CYBERSECURITY BLUE TEAM TOOLKIT

NADEAN H. TANNER

WILEY

Table of Contents

List of Tables

Chapter 1

Chapter 3

Chapter 4

Chapter 6

Chapter 7

Chapter 9

Chapter 14

List of Illustrations

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 9

Chapter 10

Chapter 11

Chapter 12

Chapter 13

Chapter 14

Chapter 15

Cybersecurity Blue Team Toolkit

Nadean H. Tanner

WILEY

Foreword

The year was 2012 and I took a big leap in my own career to move across the country. I filled a role to lead a three-person team providing information technology and security training to Department of Defense personnel. This leadership role was new to me having worked for the past eight years in the intelligence and information security world for the most part as a trainer. While building out the team in the fall of 2012, I interviewed a wonderful candidate from Louisiana named Nadean Tanner. She was full of personality, charisma, knowledge, and most importantly, she had the ability to train. She proved this as part of her training demonstration in the interview process. I knew she was the right candidate and hired her almost immediately. Hiring Nadean is still one of the best decisions I made, and she is one of the greatest trainers I know. My philosophy is that a great trainer does not simply regurgitate what they know. Rather, they have the ability to explain a topic in different ways so that each learner can comprehend. Nadean embodies this philosophy.

Nadean has trained thousands of learners on topics from hardware to advanced security. In each class, she takes the time and effort to ensure every learner gets what they need. Whether learning a product for performing their job, building out their professional development, or advancing their career with a certification, Nadean covers it all. If you had the opportunity to attend one of her training classes, consider yourself blessed by a great trainer. If you have not, you picked up this book, which is the next best thing. I am glad to see her move to authorship, allowing everyone to experience her ability to explain complicated topics in simple ways.

In the world of cybersecurity we are constantly bombarded with new products, new tools, and new attack techniques. We are pulled daily in multiple directions on what to secure and how to secure it. In this book, Nadean will break down fundamental tools available to you. This includes general IT tools used for troubleshooting, but ones that can also help the security team understand the environment. She will cover tools attackers use, but also empower you and your team to use them to be proactive in your security. Specifically, you as the reader get to enjoy not only Nadean's ability to impart knowledge but her uncanny ability to explain why. Rather than being technical documentation focusing on the how, Nadean will delve into why use the tools and the specific use cases. For many users fresh to the cybersecurity world, this should be considered a getting started guide. For those in the middle of or more senior in their careers, this book will serve as a reference guide you want to have on your desk. It is not a book that makes it to your shelf and collects dust.

Throughout the years I have been Nadean's manager, colleague, peer, and most importantly dear friend. We have shared stories about how we learned, what we learned, and how we passed the information along to our learners. As the owner of this book, you are well on your way to enjoying Nadean's simple yet thorough explanations of advanced security topics. Rather than spending more of your time on reading this foreword, jump into the book to learn, refresh, or hone your cybersecurity skills.

Ryan Hendricks, CISSP

Training Manager, CarbonBlack

Introduction

> **“The more you know, the more you know you don't know.”**
>
> ***—Aristotle***

> **“If you can't explain it simply, you don't understand it well enough.”**
>
> ***—Einstein***

If you have ever been a fisherman or been friends with or related to a fisherman, you know one of their favorite things is their tackle box ... and telling stories. If you ask a question about anything in that tackle box, be prepared to be entertained while you listen to stories of past fishing expeditions, how big was the one that got away, the one that did get caught, and future plans to use certain hooks, feathers, and wiggly things. A great fisherman learns to adapt to the situation they are in, and it takes special knowledge of all the fun things in that tackle box—when and where and how to use them—to be successful in their endeavor.

In cybersecurity, we have our own form of a tackle box. We have our own versions of wiggly things. To be successful, we have to learn when and where and how to use our tools and adapt to the technical situation we find ourselves in. It can take time to develop the expertise to know when to use which tool, and what product to find vulnerabilities, fix them, and, when necessary, catch the bad guys.

There are so many philosophies, frameworks, compliances, and vendors. How do you know when to use which wiggly thing? Once you know which wiggly thing to use, how do you use it? This book will teach you how to apply best-practice cybersecurity strategies and scenarios in a multitude of situations and which open source tools are most beneficial to protect our dynamic and multifaceted environments.

This book will take a simple and strategic look at best practices and readily available tools that are accessible to both cybersecurity management and hands-on professionals—whether they be new to the industry or simply are looking to gain expertise.

CHAPTER 1
Fundamental Networking and Security Tools

WHAT YOU WILL LEARN IN THIS CHAPTER:

- Ping
- IPConfig
- Tracert
- NSLookup
- NetStat
- PuTTY

Before heading off to the cybersecurity conference Black Hat in Las Vegas, a friend of mine, Douglas Brush, posted on his LinkedIn page a warning for other InfoSec professionals. He said, “Don't go to these events to buy curtains for the house when you don't have the concrete for the foundation poured yet.”

Too many times in the many years I've been in information technology (IT), I have seen people forget they need the basics in place before they try to use their shiny new tools. Before you can use any new tools, you must have a foundation to build upon. In IT, these tools are fundamental. They are a must for any computer/InfoSec/analyst to know how to use and when to use them. It's also rather impressive when a manager who you assumed was nontechnical asks you to ping that asset, run a tracert, and discover the physical and logical addresses of the web server that is down. Sometimes they *do* speak your language!

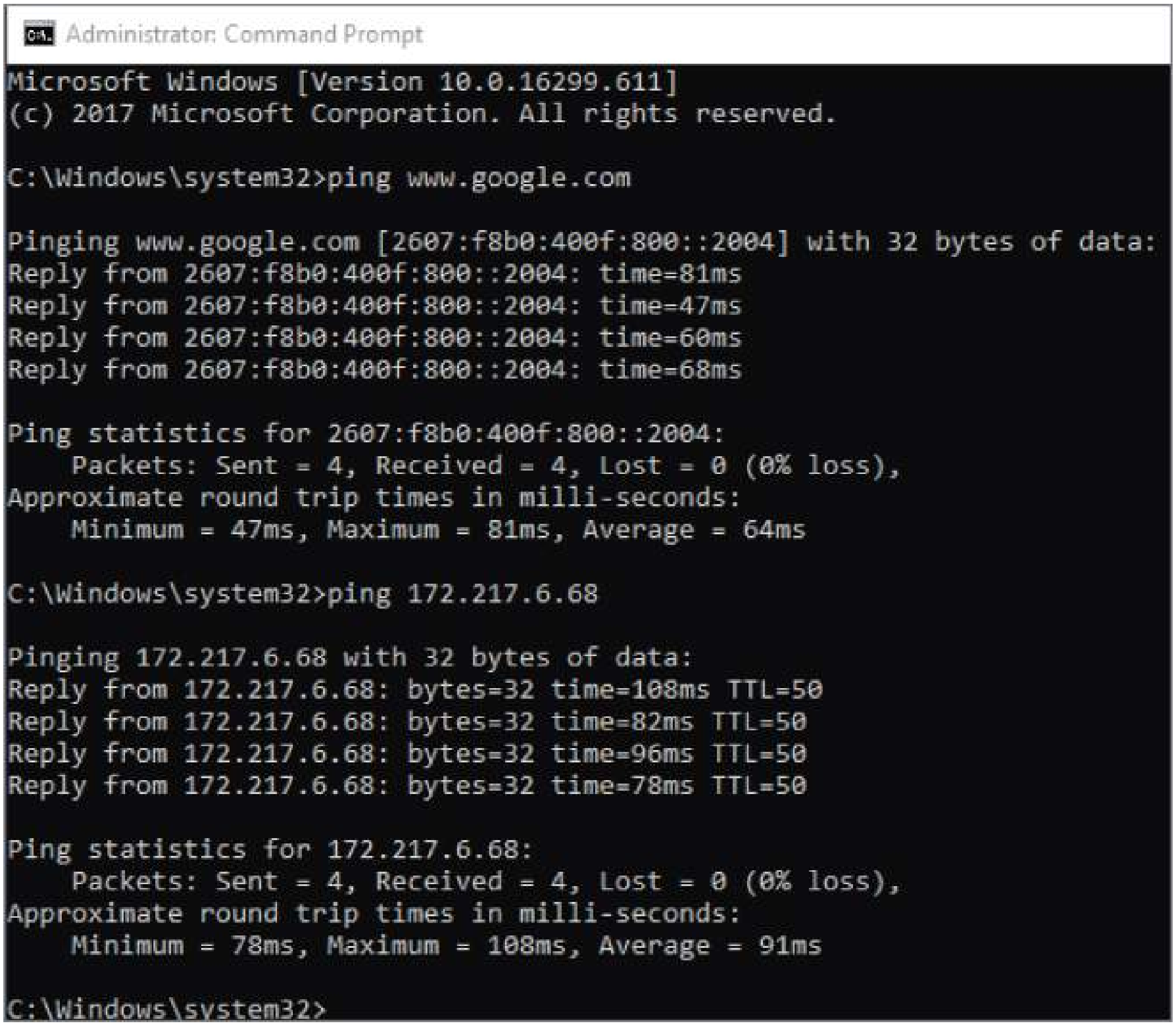
Ping

Ping will make you think one of two things. If it makes you think of irons and drivers and 18 holes of beautiful green fairway, then you are definitely CIO/CEO/CISO material. If it makes you think of submarines or bats, then you're probably geekier like me.

Packet InterNet Groper, or what we affectionately call *ping*, is a networking utility. It is used to test whether a host is “alive” on an Internet Protocol (IP) network. A host is a computer or other device that is connected to a network. It will measure the time it takes for a message sent from one host to reach another and echo back to the original host. Bats are able to use *echo-location*, or bio sonar, to locate and identify objects. We do the same in our networked environments.

Ping will send an Internet Control Message Protocol (ICMP) echo request to the target and wait for a reply. This will report problems, trip time, and packet loss if the asset has a heartbeat. If the asset is not alive, you will get back an ICMP error. The command-line option for ping is easy to use no matter what operating system you are using and comes with multiple options such as the size of the packet, how many requests, and time to live (TTL) in seconds. This field is decremented at each machine where data is processed. The value in this field will be at least as great as the number of gateways it has to hop. Once a connection is made between the two systems, this tool can test the latency or the delay between them.

Figure 1.1 shows a running ping on a Windows operating system sending four echo requests to `www.google.com` using both IPv4 and IPv6.



```
Microsoft Windows [Version 10.0.16299.611]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping www.google.com

Pinging www.google.com [2607:f8b0:400f:800::2004] with 32 bytes of data:
Reply from 2607:f8b0:400f:800::2004: time=81ms
Reply from 2607:f8b0:400f:800::2004: time=47ms
Reply from 2607:f8b0:400f:800::2004: time=60ms
Reply from 2607:f8b0:400f:800::2004: time=68ms

Ping statistics for 2607:f8b0:400f:800::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 47ms, Maximum = 81ms, Average = 64ms

C:\Windows\system32>ping 172.217.6.68

Pinging 172.217.6.68 with 32 bytes of data:
Reply from 172.217.6.68: bytes=32 time=108ms TTL=50
Reply from 172.217.6.68: bytes=32 time=82ms TTL=50
Reply from 172.217.6.68: bytes=32 time=96ms TTL=50
Reply from 172.217.6.68: bytes=32 time=78ms TTL=50

Ping statistics for 172.217.6.68:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 78ms, Maximum = 108ms, Average = 91ms

C:\Windows\system32>
```

Figure 1.1: Running a ping against a URL and IP address

What this figure translates to is that my computer can reach through the network and touch a Google server. The `www.google.com` part of this request is called a *uniform resource locator* (URL). A URL is the address of a page on the World Wide Web (WWW). The numbers you see next to the URL is called an *IP address*. Every device on a network must have a unique IP network address. If you are attempting to echo-locate another host, you could substitute the URL `www.google.com` for an IP address. We will do a deeper dive on IPv4 and IPv6 in Chapter 9, Log Management.

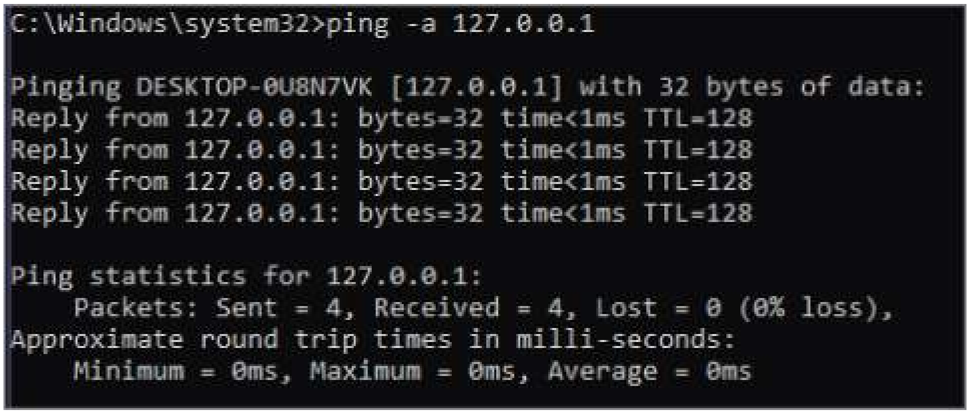
There are more granular `ping` commands. If you type **`ping`** along with an option or switch, you can troubleshoot issues that might be occurring in your network. Sometimes these issues are naturally occurring problems. Sometimes they could signal some type of attack.

Table 1.1 shows different options you can add to the base command `ping`.

Table 1.1: `ping` command syntax

OPTION	MEANING
`/?`	Lists command syntax options.
`-t`	Pings the specified host until stopped with Ctrl+C. `ping-t` is also known as the *ping of death*. It can be used as a denial-of-service (DoS) attack to cause a target machine to crash.
`-a`	Resolves address to hostname if possible.
`-n count`	How many echo requests to send from 1 to 4.2 billion. (In Windows operating systems, 4 is the default.)
`-r count`	Records route for count hops (IPv4 only). The maximum is 9, so if you need more than 9, `tracert` might work better (covered later in the chapter).
`-s count`	Timestamp for count hops (IPv4 only).
`-i TTL`	Time to live; maximum is 255.

Did you know that you could ping yourself? Figure 1.2 shows that 127.0.0.1 is a special reserved IP address. It is traditionally called a *loopback address*. When you ping this IP address, you are testing your own system to make sure it is working properly. If this IP doesn't return an appropriate response, you know the problem is with your system, not the network, the Internet service provider (ISP), or your target URL.



```
C:\Windows\system32>ping -a 127.0.0.1

Pinging DESKTOP-0U8N7VK [127.0.0.1] with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 1.2: Pinging a lookback address

If you are experiencing network difficulties, this is the first tool to pull out of your toolkit. Go ping yourself and make sure everything is working as it should (see Lab 1.1).

LAB 1.1: PING

1. Open a command prompt or a terminal window.
2. Type `ping -t www.example.com` and then press Enter. (You can use another URL or hostname of your choice.)
3. After a few seconds, hold the Ctrl button and press C (abbreviated as Ctrl+C in subsequent instructions in this book).
4. When the command prompt returns, type `ping -a 127.0.0.1` and press Enter.

What is the name of your host? As you can see in Figure 1.2, mine is DESKTOP-OU8N7VK. A hostname is comprised of alphanumeric characters and possibly a hyphen. There may be times in the future you know an IP address but not the hostname or you know a hostname but not the IP address. For certain troubleshooting steps, you will need to be able to resolve the two on a single machine.

IPConfig

The command `ipconfig` is usually the next tool you will pull out of your toolbox when you're networking a system. A lot of valuable knowledge can be gleaned from this tool.

Internet Protocol is a set of rules that govern how data is sent over the Internet or another network. This routing function essentially creates the Internet we know and love.

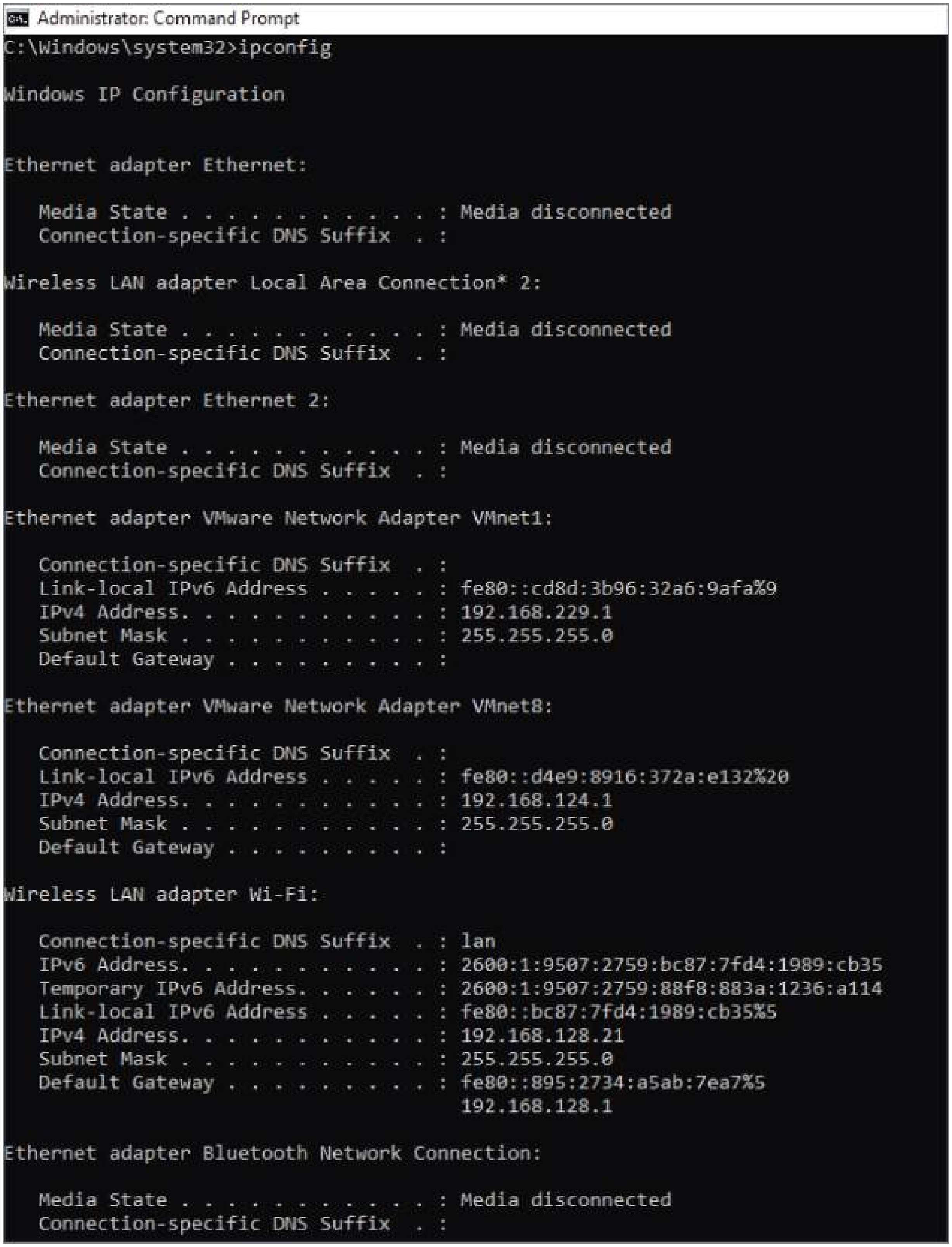
IP has the function of taking packets from the source host and delivering them to the proper destination host based solely on the IP addresses in a packet. The datagram that is being sent has two parts: a header and a payload. The header has the information needed to get the information where it should go. The payload is the stuff you want the other host to have.

In Lab 1.2, you'll use the `ipconfig` command.

LAB 1.2: IPCONFIG

1. Open a command prompt or a terminal window.
2. Type **`ipconfig`** and press Enter if you are on a Windows system. If you are on Linux, try **`ifconfig`**.
3. Scroll through your adapters and note the ones that are for Ethernet or Wi-Fi or Bluetooth.
4. With the preceding steps, you can answer the following questions: Which adapters are connected with an IP address? Which ones are disconnected?
5. At the command prompt, type **`ipconfig /all`** and press Enter.

Now you have a wealth of information to begin your troubleshooting hypothesis. In Figure 1.3, you see the IP addresses and default gateways for each network adapter on the machine.



