to the westward, so that I thought they had sighted me and were going about in chase. At last, however, she fell right into the wind's eye, was taken dead aback, and stood there awhile helpless, with her sails shivering.

'Clumsy fellows,' said I; 'they must still be drunk as owls.' And I thought how Captain Smollett would have set them skipping.

Meanwhile the schooner gradually fell off and filled again upon another tack, sailed swiftly for a minute or so, and brought up once more dead in the wind's eye. Again and again was this repeated. To and fro, up and down, north, south, east, and west, the HISPANIOLA sailed by swoops and dashes, and at each repetition ended as she had begun, with idly flapping canvas. It became plain to me that nobody was steering. And if so, where were the men? Either they were dead drunk or had deserted her, I thought, and perhaps if I could get on board I might return the vessel to her captain.

The current was bearing coracle and schooner southward at an equal rate. As for the latter's sailing, it was so wild and intermittent, and she hung each time so long in irons, that she certainly gained nothing, if she did not even lose. If only I dared to sit up and paddle, I made

sure that I could overhaul her. The scheme had an air of adventure that inspired me, and the thought of the water breaker beside the fore companion doubled my growing courage.

Up I got, was welcomed almost instantly by another cloud of spray, but this time stuck to my purpose and set myself, with all my strength and caution, to paddle after the unsteered HISPANIOLA. Once I shipped a sea so heavy that I had to stop and bail, with my heart fluttering like a bird, but gradually I got into the way of the thing and guided my coracle among the waves, with only now and then a blow upon her bows and a dash of foam in my face.

I was now gaining rapidly on the schooner; I could see the brass glisten on the tiller as it banged about, and still no soul appeared upon her decks. I could not choose but suppose she was deserted. If not, the men were lying drunk below, where I might batten them down, perhaps, and do what I chose with the ship.

For some time she had been doing the worse thing possible for me—standing still. She headed nearly due south, yawning, of course, all the time. Each time she fell off, her sails partly filled, and these brought her in a moment right to the wind again. I have said this was the

worst thing possible for me, for helpless as she looked in this situation, with the canvas cracking like cannon and the blocks trundling and banging on the deck, she still continued to run away from me, not only with the speed of the current, but by the whole amount of her leeway, which was naturally great.

But now, at last, I had my chance. The breeze fell for some seconds, very low, and the current gradually turning her, the *HISPANIOLA* revolved slowly round her centre and at last presented me her stern, with the cabin window still gaping open and the lamp over the table still burning on into the day. The main-sail hung drooped like a banner. She was stock-still but for the current.

For the last little while I had even lost, but now redoubling my efforts, I began once more to overhaul the chase.

I was not a hundred yards from her when the wind came again in a clap; she filled on the port tack and was off again, stooping and skimming like a swallow.

My first impulse was one of despair, but my second was towards joy. Round she came, till she was broadside on to me—round still till she had covered a half and then two thirds and then three quarters of the distance that separated us. I could see the waves boiling white under

her forefoot. Immensely tall she looked to me from my low station in the coracle.

And then, of a sudden, I began to comprehend. I had scarce time to think—scarce time to act and save myself. I was on the summit of one swell when the schooner came stooping over the next. The bowsprit was over my head. I sprang to my feet and leaped, stamping the coracle under water. With one hand I caught the jib-boom, while my foot was lodged between the stay and the brace; and as I still clung there panting, a dull blow told me that the schooner had charged down upon and struck the coracle and that I was left without retreat on the HISPANIOLA.

## I Strike the Jolly Roger

I HAD scarce gained a position on the bowsprit when the flying jib flapped and filled upon the other tack, with a report like a gun. The schooner trembled to her keel under the reverse, but next moment, the other sails still drawing, the jib flapped back again and hung idle.

This had nearly tossed me off into the sea; and now I lost no time, crawled back along the bowsprit, and tumbled head foremost on the deck.

I was on the lee side of the forecastle, and the main-sail, which was still drawing, concealed from me a certain portion of the after-deck. Not a soul was to be seen. The planks, which had not been swabbed since the mutiny, bore the print of many feet, and an empty bottle, broken by the neck, tumbled to and fro like a live thing in the scuppers.

Suddenly the HISPANIOLA came right into the wind. The jibs behind me cracked aloud, the rudder slammed to, the whole ship gave a sickening heave and shudder, and at the same moment the main-boom swung inboard, the

sheet groaning in the blocks, and showed me the lee after-deck.

There were the two watchmen, sure enough: red-cap on his back, as stiff as a handspike, with his arms stretched out like those of a crucifix and his teeth showing through his open lips; Israel Hands propped against the bulwarks, his chin on his chest, his hands lying open before him on the deck, his face as white, under its tan, as a tallow candle.

For a while the ship kept bucking and sidling like a vicious horse, the sails filling, now on one tack, now on another, and the boom swinging to and fro till the mast groaned aloud under the strain. Now and again too there would come a cloud of light sprays over the bulwark and a heavy blow of the ship's bows against the swell; so much heavier weather was made of it by this great rigged ship than by my home-made, lop-sided coracle, now gone to the bottom of the sea.

At every jump of the schooner, red-cap slipped to and fro, but—what was ghastly to behold—neither his attitude nor his fixed teeth-disclosing grin was anyway disturbed by this rough usage. At every jump too, Hands appeared still more to sink into himself and settle down upon the deck, his feet sliding ever the farther out, and the whole

body canting towards the stern, so that his face became, little by little, hid from me; and at last I could see nothing beyond his ear and the frayed ringlet of one whisker.

At the same time, I observed, around both of them, splashes of dark blood upon the planks and began to feel sure that they had killed each other in their drunken wrath.

While I was thus looking and wondering, in a calm moment, when the ship was still, Israel Hands turned partly round and with a low moan writhed himself back to the position in which I had seen him first. The moan, which told of pain and deadly weakness, and the way in which his jaw hung open went right to my heart. But when I remembered the talk I had overheard from the apple barrel, all pity left me.

I walked aft until I reached the main-mast.

‘Come aboard, Mr. Hands,’ I said ironically.

He rolled his eyes round heavily, but he was too far gone to express surprise. All he could do was to utter one word, ‘Brandy.’

It occurred to me there was no time to lose, and dodging the boom as it once more lurched across the deck, I slipped aft and down the companion stairs into the cabin.

It was such a scene of confusion as you can hardly fancy. All the lockfast places had been broken open in quest of the chart. The floor was thick with mud where ruffians had sat down to drink or consult after wading in the marshes round their camp. The bulkheads, all painted in clear white and beaded round with gilt, bore a pattern of dirty hands. Dozens of empty bottles clinked together in corners to the rolling of the ship. One of the doctor's medical books lay open on the table, half of the leaves gutted out, I suppose, for pipelights. In the midst of all this the lamp still cast a smoky glow, obscure and brown as umber.

I went into the cellar; all the barrels were gone, and of the bottles a most surprising number had been drunk out and thrown away. Certainly, since the mutiny began, not a man of them could ever have been sober.

Foraging about, I found a bottle with some brandy left, for Hands; and for myself I routed out some biscuit, some pickled fruits, a great bunch of raisins, and a piece of cheese. With these I came on deck, put down my own stock behind the rudder head and well out of the coxswain's reach, went forward to the water-breaker, and had a good deep drink of water, and then, and not till then, gave Hands the brandy.

## Treasure Island

He must have drunk a gill before he took the bottle from his mouth.

‘Aye,’ said he, ‘by thunder, but I wanted some o’ that!’

I had sat down already in my own corner and begun to eat.

‘Much hurt?’ I asked him.

He grunted, or rather, I might say, he barked.

‘If that doctor was aboard,’ he said, ‘I’d be right enough in a couple of turns, but I don’t have no manner of luck, you see, and that’s what’s the matter with me. As for that swab, he’s good and dead, he is,’ he added, indicating the man with the red cap. ‘He warn’t no seaman anyhow. And where mought you have come from?’

‘Well,’ said I, ‘I’ve come aboard to take possession of this ship, Mr. Hands; and you’ll please regard me as your captain until further notice.’

He looked at me sourly enough but said nothing. Some of the colour had come back into his cheeks, though he still looked very sick and still continued to slip out and settle down as the ship banged about.

‘By the by,’ I continued, ‘I can’t have these colours, Mr. Hands; and by your leave, I’ll strike ‘em. Better none than these.’

And again dodging the boom, I ran to the colour lines, handed down their cursed black flag, and chucked it overboard.

‘God save the king!’ said I, waving my cap. ‘And there’s an end to Captain Silver!’

He watched me keenly and slyly, his chin all the while on his breast.

‘I reckon,’ he said at last, ‘I reckon, Cap’n Hawkins, you’ll kind of want to get ashore now. S’pose we talks.’

‘Why, yes,’ says I, ‘with all my heart, Mr. Hands. Say on.’ And I went back to my meal with a good appetite.

‘This man,’ he began, nodding feebly at the corpse ‘— O’Brien were his name, a rank Irisher—this man and me got the canvas on her, meaning for to sail her back. Well, HE’S dead now, he is—as dead as bilge; and who’s to sail this ship, I don’t see. Without I gives you a hint, you ain’t that man, as far’s I can tell. Now, look here, you gives me food and drink and a old scarf or ankecher to tie my wound up, you do, and I’ll tell you how to tail her, and that’s about square all round, I take it.’

‘I’ll tell you one thing,’ says I: ‘I’m not going back to Captain Kidd’s anchorage. I mean to get into North Inlet and beach her quietly there.’

‘To be sure you did,’ he cried. ‘Why, I ain’t sich an infernal lubber after all. I can see, can’t I? I’ve tried my fling, I have, and I’ve lost, and it’s you has the wind of me. North Inlet? Why, I haven’t no ch’ice, not I! I’d help you sail her up to Execution Dock, by thunder! So I would.’

Well, as it seemed to me, there was some sense in this. We struck our bargain on the spot. In three minutes I had the **HISPANIOLA** sailing easily before the wind along the coast of Treasure Island, with good hopes of turning the northern point ere noon and beating down again as far as North Inlet before high water, when we might beach her safely and wait till the subsiding tide permitted us to land.

Then I lashed the tiller and went below to my own chest, where I got a soft silk handkerchief of my mother’s. With this, and with my aid, Hands bound up the great bleeding stab he had received in the thigh, and after he had eaten a little and had a swallow or two more of the brandy, he began to pick up visibly, sat straighter up, spoke louder and clearer, and looked in every way another man.

The breeze served us admirably. We skimmed before it like a bird, the coast of the island flashing by and the view

changing every minute. Soon we were past the high lands and bowling beside low, sandy country, sparsely dotted with dwarf pines, and soon we were beyond that again and had turned the corner of the rocky hill that ends the island on the north.

I was greatly elated with my new command, and pleased with the bright, sunshiny weather and these different prospects of the coast. I had now plenty of water and good things to eat, and my conscience, which had smitten me hard for my desertion, was quieted by the great conquest I had made. I should, I think, have had nothing left me to desire but for the eyes of the coxswain as they followed me derisively about the deck and the odd smile that appeared continually on his face. It was a smile that had in it something both of pain and weakness—a haggard old man's smile; but there was, besides that, a grain of derision, a shadow of treachery, in his expression as he craftily watched, and watched, and watched me at my work.

## **Israel Hands**

THE wind, serving us to a desire, now hauled into the west. We could run so much the easier from the north-east corner of the island to the mouth of the North Inlet. Only, as we had no power to anchor and dared not beach her till the tide had flowed a good deal farther, time hung on our hands. The coxswain told me how to lay the ship to; after a good many trials I succeeded, and we both sat in silence over another meal.

‘Cap’n,’ said he at length with that same uncomfortable smile, ‘here’s my old shipmate, O’Brien; s’pose you was to heave him overboard. I ain’t partic’lar as a rule, and I don’t take no blame for settling his hash, but I don’t reckon him ornamental now, do you?’

‘I’m not strong enough, and I don’t like the job; and there he lies, for me,’ said I.

‘This here’s an unlucky ship, this HISPANIOLA, Jim,’ he went on, blinking. ‘There’s a power of men been killed in this HISPANIOLA—a sight o’ poor seamen dead and gone since you and me took ship to Bristol. I never seen

sich dirty luck, not I. There was this here O'Brien now—he's dead, ain't he? Well now, I'm no scholar, and you're a lad as can read and figure, and to put it straight, do you take it as a dead man is dead for good, or do he come alive again?"

'You can kill the body, Mr. Hands, but not the spirit; you must know that already,' I replied. 'O'Brien there is in another world, and may be watching us.'

'Ah!' says he. 'Well, that's unfort'nate—appears as if killing parties was a waste of time. Howsomever, sperrits don't reckon for much, by what I've seen. I'll chance it with the sperrits, Jim. And now, you've spoke up free, and I'll take it kind if you'd step down into that there cabin and get me a—well, a—shiver my timbers! I can't hit the name on 't; well, you get me a bottle of wine, Jim—this here brandy's too strong for my head.'