```
C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::cd8d:3b96:32a6:9afa%9
   IPv4 Address. . . . . . . . . . . : 192.168.229.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d4e9:8916:372a:e132%20
   IPv4 Address. . . . . . . . . . . : 192.168.124.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   IPv6 Address. . . . . . . . . . . : 2600:1:9507:2759:bc87:7fd4:1989:cb35
   Temporary IPv6 Address. . . . . . : 2600:1:9507:2759:88f8:883a:1236:a114
   Link-local IPv6 Address . . . . . : fe80::bc87:7fd4:1989:cb35%5
   IPv4 Address. . . . . . . . . . . : 192.168.128.21
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::895:2734:a5ab:7ea7%5
                                       192.168.128.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Figure 1.3: Using `ipconfig /all`

To find your router's private IP address, look for the default gateway. Think of this machine as a literal gateway that you will use to access the Internet or another network. What tool would you use to make sure that the router is alive? Why, ping of course!

THE INTERNET IS DOWN—NOW WHAT?

The Internet is down.

You ping yourself at 127.0.0.1, and everything is fine on your machine. You ping `www.google.com`, and it times out. You do an `ipconfig /all` on your host machine. What can you assume if your `ipconfig /all` command listed the default gateway as being 0.0.0.0? The router!

As an experienced IT person will tell you, the best thing to do is turn any device off and on again—first your host and then the router. Still not working? Expand your hypothesis to another host on your network—can it reach the Internet or the router? Does it pull an IP address from the router? When you are troubleshooting, it is all about the scientific method. Form a hypothesis, test, modify, and form a new hypothesis.

Here are two more acronyms to add to your IT vernacular: DHCP and DNS. DHCP stands for Dynamic Host Configuration Protocol. Let's isolate each word.

Dynamic: Ever-changing, fluid

Host: Asset on a network

Configuration: How the asset is supposed to work

Protocol: Rules that allow two more assets to talk

DHCP is a network management tool. This is the tool that dynamically assigns an IP address to a host on a network that lets it talk to other hosts. Most simply, a router or a gateway can be used to act as a DHCP server. Most residential routers will get their unique public IP address from their ISP. This is who you write the check to each month.

In a large enterprise, DHCP is configured on servers to handle large networks' IP addressing. DHCP decides which machine gets what IP address and for how long. If your machine is using DHCP, did you notice in your `ipconfig /all` command how long your lease was? If you are not leasing, then you are using a static IP address.

Here are two more commands for you to use if you want a new IP address:

> `ipconfig /release`: This releases all IPv4 addresses.
>
> `ipconfig /renew`: This retrieves a new IP address, which may take a few moments.

DNS is an acronym for Domain Name System. This is a naming system for all hosts that are connected to the Internet or your private network. As you do what you do on the Internet or in a private network, DNS will remember domain names. It will store this data in something we call a *cache* (pronounced "cash"). This is done to speed up subsequent requests to the same host. Sometimes your DNS cache can get all wonky—sometimes by accident, sometimes by a hacker.

NOTE

Cache poisoning—sometimes called *DNS spoofing*—is an attack where a malicious party corrupts the DNS cache or table, causing the nameserver to return an incorrect IP address and network traffic to be diverted.

Here are two more commands to try:

> `ipconfig /displaydns`: This may scroll for a while because this is a record of all the domain names and their IP addresses you have visited on a host.

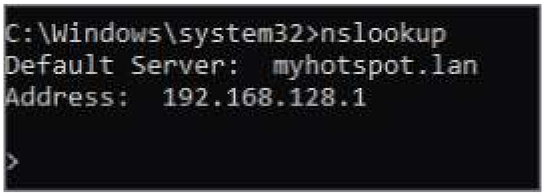
`ipconfig /flushdns`: If you start encountering HTML 404 error codes, you may need to flush your cache clean. This will force your host to query nameservers for the latest and greatest information.

NSLookup

The main use of `nslookup` is to help with any DNS issues you may have. You can use it to find the IP address of a host, find the domain name of an IP address, or find mail servers on a domain. This tool can be used in an interactive and a noninteractive mode. In Lab 1.3, you'll use `nslookup`.

LAB 1.3: NSLOOKUP

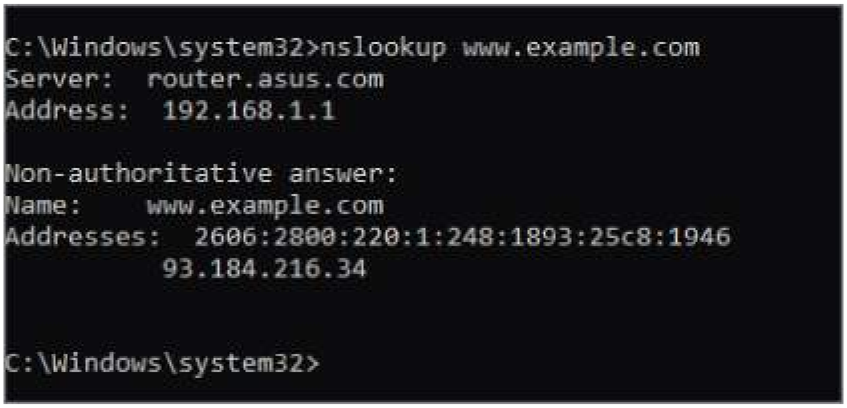
1. Open a command prompt or a terminal window.
2. To work in interactive mode, type **`nslookup`** at the prompt and press Enter. You will get an `nslookup` prompt, as you see in Figure 1.4. To escape the prompt, press Ctrl+C.



```
C:\Windows\system32>nslookup
Default Server:  myhotspot.lan
Address:  192.168.128.1

>
```

Figure 1.4: Using `nslookup`

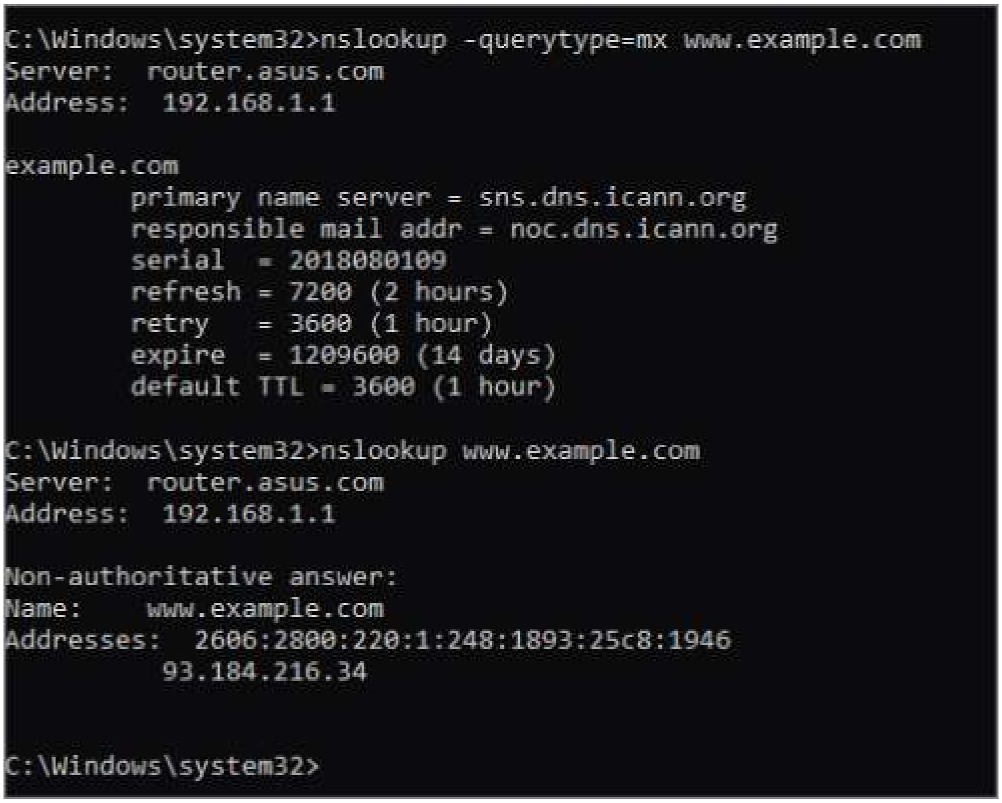
3. To work in noninteractive mode, type **`nslookup www.example.com`** at the prompt to acquire DNS information for the specific site such as Figure 1.5.



```
C:\Windows\system32>nslookup www.example.com
Server:  router.asus.com
Address:  192.168.1.1

Non-authoritative answer:
Name:    www.example.com
Addresses:  2606:2800:220:1:248:1893:25c8:1946
          93.184.216.34


C:\Windows\system32>
```

Figure 1.5: Using `nslookup` on a URL

4. Now try `nslookup` with one of the IP addresses displayed in your terminal window attributed to `www.wiley.com`. This will do a reverse lookup for the IP address and resolve to a domain name.
5. To find specific type assets, you can use **`nslookup -querytype=mx www.example.com`**. In Figure 1.6, you see the result of using `qureytype=mx`.



```
C:\Windows\system32>nslookup -querytype=mx www.example.com
Server:  router.asus.com
Address:  192.168.1.1

example.com
        primary name server = sns.dns.icann.org
        responsible mail addr = noc.dns.icann.org
        serial  = 2018080109
        refresh = 7200 (2 hours)
        retry   = 3600 (1 hour)
        expire  = 1209600 (14 days)
        default TTL = 3600 (1 hour)

C:\Windows\system32>nslookup www.example.com
Server:  router.asus.com
Address:  192.168.1.1

Non-authoritative answer:
Name:    www.example.com
Addresses:  2606:2800:220:1:248:1893:25c8:1946
          93.184.216.34


C:\Windows\system32>
```

Figure 1.6: Using `nslookup` with `-querytype=mx`

Instead of `-querytype=mx`, you can use any of the following:

`HINFO`	Specifies a computer's CPU and type of operating system
`UNIFO`	Specifies the user information
`MB`	Specifies a mailbox domain name
`MG`	Specifies an email group member
`MX`	Specifies the email server

Tracert

So, now you know that all machines that are on a network need to have an IP address. I live in Denver, Colorado, and one of my best friends, Ryan, lives in Albuquerque, New Mexico. When I send him a message, it does not travel from my house through the wires directly to his house. It goes through “hops” (and not the beer kind, unfortunately for him). These hops are the routers between us.

Tracert is a cool diagnostic utility. It will determine the route the message takes from Denver to Albuquerque by using ICMP echo packets sent to the destination. You've seen ICMP in action before—with the `ping` command.

ICMP is one of the Internet's original protocols used by network devices to send operational information or error messages. ICMP is not usually used to send data between computers, with the exception of `ping` and `traceroute`. It is used to report errors in the processing of datagrams.

Each router along the path subtracts the packets TTL value by 1 and forwards the packet, giving you the time and the intermediate routers between you and the destination. Tracert will print the trace of the packet's travels.

Why is this an important part of your toolkit? This is how you find out where a packet gets stopped or blocked on the enterprise network. There may be a router with a configuration issue. Firewalls can be configured to filter packets. Perhaps your website is responding slowly. If packets are being dropped, this will be displayed in the tracert as an asterisk.

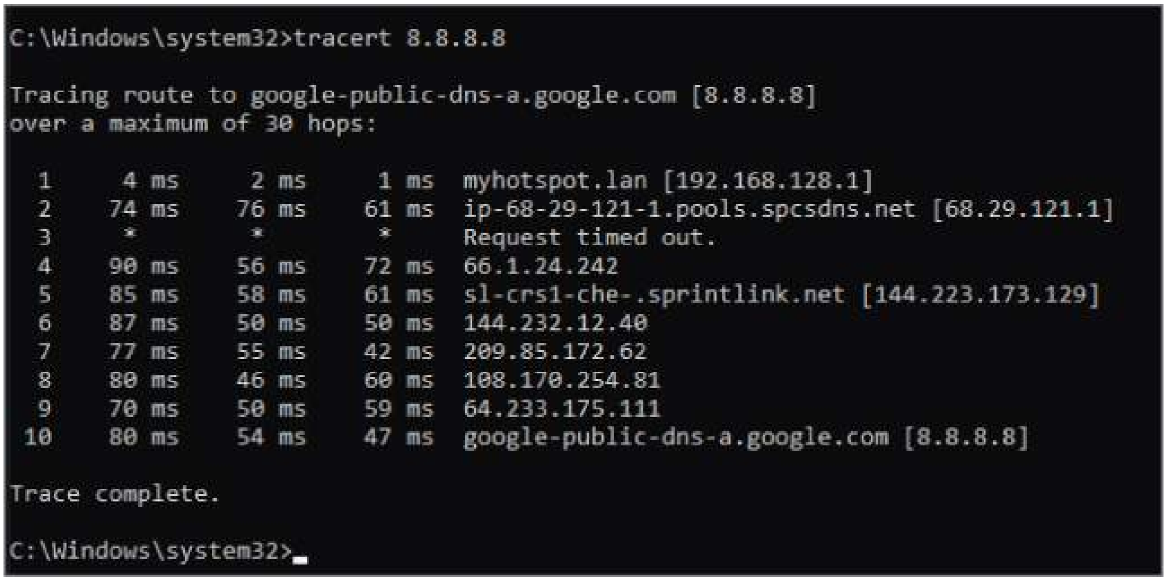
This is a good tool when you have many paths that lead to the same destination but several intermediary routers are involved.

One caveat before Lab 1.4: As I mentioned previously, most of my strengths lie in Windows machines. If you are on a Linux or Mac/Unix-type operating system (OS), then you will want to use the tool `traceroute`. The commands `tracert` and `traceroute` are basically the same thing. The difference lies in which OS you are troubleshooting. If you want to get supremely technical, in Linux the command sends a UDP packet. In Windows, it sends an ICMP echo request.

LAB 1.4: TRACERT

1. Open a command prompt or a terminal window.
2. At the command prompt, type **`tracert 8.8.8.8`** and press Enter.

In Figure 1.7, you can see the hops my machine takes to reach that public Google DNS server. How many hops does yours take?



```
C:\Windows\system32>tracert 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:

  1     4 ms     2 ms     1 ms  myhotspot.lan [192.168.128.1]
  2    74 ms    76 ms    61 ms  ip-68-29-121-1.pools.spcsdns.net [68.29.121.1]
  3     *        *        *     Request timed out.
  4    90 ms    56 ms    72 ms  66.1.24.242
  5    85 ms    58 ms    61 ms  sl-crs1-che-.sprintlink.net [144.223.173.129]
  6    87 ms    50 ms    50 ms  144.232.12.40
  7    77 ms    55 ms    42 ms  209.85.172.62
  8    80 ms    46 ms    60 ms  108.170.254.81
  9    70 ms    50 ms    59 ms  64.233.175.111
 10    80 ms    54 ms    47 ms  google-public-dns-a.google.com [8.8.8.8]

Trace complete.

C:\Windows\system32>_
```

Figure 1.7: Using `tracert`, counting hops

3. Now try **`tracert -d 8.8.4.4`**.

This is another public Google DNS server, but now tracert will not try to resolve DNS while counting the hops.