Now, the coxswain's hesitation seemed to be unnatural, and as for the notion of his preferring wine to brandy, I entirely disbelieved it. The whole story was a pretext. He wanted me to leave the deck—so much was plain; but with what purpose I could in no way imagine. His eyes never met mine; they kept wandering to and fro, up and down, now with a look to the sky, now with a flitting glance upon the dead O'Brien. All the time he

kept smiling and putting his tongue out in the most guilty, embarrassed manner, so that a child could have told that he was bent on some deception. I was prompt with my answer, however, for I saw where my advantage lay and that with a fellow so densely stupid I could easily conceal my suspicions to the end.

‘Some wine?’ I said. ‘Far better. Will you have white or red?’

‘Well, I reckon it’s about the blessed same to me, shipmate,’ he replied; ‘so it’s strong, and plenty of it, what’s the odds?’

‘All right,’ I answered. ‘I’ll bring you port, Mr. Hands. But I’ll have to dig for it.’

With that I scuttled down the companion with all the noise I could, slipped off my shoes, ran quietly along the sparr'd gallery, mounted the forecastle ladder, and popped my head out of the fore companion. I knew he would not expect to see me there, yet I took every precaution possible, and certainly the worst of my suspicions proved too true.

He had risen from his position to his hands and knees, and though his leg obviously hurt him pretty sharply when he moved—for I could hear him stifle a groan—yet it was at a good, rattling rate that he trailed himself across

the deck. In half a minute he had reached the port scuppers and picked, out of a coil of rope, a long knife, or rather a short dirk, discoloured to the hilt with blood. He looked upon it for a moment, thrusting forth his under jaw, tried the point upon his hand, and then, hastily concealing it in the bosom of his jacket, trundled back again into his old place against the bulwark.

This was all that I required to know. Israel could move about, he was now armed, and if he had been at so much trouble to get rid of me, it was plain that I was meant to be the victim. What he would do afterwards—whether he would try to crawl right across the island from North Inlet to the camp among the swamps or whether he would fire Long Tom, trusting that his own comrades might come first to help him—was, of course, more than I could say.

Yet I felt sure that I could trust him in one point, since in that our interests jumped together, and that was in the disposition of the schooner. We both desired to have her stranded safe enough, in a sheltered place, and so that, when the time came, she could be got off again with as little labour and danger as might be; and until that was done I considered that my life would certainly be spared.

While I was thus turning the business over in my mind, I had not been idle with my body. I had stolen back to the

cabin, slipped once more into my shoes, and laid my hand at random on a bottle of wine, and now, with this for an excuse, I made my reappearance on the deck.

Hands lay as I had left him, all fallen together in a bundle and with his eyelids lowered as though he were too weak to bear the light. He looked up, however, at my coming, knocked the neck off the bottle like a man who had done the same thing often, and took a good swig, with his favourite toast of ‘Here’s luck!’ Then he lay quiet for a little, and then, pulling out a stick of tobacco, begged me to cut him a quid.

‘Cut me a junk o’ that,’ says he, ‘for I haven’t no knife and hardly strength enough, so be as I had. Ah, Jim, Jim, I reckon I’ve missed stays! Cut me a quid, as’ll likely be the last, lad, for I’m for my long home, and no mistake.’

‘Well,’ said I, ‘I’ll cut you some tobacco, but if I was you and thought myself so badly, I would go to my prayers like a Christian man.’

‘Why?’ said he. ‘Now, you tell me why.’

‘Why?’ I cried. ‘You were asking me just now about the dead. You’ve broken your trust; you’ve lived in sin and lies and blood; there’s a man you killed lying at your feet this moment, and you ask me why! For God’s mercy, Mr. Hands, that’s why.’

I spoke with a little heat, thinking of the bloody dirk he had hidden in his pocket and designed, in his ill thoughts, to end me with. He, for his part, took a great draught of the wine and spoke with the most unusual solemnity.

'For thirty years,' he said, 'I've sailed the seas and seen good and bad, better and worse, fair weather and foul, provisions running out, knives going, and what not. Well, now I tell you, I never seen good come o' goodness yet. Him as strikes first is my fancy; dead men don't bite; them's my views—amen, so be it. And now, you look here,' he added, suddenly changing his tone, 'we've had about enough of this foolery. The tide's made good enough by now. You just take my orders, Cap'n Hawkins, and we'll sail slap in and be done with it.'

All told, we had scarce two miles to run; but the navigation was delicate, the entrance to this northern anchorage was not only narrow and shoal, but lay east and west, so that the schooner must be nicely handled to be got in. I think I was a good, prompt subaltern, and I am very sure that Hands was an excellent pilot, for we went about and about and dodged in, shaving the banks, with a certainty and a neatness that were a pleasure to behold.

Scarcely had we passed the heads before the land closed around us. The shores of North Inlet were as

thickly wooded as those of the southern anchorage, but the space was longer and narrower and more like, what in truth it was, the estuary of a river. Right before us, at the southern end, we saw the wreck of a ship in the last stages of dilapidation. It had been a great vessel of three masts but had lain so long exposed to the injuries of the weather that it was hung about with great webs of dripping seaweed, and on the deck of it shore bushes had taken root and now flourished thick with flowers. It was a sad sight, but it showed us that the anchorage was calm.

‘Now,’ said Hands, ‘look there; there’s a pet bit for to beach a ship in. Fine flat sand, never a cat’s paw, trees all around of it, and flowers a-blowing like a garding on that old ship.’

‘And once beached,’ I inquired, ‘how shall we get her off again?’

‘Why, so,’ he replied: ‘you take a line ashore there on the other side at low water, take a turn about one of them big pines; bring it back, take a turn around the capstan, and lie to for the tide. Come high water, all hands take a pull upon the line, and off she comes as sweet as natur’. And now, boy, you stand by. We’re near the bit now, and she’s too much way on her. Starboard a little—so—steady—starboard—larboard a little—steady—steady!’

So he issued his commands, which I breathlessly obeyed, till, all of a sudden, he cried, ‘Now, my hearty, luff!’ And I put the helm hard up, and the HISPANIOLA swung round rapidly and ran stem on for the low, wooded shore.

The excitement of these last manoeuvres had somewhat interfered with the watch I had kept hitherto, sharply enough, upon the coxswain. Even then I was still so much interested, waiting for the ship to touch, that I had quite forgot the peril that hung over my head and stood craning over the starboard bulwarks and watching the ripples spreading wide before the bows. I might have fallen without a struggle for my life had not a sudden disquietude seized upon me and made me turn my head. Perhaps I had heard a creak or seen his shadow moving with the tail of my eye; perhaps it was an instinct like a cat’s; but, sure enough, when I looked round, there was Hands, already half-way towards me, with the dirk in his right hand.

We must both have cried out aloud when our eyes met, but while mine was the shrill cry of terror, his was a roar of fury like a charging bully’s. At the same instant, he threw himself forward and I leapt sideways towards the bows. As I did so, I let go of the tiller, which sprang sharp

## *Treasure Island*

to leeward, and I think this saved my life, for it struck Hands across the chest and stopped him, for the moment, dead.

Before he could recover, I was safe out of the corner where he had me trapped, with all the deck to dodge about. Just forward of the main-mast I stopped, drew a pistol from my pocket, took a cool aim, though he had already turned and was once more coming directly after me, and drew the trigger. The hammer fell, but there followed neither flash nor sound; the priming was useless with sea-water. I cursed myself for my neglect. Why had not I, long before, reprimed and reloaded my only weapons? Then I should not have been as now, a mere fleeing sheep before this butcher.

Wounded as he was, it was wonderful how fast he could move, his grizzled hair tumbling over his face, and his face itself as red as a red ensign with his haste and fury. I had no time to try my other pistol, nor indeed much inclination, for I was sure it would be useless. One thing I saw plainly: I must not simply retreat before him, or he would speedily hold me boxed into the bows, as a moment since he had so nearly boxed me in the stern. Once so caught, and nine or ten inches of the blood-stained dirk would be my last experience on this side of

eternity. I placed my palms against the main-mast, which was of a goodish bigness, and waited, every nerve upon the stretch.

Seeing that I meant to dodge, he also paused; and a moment or two passed in feints on his part and corresponding movements upon mine. It was such a game as I had often played at home about the rocks of Black Hill Cove, but never before, you may be sure, with such a wildly beating heart as now. Still, as I say, it was a boy's game, and I thought I could hold my own at it against an elderly seaman with a wounded thigh. Indeed my courage had begun to rise so high that I allowed myself a few darting thoughts on what would be the end of the affair, and while I saw certainly that I could spin it out for long, I saw no hope of any ultimate escape.

Well, while things stood thus, suddenly the HISPANIOLA struck, staggered, ground for an instant in the sand, and then, swift as a blow, canted over to the port side till the deck stood at an angle of forty-five degrees and about a puncheon of water splashed into the scupper holes and lay, in a pool, between the deck and bulwark.

We were both of us capsized in a second, and both of us rolled, almost together, into the scuppers, the dead red-cap, with his arms still spread out, tumbling stiffly after

us. So near were we, indeed, that my head came against the coxswain's foot with a crack that made my teeth rattle. Blow and all, I was the first afoot again, for Hands had got involved with the dead body. The sudden canting of the ship had made the deck no place for running on; I had to find some new way of escape, and that upon the instant, for my foe was almost touching me. Quick as thought, I sprang into the mizzen shrouds, rattled up hand over hand, and did not draw a breath till I was seated on the cross-trees.

I had been saved by being prompt; the dirk had struck not half a foot below me as I pursued my upward flight; and there stood Israel Hands with his mouth open and his face upturned to mine, a perfect statue of surprise and disappointment.

Now that I had a moment to myself, I lost no time in changing the priming of my pistol, and then, having one ready for service, and to make assurance doubly sure, I proceeded to draw the load of the other and recharge it afresh from the beginning.

My new employment struck Hands all of a heap; he began to see the dice going against him, and after an obvious hesitation, he also hauled himself heavily into the shrouds, and with the dirk in his teeth, began slowly and

painfully to mount. It cost him no end of time and groans to haul his wounded leg behind him, and I had quietly finished my arrangements before he was much more than a third of the way up. Then, with a pistol in either hand, I addressed him.

‘One more step, Mr. Hands,’ said I, ‘and I’ll blow your brains out! Dead men don’t bite, you know,’ I added with a chuckle.

He stopped instantly. I could see by the working of his face that he was trying to think, and the process was so slow and laborious that, in my new-found security, I laughed aloud. At last, with a swallow or two, he spoke, his face still wearing the same expression of extreme perplexity. In order to speak he had to take the dagger from his mouth, but in all else he remained unmoved.

‘Jim,’ says he, ‘I reckon we’re fouled, you and me, and we’ll have to sign articles. I’d have had you but for that there lurch, but I don’t have no luck, not I; and I reckon I’ll have to strike, which comes hard, you see, for a master mariner to a ship’s younker like you, Jim.’

I was drinking in his words and smiling away, as conceited as a cock upon a wall, when, all in a breath, back went his right hand over his shoulder. Something sang like an arrow through the air; I felt a blow and then a

sharp pang, and there I was pinned by the shoulder to the mast. In the horrid pain and surprise of the moment—I scarce can say it was by my own volition, and I am sure it was without a conscious aim— both my pistols went off, and both escaped out of my hands. They did not fall alone; with a choked cry, the coxswain loosed his grasp upon the shrouds and plunged head first into the water.

### "Pieces of Eight"

OWING to the cant of the vessel, the masts hung far out over the water, and from my perch on the cross-trees I had nothing below me but the surface of the bay. Hands, who was not so far up, was in consequence nearer to the ship and fell between me and the bulwarks. He rose once to the surface in a lather of foam and blood and then sank again for good. As the water settled, I could see him lying huddled together on the clean, bright sand in the shadow of the vessel's sides. A fish or two whipped past his body. Sometimes, by the quivering of the water, he appeared to move a little, as if he were trying to rise. But he was dead enough, for all that, being both shot and drowned, and was food for fish in the very place where he had designed my slaughter.

I was no sooner certain of this than I began to feel sick, faint, and terrified. The hot blood was running over my back and chest. The dirk, where it had pinned my shoulder to the mast, seemed to burn like a hot iron; yet it was not so much these real sufferings that distressed me,

for these, it seemed to me, I could bear without a murmur; it was the horror I had upon my mind of falling from the cross-trees into that still green water, beside the body of the coxswain.

I clung with both hands till my nails ached, and I shut my eyes as if to cover up the peril. Gradually my mind came back again, my pulses quieted down to a more natural time, and I was once more in possession of myself.

It was my first thought to pluck forth the dirk, but either it stuck too hard or my nerve failed me, and I desisted with a violent shudder. Oddly enough, that very shudder did the business. The knife, in fact, had come the nearest in the world to missing me altogether; it held me by a mere pinch of skin, and this the shudder tore away. The blood ran down the faster, to be sure, but I was my own master again and only tacked to the mast by my coat and shirt.

These last I broke through with a sudden jerk, and then regained the deck by the starboard shrouds. For nothing in the world would I have again ventured, shaken as I was, upon the overhanging port shrouds from which Israel had so lately fallen.

I went below and did what I could for my wound; it pained me a good deal and still bled freely, but it was neither deep nor dangerous, nor did it greatly gall me when I used my arm. Then I looked around me, and as the ship was now, in a sense, my own, I began to think of clearing it from its last passenger—the dead man, O'Brien.