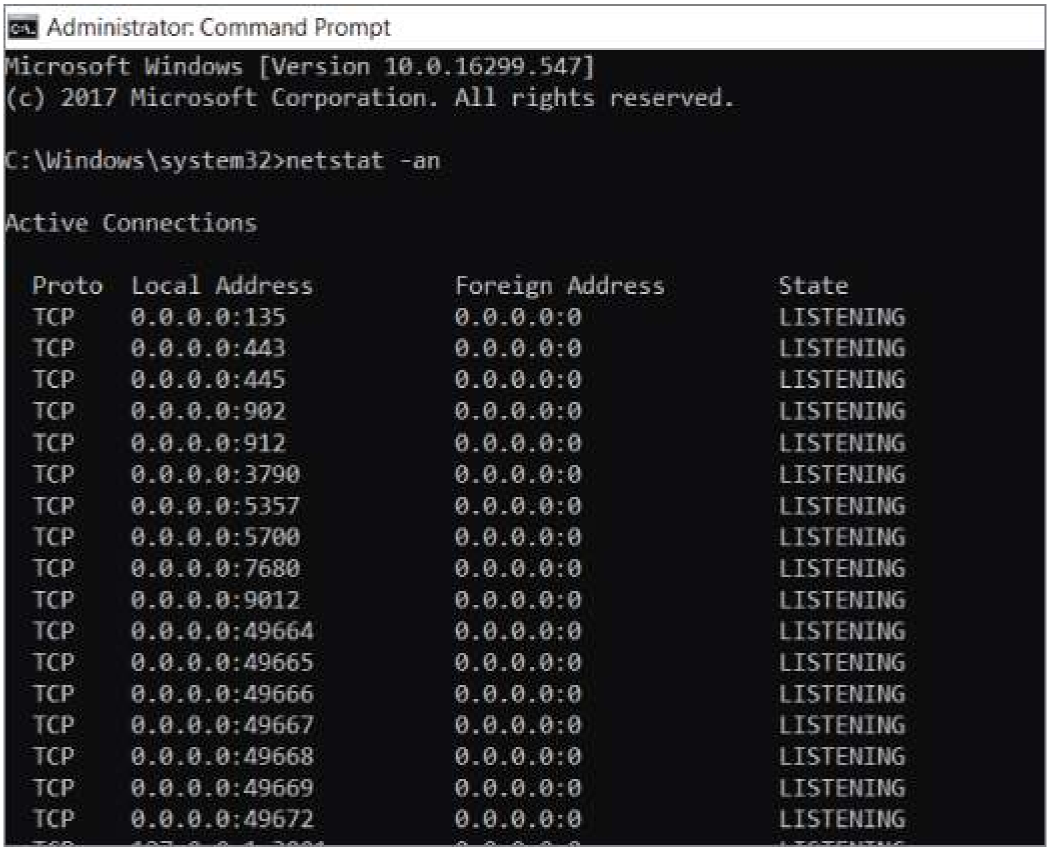
4. For fun, try **`tracert 127.0.0.1`**. Why is it only one hop?

NetStat

Mathematical statistics is the collection, organization, and presentation of data to be used in solving problems. When you analyze statistics, you are going to use probability to fix issues. For example, in a room of 23 people, there is a 50 percent probability that two of those people share the same birthday. In cybersecurity, a birthday attack is a type of cryptographic attack that exploits the math behind the birthday statistic. This attack can be used to find collisions in a hash function. In our world of networking, learning your network statistics can be quite valuable.

NetStat is a network utility tool that displays networking connections (incoming and outgoing), routing tables, and some other details such as protocol statistics. It will help you gauge the amount of network traffic and diagnose slow network speeds. Sounds simple, yes? From a cybersecurity standpoint, how quickly can you tell which ports are open for incoming connections? What ports are currently in use? What is the current state of connections that already exist?

The output from the `netstat` command is used to display the current state of all the connections on the device. This is an important part of configuration and troubleshooting. NetStat also has many parameters to choose from to answer the questions presented in the previous paragraph. One thing to remember about the parameters discussed next is that when you type them into your `cmd` shell, you can literally squish them together. For example, when I am teaching my Metasploit Pro class, we launch a proxy pivot via a Meterpreter shell and scan another network segment. (That might sound like gibberish now, but just finish the book.) How do you know what is actually transpiring on the compromised system? Using the `netstat` command and the options `-a` for all and `-n` for addresses and ports, you will have a list of all active network conversations this machine is having, as shown in Figure 1.8.



```
Microsoft Windows [Version 10.0.16299.547]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3790           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5700           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9012           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49672          0.0.0.0:0              LISTENING
```

Figure 1.8: NetStat finding active connections

To translate the figure, when running `netstat` on your host, you may see both 0.0.0.0 and 127.0.0.1 in this list. You already know what a loopback address is. A loopback address is accessible only from the machine you're running `netstat` on. The 0.0.0.0 is basically a "no particular address" placeholder. What you see after the 0.0.0.0 is called a *port*.

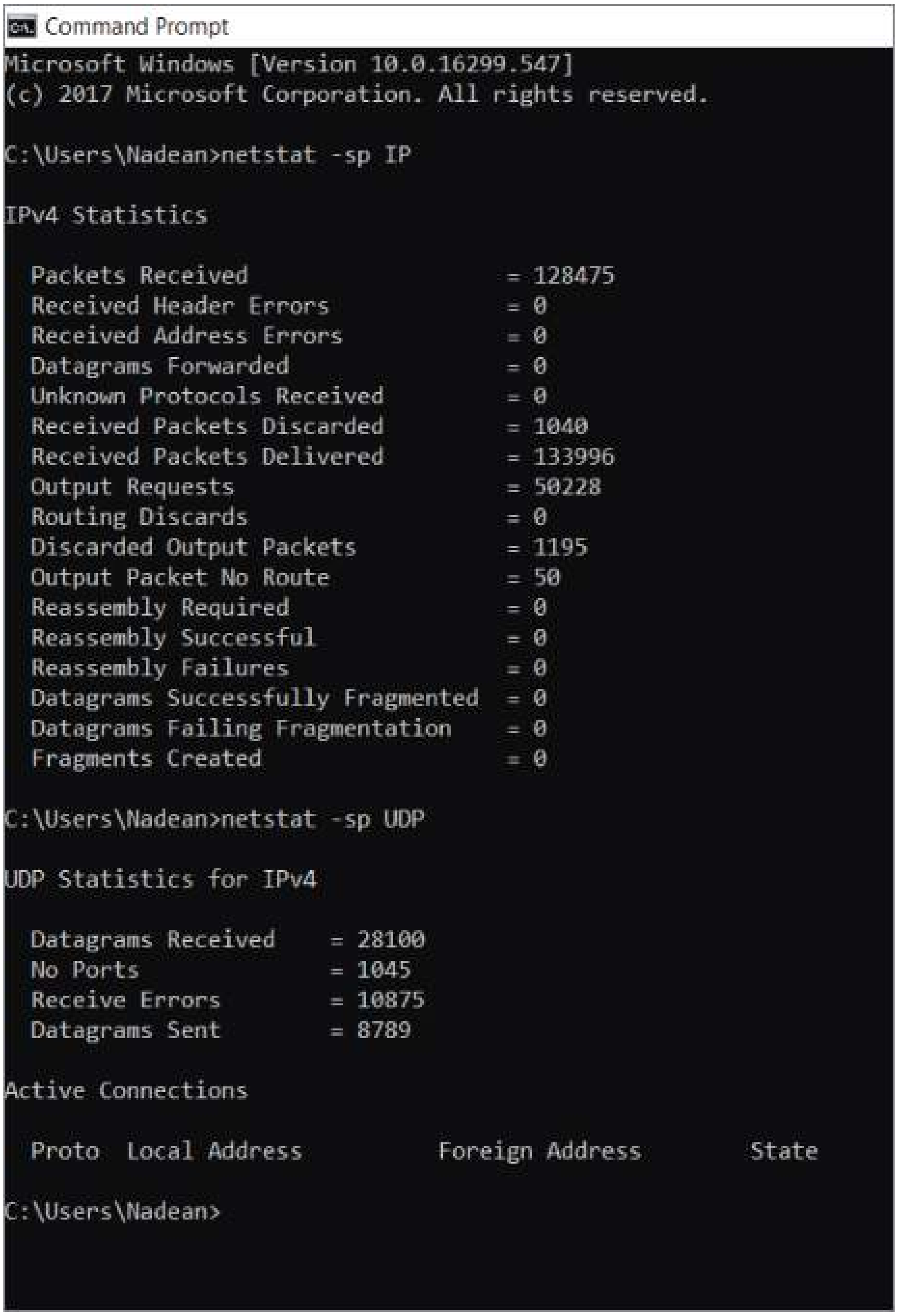
One of my favorite explanations of ports is that you have 65,536 windows and doors in your network ranging from 0 to 65,535. Computers start counting at 0. Network admins are constantly yelling, "Shut the windows and close the doors—you're letting the data out!" Ports can be TCP or UDP. Simply put, TCP means there is a connection made between the host and the destination. UDP doesn't worry about whether there is a connection made. Both TCP and UDP have 65,535 ports available to them. This was the highest number that could be represented by a 16-bit, or 2-byte, number. You may see this represented mathematically as $2^{16} - 1$.

The Internet Assigned Numbers Authority (IANA) maintains an official assignment of port numbers for specific uses. Sometimes this list becomes antiquated at the same time new technologies are becoming available. Some of the most common ones you might see are the “well-known” ports, which are 0–1023. Looking at the list in the previous figure, you see this machine is listening on port 135. Port 135 is traditionally used for a service called `epmap/loc-srv`. That should tell you, among other things in Figure 1.8, that this is a Windows host. When a Windows host wants to connect to an RPC service on a remote machine, it checks for port 135.

The next port that is listening is 443. Most IT professionals memorize this port early in their career. Port 443 is Hypertext Transfer Protocol over TLS/SSL—better known as HTTPS. HTTPS is the authentication of a website that is being accessed and protecting the confidentiality of the data being exchanged. Ports from 1023 all the way up to 49151 are “registered” ports. Above that, you have dynamic or private ports.

NetStat is an abbreviation for “network statistics.” If a host is not listening on the correct port for a specific service, then no communication can occur. Take another step in your network path, and these ports may be listening, but this does not mean that a firewall is allowing the traffic to get to the device. To test that hypothesis, you can temporarily disable your host-based firewall causing the networking issue.

Among my favorite `netstat` commands are the statistics options shown in Figure 1.9. In Lab 1.5, you'll use the `netstat` command.



```
Microsoft Windows [Version 10.0.16299.547]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Nadean>netstat -sp IP

IPv4 Statistics

  Packets Received                   = 128475
  Received Header Errors             = 0
  Received Address Errors            = 0
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 1040
  Received Packets Delivered         = 133996
  Output Requests                    = 50228
  Routing Discards                   = 0
  Discarded Output Packets           = 1195
  Output Packet No Route             = 50
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

C:\Users\Nadean>netstat -sp UDP

UDP Statistics for IPv4

  Datagrams Received    = 28100
  No Ports              = 1045
  Receive Errors        = 10875
  Datagrams Sent        = 8789

Active Connections

  Proto  Local Address          Foreign Address        State

C:\Users\Nadean>
```

Figure 1.9: NetStat statistics

LAB 1.5: NETSTAT

1. Open a command prompt or a terminal window.
2. At the command prompt, type `netstat -help`.
3. When the prompt is available, use `netstat -an -p TCP`.
4. Next try `netstat -sp TCP`.

INVESTIGATING THE UNEXPECTED

You're sitting in your office, putting the final touches on a presentation that you're giving in an hour on cybersecurity trends that your specific industry is experiencing to the C-level employees at your company. You're feeling confident with your data. You are hitting the Save button after every major change. You're concentrating on the agenda in your presentation when a balloon in your task pane from your antivirus software pops up and notifies you that an IP address will be blocked for 600 seconds.

As most end users do, you click the X with no hesitation and continue building your presentation. Then you notice you have mail in your inbox from your firewall. It is an alert notification. You start to worry less about your presentation and start thinking a possible breach is being attempted against your host.

You open a command shell and drop a `netstat -nao`. Not only will this give you the protocol, local/foreign address, and state but also the process identifier (PID) associated with that communication. You can easily get overwhelmed by the data displayed, but check your taskbar. Are there any network-centric applications running? Close your browsers and try `netstat -nao` again.

Did anything change? Are there any foreign addresses or odd port numbers that you've never seen before?

Two ports to be wary of are 4444 and 31337. Port 4444 is the default port that Metasploit will use as a default listening port. Port 31337 spells *eleet*.

Leet speak originated in the 1980s when message boards discouraged the discussion of hacking. The purposeful misspelling of words and substitution of letters for numbers was a way to indicate you were knowledgeable about hackers and circumvent the message board police. When we substitute letters with numbers to enhance our passwords, we are using leet speak for good.

If either of these two ports shows up in your NetStat statistics, it's time for a procedure that has been previously agreed upon to kick in. Either pull the network cable on this machine or alert your incident response (IR) team so they can triage the situation and make the best decision on how to stop the attack. My own personal recommendation is that if you have an IR team, use it. If you pull the plug on an attacker, you lose valuable forensic information.

PuTTY

Up until now, all the tools discussed are embedded in your operating systems. This tool will require a little more effort on your part. PuTTY is a free, open-source terminal emulation, serial console, and network file transfer program. Originally written for Windows, it has evolved to be used with other operating systems. PuTTY is an amazingly versatile tool that allows you to gain secure remote access to another computer and is most likely the most highly used SSH client for the Microsoft Windows platform.

I believe that many IT professionals who have been in the industry for a while lose track of where we have been. We keep adding knowledge and experience and expertise to our repertoire and think, “Everyone should know that.” As an educator, I am not allowed to do that. It's my job to show you how to use all these new shiny things in your toolbox. I can hear some people saying, “You had me until SSH!”

Secure Shell (SSH) is a network protocol for creating an encrypted channel over an unencrypted network. The Internet is *way* unsecured. You don't want your data out there in the World Wide Web dangling freely for all to see! SSH provides a computer administrator with a safe way to reach a system that is remote using strong authentication and secure, encrypted data transmission. There have been times as an administrator when part of my responsibilities were to manage computers I could not reach out and physically touch—execute commands or move files from one computer to another. SSH is the protocol most hosts support. An SSH server, by default, will listen on TCP port 22.

As I mentioned earlier in this chapter, SSH creates an encrypted channel to communicate over. The first version of SSH debuted in 1995. Brad Pitt was the Sexiest Man Alive, Mel Gibson's *Braveheart* won Best Picture, and Match.com was new and the only online dating site. A lot...and I mean a lot has changed since then. Over the years, several flaws were found in SSH1, and it is no longer used. The current SSH2 was adopted in 2006 and uses a stronger encryption algorithm to improve security. As of yet, there are no known exploitable vulnerabilities in SSH2, although there have been rumors that the National Security Agency (NSA) may be able to decrypt some SSH2 traffic.

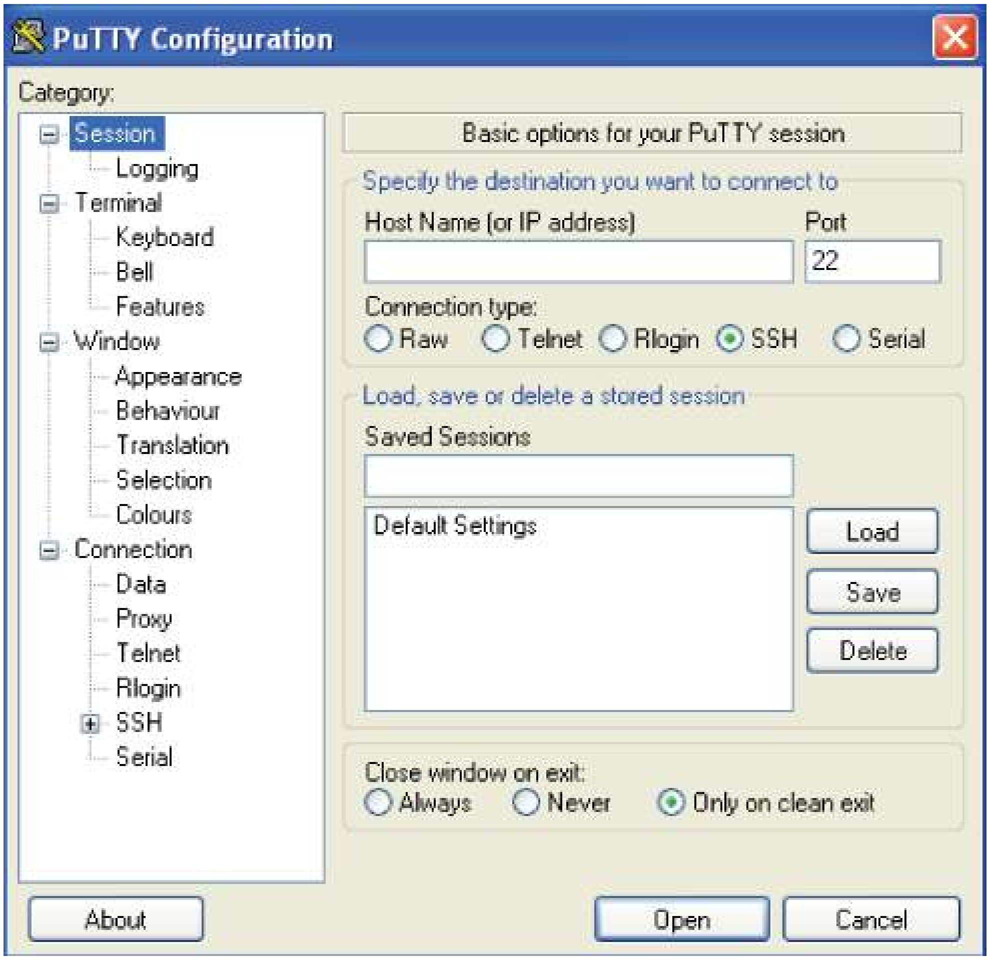
In Lab 1.6, you'll use PuTTY.

LAB 1.6: PuTTY

1. You can download a copy of PuTTY from `www.putty.org`. There will be a link on the page that takes you to the package file. Make sure you are getting the correct version for the hardware you are running. One size does not fit all.

2. Double-click the file you just downloaded. Follow the instructions until you finish the installation and then open PuTTY by double-clicking the icon that looks like two old computers linked together with a lightning bolt.

   When the software starts, a PuTTY Configuration window should open, such as what you see in Figure 1.10. The window pane on the left side lists the categories: Session, Terminal, Window, and Connection. The right side of the window will change depending on what category you have selected on the left.



Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 1.10: PuTTY Configuration window

3. In the Session view, enter the domain name or IP address you want to connect to. Port 22 specifies that you will be using SSH. The Connection Type setting lets you choose one of the following options:

   - **Raw**: This is usually used by developers for testing.
   - **Telnet**: Telnet is no longer secure. Passwords are sent in clear text. This is a bad idea.
   - **Rlogin**: This is legacy, which means old (like 1982 old). It uses port 513 and only connects Unix to Unix. Ignore it.
   - **SSH**: This is the protocol most hosts support. An SSH server, by default, will listen on TCP port 22.

   - **Serial**: This is used for controlling some physical machinery or communication devices.

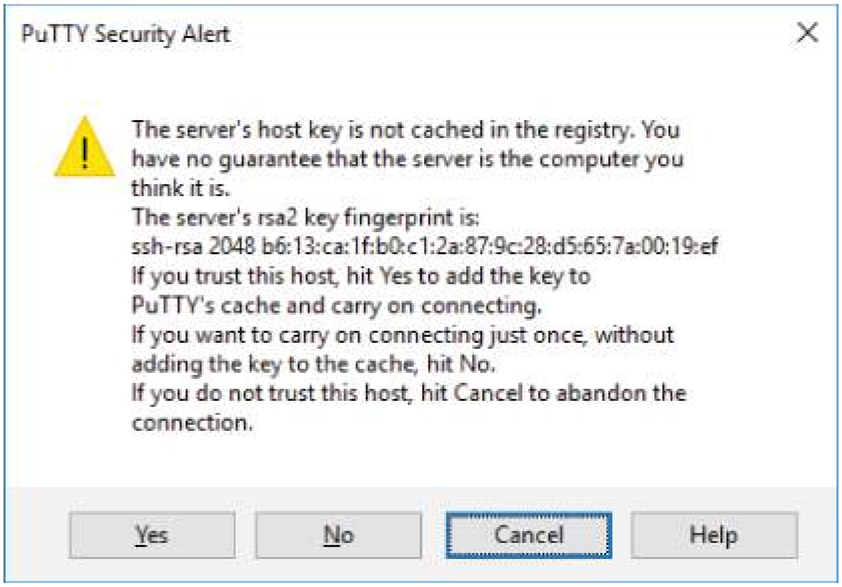
4. After you have supplied the IP or domain address, you should get a terminal window, which will ask for your credentials. If you are able to supply them, you will have a command-line terminal on the machine you just accessed. Some useful commands include the following:

`pwd`	Present working directory
`cd`	Change directory
`cd ~`	Go to the home folder
`ls`	List files
`ls -h`	List files with the size
`cp`	Copy a file
`cp -r`	Copy a folder with all the files inside
`mv`	Move a file
`mkdir`	Make a directory
`rm`	Delete a file

The session will terminate when you press Ctrl+D.

NOTE

The first time you connect another system, you may be prompted to accept the server's SSH key or certificate. It might have some wording like "The server's host key is not cached in the registry." You see an example in Figure 1.11. This is normal. When you click Yes, you are establishing trust between the two hosts.



PuTTY Security Alert

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 b6:13:ca:1f:b0:c1:2a:87:9c:28:d5:65:7a:00:19:ef
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

Figure 1.11: PuTTY security alert

I truly hope that I have given you a foundation to start to build on and that you have added these tools to your cybersecurity toolkit. Some of these tools may have just been a review for you, and some of them might have been new. These tools will help you not only with troubleshooting networks but with securing them as well.

CHAPTER 2
Troubleshooting Microsoft Windows

WHAT YOU WILL LEARN IN THIS CHAPTER:

- RELI
- PSR
- PathPing
- MTR
- Sysinternals
- GodMode

In 2012, I left the great state of Louisiana for Colorado to take a position with the Communications-Electronics Command (CECOM) at Fort Carson for the U.S. Army. My job was to train soldiers for information assurance (IA). The Department of Defense has a requirement that any full- or part-time military service member or contractor with privileged access must have certain computer certifications. This was known as DoDD 8570. My role was to teach these certification classes to help soldiers achieve the correct IA level needed so they could perform their job.

My commandant Ryan Hendricks is a networking guru, and he wanted to stay in his Cisco classes. Someone was needed to teach A+, Network+, Security+, Server+, CASP, and CISSP as well as Microsoft Active Directory, SCCM, and SharePoint. We both held the opinion that it wasn't fair for us to teach the class if we didn't hold the certification. He continued down the Cisco path, and I skipped down the CompTIA/Microsoft certification path.

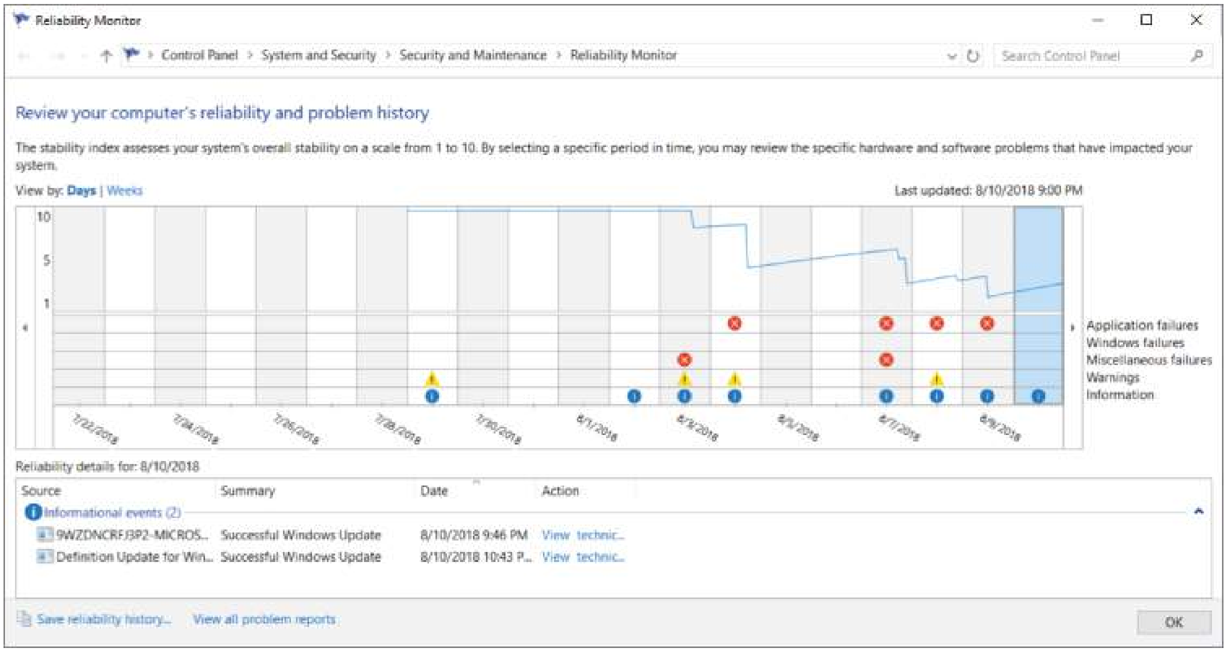
While studying for these certifications, I had many “aha” moments that are still relative today. In fact, when I am teaching my certification classes for Rapid7, I often take a few moments while everyone is getting settled into his or her seat after lunch to show class members some of these cool troubleshooting tricks for Windows. It's a bit of a bonus for coming back to class on time.

Even seasoned professionals who work with massive networks and have years of experience have uttered a few choice words when they see tools that are meant to make their life easier after they've been doing it the hard way for years and years. If nearly 90 percent of your network is Windows, you need these tools to make your administrative life easier.

RELI

I call this tool RELI because when you type these four letters in the Windows search box on the taskbar, there is usually nothing else to choose from besides this one, the Reliability History/Monitor. RELI traces its roots all the way back to Windows Vista. It allows you to see the stability of a machine in a timeline. When you start typing it in the Start menu, you'll notice the name of the tool displays as Reliability History. Once you open the tool, it renames itself to Reliability Monitor. (Thank you, Microsoft.)

Reliability Monitor will build a graph for you of important events, application and Windows failures, and updates and other information that might be important. Figure 2.1 shows the graph that gets generated from application, Windows, and miscellaneous failures. In Lab 2.1, you'll use RELI.



Review your computer's reliability and problem history

The stability index assesses your system's overall stability on a scale from 1 to 10. By selecting a specific period in time, you may review the specific hardware and software problems that have impacted your system.

View by: **Days** | Weeks

Last updated: 8/10/2018 9:00 PM

Reliability details for: 8/10/2018

Source	Summary	Date	Action
Informational events (2)			
9WZDNCRFJ3P2-MICROS...	Successful Windows Update	8/10/2018 9:46 PM	View technic...
Definition Update for Win...	Successful Windows Update	8/10/2018 10:43 P...	View technic...

Figure 2.1: Reliability Monitor graph

LAB 2.1: RELI

1. To open this tool, open the Start menu and begin typing **reli**.
2. When you see the blue flag icon next to Reliability History in your Start menu, press the Enter key. Wait while it builds your graphic timeline.
3. Above the graphic in the upper left, notice you can shift your timeline view from Days to Weeks.
   - The first three lines of the graph indicated on the right side are the application, Windows, and miscellaneous failures this system has experienced. These can include when a program stopped working or when Windows did not properly shut down. It is a fantastic indicator of a Blue/Black Screen of Death (BSOD). This will be displayed as a red circle with a white X inside.
   - Under the failures, the yellow triangles with an exclamation point inside indicate a warning. These triangles are called *splats*. They could indicate whether the software did not update properly or errored but did not fail completely.
   - The blue circles across the bottom are informational. They will inform you if software updates were successful or drivers were installed correctly.
4. In the lower-left corner of the Reliability Monitor screen, click the Save Reliability History link to save this timeline as an XML file. This file can be exported and analyzed by other reporting applications.
5. Click the View All Problem Reports link in the lower-right corner next to the Save Reliability History link. This will open a new page that includes all the problems this device has experienced and can be reported directly to Microsoft. When there is a solution, it will appear in Security And Maintenance.

USING RELI

Let's say you are a system administrator. Most system administrators install, upgrade, and monitor software and hardware for their organizations. You have a server in your datacenter that is periodically misbehaving. You attempt to troubleshoot the issue and cannot duplicate the problem that was reported to you. Instead, you get the infamous BSOD.

You will learn that the first thing you ask customers when they report a problem is, “Have you tried turning it off and on again?” If you do unfortunately experience a BSOD, then your only option is to power down and turn the device back on. Check `reli` to determine what caused that crash.

It has been my experience that a BSOD is caused by bad drivers, overheating, or someone installing new software that is incompatible with either the hardware or the operating system. Using `reli` is how you figure out what really happened.

No one ever admits to downloading and playing *Duke Nukem Forever*.

PSR

Are you the one in your organization who is responsible for continuance or documentation? Do you have to train others how to do their job, or have you been asked to train someone to do yours? Do you ever have to troubleshoot an environmental problem on a system or give a presentation at the last minute?

Problem Steps Recorder (PSR) goes back to Windows 7 and Server 2008. PSR is a combination troubleshooting, assistance, screen capture, annotation tool that few IT professionals know about. You can use it to document your steps quickly with annotated screenshots and instructions. You can use it to troubleshoot an issue for a customer who is not as IT-savvy as you. My favorite way to use it is to build documentation.

One of the best questions you can as your IT manager is, “What keeps you up at night?” When I am teaching, I try to learn as much as I can about my students' needs and goals. One of the biggest responses to the question about their security challenges is lack of documentation and continuance. This tool will help solve that problem.

In my experience, I have managed people new to IT who often ask the same questions over and over again. To empower them to find the answers, I created PSRs for repetitive questions like the following and store them on an easily searchable SharePoint site:

> “How do I add a static IP?”
>
> “How do I configure a network printer?”
>
> “How do I add a user in Active Directory?”

In Lab 2.2, you'll use PSR.

LAB 2.2: PSR

1. To open Problem Steps Recorder, go to your Start menu and type in **PSR**. Press Enter. You will see a menu like Figure 2.2.

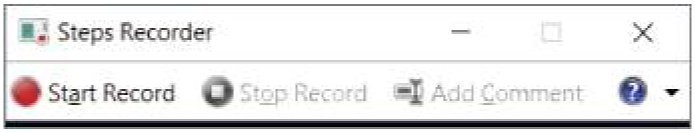


Figure 2.2: Steps Recorder menu

2. Click Start Record.
3. Open your Calculator application, and on your keyboard, type **9+9** and press Enter. You should get 18 as the answer. As you clicked the screen or typed on the keyboard, a small red bubble indicates that Problem Steps Recorder is taking a picture of the screen.
4. Click Stop Record and wait to review your recording.

To review the Problem Steps Recorder file you just created, in the upper-left corner of the recording, you could click the New Recording button if this did not capture exactly the process you were looking for. If it is a file that you will want to use, click the Save button. When you save this file, it is saved in a `.zip`file by default. If customers/employees are having an IT issue, they can easily email you this file with all the contents for you to examine the issue. When you open the `.zip` file, you'll notice the file type is MHTML. You can right-click and open this file type with Word and edit it until it reads exactly as you want it to for your continuance or documentation.

Each step recorded has a date and time and is annotated in bright green in the screenshot surrounding what you clicked. Examine your screenshots. In the first frame, your Start button will be highlighted in green with an arrow on it. The explanation at the top of each picture will tell you how the data was entered. When you're troubleshooting, sometimes input makes a difference.

At the bottom of the Recorded Steps page, there will be an Additional Details section. This section contains specific details about software and operating systems that only programmers or advanced IT people will understand. Review this to make sure nothing is in here that you don't want shared.

Have you ever been asked to present in a meeting with 15 minutes prep time? I'm good, but I'm not that good. If you are being asked to present on something that you can show in PSR, scroll up to the top of the page and click the hyperlink “Review the recorded steps as a slide show.”

There are a few caveats to PSR. It will look much more professional if you record on just one monitor. This tool will not record text that you type such as passwords; it will record only function and shortcut keys. It also will not capture streaming video or a full-screen game.

You may get a static picture, but this tool delivers a flat, one-dimensional file. You are also limited by default to only 25 screenshots. If you need more than 25, you will have to go to the Help menu and adjust the settings. These settings will be temporary and not retained. They go back to the default when you close and reopen the program.

I have had professional IT students tell me this tool alone was worth the price of admission to class.

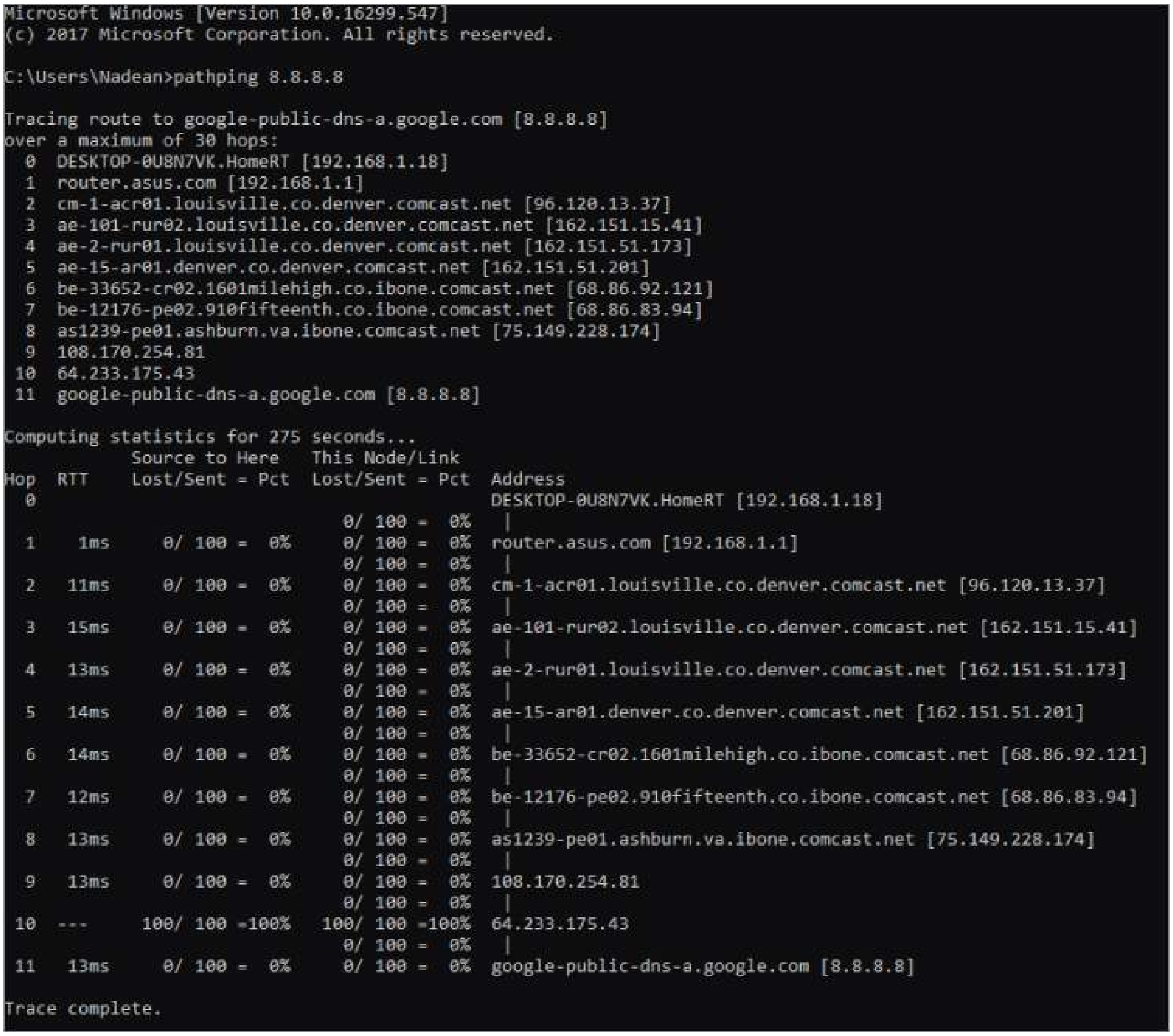
PathPing

In 2017, Panasonic developed a prototype that not only washes and dries but also folds your clothes. There are some technologies that just belong together.