He had pitched, as I have said, against the bulwarks, where he lay like some horrible, ungainly sort of puppet, life-size, indeed, but how different from life's colour or life's comeliness! In that position I could easily have my way with him, and as the habit of tragical adventures had worn off almost all my terror for the dead, I took him by the waist as if he had been a sack of bran and with one good heave, tumbled him overboard. He went in with a sounding plunge; the red cap came off and remained floating on the surface; and as soon as the splash subsided, I could see him and Israel lying side by side, both wavering with the tremulous movement of the water. O'Brien, though still quite a young man, was very bald. There he lay, with that bald head across the knees of the man who had killed him and the quick fishes steering to and fro over both.

I was now alone upon the ship; the tide had just turned. The sun was within so few degrees of setting that already the shadow of the pines upon the western shore began to reach right across the anchorage and fall in patterns on the deck. The evening breeze had sprung up, and though it was well warded off by the hill with the two peaks upon the east, the cordage had begun to sing a little softly to itself and the idle sails to rattle to and fro.

I began to see a danger to the ship. The jibs I speedily doused and brought tumbling to the deck, but the main-sail was a harder matter. Of course, when the schooner canted over, the boom had swung out-board, and the cap of it and a foot or two of sail hung even under water. I thought this made it still more dangerous; yet the strain was so heavy that I half feared to meddle. At last I got my knife and cut the halyards. The peak dropped instantly, a great belly of loose canvas floated broad upon the water, and since, pull as I liked, I could not budge the downhall, that was the extent of what I could accomplish. For the rest, the **HISPANIOLA** must trust to luck, like myself.

By this time the whole anchorage had fallen into shadow—the last rays, I remember, falling through a glade of the wood and shining bright as jewels on the flowery mantle of the wreck. It began to be chill; the tide

was rapidly fleeting seaward, the schooner settling more and more on her beam-ends.

I scrambled forward and looked over. It seemed shallow enough, and holding the cut hawser in both hands for a last security, I let myself drop softly overboard. The water scarcely reached my waist; the sand was firm and covered with ripple marks, and I waded ashore in great spirits, leaving the *HISPAÑOLA* on her side, with her main-sail trailing wide upon the surface of the bay. About the same time, the sun went fairly down and the breeze whistled low in the dusk among the tossing pines.

At least, and at last, I was off the sea, nor had I returned thence empty-handed. There lay the schooner, clear at last from buccaneers and ready for our own men to board and get to sea again. I had nothing nearer my fancy than to get home to the stockade and boast of my achievements. Possibly I might be blamed a bit for my truancy, but the recapture of the *HISPAÑOLA* was a clenching answer, and I hoped that even Captain Smollett would confess I had not lost my time.

So thinking, and in famous spirits, I began to set my face homeward for the block house and my companions. I remembered that the most easterly of the rivers which drain into Captain Kidd's anchorage ran from the two-

peaked hill upon my left, and I bent my course in that direction that I might pass the stream while it was small. The wood was pretty open, and keeping along the lower spurs, I had soon turned the corner of that hill, and not long after waded to the mid-calf across the watercourse.

This brought me near to where I had encountered Ben Gunn, the maroon; and I walked more circumspectly, keeping an eye on every side. The dusk had come nigh hand completely, and as I opened out the cleft between the two peaks, I became aware of a wavering glow against the sky, where, as I judged, the man of the island was cooking his supper before a roaring fire. And yet I wondered, in my heart, that he should show himself so careless. For if I could see this radiance, might it not reach the eyes of Silver himself where he camped upon the shore among the marshes?

Gradually the night fell blacker; it was all I could do to guide myself even roughly towards my destination; the double hill behind me and the Spy-glass on my right hand loomed faint and fainter; the stars were few and pale; and in the low ground where I wandered I kept tripping among bushes and rolling into sandy pits.

Suddenly a kind of brightness fell about me. I looked up; a pale glimmer of moonbeams had alighted on the

summit of the Spy-glass, and soon after I saw something broad and silvery moving low down behind the trees, and knew the moon had risen.

With this to help me, I passed rapidly over what remained to me of my journey, and sometimes walking, sometimes running, impatiently drew near to the stockade. Yet, as I began to thread the grove that lies before it, I was not so thoughtless but that I slacked my pace and went a trifle warily. It would have been a poor end of my adventures to get shot down by my own party in mistake.

The moon was climbing higher and higher, its light began to fall here and there in masses through the more open districts of the wood, and right in front of me a glow of a different colour appeared among the trees. It was red and hot, and now and again it was a little darkened—as it were, the embers of a bonfire smouldering.

For the life of me I could not think what it might be.

At last I came right down upon the borders of the clearing. The western end was already steeped in moon-shine; the rest, and the block house itself, still lay in a black shadow chequered with long silvery streaks of light. On the other side of the house an immense fire had burned itself into clear embers and shed a steady, red

## Treasure Island

reverberation, contrasted strongly with the mellow paleness of the moon. There was not a soul stirring nor a sound beside the noises of the breeze.

I stopped, with much wonder in my heart, and perhaps a little terror also. It had not been our way to build great fires; we were, indeed, by the captain's orders, somewhat niggardly of firewood, and I began to fear that something had gone wrong while I was absent.

I stole round by the eastern end, keeping close in shadow, and at a convenient place, where the darkness was thickest, crossed the palisade.

To make assurance surer, I got upon my hands and knees and crawled, without a sound, towards the corner of the house. As I drew nearer, my heart was suddenly and greatly lightened. It is not a pleasant noise in itself, and I have often complained of it at other times, but just then it was like music to hear my friends snoring together so loud and peaceful in their sleep. The sea-cry of the watch, that beautiful 'All's well,' never fell more reassuringly on my ear.

In the meantime, there was no doubt of one thing; they kept an infamous bad watch. If it had been Silver and his lads that were now creeping in on them, not a soul would have seen daybreak. That was what it was, thought I, to

have the captain wounded; and again I blamed myself sharply for leaving them in that danger with so few to mount guard.

By this time I had got to the door and stood up. All was dark within, so that I could distinguish nothing by the eye. As for sounds, there was the steady drone of the snorers and a small occasional noise, a flickering or pecking that I could in no way account for.

With my arms before me I walked steadily in. I should lie down in my own place (I thought with a silent chuckle) and enjoy their faces when they found me in the morning.

My foot struck something yielding—it was a sleeper's leg; and he turned and groaned, but without awaking.

And then, all of a sudden, a shrill voice broke forth out of the darkness:

'Pieces of eight! Pieces of eight! Pieces of eight!  
Pieces of eight! Pieces of eight! and so forth, without pause or change, like the clacking of a tiny mill.

Silver's green parrot, Captain Flint! It was she whom I had heard pecking at a piece of bark; it was she, keeping better watch than any human being, who thus announced my arrival with her wearisome refrain.

I had no time left me to recover. At the sharp, clipping tone of the parrot, the sleepers awoke and sprang up; and with a mighty oath, the voice of Silver cried, ‘Who goes?’

I turned to run, struck violently against one person, recoiled, and ran full into the arms of a second, who for his part closed upon and held me tight.

‘Bring a torch, Dick,’ said Silver when my capture was thus assured.

And one of the men left the log-house and presently returned with a lighted brand.

## PART SIX

### Captain Silver

28

#### In the Enemy's Camp

THE red glare of the torch, lighting up the interior of the block house, showed me the worst of my apprehensions realized. The pirates were in possession of the house and stores: there was the cask of cognac, there were the pork and bread, as before, and what tenfold increased my horror, not a sign of any prisoner. I could only judge that all had perished, and my heart smote me sorely that I had not been there to perish with them.

There were six of the buccaneers, all told; not another man was left alive. Five of them were on their feet, flushed and swollen, suddenly called out of the first sleep of drunkenness. The sixth had only risen upon his elbow; he was deadly pale, and the blood-stained bandage round his head told that he had recently been wounded, and still more recently dressed. I remembered the man who had

been shot and had run back among the woods in the great attack, and doubted not that this was he.

The parrot sat, preening her plumage, on Long John's shoulder. He himself, I thought, looked somewhat paler and more stern than I was used to. He still wore the fine broadcloth suit in which he had fulfilled his mission, but it was bitterly the worse for wear, daubed with clay and torn with the sharp briars of the wood.

'So,' said he, 'here's Jim Hawkins, shiver my timbers! Dropped in, like, eh? Well, come, I take that friendly.'

And thereupon he sat down across the brandy cask and began to fill a pipe.

'Give me a loan of the link, Dick,' said he; and then, when he had a good light, 'That'll do, lad,' he added; 'stick the glim in the wood heap; and you, gentlemen, bring yourselves to! You needn't stand up for Mr. Hawkins; HE'LL excuse you, you may lay to that. And so, Jim'—stopping the tobacco—'here you were, and quite a pleasant surprise for poor old John. I see you were smart when first I set my eyes on you, but this here gets away from me clean, it do.'

To all this, as may be well supposed, I made no answer. They had set me with my back against the wall, and I stood there, looking Silver in the face, pluckily

enough, I hope, to all outward appearance, but with black despair in my heart.

Silver took a whiff or two of his pipe with great composure and then ran on again.

‘Now, you see, Jim, so be as you ARE here,’ says he, ‘I’ll give you a piece of my mind. I’ve always liked you, I have, for a lad of spirit, and the picter of my own self when I was young and handsome. I always wanted you to jine and take your share, and die a gentleman, and now, my cock, you’ve got to. Cap’n Smollett’s a fine seaman, as I’ll own up to any day, but stiff on discipline. ‘Dooty is dooty,’ says he, and right he is. Just you keep clear of the cap’n. The doctor himself is gone dead again you—‘ungrateful scamp’ was what he said; and the short and the long of the whole story is about here: you can’t go back to your own lot, for they won’t have you; and without you start a third ship’s company all by yourself, which might be lonely, you’ll have to jine with Cap’n Silver.’

So far so good. My friends, then, were still alive, and though I partly believed the truth of Silver’s statement, that the cabin party were incensed at me for my desertion, I was more relieved than distressed by what I heard.

‘I don’t say nothing as to your being in our hands,’ continued Silver, ‘though there you are, and you may lay to it. I’m all for argyment; I never seen good come out o’ threatening. If you like the service, well, you’ll jine; and if you don’t, Jim, why, you’re free to answer no—free and welcome, shipmate; and if fairer can be said by mortal seaman, shiver my sides!’

‘Am I to answer, then?’ I asked with a very tremulous voice. Through all this sneering talk, I was made to feel the threat of death that overhung me, and my cheeks burned and my heart beat painfully in my breast.

‘Lad,’ said Silver, ‘no one’s a-pressing of you. Take your bearings. None of us won’t hurry you, mate; time goes so pleasant in your company, you see.’

‘Well,’ says I, growing a bit bolder, ‘if I’m to choose, I declare I have a right to know what’s what, and why you’re here, and where my friends are.’

‘Wot’s wot?’ repeated one of the buccaneers in a deep growl. ‘Ah, he’d be a lucky one as knowed that!’

‘You’ll perhaps batten down your hatches till you’re spoke to, my friend,’ cried Silver truculently to this speaker. And then, in his first gracious tones, he replied to me, ‘Yesterday morning, Mr. Hawkins,’ said he, ‘in the dog-watch, down came Doctor Livesey with a flag of

truce. Says he, ‘Cap’n Silver, you’re sold out. Ship’s gone.’ Well, maybe we’d been taking a glass, and a song to help it round. I won’t say no. Leastways, none of us had looked out. We looked out, and by thunder, the old ship was gone! I never seen a pack o’ fools look fishier; and you may lay to that, if I tells you that looked the fishiest. ‘Well,’ says the doctor, ‘let’s bargain.’ We bargained, him and I, and here we are: stores, brandy, block house, the firewood you was thoughtful enough to cut, and in a manner of speaking, the whole blessed boat, from cross-trees to kelson. As for them, they’ve tramped; I don’t know where’s they are.’

He drew again quietly at his pipe.

‘And lest you should take it into that head of yours,’ he went on, ‘that you was included in the treaty, here’s the last word that was said: ‘How many are you,’ says I, ‘to leave?’ ‘Four,’ says he; ‘four, and one of us wounded. As for that boy, I don’t know where he is, confound him,’ says he, ‘nor I don’t much care. We’re about sick of him.’ These was his words.

‘Is that all?’ I asked.

‘Well, it’s all that you’re to hear, my son,’ returned Silver.

‘And now I am to choose?’

‘And now you are to choose, and you may lay to that,’ said Silver.

‘Well,’ said I, ‘I am not such a fool but I know pretty well what I have to look for. Let the worst come to the worst, it’s little I care. I’ve seen too many die since I fell in with you. But there’s a thing or two I have to tell you,’ I said, and by this time I was quite excited; ‘and the first is this: here you are, in a bad way—ship lost, treasure lost, men lost, your whole business gone to wreck; and if you want to know who did it—it was I! I was in the apple barrel the night we sighted land, and I heard you, John, and you, Dick Johnson, and Hands, who is now at the bottom of the sea, and told every word you said before the hour was out. And as for the schooner, it was I who cut her cable, and it was I that killed the men you had aboard of her, and it was I who brought her where you’ll never see her more, not one of you. The laugh’s on my side; I’ve had the top of this business from the first; I no more fear you than I fear a fly. Kill me, if you please, or spare me. But one thing I’ll say, and no more; if you spare me, bygones are bygones, and when you fellows are in court for piracy, I’ll save you all I can. It is for you to choose. Kill another and do yourselves no good, or spare me and keep a witness to save you from the gallows.’