PathPing is the washer/dryer/folder combination of Windows. If you take a ping and squish it together with a tracert, you have PathPing. Each node is pinged as the result of a single command. Details of the path between two hosts and the echo-location statistics for each node are displayed. The behavior of nodes is studied over an extended time period—25 seconds each, to be exact. This is in comparison to the default ping sample of four messages or default tracert single-route trace.

PathPing will first do a tracert to the destination. Second, it uses ICMP to ping each hop 100 times. This is used to verify latency between the source host and the destination. You cannot completely rely on ICMP when public devices are involved. They are public devices. Occasionally on the Internet, you will run into situations where an ICMP ping destined for one host has 50 percent failure and the next hop has 100 percent success.

Figure 2.3 shows the tracing route to Google's public DNS server 8.8.8.8. From my desktop to the server, it takes 11 hops. Then PathPing will compute the statistics of round-trip time (RTT) as well as the percentage of how many packets were dropped between the two IP addresses. When you see loss rates, it might indicate that these routers are overloaded.



```
Microsoft Windows [Version 10.0.16299.547]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Nadean>pathping 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:
  0  DESKTOP-0U8N7VK.HomeRT [192.168.1.18]
  1  router.asus.com [192.168.1.1]
  2  cm-1-acr01.louisville.co.denver.comcast.net [96.120.13.37]
  3  ae-101-rur02.louisville.co.denver.comcast.net [162.151.15.41]
  4  ae-2-rur01.louisville.co.denver.comcast.net [162.151.51.173]
  5  ae-15-ar01.denver.co.denver.comcast.net [162.151.51.201]
  6  be-33652-cr02.1601milehigh.co.ibone.comcast.net [68.86.92.121]
  7  be-12176-pe02.910fifteenth.co.ibone.comcast.net [68.86.83.94]
  8  as1239-pe01.ashburn.va.ibone.comcast.net [75.149.228.174]
  9  108.170.254.81
 10  64.233.175.43
 11  google-public-dns-a.google.com [8.8.8.8]

Computing statistics for 275 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           DESKTOP-0U8N7VK.HomeRT [192.168.1.18]
                                0/ 100 =  0%   |
  1    1ms     0/ 100 =  0%     0/ 100 =  0%  router.asus.com [192.168.1.1]
                                0/ 100 =  0%   |
  2   11ms     0/ 100 =  0%     0/ 100 =  0%  cm-1-acr01.louisville.co.denver.comcast.net [96.120.13.37]
                                0/ 100 =  0%   |
  3   15ms     0/ 100 =  0%     0/ 100 =  0%  ae-101-rur02.louisville.co.denver.comcast.net [162.151.15.41]
                                0/ 100 =  0%   |
  4   13ms     0/ 100 =  0%     0/ 100 =  0%  ae-2-rur01.louisville.co.denver.comcast.net [162.151.51.173]
                                0/ 100 =  0%   |
  5   14ms     0/ 100 =  0%     0/ 100 =  0%  ae-15-ar01.denver.co.denver.comcast.net [162.151.51.201]
                                0/ 100 =  0%   |
  6   14ms     0/ 100 =  0%     0/ 100 =  0%  be-33652-cr02.1601milehigh.co.ibone.comcast.net [68.86.92.121]
                                0/ 100 =  0%   |
  7   12ms     0/ 100 =  0%     0/ 100 =  0%  be-12176-pe02.910fifteenth.co.ibone.comcast.net [68.86.83.94]
                                0/ 100 =  0%   |
  8   13ms     0/ 100 =  0%     0/ 100 =  0%  as1239-pe01.ashburn.va.ibone.comcast.net [75.149.228.174]
                                0/ 100 =  0%   |
  9   13ms     0/ 100 =  0%     0/ 100 =  0%  108.170.254.81
                                0/ 100 =  0%   |
 10  ---     100/ 100 =100%   100/ 100 =100%  64.233.175.43
                                0/ 100 =  0%   |
 11   13ms     0/ 100 =  0%     0/ 100 =  0%  google-public-dns-a.google.com [8.8.8.8]

Trace complete.
```

Figure 2.3: PathPing combining both traceroute and statistics of each hop

PathPing is a better diagnostic tool to use if latency in your network is a concern. The interpretation of the data from a PathPing will give you a more robust hypothesis. If you see anomalies or peaks and valleys in the data on hop 6, it doesn't necessarily mean that hop 6 is the problem. It could be that hop 6 just happens to be under immense pressure or the processor has priorities other than your PathPing at the moment. A tool that ISPs use to prevent overwhelming floods of ICMP is called *control-plane policing* (CoPP). This type of flood prevention can also alter the results you see from PathPing. In Lab 2.3, you'll use PathPing.

LAB 2.3: PATHPING

1. Open a command prompt, PowerShell, or a terminal window.
2. Type the following command to display options that you can use with the PathPing tool:

   ```
   pathping /?
   ```

3. At the next command prompt, type the following:

   ```
   pathping -q 50 8.8.8.8
   ```

   By using`-q 50` as an option, you cut your time in half, although it will still be a very long 137 seconds.

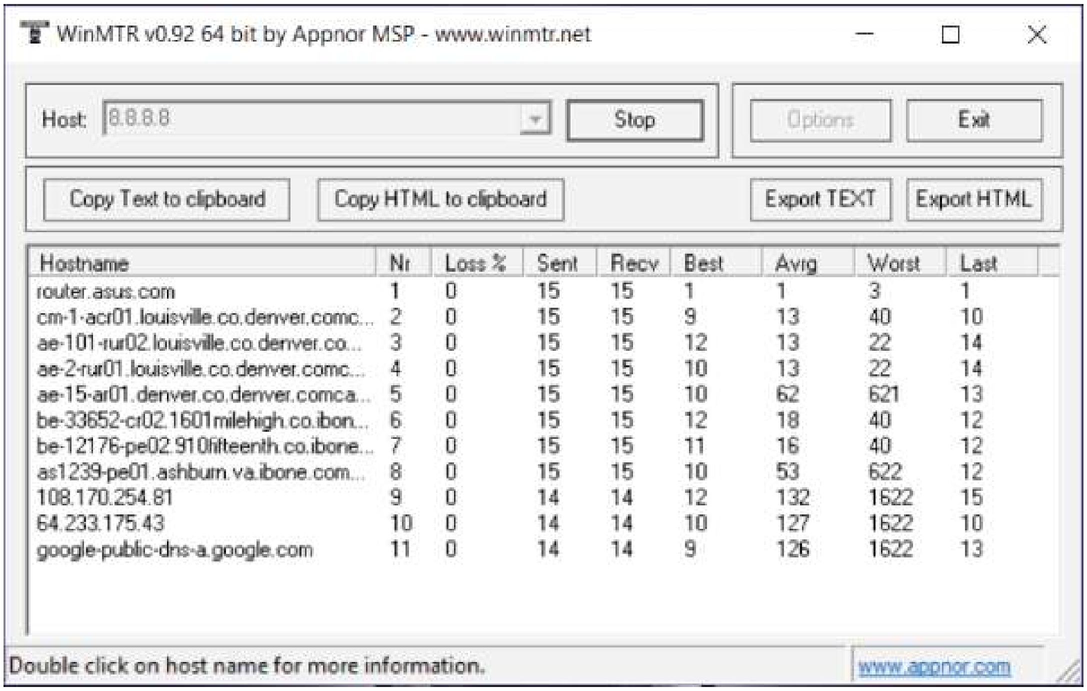
MTR

My TraceRoute (MTR) is another tool that combines multiple tools into one. MTR was originally named for Matt Kimball in 1997 and was called Matt's TraceRoute.

WinMTR is a Windows application that combines the `tracert` and `ping` commands. At the time of publication, it can be downloaded from `www.winmtr.net`. The tool is often used for network troubleshooting. By showing a list of routers traveled and average time and packet loss, it allows administrators to identify issues between two routers responsible for overall latency. This can help identify network overuse problems. In Lab 2.4, you'll use MTR.

LAB 2.4: MTR

1. Open a command prompt or a terminal window.
2. Download the WinMTR file from www.winmtr.net, and choose the appropriate file for your hardware (e.g., x86 x64).
3. Extract the `.zip` file, making note of the location.
4. Open the WinMTR folder and double-click the application. PathPing along with other information will be displayed in a graphical user interface (GUI), making the data much easier to document.
5. Next to Host, type **8.8.8.8** and click Start. In Figure 2.4, you see the results.



Host: 8.8.8.8

Hostname	Nr	Loss %	Sent	Recv	Best	Avrg	Worst	Last
router.asus.com	1	0	15	15	1	1	3	1
cm-1-acr01.louisville.co.denver.comc...	2	0	15	15	9	13	40	10
ae-101-rur02.louisville.co.denver.co...	3	0	15	15	12	13	22	14
ae-2-rur01.louisville.co.denver.comc...	4	0	15	15	10	13	22	14
ae-15-ar01.denver.co.denver.comca...	5	0	15	15	10	62	621	13
be-33652-cr02.1601milehigh.co.ibon...	6	0	15	15	12	18	40	12
be-12176-pe02.910fifteenth.co.ibone...	7	0	15	15	11	16	40	12
as1239-pe01.ashburn.va.ibone.com...	8	0	15	15	10	53	622	12
108.170.254.81	9	0	14	14	12	132	1622	15
64.233.175.43	10	0	14	14	10	127	1622	10
google-public-dns-a.google.com	11	0	14	14	9	126	1622	13

Double click on host name for more information.

Figure 2.4: WinMTR combining ping with traceroute

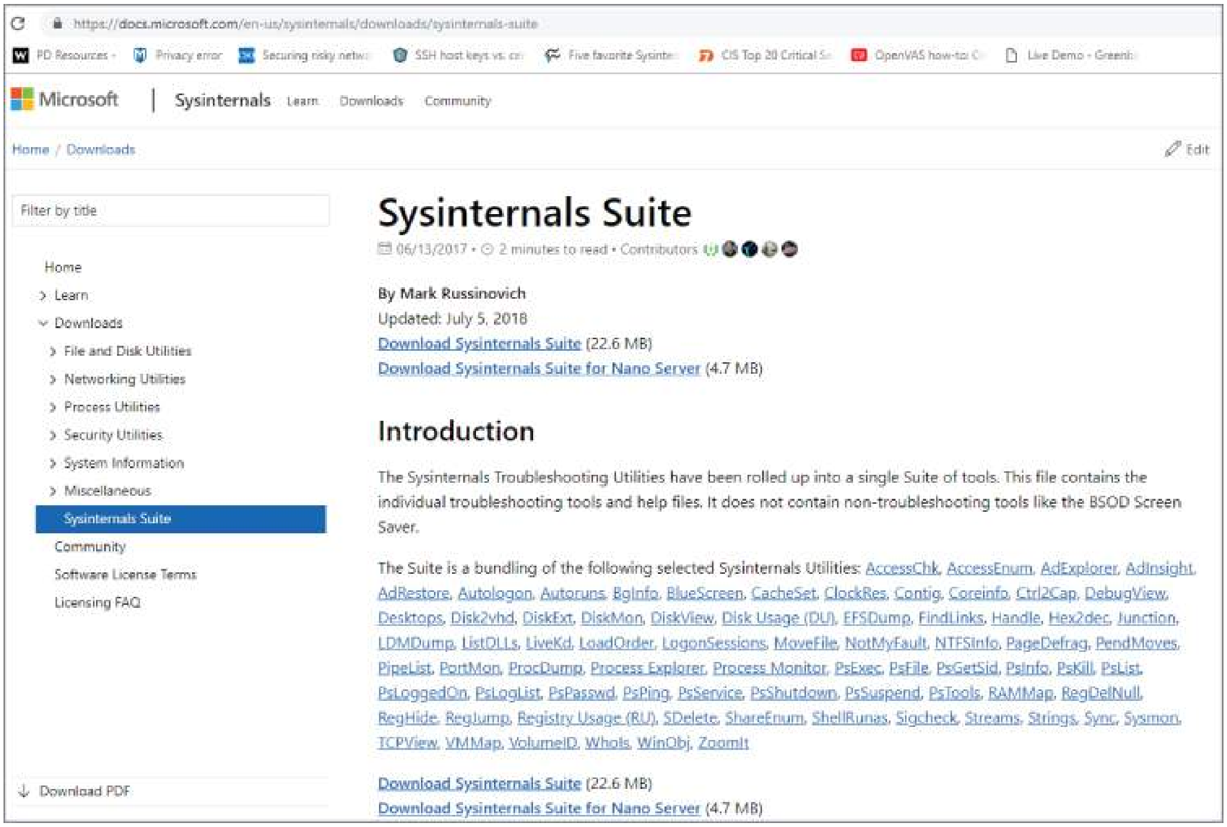
6. Copy or export your results by clicking either the Export TEXT or Export HTML button.
7. Double-click a hostname for more information. Select the down arrow at the end of the host field and clear your

history.

Sysinternals

Microsoft TechNet is a treasure-trove of all things Microsoft, including troubleshooting, downloads, and training. From the website `https://technet.microsoft.com`, you can find free training, libraries, wikis, forums, and blogs. When your Microsoft workstation fails hard with a BSOD, where do you go to look up the error codes and event IDs? TechNet! Where do you go to find utilities to help you manage, troubleshoot, and diagnose your Windows machines *and* applications? TechNet!

When you visit the TechNet website, the fastest way to find the Sysinternals suite is to just search for it in the upper-right corner. The Sysinternals suite bundles many smaller utilities into one big beautiful tool. One of the best things about the Sysinternals suite is that it is portable. Figure 2.5 shows the download link. You do not have to install each tool. You can put the entire suite of tools on a USB drive and use them from any PC.



Sysinternals Suite

06/13/2017 • 2 minutes to read • Contributors

By Mark Russinovich
Updated: July 5, 2018
Download Sysinternals Suite (22.6 MB)
Download Sysinternals Suite for Nano Server (4.7 MB)

Introduction

The Sysinternals Troubleshooting Utilities have been rolled up into a single Suite of tools. This file contains the individual troubleshooting tools and help files. It does not contain non-troubleshooting tools like the BSOD Screen Saver.

The Suite is a bundling of the following selected Sysinternals Utilities: AccessChk, AccessEnum, AdExplorer, AdInsight, AdRestore, Autologon, Autoruns, BgInfo, BlueScreen, CacheSet, ClockRes, Contig, Coreinfo, Ctrl2Cap, DebugView, Desktops, Disk2vhd, DiskExt, DiskMon, DiskView, Disk Usage (DU), EFSDump, FindLinks, Handle, Hex2dec, Junction, LDMDump, ListDLLs, LiveKd, LoadOrder, LogonSessions, MoveFile, NotMyFault, NTFSInfo, PageDefrag, PendMoves, PipeList, PortMon, ProcDump, Process Explorer, Process Monitor, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsList, PsLoggedOn, PsLogList, PsPasswd, PsPing, PsService, PsShutdown, PsSuspend, PsTools, RAMMap, RegDelNull, RegHide, RegJump, Registry Usage (RU), SDelete, ShareEnum, ShellRunas, Sigcheck, Streams, Strings, Sync, Sysmon, TCPView, VMMap, VolumeID, WhoIs, WinObj, ZoomIt

Download Sysinternals Suite (22.6 MB)
Download Sysinternals Suite for Nano Server (4.7 MB)

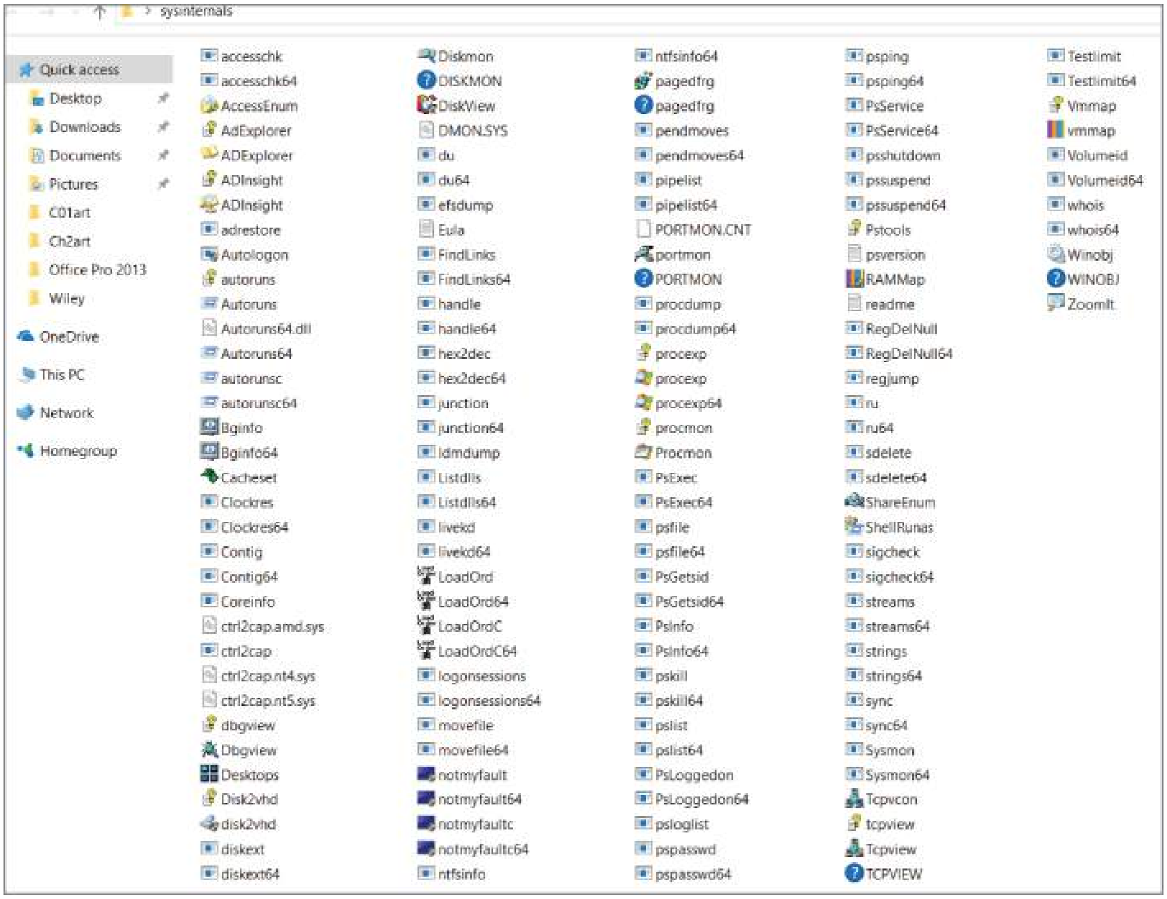
Figure 2.5: Microsoft Sysinternals suite download

The tools include utilities such as Process Explorer, which is a lot like Task Manager with a ton of extra features, or Autoruns, which helps you deal with startup processes. Another tool inside the suite is PsExec, which is a lightweight replacement for Telnet. One of my favorite tools is Notmyfault. Seriously, that's the name of the tool. You can use it to crash or handle kernel memory leaks—helpful when troubleshooting device driver issues, which has been the cause of at least half of my BSODs. In Lab 2.5, you'll use Sysinternals.

LAB 2.5: SYSINTERNALS

1. Open a browser and navigate to `https://technet.microsoft.com`.
2. In the Search field, look for *Sysinternals*. The first link you should see is "Download Sysinternals Suite."

   The zipped file will be about 24MB. Unzipped, it will be approximately 60MB. It will easily fit on a USB drive.
3. Save the file to your hard drive and extract all files. Make a conscious note of the location. (I say this because I have been known to misplace my tools.)
4. Once the tools are unzipped, open the folder and change the view to List, as you see in Figure 2.6. This will allow you to see everything at one time.

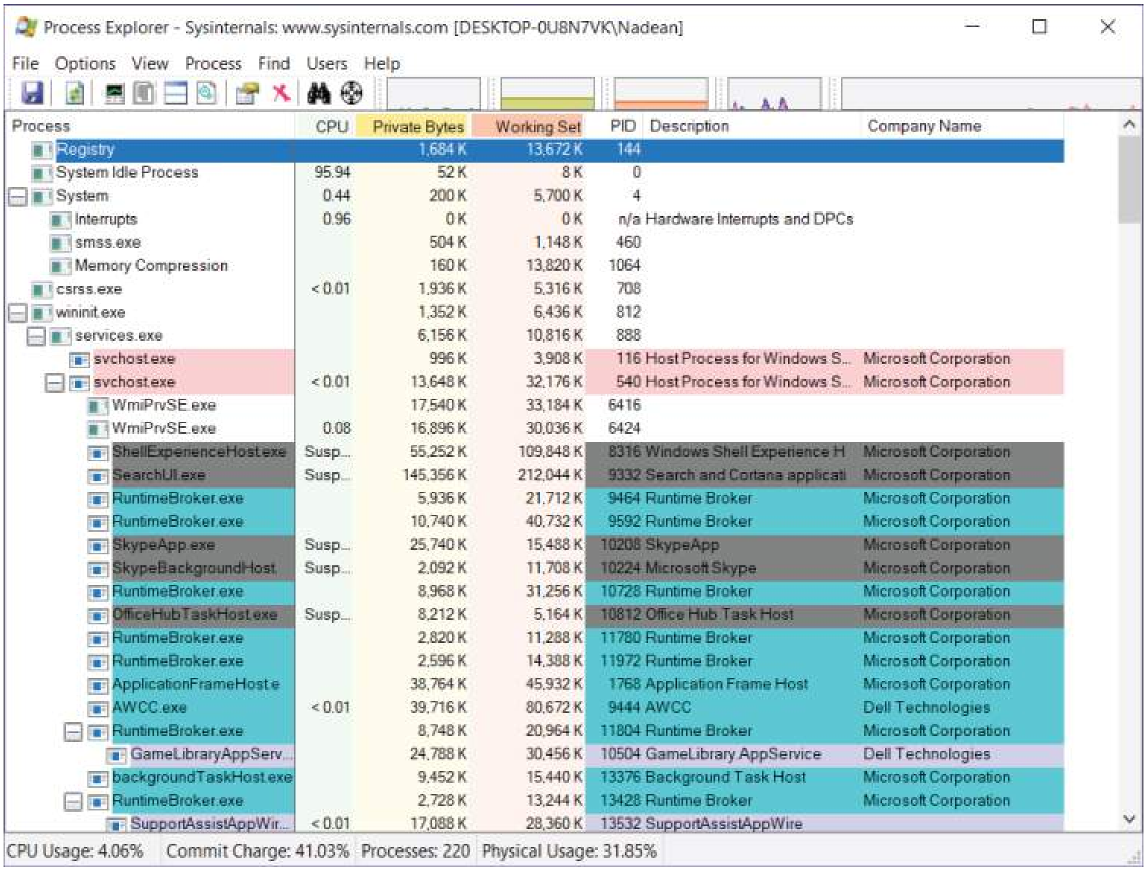


accesschk
accesschk64
AccessEnum
AdExplorer
ADExplorer
ADInsight
ADInsight
adrestore
Autologon
autoruns
Autoruns
Autoruns64.dll
Autoruns64
autorunsc
autorunsc64
Bginfo
Bginfo64
Cacheset
Clockres
Clockres64
Contig
Contig64
Coreinfo
ctrl2cap.amd.sys
ctrl2cap
ctrl2cap.nt4.sys
ctrl2cap.nt5.sys
dbgview
Dbgview
Desktops
Disk2vhd
disk2vhd
diskext
diskext64
Diskmon
DISKMON
DiskView
DMON.SYS
du
du64
efsdump
Eula
FindLinks
FindLinks64
handle
handle64
hex2dec
hex2dec64
junction
junction64
ldmdump
Listdlls
Listdlls64
livekd
livekd64
LoadOrd
LoadOrd64
LoadOrdC
LoadOrdC64
logonsessions
logonsessions64
movefile
movefile64
notmyfault
notmyfault64
notmyfaultc
notmyfaultc64
ntfsinfo
ntfsinfo64
pagedfrg
pagedfrg
pendmoves
pendmoves64
pipelist
pipelist64
PORTMON.CNT
portmon
PORTMON
procdump
procdump64
procexp
procexp
procexp64
procmon
Procmon
PsExec
PsExec64
psfile
psfile64
PsGetsid
PsGetsid64
PsInfo
PsInfo64
pskill
pskill64
pslist
pslist64
PsLoggedon
PsLoggedon64
psloglist
pspasswd
pspasswd64
psping
psping64
PsService
PsService64
psshutdown
pssuspend
pssuspend64
Pstools
psversion
RAMMap
readme
RegDelNull
RegDelNull64
regjump
ru
ru64
sdelete
sdelete64
ShareEnum
ShellRunas
sigcheck
sigcheck64
streams
streams64
strings
strings64
sync
sync64
Sysmon
Sysmon64
Tcpvcon
tcpview
Tcpview
TCPVIEW
Testlimit
Testlimit64
Vmmap
vmmap
Volumeid
Volumeid64
whois
whois64
Winobj
WINOBJ
ZoomIt

Figure 2.6: List of all Sysinternals tools

There are so many wonderful tools in this file that it can be difficult to know where to start. The following list includes the tools that I have used quite regularly as well as some that I may not use as much but have been helpful in certain situations:

Process Explorer This tool is one of the most used utilities in Sysinternals. It is a simple tool, but it can clue you in on every process, every DLL, and every activity occurring on your PC. In Figure 2.7, you see processes, CPU usage, PID, and other information. One of my favorite features of Process Explorer is the ability to check processes with VirusTotal if you suspect your machine is compromised.



Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-0U8N7VK\Nadean]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		1,684 K	13,672 K	144		
System Idle Process	95.94	52 K	8 K	0		
System	0.44	200 K	5,700 K	4		
Interrupts	0.96	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		504 K	1,148 K	460		
Memory Compression		160 K	13,820 K	1064		
csrss.exe	< 0.01	1,936 K	5,316 K	708		
wininit.exe		1,352 K	6,436 K	812		
services.exe		6,156 K	10,816 K	888		
svchost.exe		996 K	3,908 K	116	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	13,648 K	32,176 K	540	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		17,540 K	33,184 K	6416		
WmiPrvSE.exe	0.08	16,896 K	30,036 K	6424		
ShellExperienceHost.exe	Susp...	55,252 K	109,848 K	8316	Windows Shell Experience H	Microsoft Corporation
SearchUI.exe	Susp...	145,356 K	212,044 K	9332	Search and Cortana applicati	Microsoft Corporation
RuntimeBroker.exe		5,936 K	21,712 K	9464	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		10,740 K	40,732 K	9592	Runtime Broker	Microsoft Corporation
SkypeApp.exe	Susp...	25,740 K	15,488 K	10208	SkypeApp	Microsoft Corporation
SkypeBackgroundHost	Susp...	2,092 K	11,708 K	10224	Microsoft Skype	Microsoft Corporation
RuntimeBroker.exe		8,968 K	31,256 K	10728	Runtime Broker	Microsoft Corporation
OfficeHubTaskHost.exe	Susp...	8,212 K	5,164 K	10812	Office Hub Task Host	Microsoft Corporation
RuntimeBroker.exe		2,820 K	11,288 K	11780	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2,596 K	14,388 K	11972	Runtime Broker	Microsoft Corporation
ApplicationFrameHost.e		38,764 K	45,932 K	1768	Application Frame Host	Microsoft Corporation
AWCC.exe	< 0.01	39,716 K	80,672 K	9444	AWCC	Dell Technologies
RuntimeBroker.exe		8,748 K	20,964 K	11804	Runtime Broker	Microsoft Corporation
GameLibraryAppServ...		24,788 K	30,456 K	10504	GameLibrary AppService	Dell Technologies
backgroundTaskHost.exe		9,452 K	15,440 K	13376	Background Task Host	Microsoft Corporation
RuntimeBroker.exe		2,728 K	13,244 K	13428	Runtime Broker	Microsoft Corporation
SupportAssistAppWir...	< 0.01	17,088 K	28,360 K	13532	SupportAssistAppWire	

CPU Usage: 4.06% Commit Charge: 41.03% Processes: 220 Physical Usage: 31.85%

Figure 2.7: Sysinternals Process Explorer

PsList One way to see processes on a machine is to press Ctrl+Alt+Delete on your keyboard and navigate to your Task Manager. The Task Manager is a great tool but works only on the local machine. You can run PsList remotely to get a list of processes running on someone else's machine.

PsKill This tool can be used to kill or terminate processes running on either your machine or someone else's machine. Find the process ID with PsList and terminate it with PsKill.

Autoruns Malware is the bane of our IT existence. It can be insidious and invade the startup folder. It will be one the hardest things you will ever try to clean. Autoruns can help by looking through all possible locations where applications are listed to autostart. You can filter Autoruns so that the good things you need to start are not listed, and you can concentrate on the number of things that invade a system.

ZoomIt This utility can be used to magnify a certain area of the screen. It can integrate with PowerPoint so that during a presentation you can trigger certain functions with macro keys. You can live zoom, draw, type, and even configure a break timer if your audience requires one during a class.

PsLoggedOn This tool can find users who are logged on to a system. PsLoggedOn uses a scan of the registry to look through the HKEY_USERS key to see what profiles are loaded. This can be extremely helpful when you need to know who has a session established on a PC.

SDelete This is a tool that you should not need often but could definitely come in handy. If you ever need to delete something permanently so that even the best of the best file recovery tools cannot retrieve the data, SDelete will take the sectors where the file is stored and write over them with 0s. If you are ever in need of a permanent disposal of a file or folder, you will want to use this tool.

PsExec There will be times that you will want to execute programs on remote systems. Telnet runs on port 23 and sends credentials over a network in the clear. PsExec is a much better choice, allowing you to execute processes without having to manually install other software. You can launch interactive command prompts and enable remote tools.

Notmyfault If you have a server that is not performing as it should or you are seeing out-of-resources errors and the machine is very slow, you can use Notmyfault to troubleshoot more advanced operating system performance issues and application or process crashes.

The Legendary God Mode

My first experience with invulnerability came in 1993 when I started playing *Doom*. *Doom* was a first-person shooter game that was divided up into nine level episodes. You played a character nicknamed DoomGuy who was a space marine who finds himself in

Hell. There was a particular IDBEHOLDV cheat that made you invulnerable. This was considered God mode.

In 2007, with the debut of Windows 7 came a tool that was nicknamed *God mode*. Its real name is Windows Master Control Panel, although I personally think God mode sounds more epic.

Windows Master Control Panel gives you access to all the operating systems control panels within one folder. You can enable God mode in Windows 8.1 and Windows 10 as well. The feature is useful for those in IT, those who manage a computer, and advanced Windows experts. Enabling God mode creates a folder that gives you access to every single Windows OS setting. The icon you see in Figure 2.8 is for the folder that gets created.

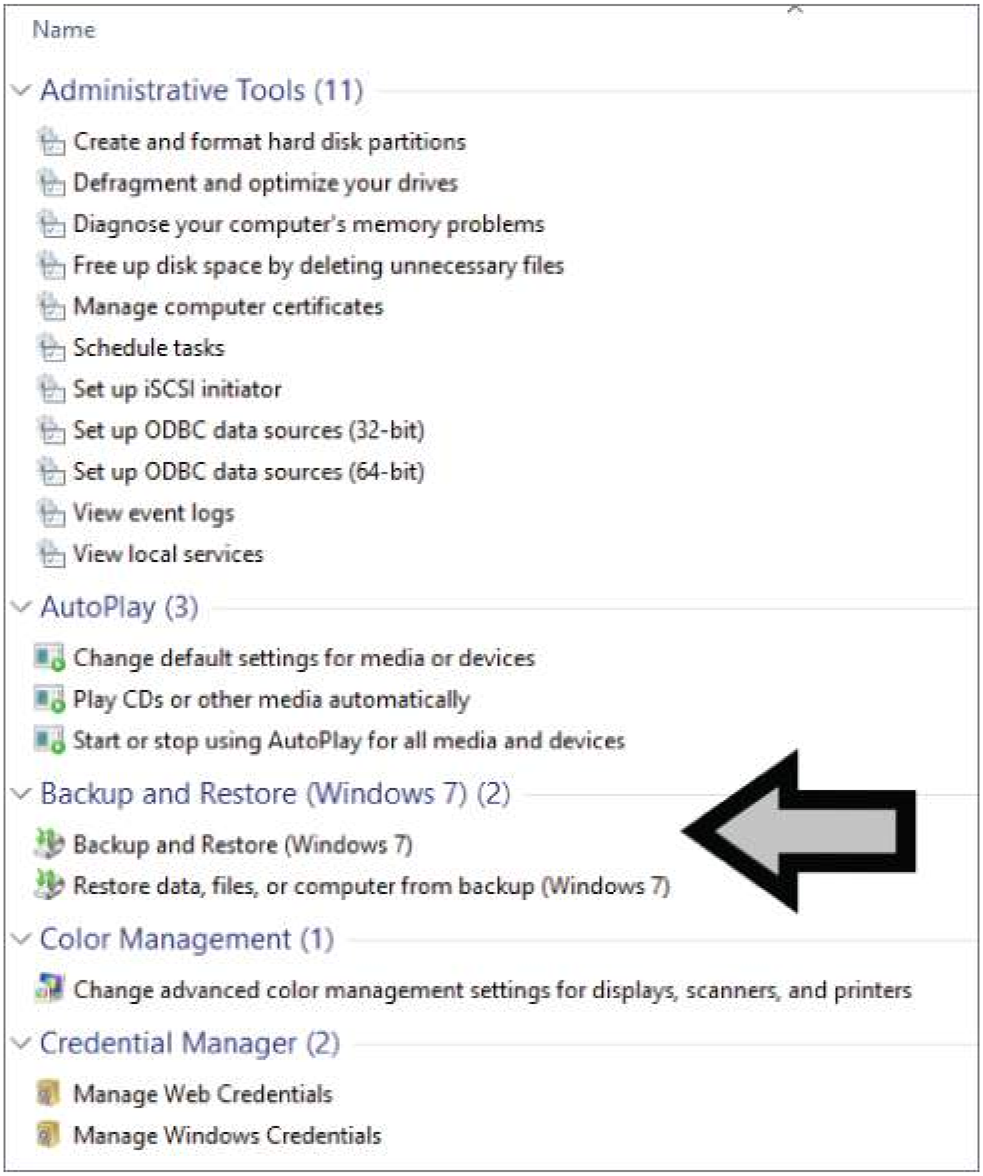
Figure 2.8: God mode folder

In Lab 2.6, you'll enable Windows Master Control Panel.