I stopped, for, I tell you, I was out of breath, and to my wonder, not a man of them moved, but all sat staring at me like as many sheep. And while they were still staring, I broke out again, ‘And now, Mr. Silver,’ I said, ‘I believe you’re the best man here, and if things go to the worst, I’ll take it kind of you to let the doctor know the way I took it.’

‘I’ll bear it in mind,’ said Silver with an accent so curious that I could not, for the life of me, decide whether he were laughing at my request or had been favourably affected by my courage.

‘I’ll put one to that,’ cried the old mahogany-faced seaman—Morgan by name—whom I had seen in Long John’s public-house upon the quays of Bristol. ‘It was him that knowed Black Dog.’

‘Well, and see here,’ added the sea-cook. ‘I’ll put another again to that, by thunder! For it was this same boy that faked the chart from Billy Bones. First and last, we’ve split upon Jim Hawkins!’

‘Then here goes!’ said Morgan with an oath.

And he sprang up, drawing his knife as if he had been twenty.

‘Avast, there!’ cried Silver. ‘Who are you, Tom Morgan? Maybe you thought you was cap’n here,

perhaps. By the powers, but I'll teach you better! Cross me, and you'll go where many a good man's gone before you, first and last, these thirty year back—some to the yard-arm, shiver my timbers, and some by the board, and all to feed the fishes. There's never a man looked me between the eyes and seen a good day a'terwards, Tom Morgan, you may lay to that.'

Morgan paused, but a hoarse murmur rose from the others.

'Tom's right,' said one.

'I stood hazing long enough from one,' added another. 'I'll be hanged if I'll be hazed by you, John Silver.'

'Did any of you gentlemen want to have it out with ME?' roared Silver, bending far forward from his position on the keg, with his pipe still glowing in his right hand. 'Put a name on what you're at; you ain't dumb, I reckon. Him that wants shall get it. Have I lived this many years, and a son of a rum puncheon cock his hat athwart my hawse at the latter end of it? You know the way; you're all gentlemen o' fortune, by your account. Well, I'm ready. Take a cutlass, him that dares, and I'll see the colour of his inside, crutch and all, before that pipe's empty.'

Not a man stirred; not a man answered.

‘That’s your sort, is it?’ he added, returning his pipe to his mouth. ‘Well, you’re a gay lot to look at, anyway. Not much worth to fight, you ain’t. P’raps you can understand King George’s English. I’m cap’n here by ‘lection. I’m cap’n here because I’m the best man by a long sea-mile. You won’t fight, as gentlemen o’ fortune should; then, by thunder, you’ll obey, and you may lay to it! I like that boy, now; I never seen a better boy than that. He’s more a man than any pair of rats of you in this here house, and what I say is this: let me see him that’ll lay a hand on him—that’s what I say, and you may lay to it.’

There was a long pause after this. I stood straight up against the wall, my heart still going like a sledge-hammer, but with a ray of hope now shining in my bosom. Silver leant back against the wall, his arms crossed, his pipe in the corner of his mouth, as calm as though he had been in church; yet his eye kept wandering furtively, and he kept the tail of it on his unruly followers. They, on their part, drew gradually together towards the far end of the block house, and the low hiss of their whispering sounded in my ear continuously, like a stream. One after another, they would look up, and the red light of the torch would fall for a second on their nervous faces;

## *Treasure Island*

but it was not towards me, it was towards Silver that they turned their eyes.

‘You seem to have a lot to say,’ remarked Silver, spitting far into the air. ‘Pipe up and let me hear it, or lay to.’

‘Ax your pardon, sir,’ returned one of the men; ‘you’re pretty free with some of the rules; maybe you’ll kindly keep an eye upon the rest. This crew’s dissatisfied; this crew don’t vally bullying a marlin-spike; this crew has its rights like other crews, I’ll make so free as that; and by your own rules, I take it we can talk together. I ax your pardon, sir, acknowledging you for to be captaining at this present; but I claim my right, and steps outside for a council.’

And with an elaborate sea-salute, this fellow, a long, ill-looking, yellow-eyed man of five and thirty, stepped coolly towards the door and disappeared out of the house. One after another the rest followed his example, each making a salute as he passed, each adding some apology. ‘According to rules,’ said one. ‘Forecastle council,’ said Morgan. And so with one remark or another all marched out and left Silver and me alone with the torch.

The sea-cook instantly removed his pipe.

‘Now, look you here, Jim Hawkins,’ he said in a steady whisper that was no more than audible, ‘you’re within half a plank of death, and what’s a long sight worse, of torture. They’re going to throw me off. But, you mark, I stand by you through thick and thin. I didn’t mean to; no, not till you spoke up. I was about desperate to lose that much blunt, and be hanged into the bargain. But I see you was the right sort. I says to myself, you stand by Hawkins, John, and Hawkins’ll stand by you. You’re his last card, and by the living thunder, John, he’s yours! Back to back, says I. You save your witness, and he’ll save your neck!’

I began dimly to understand.

‘You mean all’s lost?’ I asked.

‘Aye, by gum, I do!’ he answered. ‘Ship gone, neck gone —that’s the size of it. Once I looked into that bay, Jim Hawkins, and seen no schooner—well, I’m tough, but I gave out. As for that lot and their council, mark me, they’re outright fools and cowards. I’ll save your life—if so be as I can—from them. But, see here, Jim—tit for tat—you save Long John from swinging.’

I was bewildered; it seemed a thing so hopeless he was asking—he, the old buccaneer, the ringleader throughout.

‘What I can do, that I’ll do,’ I said.

‘It’s a bargain!’ cried Long John. ‘You speak up plucky, and by thunder, I’ve a chance!’

He hobbled to the torch, where it stood propped among the firewood, and took a fresh light to his pipe.

‘Understand me, Jim,’ he said, returning. ‘I’ve a head on my shoulders, I have. I’m on squire’s side now. I know you’ve got that ship safe somewhere. How you done it, I don’t know, but safe it is. I guess Hands and O’Brien turned soft. I never much believed in either of THEM. Now you mark me. I ask no questions, nor I won’t let others. I know when a game’s up, I do; and I know a lad that’s staunch. Ah, you that’s young—you and me might have done a power of good together!’

He drew some cognac from the cask into a tin cannikin.

‘Will you taste, messmate?’ he asked; and when I had refused: ‘Well, I’ll take a drain myself, Jim,’ said he. ‘I need a caulk, for there’s trouble on hand. And talking o’ trouble, why did that doctor give me the chart, Jim?’

My face expressed a wonder so unaffected that he saw the needlessness of further questions.

‘Ah, well, he did, though,’ said he. ‘And there’s something under that, no doubt—something, surely, under that, Jim—bad or good.’

And he took another swallow of the brandy, shaking his great fair head like a man who looks forward to the worst.

## **The Black Spot Again**

THE council of buccaneers had lasted some time, when one of them re-entered the house, and with a repetition of the same salute, which had in my eyes an ironical air, begged for a moment's loan of the torch. Silver briefly agreed, and this emissary retired again, leaving us together in the dark.

'There's a breeze coming, Jim,' said Silver, who had by this time adopted quite a friendly and familiar tone.

I turned to the loophole nearest me and looked out. The embers of the great fire had so far burned themselves out and now glowed so low and duskily that I understood why these conspirators desired a torch. About half-way down the slope to the stockade, they were collected in a group; one held the light, another was on his knees in their midst, and I saw the blade of an open knife shine in his hand with varying colours in the moon and torchlight. The rest were all somewhat stooping, as though watching the manoeuvres of this last. I could just make out that he had a book as well as a knife in his hand, and was still

wondering how anything so incongruous had come in their possession when the kneeling figure rose once more to his feet and the whole party began to move together towards the house.

‘Here they come,’ said I; and I returned to my former position, for it seemed beneath my dignity that they should find me watching them.

‘Well, let ‘em come, lad—let ‘em come,’ said Silver cheerily. ‘I’ve still a shot in my locker.’

The door opened, and the five men, standing huddled together just inside, pushed one of their number forward. In any other circumstances it would have been comical to see his slow advance, hesitating as he set down each foot, but holding his closed right hand in front of him.

‘Step up, lad,’ cried Silver. ‘I won’t eat you. Hand it over, lubber. I know the rules, I do; I won’t hurt a depytation.’

Thus encouraged, the buccaneer stepped forth more briskly, and having passed something to Silver, from hand to hand, slipped yet more smartly back again to his companions.

The sea-cook looked at what had been given him.

‘The black spot! I thought so,’ he observed. ‘Where might you have got the paper? Why, hillo! Look here,

now; this ain't lucky! You've gone and cut this out of a Bible. What fool's cut a Bible?"

'Ah, there!' said Morgan. 'There! Wot did I say? No good'll come o' that, I said.'

'Well, you've about fixed it now, among you,' continued Silver. 'You'll all swing now, I reckon. What soft-headed lubber had a Bible?"

'It was Dick,' said one.

'Dick, was it? Then Dick can get to prayers,' said Silver. 'He's seen his slice of luck, has Dick, and you may lay to that.'

But here the long man with the yellow eyes struck in.

'Belay that talk, John Silver,' he said. 'This crew has tipped you the black spot in full council, as in dooty bound; just you turn it over, as in dooty bound, and see what's wrote there. Then you can talk.'

'Thanky, George,' replied the sea-cook. 'You always was brisk for business, and has the rules by heart, George, as I'm pleased to see. Well, what is it, anyway? Ah! 'Deposed'—that's it, is it? Very pretty wrote, to be sure; like print, I swear. Your hand o' write, George? Why, you was gettin' quite a leadin' man in this here crew. You'll be cap'n next, I shouldn't wonder. Just oblige me with that torch again, will you? This pipe don't draw.'

‘Come, now,’ said George, ‘you don’t fool this crew no more. You’re a funny man, by your account; but you’re over now, and you’ll maybe step down off that barrel and help vote.’

‘I thought you said you knowed the rules,’ returned Silver contemptuously. ‘Leastways, if you don’t, I do; and I wait here—and I’m still your cap’n, mind—till you outs with your grievances and I reply; in the meantime, your black spot ain’t worth a biscuit. After that, we’ll see.’

‘Oh,’ replied George, ‘you don’t be under no kind of apprehension; WE’RE all square, we are. First, you’ve made a hash of this cruise—you’ll be a bold man to say no to that. Second, you let the enemy out o’ this here trap for nothing. Why did they want out? I dunno, but it’s pretty plain they wanted it. Third, you wouldn’t let us go at them upon the march. Oh, we see through you, John Silver; you want to play booty, that’s what’s wrong with you. And then, fourth, there’s this here boy.’

‘Is that all?’ asked Silver quietly.

‘Enough, too,’ retorted George. ‘We’ll all swing and sun-dry for your bungling.’

‘Well now, look here, I’ll answer these four p’ints; one after another I’ll answer ‘em. I made a hash o’ this cruise, did I? Well now, you all know what I wanted, and you all

know if that had been done that we'd 'a been aboard the HISPANIOLA this night as ever was, every man of us alive, and fit, and full of good plum-duff, and the treasure in the hold of her, by thunder! Well, who crossed me? Who forced my hand, as was the lawful cap'n? Who tipped me the black spot the day we landed and began this dance? Ah, it's a fine dance—I'm with you there—and looks mighty like a hornpipe in a rope's end at Execution Dock by London town, it does. But who done it? Why, it was Anderson, and Hands, and you, George Merry! And you're the last above board of that same meddling crew; and you have the Davy Jones's insolence to up and stand for cap'n over me—you, that sank the lot of us! By the powers! But this tops the stiffest yarn to nothing.'

Silver paused, and I could see by the faces of George and his late comrades that these words had not been said in vain.

'That's for number one,' cried the accused, wiping the sweat from his brow, for he had been talking with a vehemence that shook the house. 'Why, I give you my word, I'm sick to speak to you. You've neither sense nor memory, and I leave it to fancy where your mothers was that let you come to sea. Sea! Gentlemen o' fortune! I reckon tailors is your trade.'

‘Go on, John,’ said Morgan. ‘Speak up to the others.’