LAB 2.6: ENABLING WINDOWS MASTER CONTROL PANEL

1. Make sure you are using an account with administrative privileges.
2. Right-click your Windows 7, 8.1, or 10 desktop and choose New ➪ Folder.
3. Name the folder **GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}**.
4. Press Enter and double-click the Windows Master Control Panel icon to open the file.

It's not quite as exciting as being completely invulnerable in *Doom*, but as far as being in IT, having all these tools in one spot is pretty awesome. Before you start experimenting with the wide assortment of tools, you may want to consider taking a backup of your machine. As shown in Figure 2.9, when you open the `GodMode` folder, creating a backup and restore file will be one of the first options you see.



Name

Administrative Tools (11)

- Create and format hard disk partitions
- Defragment and optimize your drives
- Diagnose your computer's memory problems
- Free up disk space by deleting unnecessary files
- Manage computer certificates
- Schedule tasks
- Set up iSCSI initiator
- Set up ODBC data sources (32-bit)
- Set up ODBC data sources (64-bit)
- View event logs
- View local services

AutoPlay (3)

- Change default settings for media or devices
- Play CDs or other media automatically
- Start or stop using AutoPlay for all media and devices

Backup and Restore (Windows 7) (2)

- Backup and Restore (Windows 7)
- Restore data, files, or computer from backup (Windows 7)

Color Management (1)

- Change advanced color management settings for displays, scanners, and printers

Credential Manager (2)

- Manage Web Credentials
- Manage Windows Credentials

Figure 2.9: Just a few of the 260+ tools in God mode

CHAPTER 3
Nmap—The Network Mapper

WHAT YOU WILL LEARN IN THIS CHAPTER:

- Ports
- Protocols
- Services
- OS
- ZenMap

One of my favorite nonprofit organizations is the Center for Internet Security (CIS). The mission of CIS is to “identify, develop, validate, promote, and sustain best-practice solutions for cyber defense and build and lead communities to enable an environment of trust in cyberspace.” CIS is a collection of subject-matter experts (SMEs) who are able to work together to identify effective security measures for the good of everyone. CIS has an important role in cybersecurity. One of its many contributions is maintaining the most powerful and current cybersecurity best-practices documentation called the “CIS Controls Version 7.”

The controls are divided into basic, foundational, and organizational actions so that you can protect your organization and safeguard your data from cyberattacks. Attackers all over the world are scanning public-facing IP addresses, attempting to find weaknesses in a network.

This chapter will focus on the top CIS-recommended set of actions that all organizations should take. The first is the inventory and control of hardware assets, and the second is the inventory and control of software on those assets. When you are able to track and manage devices and software on your network, you ultimately prevent unauthorized devices and software. You have increased your security posture.

One of the first things you will do to build a security program is implement inventory control. The tool we will start this process with is Nmap, an open source network mapper. Many system administrators find Nmap to be useful when they need to build their documentation around network inventory and topology. In the background, Nmap manipulates IP packets in several ways, attempting to determine what assets are on the network. It will also attempt to find what services, applications, and operating systems are on those assets.

Nmap was originally built as a command-line tool you could execute through a shell or terminal window. The goal was to build a flexible and extremely powerful free open source tool. Originally built on Linux for pure-hearted system administrators, it evolved and is available for Windows as well as in a graphical user interface (GUI) format, Zenmap. There are more than 100 command-line options in Nmap, and some of these were never fully documented by the author, Gordon Lyon.

In any size network but especially large, dynamic networks, it is vitally important to break down these complex networks and analyze traffic, facilitate issues, and fix connection problems. Network scanning is a process of finding assets that are alive or have a heartbeat, communicating and then gathering as much vital information about those assets as possible. Network scanning can be divided into four stages:

- Network mapping
- Open ports
- Services running
- Operating systems

Network Mapping

Network mapping uses a process to discover and visualize assets by actively probing them. Nmap sends both TCP and UDP packets to a targeted machine. These are called *probe packets*. A probe packet is a packet used in an active tool to collect information on a network segment of interest. Data is collected after sending those probe packets that hop from node to node and asset to asset, which returns that information to Nmap.

If you were to scan 65,536 ports on every single machine in your ecosystem, this scan could take an astronomically long time and is really unnecessary. Occasionally, you may hear someone refer to a host discovery scan as a ping scan. In Nmap, you could choose to skip the ping itself and use other targeted methods to find the active hosts on your network.

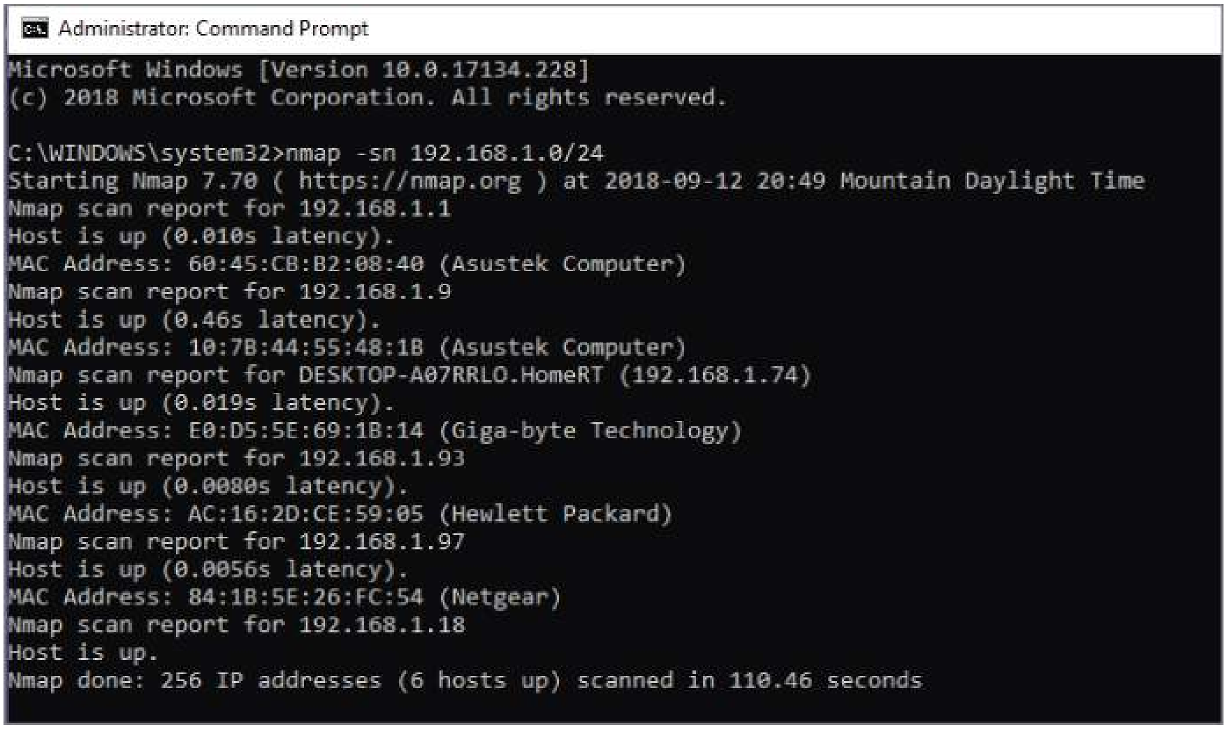
Network environments are all different; therefore, host discovery needs are going to be very different. The hosts on your network serve multiple purposes, and from a priority standpoint, not all assets are created equal. Some assets are mission critical, while some are used only occasionally and are not as important.

By default, Nmap starts its process by launching host discovery. By default, Nmap will send an ICMP echo request, ICMP timestamp request, and a TCP packet to port 80 (HTTP) and a TCP packet to port 443 (HTTPS). There are several options you can add to a basic Nmap scan to tailor it to your environment. You will definitely want to be using administrator credentials to execute these commands to achieve the best results. For example, Address Resolution Protocol (ARP) is enabled when scanning networks when you are using administrator credentials. ARP is a protocol for mapping an IP address to a physical address on a host called a *Media Access Control (MAC) address*. The table that gets created during an ARP request is called the ARP cache and matches a host's network address with its physical address.

To launch a scan on a network segment, use the following command:

```
>nmap -sn <target addresses>
```

The results will include all active hosts that respond to the probes sent by Nmap. The option `-sn` disables port scanning while leaving the discovery phase untouched. Figure 3.1 shows how Nmap does a ping sweep of assets, meaning you will see only the available hosts that responded to the probes sent out. Most system administrators find this option to be extremely useful and quick to verify which assets are active on the network.



```
Microsoft Windows [Version 10.0.17134.228]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>nmap -sn 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-12 20:49 Mountain Daylight Time
Nmap scan report for 192.168.1.1
Host is up (0.010s latency).
MAC Address: 60:45:CB:B2:08:40 (Asustek Computer)
Nmap scan report for 192.168.1.9
Host is up (0.46s latency).
MAC Address: 10:7B:44:55:48:1B (Asustek Computer)
Nmap scan report for DESKTOP-A07RRLO.HomeRT (192.168.1.74)
Host is up (0.019s latency).
MAC Address: E0:D5:5E:69:1B:14 (Giga-byte Technology)
Nmap scan report for 192.168.1.93
Host is up (0.0080s latency).
MAC Address: AC:16:2D:CE:59:05 (Hewlett Packard)
Nmap scan report for 192.168.1.97
Host is up (0.0056s latency).
MAC Address: 84:1B:5E:26:FC:54 (Netgear)
Nmap scan report for 192.168.1.18
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 110.46 seconds
```

Figure 3.1: `nmap` command

It is important to scan periodically for new assets that have been added to your network without notification. Change management procedures are not followed or, in a new business, not even written. New machines can be added to networks without being scanned for vulnerabilities.

I had a situation once where the system administrator would scan systems for vulnerabilities in the evenings and on weekends to avoid production hours. Over the weekend, he would see a server pop up in his scans. When this admin would come back in on Monday, he couldn't ping this server. It had disappeared. This happened for a couple weeks until he finally found the problem. One of the networking support people who were supposed to be working over the weekend had a gaming server under his desk. They were having LAN wars instead of patching systems. When they were done “working,” the server was unplugged from the network.

Port Scanning

A port scan is a way to figure out which ports on a network are open and which are listening and possibly show whether there are any security devices such as firewalls between the sender and receiver. This process is called *fingerprinting*.

Ports are numbered from 0 to 65,535, but the lower range of 0 to 1,023 consists of the “well-known” ones. A port scan will carefully craft a packet to each destination port. There are some basic techniques to choose from, depending on the network topology and scanning goals.

- **Vanilla scan**: This is the most basic scan, fully connecting to 65,536 ports. It's accurate but easily detectable.
- **SYN scan**: This scan sends a SYN but does not wait for a response. It's faster, but you still learn if the port is open.
- **Strobe scan**: This selectively attempts to connect to only a few ports, typically fewer than 20.

There are some other techniques that penetration testers use, such as Stealth, FTP Bounce, and XMAS, which are scans that were developed so the sender could scan undetected. The sender's location can be obfuscated so that an attacker can get the information while not being tracked.

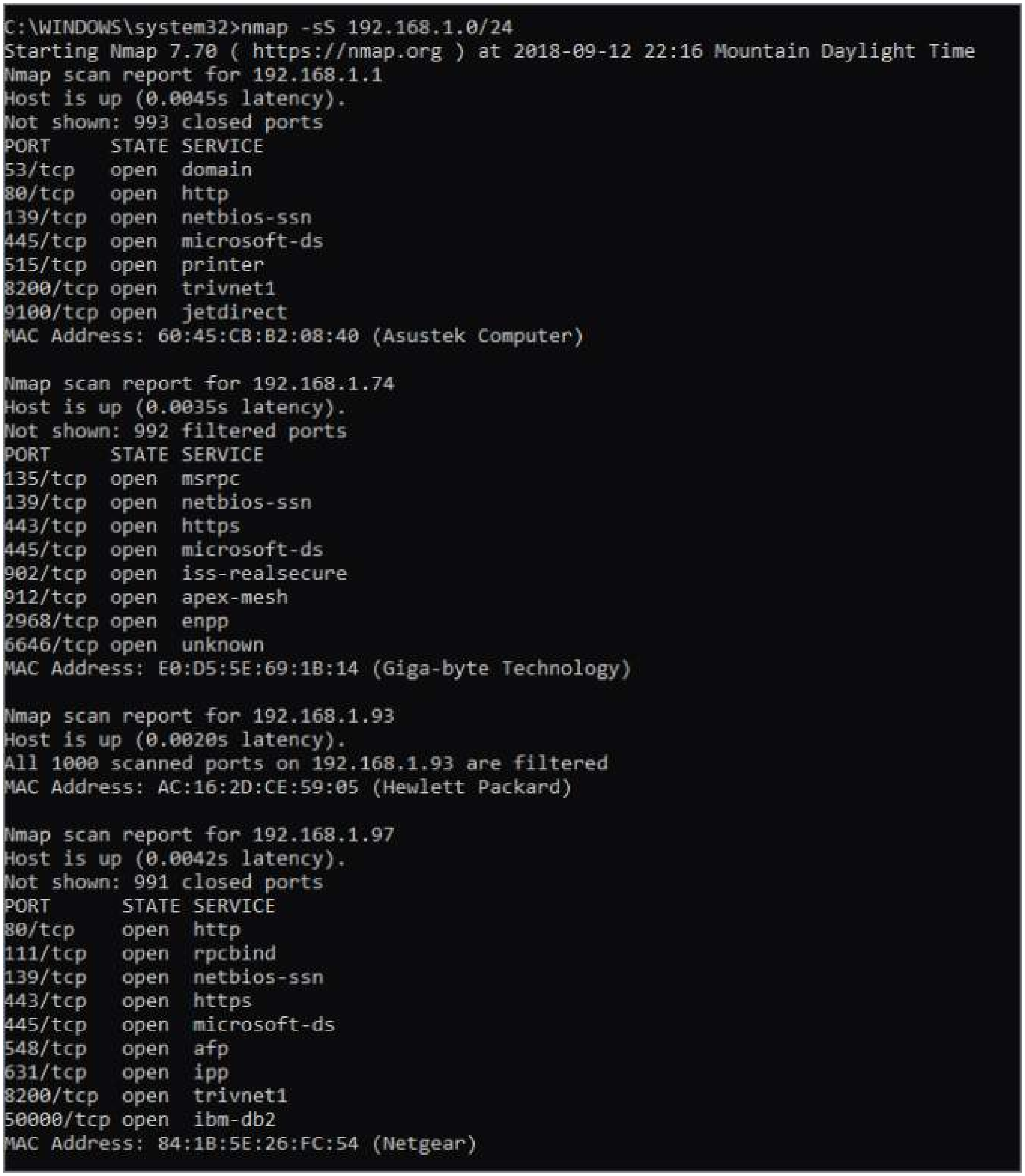
Now that you know a machine is alive on the network, it's time to determine which ports are open on that host. From a security viewpoint, it is vital to the health and well-being of your network to know exactly which of the 65,536 ports might be exposed. There are six port states that are currently recognized by Nmap.

- **Open**: An application is actively listening for a connection.
- **Closed**: A probe has been received, but no application is listening.
- **Filtered**: It's unknown if port is open; packet filtering typically from a firewall has prevented a probe from reaching the port.

Sometimes you get an error response, and sometimes filters will just drop the probe.

- **Unfiltered**: A port is accessible, but Nmap hasn't a clue if the port is open or closed.
- **Open/filtered**: The port is filtered or open, but no state is established.
- **Closed/filtered**: Nmap is unable to determine whether the port is closed or filtered.

The most popular port scan to use by default is the `-sS`, or SYN, scan you see in Figure 3.2. It is a fast scan, scanning thousands of ports per second relatively stealthily since it's not waiting around for an acknowledgment.



```
C:\WINDOWS\system32>nmap -sS 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-12 22:16 Mountain Daylight Time
Nmap scan report for 192.168.1.1
Host is up (0.0045s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
515/tcp  open  printer
8200/tcp open  trivnet1
9100/tcp open  jetdirect
MAC Address: 60:45:CB:B2:08:40 (Asustek Computer)

Nmap scan report for 192.168.1.74
Host is up (0.0035s latency).
Not shown: 992 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
2968/tcp open  enpp
6646/tcp open  unknown
MAC Address: E0:D5:5E:69:1B:14 (Giga-byte Technology)

Nmap scan report for 192.168.1.93
Host is up (0.0020s latency).
All 1000 scanned ports on 192.168.1.93 are filtered
MAC Address: AC:16:2D:CE:59:05 (Hewlett Packard)

Nmap scan report for 192.168.1.97
Host is up (0.0042s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
548/tcp   open  afp
631/tcp   open  ipp
8200/tcp  open  trivnet1
50000/tcp open  ibm-db2
MAC Address: 84:1B:5E:26:FC:54 (Netgear)
```

Figure 3.2: Nmap SYN scan

To launch a port scan on a network segment, use the following command:

```
>nmap -sS <target addresses>
```

Services Running

Many moons ago, I taught the CompTIA classes for Iron Horse University at Fort Carson in Colorado Springs. My soldiers would sit in my classroom for two weeks of instruction and hands-on learning. So, if someone wanted to talk to one of my soldiers, they would come down the hall and into classroom 4. They needed a specific person, so they would go to that person's seat so they could talk to him or her.