‘Ah, the others!’ returned John. ‘They’re a nice lot, ain’t they? You say this cruise is bungled. Ah! By gum, if you could understand how bad it’s bungled, you would see! We’re that near the gibbet that my neck’s stiff with thinking on it. You’ve seen ‘em, maybe, hanged in chains, birds about ‘em, seamen p’inting ‘em out as they go down with the tide. ‘Who’s that?’ says one. ‘That! Why, that’s John Silver. I knowed him well,’ says another. And you can hear the chains a-jangle as you go about and reach for the other buoy. Now, that’s about where we are, every mother’s son of us, thanks to him, and Hands, and Anderson, and other ruination fools of you. And if you want to know about number four, and that boy, why, shiver my timbers, isn’t he a hostage? Are we a-going to waste a hostage? No, not us; he might be our last chance, and I shouldn’t wonder. Kill that boy? Not me, mates! And number three? Ah, well, there’s a deal to say to number three. Maybe you don’t count it nothing to have a real college doctor to see you every day—you, John, with your head broke—or you, George Merry, that had the ague shakes upon you not six hours agone, and has your eyes the colour of lemon peel to this same moment on the clock? And maybe, perhaps, you didn’t know there was a

consort coming either? But there is, and not so long till then; and we'll see who'll be glad to have a hostage when it comes to that. And as for number two, and why I made a bargain—well, you came crawling on your knees to me to make it—on your knees you came, you was that downhearted—and you'd have starved too if I hadn't—but that's a trifle! You look there—that's why!’

And he cast down upon the floor a paper that I instantly recognized—none other than the chart on yellow paper, with the three red crosses, that I had found in the oilcloth at the bottom of the captain’s chest. Why the doctor had given it to him was more than I could fancy.

But if it were inexplicable to me, the appearance of the chart was incredible to the surviving mutineers. They leaped upon it like cats upon a mouse. It went from hand to hand, one tearing it from another; and by the oaths and the cries and the childish laughter with which they accompanied their examination, you would have thought, not only they were fingering the very gold, but were at sea with it, besides, in safety.

‘Yes,’ said one, ‘that’s Flint, sure enough. J. F., and a score below, with a clove hitch to it; so he done ever.’

‘Mighty pretty,’ said George. ‘But how are we to get away with it, and us no ship.’

Silver suddenly sprang up, and supporting himself with a hand against the wall: ‘Now I give you warning, George,’ he cried. ‘One more word of your sauce, and I’ll call you down and fight you. How? Why, how do I know? You had ought to tell me that—you and the rest, that lost me my schooner, with your interference, burn you! But not you, you can’t; you hain’t got the invention of a cockroach. But civil you can speak, and shall, George Merry, you may lay to that.’

‘That’s fair enow,’ said the old man Morgan.

‘Fair! I reckon so,’ said the sea-cook. ‘You lost the ship; I found the treasure. Who’s the better man at that? And now I resign, by thunder! Elect whom you please to be your cap’n now; I’m done with it.’

‘Silver!’ they cried. ‘Barbecue forever! Barbecue for cap’n!’

‘So that’s the toon, is it?’ cried the cook. ‘George, I reckon you’ll have to wait another turn, friend; and lucky for you as I’m not a revengeful man. But that was never my way. And now, shipmates, this black spot? ‘Tain’t much good now, is it? Dick’s crossed his luck and spoiled his Bible, and that’s about all.’

## *Treasure Island*

‘It’ll do to kiss the book on still, won’t it?’ growled Dick, who was evidently uneasy at the curse he had brought upon himself.

‘A Bible with a bit cut out!’ returned Silver derisively.  
‘Not it. It don’t bind no more’n a ballad-book.’

‘Don’t it, though?’ cried Dick with a sort of joy. ‘Well, I reckon that’s worth having too.’

‘Here, Jim—here’s a cur’osity for you,’ said Silver, and he tossed me the paper.

It was around about the size of a crown piece. One side was blank, for it had been the last leaf; the other contained a verse or two of Revelation—these words among the rest, which struck sharply home upon my mind: ‘Without are dogs and murderers.’ The printed side had been blackened with wood ash, which already began to come off and soil my fingers; on the blank side had been written with the same material the one word ‘Deposed.’ I have that curiosity beside me at this moment, but not a trace of writing now remains beyond a single scratch, such as a man might make with his thumb-nail.

That was the end of the night’s business. Soon after, with a drink all round, we lay down to sleep, and the outside of Silver’s vengeance was to put George Merry up

for sentinel and threaten him with death if he should prove unfaithful.

It was long ere I could close an eye, and heaven knows I had matter enough for thought in the man whom I had slain that afternoon, in my own most perilous position, and above all, in the remarkable game that I saw Silver now engaged upon—keeping the mutineers together with one hand and grasping with the other after every means, possible and impossible, to make his peace and save his miserable life. He himself slept peacefully and snored aloud, yet my heart was sore for him, wicked as he was, to think on the dark perils that environed and the shameful gibbet that awaited him.

**30**

## **On Parole**

I WAS wakened—indeed, we were all wakened, for I could see even the sentinel shake himself together from where he had fallen against the door-post—by a clear, hearty voice hailing us from the margin of the wood:

‘Block house, ahoy!’ it cried. ‘Here’s the doctor.’

And the doctor it was. Although I was glad to hear the sound, yet my gladness was not without admixture. I remembered with confusion my insubordinate and stealthy conduct, and when I saw where it had brought me—among what companions and surrounded by what dangers—I felt ashamed to look him in the face.

He must have risen in the dark, for the day had hardly come; and when I ran to a loophole and looked out, I saw him standing, like Silver once before, up to the mid-leg in creeping vapour.

‘You, doctor! Top o’ the morning to you, sir!’ cried Silver, broad awake and beaming with good nature in a moment. ‘Bright and early, to be sure; and it’s the early bird, as the saying goes, that gets the rations. George,

shake up your timbers, son, and help Dr. Livesey over the ship's side. All a-doin' well, your patients was—all well and merry.'

So he pattered on, standing on the hilltop with his crutch under his elbow and one hand upon the side of the log-house —quite the old John in voice, manner, and expression.

'We've quite a surprise for you too, sir,' he continued. 'We've a little stranger here—he! he! A noo boarder and lodger, sir, and looking fit and taut as a fiddle; slep' like a supercargo, he did, right alongside of John—stem to stem we was, all night.'

Dr. Livesey was by this time across the stockade and pretty near the cook, and I could hear the alteration in his voice as he said, 'Not Jim?'

'The very same Jim as ever was,' says Silver.

The doctor stopped outright, although he did not speak, and it was some seconds before he seemed able to move on.

'Well, well,' he said at last, 'duty first and pleasure afterwards, as you might have said yourself, Silver. Let us overhaul these patients of yours.'

A moment afterwards he had entered the block house and with one grim nod to me proceeded with his work

among the sick. He seemed under no apprehension, though he must have known that his life, among these treacherous demons, depended on a hair; and he rattled on to his patients as if he were paying an ordinary professional visit in a quiet English family. His manner, I suppose, reacted on the men, for they behaved to him as if nothing had occurred, as if he were still ship's doctor and they still faithful hands before the mast.

'You're doing well, my friend,' he said to the fellow with the bandaged head, 'and if ever any person had a close shave, it was you; your head must be as hard as iron. Well, George, how goes it? You're a pretty colour, certainly; why, your liver, man, is upside down. Did you take that medicine? Did he take that medicine, men?'

'Aye, aye, sir, he took it, sure enough,' returned Morgan.

'Because, you see, since I am mutineers' doctor, or prison doctor as I prefer to call it,' says Doctor Livesey in his pleasantest way, 'I make it a point of honour not to lose a man for King George (God bless him!) and the gallows.'

The rogues looked at each other but swallowed the home-thrust in silence.

'Dick don't feel well, sir,' said one.

‘Don’t he?’ replied the doctor. ‘Well, step up here, Dick, and let me see your tongue. No, I should be surprised if he did! The man’s tongue is fit to frighten the French. Another fever.’

‘Ah, there,’ said Morgan, ‘that comed of sp’iling Bibles.’

‘That comes—as you call it—of being arrant asses,’ retorted the doctor, ‘and not having sense enough to know honest air from poison, and the dry land from a vile, pestiferous slough. I think it most probable— though of course it’s only an opinion—that you’ll all have the deuce to pay before you get that malaria out of your systems. Camp in a bog, would you? Silver, I’m surprised at you. You’re less of a fool than many, take you all round; but you don’t appear to me to have the rudiments of a notion of the rules of health.

‘Well,’ he added after he had dosed them round and they had taken his prescriptions, with really laughable humility, more like charity schoolchildren than blood-guilty mutineers and pirates—‘well, that’s done for today. And now I should wish to have a talk with that boy, please.’

And he nodded his head in my direction carelessly.

George Merry was at the door, spitting and spluttering over some bad-tasted medicine; but at the first word of the doctor's proposal he swung round with a deep flush and cried 'No!' and swore.

Silver struck the barrel with his open hand.

'Si-lence!' he roared and looked about him positively like a lion. 'Doctor,' he went on in his usual tones, 'I was a-thinking of that, knowing as how you had a fancy for the boy. We're all humbly grateful for your kindness, and as you see, puts faith in you and takes the drugs down like that much grog. And I take it I've found a way as'll suit all. Hawkins, will you give me your word of honour as a young gentleman—for a young gentleman you are, although poor born—your word of honour not to slip your cable?'

I readily gave the pledge required.

'Then, doctor,' said Silver, 'you just step outside o' that stockade, and once you're there I'll bring the boy down on the inside, and I reckon you can yarn through the spars. Good day to you, sir, and all our dooties to the squire and Cap'n Smollett.'

The explosion of disapproval, which nothing but Silver's black looks had restrained, broke out immediately the doctor had left the house. Silver was roundly accused

of playing double—of trying to make a separate peace for himself, of sacrificing the interests of his accomplices and victims, and, in one word, of the identical, exact thing that he was doing. It seemed to me so obvious, in this case, that I could not imagine how he was to turn their anger. But he was twice the man the rest were, and his last night's victory had given him a huge preponderance on their minds. He called them all the fools and dolts you can imagine, said it was necessary I should talk to the doctor, fluttered the chart in their faces, asked them if they could afford to break the treaty the very day they were bound a-treasure-hunting.

'No, by thunder!' he cried. 'It's us must break the treaty when the time comes; and till then I'll gammon that doctor, if I have to ile his boots with brandy.'

And then he bade them get the fire lit, and stalked out upon his crutch, with his hand on my shoulder, leaving them in a disarray, and silenced by his volubility rather than convinced.

'Slow, lad, slow,' he said. 'They might round upon us in a twinkle of an eye if we was seen to hurry.'

Very deliberately, then, did we advance across the sand to where the doctor awaited us on the other side of

the stockade, and as soon as we were within easy speaking distance Silver stopped.

‘You’ll make a note of this here also, doctor,’ says he, ‘and the boy’ll tell you how I saved his life, and were deposed for it too, and you may lay to that. Doctor, when a man’s steering as near the wind as me—playing chuck-farthing with the last breath in his body, like—you wouldn’t think it too much, mayhap, to give him one good word? You’ll please bear in mind it’s not my life only now—it’s that boy’s into the bargain; and you’ll speak me fair, doctor, and give me a bit o’ hope to go on, for the sake of mercy.’

Silver was a changed man once he was out there and had his back to his friends and the block house; his cheeks seemed to have fallen in, his voice trembled; never was a soul more dead in earnest.

‘Why, John, you’re not afraid?’ asked Dr. Livesey.

‘Doctor, I’m no coward; no, not I—not SO much!’ and he snapped his fingers. ‘If I was I wouldn’t say it. But I’ll own up fairly, I’ve the shakes upon me for the gallows. You’re a good man and a true; I never seen a better man! And you’ll not forget what I done good, not any more than you’ll forget the bad, I know. And I step aside—see

here—and leave you and Jim alone. And you'll put that down for me too, for it's a long stretch, is that!&#x2019;

So saying, he stepped back a little way, till he was out of earshot, and there sat down upon a tree-stump and began to whistle, spinning round now and again upon his seat so as to command a sight, sometimes of me and the doctor and sometimes of his unruly ruffians as they went to and fro in the sand between the fire—which they were busy rekindling—and the house, from which they brought forth pork and bread to make the breakfast.

‘So, Jim,’ said the doctor sadly, ‘here you are. As you have brewed, so shall you drink, my boy. Heaven knows, I cannot find it in my heart to blame you, but this much I will say, be it kind or unkind: when Captain Smollett was well, you dared not have gone off; and when he was ill and couldn’t help it, by George, it was downright cowardly!’

I will own that I here began to weep. ‘Doctor,’ I said, ‘you might spare me. I have blamed myself enough; my life’s forfeit anyway, and I should have been dead by now if Silver hadn’t stood for me; and doctor, believe this, I can die—and I dare say I deserve it—but what I fear is torture. If they come to torture me—‘

‘Jim,’ the doctor interrupted, and his voice was quite changed, ‘Jim, I can’t have this. Whip over, and we’ll run for it.’

‘Doctor,’ said I, ‘I passed my word.’

‘I know, I know,’ he cried. ‘We can’t help that, Jim, now. I’ll take it on my shoulders, holus bolus, blame and shame, my boy; but stay here, I cannot let you. Jump! One jump, and you’re out, and we’ll run for it like antelopes.’

‘No,’ I replied; ‘you know right well you wouldn’t do the thing yourself—neither you nor squire nor captain; and no more will I. Silver trusted me; I passed my word, and back I go. But, doctor, you did not let me finish. If they come to torture me, I might let slip a word of where the ship is, for I got the ship, part by luck and part by risking, and she lies in North Inlet, on the southern beach, and just below high water. At half tide she must be high and dry.’

‘The ship!’ exclaimed the doctor.

Rapidly I described to him my adventures, and he heard me out in silence.

‘There is a kind of fate in this,’ he observed when I had done. ‘Every step, it’s you that saves our lives; and do you suppose by any chance that we are going to let you lose yours? That would be a poor return, my boy. You

found out the plot; you found Ben Gunn—the best deed that ever you did, or will do, though you live to ninety. Oh, by Jupiter, and talking of Ben Gunn! Why, this is the mischief in person. Silver!' he cried. 'Silver! I'll give you a piece of advice,' he continued as the cook drew near again; 'don't you be in any great hurry after that treasure.'

'Why, sir, I do my possible, which that ain't,' said Silver. 'I can only, asking your pardon, save my life and the boy's by seeking for that treasure; and you may lay to that.'

'Well, Silver,' replied the doctor, 'if that is so, I'll go one step further: look out for squalls when you find it.'

'Sir,' said Silver, 'as between man and man, that's too much and too little. What you're after, why you left the block house, why you given me that there chart, I don't know, now, do I? And yet I done your bidding with my eyes shut and never a word of hope! But no, this here's too much. If you won't tell me what you mean plain out, just say so and I'll leave the helm.'

'No,' said the doctor musingly; 'I've no right to say more; it's not my secret, you see, Silver, or, I give you my word, I'd tell it you. But I'll go as far with you as I dare go, and a step beyond, for I'll have my wig sorted by the captain or I'm mistaken! And first, I'll give you a bit of

## *Treasure Island*

hope; Silver, if we both get alive out of this wolf-trap, I'll do my best to save you, short of perjury.'

Silver's face was radiant. 'You couldn't say more, I'm sure, sir, not if you was my mother,' he cried.

'Well, that's my first concession,' added the doctor. 'My second is a piece of advice: keep the boy close beside you, and when you need help, halloo. I'm off to seek it for you, and that itself will show you if I speak at random. Good-bye, Jim.'

And Dr. Livesey shook hands with me through the stockade, nodded to Silver, and set off at a brisk pace into the wood.

## The Treasure-hunt—Flint's Pointer

‘JIM,’ said Silver when we were alone, ‘if I saved your life, you saved mine; and I’ll not forget it. I seen the doctor waving you to run for it—with the tail of my eye, I did; and I seen you say no, as plain as hearing. Jim, that’s one to you. This is the first glint of hope I had since the attack failed, and I owe it you. And now, Jim, we’re to go in for this here treasure-hunting, with sealed orders too, and I don’t like it; and you and me must stick close, back to back like, and we’ll save our necks in spite o’ fate and fortune.’

Just then a man hailed us from the fire that breakfast was ready, and we were soon seated here and there about the sand over biscuit and fried junk. They had lit a fire fit to roast an ox, and it was now grown so hot that they could only approach it from the windward, and even there not without precaution. In the same wasteful spirit, they had cooked, I suppose, three times more than we could eat; and one of them, with an empty laugh, threw what was left into the fire, which blazed and roared again over

this unusual fuel. I never in my life saw men so careless of the morrow; hand to mouth is the only word that can describe their way of doing; and what with wasted food and sleeping sentries, though they were bold enough for a brush and be done with it, I could see their entire unfitness for anything like a prolonged campaign.

Even Silver, eating away, with Captain Flint upon his shoulder, had not a word of blame for their recklessness. And this the more surprised me, for I thought he had never shown himself so cunning as he did then.

‘Aye, mates,’ said he, ‘it’s lucky you have Barbecue to think for you with this here head. I got what I wanted, I did. Sure enough, they have the ship. Where they have it, I don’t know yet; but once we hit the treasure, we’ll have to jump about and find out. And then, mates, us that has the boats, I reckon, has the upper hand.’

Thus he kept running on, with his mouth full of the hot bacon; thus he restored their hope and confidence, and, I more than suspect, repaired his own at the same time.

‘As for hostage,’ he continued, ‘that’s his last talk, I guess, with them he loves so dear. I’ve got my piece o’ news, and thanky to him for that; but it’s over and done. I’ll take him in a line when we go treasure-hunting, for we’ll keep him like so much gold, in case of accidents,

you mark, and in the meantime. Once we got the ship and treasure both and off to sea like jolly companions, why then we'll talk Mr. Hawkins over, we will, and we'll give him his share, to be sure, for all his kindness.'

It was no wonder the men were in a good humour now. For my part, I was horribly cast down. Should the scheme he had now sketched prove feasible, Silver, already doubly a traitor, would not hesitate to adopt it. He had still a foot in either camp, and there was no doubt he would prefer wealth and freedom with the pirates to a bare escape from hanging, which was the best he had to hope on our side.

Nay, and even if things so fell out that he was forced to keep his faith with Dr. Livesey, even then what danger lay before us! What a moment that would be when the suspicions of his followers turned to certainty and he and I should have to fight for dear life—he a cripple and I a boy—against five strong and active seamen!

Add to this double apprehension the mystery that still hung over the behaviour of my friends, their unexplained desertion of the stockade, their inexplicable cession of the chart, or harder still to understand, the doctor's last warning to Silver, 'Look out for squalls when you find it,' and you will readily believe how little taste I found in my

breakfast and with how uneasy a heart I set forth behind my captors on the quest for treasure.

We made a curious figure, had anyone been there to see us—all in soiled sailor clothes and all but me armed to the teeth. Silver had two guns slung about him—one before and one behind—besides the great cutlass at his waist and a pistol in each pocket of his square-tailed coat. To complete his strange appearance, Captain Flint sat perched upon his shoulder and gabbling odds and ends of purposeless sea-talk. I had a line about my waist and followed obediently after the sea-cook, who held the loose end of the rope, now in his free hand, now between his powerful teeth. For all the world, I was led like a dancing bear.

The other men were variously burthened, some carrying picks and shovels—for that had been the very first necessary they brought ashore from the HISPANIOLA— others laden with pork, bread, and brandy for the midday meal. All the stores, I observed, came from our stock, and I could see the truth of Silver's words the night before. Had he not struck a bargain with the doctor, he and his mutineers, deserted by the ship, must have been driven to subsist on clear water and the proceeds of their hunting. Water would have been little to

their taste; a sailor is not usually a good shot; and besides all that, when they were so short of eatables, it was not likely they would be very flush of powder.

Well, thus equipped, we all set out—even the fellow with the broken head, who should certainly have kept in shadow—and straggled, one after another, to the beach, where the two gigs awaited us. Even these bore trace of the drunken folly of the pirates, one in a broken thwart, and both in their muddy and unbailed condition. Both were to be carried along with us for the sake of safety; and so, with our numbers divided between them, we set forth upon the bosom of the anchorage.

As we pulled over, there was some discussion on the chart. The red cross was, of course, far too large to be a guide; and the terms of the note on the back, as you will hear, admitted of some ambiguity. They ran, the reader may remember, thus:

Tall tree, Spy-glass shoulder, bearing a point to  
the N. of N.N.E.  
Skeleton Island E.S.E. and by E.  
Ten feet.

A tall tree was thus the principal mark. Now, right before us the anchorage was bounded by a plateau from two to three hundred feet high, adjoining on the north the

sloping southern shoulder of the Spy-glass and rising again towards the south into the rough, cliffy eminence called the Mizzen-mast Hill. The top of the plateau was dotted thickly with pine-trees of varying height. Every here and there, one of a different species rose forty or fifty feet clear above its neighbours, and which of these was the particular ‘tall tree’ of Captain Flint could only be decided on the spot, and by the readings of the compass.

Yet, although that was the case, every man on board the boats had picked a favourite of his own ere we were half-way over, Long John alone shrugging his shoulders and bidding them wait till they were there.

We pulled easily, by Silver’s directions, not to weary the hands prematurely, and after quite a long passage, landed at the mouth of the second river—that which runs down a woody cleft of the Spy-glass. Thence, bending to our left, we began to ascend the slope towards the plateau.

At the first outset, heavy, miry ground and a matted, marish vegetation greatly delayed our progress; but by little and little the hill began to steepen and become stony under foot, and the wood to change its character and to grow in a more open order. It was, indeed, a most pleasant portion of the island that we were now approaching. A heavy-scented broom and many flowering shrubs had

almost taken the place of grass. Thickets of green nutmeg-trees were dotted here and there with the red columns and the broad shadow of the pines; and the first mingled their spice with the aroma of the others. The air, besides, was fresh and stirring, and this, under the sheer sunbeams, was a wonderful refreshment to our senses.

The party spread itself abroad, in a fan shape, shouting and leaping to and fro. About the centre, and a good way behind the rest, Silver and I followed—I tethered by my rope, he ploughing, with deep pants, among the sliding gravel. From time to time, indeed, I had to lend him a hand, or he must have missed his footing and fallen backward down the hill.

We had thus proceeded for about half a mile and were approaching the brow of the plateau when the man upon the farthest left began to cry aloud, as if in terror. Shout after shout came from him, and the others began to run in his direction.

‘He can’t ‘a found the treasure,’ said old Morgan, hurrying past us from the right, ‘for that’s clean a-top.’

Indeed, as we found when we also reached the spot, it was something very different. At the foot of a pretty big pine and involved in a green creeper, which had even partly lifted some of the smaller bones, a human skeleton

lay, with a few shreds of clothing, on the ground. I believe a chill struck for a moment to every heart.

‘He was a seaman,’ said George Merry, who, bolder than the rest, had gone up close and was examining the rags of clothing. ‘Leastways, this is good sea-cloth.’

‘Aye, aye,’ said Silver; ‘like enough; you wouldn’t look to find a bishop here, I reckon. But what sort of a way is that for bones to lie? ‘Tain’t in natur’.’

Indeed, on a second glance, it seemed impossible to fancy that the body was in a natural position. But for some disarray (the work, perhaps, of the birds that had fed upon him or of the slow-growing creeper that had gradually enveloped his remains) the man lay perfectly straight—his feet pointing in one direction, his hands, raised above his head like a diver’s, pointing directly in the opposite.

‘I’ve taken a notion into my old numbskull,’ observed Silver. ‘Here’s the compass; there’s the tip-top p’int o’ Skeleton Island, stickin’ out like a tooth. Just take a bearing, will you, along the line of them bones.’

It was done. The body pointed straight in the direction of the island, and the compass read duly E.S.E. and by E.

‘I thought so,’ cried the cook; ‘this here is a p’inter. Right up there is our line for the Pole Star and the jolly

dollars. But, by thunder! If it don't make me cold inside to think of Flint. This is one of HIS jokes, and no mistake. Him and these six was alone here; he killed 'em, every man; and this one he hauled here and laid down by compass, shiver my timbers! They're long bones, and the hair's been yellow. Aye, that would be Allardyce. You mind Allardyce, Tom Morgan?"

'Aye, aye,' returned Morgan; 'I mind him; he owed me money, he did, and took my knife ashore with him.'

'Speaking of knives,' said another, 'why don't we find his'n lying round? Flint warn't the man to pick a seaman's pocket; and the birds, I guess, would leave it be.'

'By the powers, and that's true!' cried Silver.

'There ain't a thing left here,' said Merry, still feeling round among the bones; 'not a copper doit nor a baccy box. It don't look nat'ral to me.'

'No, by gum, it don't,' agreed Silver; 'not nat'ral, nor not nice, says you. Great guns! Messmates, but if Flint was living, this would be a hot spot for you and me. Six they were, and six are we; and bones is what they are now.'

‘I saw him dead with these here deadlights,’ said Morgan. ‘Billy took me in. There he laid, with penny-pieces on his eyes.’

‘Dead—aye, sure enough he’s dead and gone below,’ said the fellow with the bandage; ‘but if ever sperrit walked, it would be Flint’s. Dear heart, but he died bad, did Flint!’

‘Aye, that he did,’ observed another; ‘now he raged, and now he hollered for the rum, and now he sang. ‘Fifteen Men’ were his only song, mates; and I tell you true, I never rightly liked to hear it since. It was main hot, and the windy was open, and I hear that old song comin’ out as clear as clear—and the death-haul on the man already.’

‘Come, come,’ said Silver; ‘stow this talk. He’s dead, and he don’t walk, that I know; leastways, he won’t walk by day, and you may lay to that. Care killed a cat. Fetch ahead for the doubloons.’

We started, certainly; but in spite of the hot sun and the staring daylight, the pirates no longer ran separate and shouting through the wood, but kept side by side and spoke with bated breath. The terror of the dead buccaneer had fallen on their spirits.

## The Treasure-hunt—The Voice Among the Trees

PARTLY from the damping influence of this alarm, partly to rest Silver and the sick folk, the whole party sat down as soon as they had gained the brow of the ascent.

The plateau being somewhat tilted towards the west, this spot on which we had paused commanded a wide prospect on either hand. Before us, over the tree-tops, we beheld the Cape of the Woods fringed with surf; behind, we not only looked down upon the anchorage and Skeleton Island, but saw—clear across the spit and the eastern lowlands—a great field of open sea upon the east. Sheer above us rose the Spy-glass, here dotted with single pines, there black with precipices. There was no sound but that of the distant breakers, mounting from all round, and the chirp of countless insects in the brush. Not a man, not a sail, upon the sea; the very largeness of the view increased the sense of solitude.

Silver, as he sat, took certain bearings with his compass.

## Treasure Island

‘There are three ‘tall trees’’ said he, ‘about in the right line from Skeleton Island. ‘Spy-glass shoulder,’ I take it, means that lower p’int there. It’s child’s play to find the stuff now. I’ve half a mind to dine first.’

‘I don’t feel sharp,’ growled Morgan. ‘Thinkin’ o’ Flint—I think it were—as done me.’

‘Ah, well, my son, you praise your stars he’s dead,’ said Silver.

‘He were an ugly devil,’ cried a third pirate with a shudder; ‘that blue in the face too!’

‘That was how the rum took him,’ added Merry. ‘Blue! Well, I reckon he was blue. That’s a true word.’

Ever since they had found the skeleton and got upon this train of thought, they had spoken lower and lower, and they had almost got to whispering by now, so that the sound of their talk hardly interrupted the silence of the wood. All of a sudden, out of the middle of the trees in front of us, a thin, high, trembling voice struck up the well-known air and words:

‘Fifteen men on the dead man’s chest—  
Yo-ho-ho, and a bottle of rum!’

I never have seen men more dreadfully affected than the pirates. The colour went from their six faces like

enchantment; some leaped to their feet, some clawed hold of others; Morgan grovelled on the ground.

‘It’s Flint, by ——!’ cried Merry.

The song had stopped as suddenly as it began—broken off, you would have said, in the middle of a note, as though someone had laid his hand upon the singer’s mouth. Coming through the clear, sunny atmosphere among the green tree-tops, I thought it had sounded airily and sweetly; and the effect on my companions was the stranger.

‘Come,’ said Silver, struggling with his ashen lips to get the word out; ‘this won’t do. Stand by to go about. This is a rum start, and I can’t name the voice, but it’s someone skylarking—someone that’s flesh and blood, and you may lay to that.’

His courage had come back as he spoke, and some of the colour to his face along with it. Already the others had begun to lend an ear to this encouragement and were coming a little to themselves, when the same voice broke out again—not this time singing, but in a faint distant hail that echoed yet fainter among the clefts of the Spy-glass.

‘Darby M’Graw,’ it wailed—for that is the word that best describes the sound—‘Darby M’Graw! Darby M’Graw!’ again and again and again; and then rising a

little higher, and with an oath that I leave out: ‘Fetch aft the rum, Darby!’

The buccaneers remained rooted to the ground, their eyes starting from their heads. Long after the voice had died away they still stared in silence, dreadfully, before them.

‘That fixes it!’ gasped one. ‘Let’s go.’

‘They was his last words,’ moaned Morgan, ‘his last words above board.’

Dick had his Bible out and was praying volubly. He had been well brought up, had Dick, before he came to sea and fell among bad companions.

Still Silver was unconquered. I could hear his teeth rattle in his head, but he had not yet surrendered.

‘Nobody in this here island ever heard of Darby,’ he muttered; ‘not one but us that’s here.’ And then, making a great effort: ‘Shipmates,’ he cried, ‘I’m here to get that stuff, and I’ll not be beat by man or devil. I never was feared of Flint in his life, and, by the powers, I’ll face him dead. There’s seven hundred thousand pound not a quarter of a mile from here. When did ever a gentleman o’ fortune show his stern to that much dollars for a boozy old seaman with a blue mug—and him dead too?’

But there was no sign of reawakening courage in his followers, rather, indeed, of growing terror at the irreverence of his words.

‘Belay there, John!’ said Merry. ‘Don’t you cross a sperrit.’

And the rest were all too terrified to reply. They would have run away severally had they dared; but fear kept them together, and kept them close by John, as if his daring helped them. He, on his part, had pretty well fought his weakness down.

‘Sperrit? Well, maybe,’ he said. ‘But there’s one thing not clear to me. There was an echo. Now, no man ever seen a sperrit with a shadow; well then, what’s he doing with an echo to him, I should like to know? That ain’t in natur’, surely?’

This argument seemed weak enough to me. But you can never tell what will affect the superstitious, and to my wonder, George Merry was greatly relieved.

‘Well, that’s so,’ he said. ‘You’ve a head upon your shoulders, John, and no mistake. ‘Bout ship, mates! This here crew is on a wrong tack, I do believe. And come to think on it, it was like Flint’s voice, I grant you, but not just so clear-away like it, after all. It was liker somebody else’s voice now—it was liker—‘

‘By the powers, Ben Gunn!’ roared Silver.

‘Aye, and so it were,’ cried Morgan, springing on his knees. ‘Ben Gunn it were!’

‘It don’t make much odds, do it, now?’ asked Dick. ‘Ben Gunn’s not here in the body any more’n Flint.’

But the older hands greeted this remark with scorn.

‘Why, nobody minds Ben Gunn,’ cried Merry; ‘dead or alive, nobody minds him.’

It was extraordinary how their spirits had returned and how the natural colour had revived in their faces. Soon they were chatting together, with intervals of listening; and not long after, hearing no further sound, they shouldered the tools and set forth again, Merry walking first with Silver’s compass to keep them on the right line with Skeleton Island. He had said the truth: dead or alive, nobody minded Ben Gunn.

Dick alone still held his Bible, and looked around him as he went, with fearful glances; but he found no sympathy, and Silver even joked him on his precautions.

‘I told you,’ said he—‘I told you you had sp’iled your Bible. If it ain’t no good to swear by, what do you suppose a sperrit would give for it? Not that!’ and he snapped his big fingers, halting a moment on his crutch.

But Dick was not to be comforted; indeed, it was soon plain to me that the lad was falling sick; hastened by heat, exhaustion, and the shock of his alarm, the fever, predicted by Dr. Livesey, was evidently growing swiftly higher.

It was fine open walking here, upon the summit; our way lay a little downhill, for, as I have said, the plateau tilted towards the west. The pines, great and small, grew wide apart; and even between the clumps of nutmeg and azalea, wide open spaces baked in the hot sunshine. Striking, as we did, pretty near north-west across the island, we drew, on the one hand, ever nearer under the shoulders of the Spy-glass, and on the other, looked ever wider over that western bay where I had once tossed and trembled in the oracle.

The first of the tall trees was reached, and by the bearings proved the wrong one. So with the second. The third rose nearly two hundred feet into the air above a clump of underwood—a giant of a vegetable, with a red column as big as a cottage, and a wide shadow around in which a company could have manoeuvred. It was conspicuous far to sea both on the east and west and might have been entered as a sailing mark upon the chart.

But it was not its size that now impressed my companions; it was the knowledge that seven hundred thousand pounds in gold lay somewhere buried below its spreading shadow. The thought of the money, as they drew nearer, swallowed up their previous terrors. Their eyes burned in their heads; their feet grew speedier and lighter; their whole soul was found up in that fortune, that whole lifetime of extravagance and pleasure, that lay waiting there for each of them.

Silver hobbled, grunting, on his crutch; his nostrils stood out and quivered; he cursed like a madman when the flies settled on his hot and shiny countenance; he plucked furiously at the line that held me to him and from time to time turned his eyes upon me with a deadly look. Certainly he took no pains to hide his thoughts, and certainly I read them like print. In the immediate nearness of the gold, all else had been forgotten: his promise and the doctor's warning were both things of the past, and I could not doubt that he hoped to seize upon the treasure, find and board the HISPANIOLA under cover of night, cut every honest throat about that island, and sail away as he had at first intended, laden with crimes and riches.

Shaken as I was with these alarms, it was hard for me to keep up with the rapid pace of the treasure-hunters.

Now and again I stumbled, and it was then that Silver plucked so roughly at the rope and launched at me his murderous glances. Dick, who had dropped behind us and now brought up the rear, was babbling to himself both prayers and curses as his fever kept rising. This also added to my wretchedness, and to crown all, I was haunted by the thought of the tragedy that had once been acted on that plateau, when that ungodly buccaneer with the blue face —he who died at Savannah, singing and shouting for drink— had there, with his own hand, cut down his six accomplices. This grove that was now so peaceful must then have rung with cries, I thought; and even with the thought I could believe I heard it ringing still.

We were now at the margin of the thicket.

‘Huzza, mates, all together!’ shouted Merry; and the foremost broke into a run.

And suddenly, not ten yards further, we beheld them stop. A low cry arose. Silver doubled his pace, digging away with the foot of his crutch like one possessed; and next moment he and I had come also to a dead halt.

Before us was a great excavation, not very recent, for the sides had fallen in and grass had sprouted on the bottom. In this were the shaft of a pick broken in two and

the boards of several packing-cases strewn around. On one of these boards I saw, branded with a hot iron, the name WALRUS—the name of Flint's ship.

All was clear to probation. The CACHE had been found and rifled; the seven hundred thousand pounds were gone!

## The Fall of a Chieftain

THERE never was such an overturn in this world. Each of these six men was as though he had been struck. But with Silver the blow passed almost instantly. Every thought of his soul had been set full-stretch, like a racer, on that money; well, he was brought up, in a single second, dead; and he kept his head, found his temper, and changed his plan before the others had had time to realize the disappointment.

‘Jim,’ he whispered, ‘take that, and stand by for trouble.’

And he passed me a double-barrelled pistol.

At the same time, he began quietly moving northward, and in a few steps had put the hollow between us two and the other five. Then he looked at me and nodded, as much as to say, ‘Here is a narrow corner,’ as, indeed, I thought it was. His looks were not quite friendly, and I was so revolted at these constant changes that I could not forbear whispering, ‘So you’ve changed sides again.’

There was no time left for him to answer in. The buccaneers, with oaths and cries, began to leap, one after another, into the pit and to dig with their fingers, throwing the boards aside as they did so. Morgan found a piece of gold. He held it up with a perfect spout of oaths. It was a two-guinea piece, and it went from hand to hand among them for a quarter of a minute.

‘Two guineas!’ roared Merry, shaking it at Silver. ‘That’s your seven hundred thousand pounds, is it? You’re the man for bargains, ain’t you? You’re him that never bungled nothing, you wooden-headed lubber!’

‘Dig away, boys,’ said Silver with the coolest insolence; ‘you’ll find some pig-nuts and I shouldn’t wonder.’

‘Pig-nuts!’ repeated Merry, in a scream. ‘Mates, do you hear that? I tell you now, that man there knew it all along. Look in the face of him and you’ll see it wrote there.’

‘Ah, Merry,’ remarked Silver, ‘standing for cap’n again? You’re a pushing lad, to be sure.’

But this time everyone was entirely in Merry’s favour. They began to scramble out of the excavation, darting furious glances behind them. One thing I observed, which

looked well for us: they all got out upon the opposite side from Silver.

Well, there we stood, two on one side, five on the other, the pit between us, and nobody screwed up high enough to offer the first blow. Silver never moved; he watched them, very upright on his crutch, and looked as cool as ever I saw him. He was brave, and no mistake.

At last Merry seemed to think a speech might help matters.

‘Mates,’ says he, ‘there’s two of them alone there; one’s the old cripple that brought us all here and blundered us down to this; the other’s that cub that I mean to have the heart of. Now, mates—‘

He was raising his arm and his voice, and plainly meant to lead a charge. But just then—crack! crack! crack!— three musket-shots flashed out of the thicket. Merry tumbled head foremost into the excavation; the man with the bandage spun round like a teetotum and fell all his length upon his side, where he lay dead, but still twitching; and the other three turned and ran for it with all their might.

Before you could wink, Long John had fired two barrels of a pistol into the struggling Merry, and as the

## Treasure Island

man rolled up his eyes at him in the last agony, ‘George,’ said he, ‘I reckon I settled you.’

At the same moment, the doctor, Gray, and Ben Gunn joined us, with smoking muskets, from among the nutmeg-trees.

‘Forward!’ cried the doctor. ‘Double quick, my lads. We must head ‘em off the boats.’

And we set off at a great pace, sometimes plunging through the bushes to the chest.

I tell you, but Silver was anxious to keep up with us. The work that man went through, leaping on his crutch till the muscles of his chest were fit to burst, was work no sound man ever equalled; and so thinks the doctor. As it was, he was already thirty yards behind us and on the verge of strangling when we reached the brow of the slope.

‘Doctor,’ he hailed, ‘see there! No hurry!’

Sure enough there was no hurry. In a more open part of the plateau, we could see the three survivors still running in the same direction as they had started, right for Mizzen-mast Hill. We were already between them and the boats; and so we four sat down to breathe, while Long John, mopping his face, came slowly up with us.

‘Thank ye kindly, doctor,’ says he. ‘You came in in about the nick, I guess, for me and Hawkins. And so it’s you, Ben Gunn!’ he added. ‘Well, you’re a nice one, to be sure.’

‘I’m Ben Gunn, I am,’ replied the maroon, wriggling like an eel in his embarrassment. ‘And,’ he added, after a long pause, ‘how do, Mr. Silver? Pretty well, I thank ye, says you.’

‘Ben, Ben,’ murmured Silver, ‘to think as you’ve done me!’

The doctor sent back Gray for one of the pick-axes deserted, in their flight, by the mutineers, and then as we proceeded leisurely downhill to where the boats were lying, related in a few words what had taken place. It was a story that profoundly interested Silver; and Ben Gunn, the half-idiot maroon, was the hero from beginning to end.

Ben, in his long, lonely wanderings about the island, had found the skeleton—it was he that had rifled it; he had found the treasure; he had dug it up (it was the haft of his pick-axe that lay broken in the excavation); he had carried it on his back, in many weary journeys, from the foot of the tall pine to a cave he had on the two-pointed hill at the north-east angle of the island, and there it had

laid stored in safety since two months before the arrival of the HISPANIOLA.

When the doctor had wormed this secret from him on the afternoon of the attack, and when next morning he saw the anchorage deserted, he had gone to Silver, given him the chart, which was now useless—given him the stores, for Ben Gunn's cave was well supplied with goats' meat salted by himself—given anything and everything to get a chance of moving in safety from the stockade to the two-pointed hill, there to be clear of malaria and keep a guard upon the money.

'As for you, Jim,' he said, 'it went against my heart, but I did what I thought best for those who had stood by their duty; and if you were not one of these, whose fault was it?'

That morning, finding that I was to be involved in the horrid disappointment he had prepared for the mutineers, he had run all the way to the cave, and leaving the squire to guard the captain, had taken Gray and the maroon and started, making the diagonal across the island to be at hand beside the pine. Soon, however, he saw that our party had the start of him; and Ben Gunn, being fleet of foot, had been dispatched in front to do his best alone. Then it had occurred to him to work upon the

superstitions of his former shipmates, and he was so far successful that Gray and the doctor had come up and were already ambushed before the arrival of the treasure-hunters.

‘Ah,’ said Silver, ‘it were fortunate for me that I had Hawkins here. You would have let old John be cut to bits, and never given it a thought, doctor.’

‘Not a thought,’ replied Dr. Livesey cheerily.

And by this time we had reached the gigs. The doctor, with the pick-axe, demolished one of them, and then we all got aboard the other and set out to go round by sea for North Inlet.

This was a run of eight or nine miles. Silver, though he was almost killed already with fatigue, was set to an oar, like the rest of us, and we were soon skimming swiftly over a smooth sea. Soon we passed out of the straits and doubled the south-east corner of the island, round which, four days ago, we had towed the HISPANIOLA.

As we passed the two-pointed hill, we could see the black mouth of Ben Gunn’s cave and a figure standing by it, leaning on a musket. It was the squire, and we waved a handkerchief and gave him three cheers, in which the voice of Silver joined as heartily as any.

Three miles farther, just inside the mouth of North Inlet, what should we meet but the HISPANIOLA, cruising by herself? The last flood had lifted her, and had there been much wind or a strong tide current, as in the southern anchorage, we should never have found her more, or found her stranded beyond help. As it was, there was little amiss beyond the wreck of the main-sail. Another anchor was got ready and dropped in a fathom and a half of water. We all pulled round again to Rum Cove, the nearest point for Ben Gunn's treasure-house; and then Gray, single-handed, returned with the gig to the HISPANIOLA, where he was to pass the night on guard.

A gentle slope ran up from the beach to the entrance of the cave. At the top, the squire met us. To me he was cordial and kind, saying nothing of my escapade either in the way of blame or praise. At Silver's polite salute he somewhat flushed.

'John Silver,' he said, 'you're a prodigious villain and imposter—a monstrous imposter, sir. I am told I am not to prosecute you. Well, then, I will not. But the dead men, sir, hang about your neck like mill-stones.'

'Thank you kindly, sir,' replied Long John, again saluting.

‘I dare you to thank me!’ cried the squire. ‘It is a gross dereliction of my duty. Stand back.’

And thereupon we all entered the cave. It was a large, airy place, with a little spring and a pool of clear water, overhung with ferns. The floor was sand. Before a big fire lay Captain Smollett; and in a far corner, only duskily flickered over by the blaze, I beheld great heaps of coin and quadrilaterals built of bars of gold. That was Flint’s treasure that we had come so far to seek and that had cost already the lives of seventeen men from the HISPANIOLA. How many it had cost in the amassing, what blood and sorrow, what good ships scuttled on the deep, what brave men walking the plank blindfold, what shot of cannon, what shame and lies and cruelty, perhaps no man alive could tell. Yet there were still three upon that island—Silver, and old Morgan, and Ben Gunn—who had each taken his share in these crimes, as each had hoped in vain to share in the reward.

‘Come in, Jim,’ said the captain. ‘You’re a good boy in your line, Jim, but I don’t think you and me’ll go to sea again. You’re too much of the born favourite for me. Is that you, John Silver? What brings you here, man?’

‘Come back to my dooty, sir,’ returned Silver.

‘Ah!’ said the captain, and that was all he said.

What a supper I had of it that night, with all my friends around me; and what a meal it was, with Ben Gunn's salted goat and some delicacies and a bottle of old wine from the HISPANIOLA. Never, I am sure, were people gayer or happier. And there was Silver, sitting back almost out of the firelight, but eating heartily, prompt to spring forward when anything was wanted, even joining quietly in our laughter—the same bland, polite, obsequious seaman of the voyage out.

## 34 And Last

THE next morning we fell early to work, for the transportation of this great mass of gold near a mile by land to the beach, and thence three miles by boat to the HISPANIOLA, was a considerable task for so small a number of workmen. The three fellows still abroad upon the island did not greatly trouble us; a single sentry on the shoulder of the hill was sufficient to ensure us against any sudden onslaught, and we thought, besides, they had had more than enough of fighting.

Therefore the work was pushed on briskly. Gray and Ben Gunn came and went with the boat, while the rest during their absences piled treasure on the beach. Two of the bars, slung in a rope's end, made a good load for a grown man—one that he was glad to walk slowly with. For my part, as I was not much use at carrying, I was kept busy all day in the cave packing the minted money into bread-bags.

It was a strange collection, like Billy Bones's hoard for the diversity of coinage, but so much larger and so much more varied that I think I never had more pleasure than in

sorting them. English, French, Spanish, Portuguese, Georges, and Louises, doubloons and double guineas and moidores and sequins, the pictures of all the kings of Europe for the last hundred years, strange Oriental pieces stamped with what looked like wisps of string or bits of spider's web, round pieces and square pieces, and pieces bored through the middle, as if to wear them round your neck—nearly every variety of money in the world must, I think, have found a place in that collection; and for number, I am sure they were like autumn leaves, so that my back ached with stooping and my fingers with sorting them out.

Day after day this work went on; by every evening a fortune had been stowed aboard, but there was another fortune waiting for the morrow; and all this time we heard nothing of the three surviving mutineers.

At last—I think it was on the third night—the doctor and I were strolling on the shoulder of the hill where it overlooks the lowlands of the isle, when, from out the thick darkness below, the wind brought us a noise between shrieking and singing. It was only a snatch that reached our ears, followed by the former silence.

‘Heaven forgive them,’ said the doctor; “tis the mutineers!’

‘All drunk, sir,’ struck in the voice of Silver from behind us.

Silver, I should say, was allowed his entire liberty, and in spite of daily rebuffs, seemed to regard himself once more as quite a privileged and friendly dependent. Indeed, it was remarkable how well he bore these slights and with what unwearying politeness he kept on trying to ingratiate himself with all. Yet, I think, none treated him better than a dog, unless it was Ben Gunn, who was still terribly afraid of his old quartermaster, or myself, who had really something to thank him for; although for that matter, I suppose, I had reason to think even worse of him than anybody else, for I had seen him meditating a fresh treachery upon the plateau. Accordingly, it was pretty gruffly that the doctor answered him.

‘Drunk or raving,’ said he.

‘Right you were, sir,’ replied Silver; ‘and precious little odds which, to you and me.’

‘I suppose you would hardly ask me to call you a humane man,’ returned the doctor with a sneer, ‘and so my feelings may surprise you, Master Silver. But if I were sure they were raving—as I am morally certain one, at least, of them is down with fever—I should leave this

camp, and at whatever risk to my own carcass, take them the assistance of my skill.'

'Ask your pardon, sir, you would be very wrong,' quoth Silver. 'You would lose your precious life, and you may lay to that. I'm on your side now, hand and glove; and I shouldn't wish for to see the party weakened, let alone yourself, seeing as I know what I owes you. But these men down there, they couldn't keep their word—no, not supposing they wished to; and what's more, they couldn't believe as you could.'

'No,' said the doctor. 'You're the man to keep your word, we know that.'

Well, that was about the last news we had of the three pirates. Only once we heard a gunshot a great way off and supposed them to be hunting. A council was held, and it was decided that we must desert them on the island —to the huge glee, I must say, of Ben Gunn, and with the strong approval of Gray. We left a good stock of powder and shot, the bulk of the salt goat, a few medicines, and some other necessaries, tools, clothing, a spare sail, a fathom or two of rope, and by the particular desire of the doctor, a handsome present of tobacco.

That was about our last doing on the island. Before that, we had got the treasure stowed and had shipped

enough water and the remainder of the goat meat in case of any distress; and at last, one fine morning, we weighed anchor, which was about all that we could manage, and stood out of North Inlet, the same colours flying that the captain had flown and fought under at the palisade.

The three fellows must have been watching us closer than we thought for, as we soon had proved. For coming through the narrows, we had to lie very near the southern point, and there we saw all three of them kneeling together on a spit of sand, with their arms raised in supplication. It went to all our hearts, I think, to leave them in that wretched state; but we could not risk another mutiny; and to take them home for the gibbet would have been a cruel sort of kindness. The doctor hailed them and told them of the stores we had left, and where they were to find them. But they continued to call us by name and appeal to us, for God's sake, to be merciful and not leave them to die in such a place.

At last, seeing the ship still bore on her course and was now swiftly drawing out of earshot, one of them—I know not which it was—leapt to his feet with a hoarse cry, whipped his musket to his shoulder, and sent a shot whistling over Silver's head and through the main-sail.

## Treasure Island

After that, we kept under cover of the bulwarks, and when next I looked out they had disappeared from the spit, and the spit itself had almost melted out of sight in the growing distance. That was, at least, the end of that; and before noon, to my inexpressible joy, the highest rock of Treasure Island had sunk into the blue round of sea.

We were so short of men that everyone on board had to bear a hand—only the captain lying on a mattress in the stern and giving his orders, for though greatly recovered he was still in want of quiet. We laid her head for the nearest port in Spanish America, for we could not risk the voyage home without fresh hands; and as it was, what with baffling winds and a couple of fresh gales, we were all worn out before we reached it.

It was just at sundown when we cast anchor in a most beautiful land-locked gulf, and were immediately surrounded by shore boats full of Negroes and Mexican Indians and half-bloods selling fruits and vegetables and offering to dive for bits of money. The sight of so many good-humoured faces (especially the blacks), the taste of the tropical fruits, and above all the lights that began to shine in the town made a most charming contrast to our dark and bloody sojourn on the island; and the doctor and the squire, taking me along with them, went ashore to

pass the early part of the night. Here they met the captain of an English man-of-war, fell in talk with him, went on board his ship, and, in short, had so agreeable a time that day was breaking when we came alongside the HISPANIOLA.

Ben Gunn was on deck alone, and as soon as we came on board he began, with wonderful contortions, to make us a confession. Silver was gone. The maroon had connived at his escape in a shore boat some hours ago, and he now assured us he had only done so to preserve our lives, which would certainly have been forfeit if ‘that man with the one leg had stayed aboard.’ But this was not all. The sea-cook had not gone empty-handed. He had cut through a bulkhead unobserved and had removed one of the sacks of coin, worth perhaps three or four hundred guineas, to help him on his further wanderings.

I think we were all pleased to be so cheaply quit of him.

Well, to make a long story short, we got a few hands on board, made a good cruise home, and the HISPANIOLA reached Bristol just as Mr. Blandly was beginning to think of fitting out her consort. Five men only of those who had sailed returned with her. ‘Drink and the devil had done for the rest,’ with a vengeance,

although, to be sure, we were not quite in so bad a case as that other ship they sang about:

With one man of her crew alive,  
What put to sea with seventy-five.

All of us had an ample share of the treasure and used it wisely or foolishly, according to our natures. Captain Smollett is now retired from the sea. Gray not only saved his money, but being suddenly smit with the desire to rise, also studied his profession, and he is now mate and part owner of a fine full-rigged ship, married besides, and the father of a family. As for Ben Gunn, he got a thousand pounds, which he spent or lost in three weeks, or to be more exact, in nineteen days, for he was back begging on the twentieth. Then he was given a lodge to keep, exactly as he had feared upon the island; and he still lives, a great favourite, though something of a butt, with the country boys, and a notable singer in church on Sundays and saints' days.

Of Silver we have heard no more. That formidable seafaring man with one leg has at last gone clean out of my life; but I dare say he met his old Negress, and perhaps still lives in comfort with her and Captain Flint. It is to be hoped so, I suppose, for his chances of comfort in another world are very small.

The bar silver and the arms still lie, for all that I know, where Flint buried them; and certainly they shall lie there for me. Oxen and wain-ropes would not bring me back again to that accursed island; and the worst dreams that ever I have are when I hear the surf booming about its coasts or start upright in bed with the sharp voice of Captain Flint still ringing in my ears: ‘Pieces of eight! Pieces of eight!’