As an example, let's say the soldier's name was Carla, who was seated in seat 23. So, Carla's socket was classroom.4:23. A socket is a point of ingress or egress. The combination of an IP address and a port is called an *endpoint*. A socket is one of the endpoints in a two-way conversation between two programs communicating over a network. A socket is bound to a port number so we know which application that data is destined for.

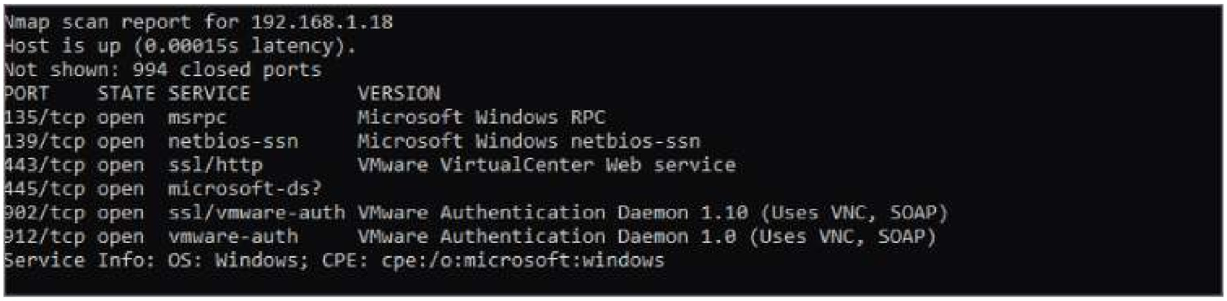
The person sitting in seat 23 is like the program that is registered with the operating system to listen at that port. What if Carla was absent? What if someone else was sitting in seat 23? Programs listening on a certain port may or may not be the usual listener. You need to know whether Carla and Robert swapped seats. Table 3.1 describes the most common ports and the services that should be running on them.

Table 3.1: Top Ports Defined

PORT NUMBER	**NAME**	**DEFINED**	**USED FOR**
20	FTP-data	File Transfer Protocol	Moving files between client and server
21	FTP-control	File Transfer Protocol	Control information for moving files
22	SSH	Secure Shell	Security for logging in and file transfer
23	Telnet	Telnet Protocol	Obsolete unencrypted communication
25	SMTP	Simple Mail Transfer Protocol	Sending/routing email
53	DNS	Domain Name System	Phonebook of the Internet; translates names of websites to IP addresses
80	HTTP	Hypertext Transfer Protocol	Foundation of the World Wide Web
110	POP3	Post Office Protocol	Receiving email by downloading to your host
123	NTP	Network Time Protocol	Synchronizes the clocks on computers on your network
143	IMAP	Internet Message Access Protocol	View email messages from any device; does not download to a host
161	SNMP	Simple Network Management Protocol	Collects information and configures different network devices

PORT NUMBER	NAME	DEFINED	USED FOR
443	HTTPS	Hypertext Transfer Protocol Secure	The secure version of HTTP; information between a browser and website is encrypted
445	Microsoft DS	Microsoft-Directory Services	SMB over IP; preferred port for Windows file sharing
465	SMTPS	Secure SMTP	Authenticated SMTP over SSL
1433	MSSQL	Microsoft SQL	Microsoft SQL database management system
3389	RDP	Remote Desktop Protocol	Application sharing protocol

If you want to run a services scan against the machines in your ecosystem, Nmap will tell you which of the hundreds of thousands of ports might be open on a host. If a port is open, communication can occur. Sometimes that communication is unwanted and is what you are trying to protect against. For example, in Figure 3.3 you see the Nmap scan report showing the ports that are open, the service, the state, and the version.



```
Nmap scan report for 192.168.1.18
Host is up (0.00015s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE         VERSION
135/tcp open  msrpc           Microsoft Windows RPC
139/tcp open  netbios-ssn     Microsoft Windows netbios-ssn
443/tcp open  ssl/http        VMware VirtualCenter Web service
445/tcp open  microsoft-ds?
902/tcp open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Figure 3.3: Nmap scan report

To launch a services scan on a network segment, use the following command:

```
>nmap -sV <target addresses>
```

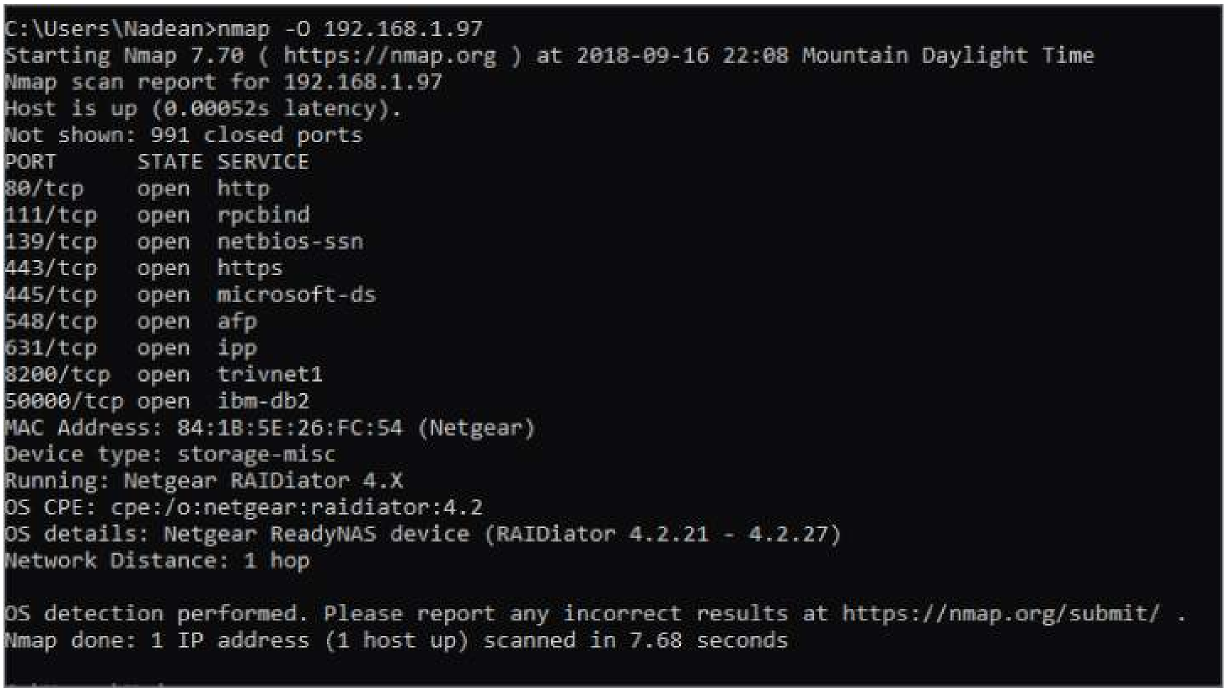
When you do a service scan with Nmap, it will tell you which ports are open and will use a database that lists more than 2,000 well-known services that are typically running on those ports. It has been my experience that network administrators are opinionated and will have their own ideas of how services in their enterprise environment should be configured, so sometimes that database and reality do not match up. If you are doing inventory or vulnerability management, you want to be as accurate as possible and know the version and patch level of systems whenever available.

Version detection investigates those ports to figure out what is actually running. The `nmap-services-probes` database contains certain probe packets for discovering services and matching them to responses. Nmap will attempt to determine the service, application, version number, hostname, device type, and operating system.

Operating Systems

Nmap is often used to detect the operating system of a machine. Being able to correctly identify the operating system is key for many reasons, including doing inventory and finding vulnerabilities and specific exploits. Nmap is known for having the most robust and comprehensive OS fingerprint database.

When you are identifying specific operating systems, the key is how the operating system responds to Nmap probe packets. Windows XP and Windows Server 2003 are nearly identical, while Windows Vista and Ubuntu Linux 16 are completely different in the way they respond. In Figure 3.4, you see the response of an `nmap -O` command. To enable operating system detection, use the following command:



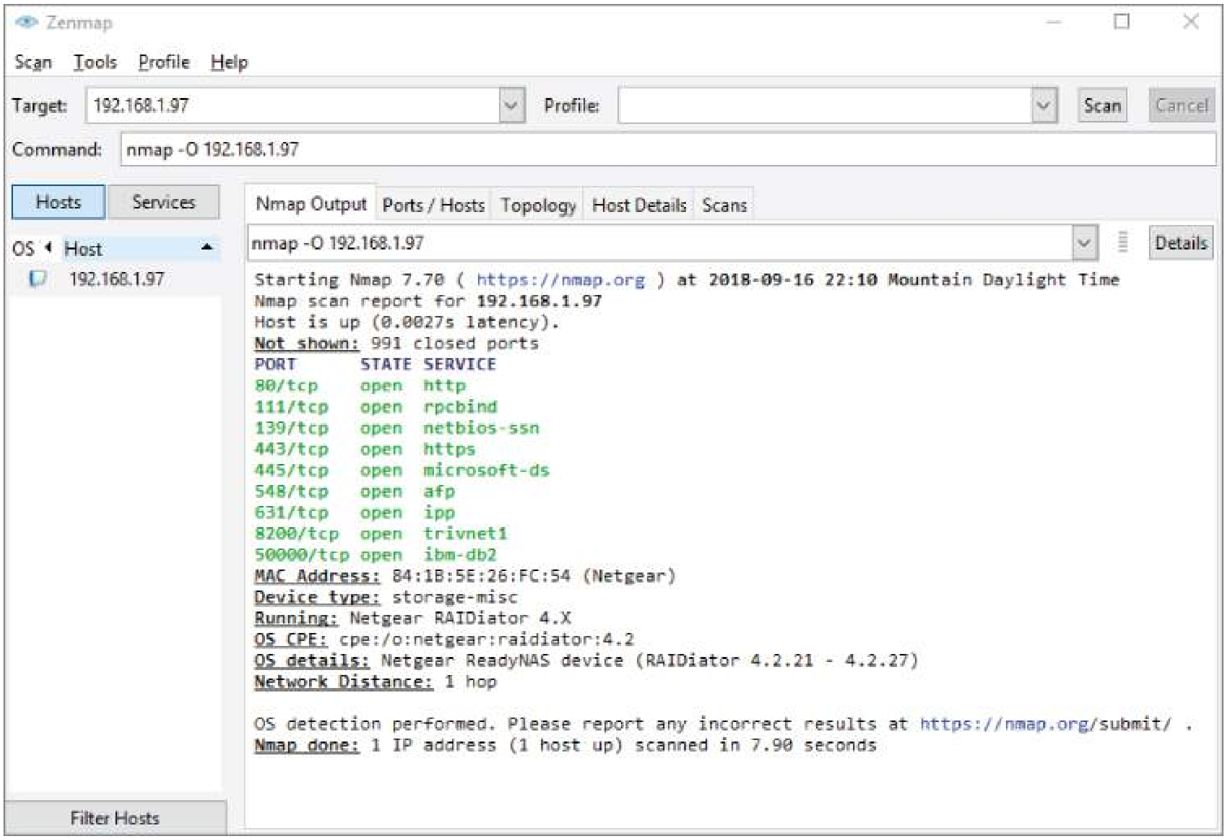
```
C:\Users\Nadean>nmap -O 192.168.1.97
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-16 22:08 Mountain Daylight Time
Nmap scan report for 192.168.1.97
Host is up (0.00052s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
548/tcp   open  afp
631/tcp   open  ipp
8200/tcp  open  trivnet1
50000/tcp open  ibm-db2
MAC Address: 84:1B:5E:26:FC:54 (Netgear)
Device type: storage-misc
Running: Netgear RAIDiator 4.X
OS CPE: cpe:/o:netgear:raidiator:4.2
OS details: Netgear ReadyNAS device (RAIDiator 4.2.21 - 4.2.27)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.68 seconds
```

Figure 3.4: `nmap -O`

```
>nmap -O <target addresses>
```

Zenmap

Everything in this chapter thus far has been done through the command line or terminal interface. As Nmap has matured, so has the interface. Zenmap is the GUI of Nmap. It is a multiplatform, free, and open source application. There are some benefits to Zenmap that the good old command-line Nmap cannot do, such as building topology, creating interactive maps, showing comparisons between two scans, keeping and tracking the results of a scan, and making the scan duplicable. Zenmap's goal is to make scanning easy and free for beginners and experts alike. You only have to identify your target and hit the Scan button, as you see in Figure 3.5.



Target: 192.168.1.97

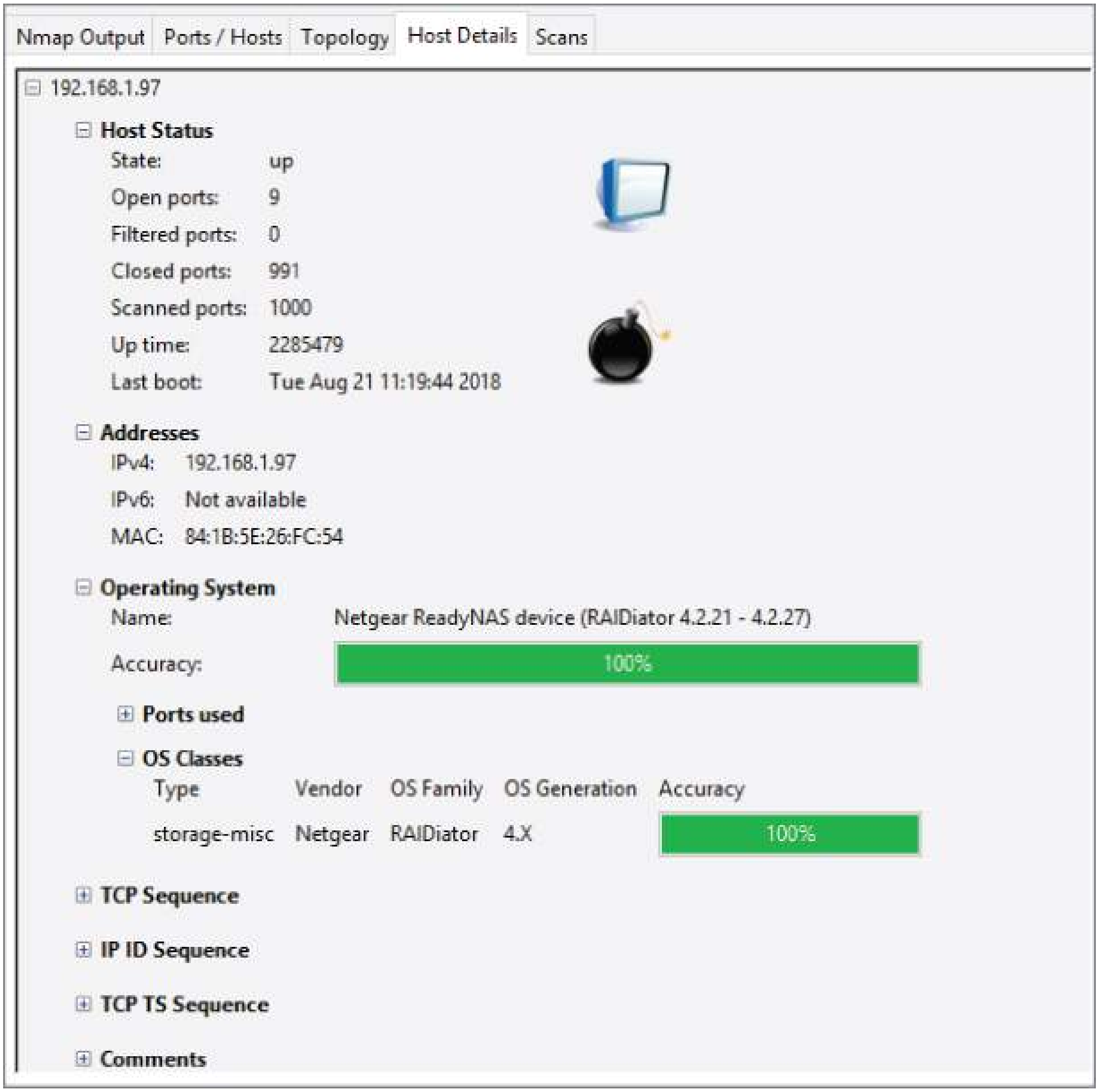
Command: nmap -O 192.168.1.97

nmap -O 192.168.1.97

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-16 22:10 Mountain Daylight Time
Nmap scan report for 192.168.1.97
Host is up (0.0027s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
548/tcp   open  afp
631/tcp   open  ipp
8200/tcp  open  trivnet1
50000/tcp open  ibm-db2
MAC Address: 84:1B:5E:26:FC:54 (Netgear)
Device type: storage-misc
Running: Netgear RAIDiator 4.X
OS CPE: cpe:/o:netgear:raidiator:4.2
OS details: Netgear ReadyNAS device (RAIDiator 4.2.21 - 4.2.27)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.90 seconds
```

Figure 3.5: Zenmap GUI scan

As you can see, this scan is the exact previous scan, just done in a GUI. If you clicked the tabs across the middle, you would see a list of all ports open, the network topology, the host details, and the history of scans of this asset, as you see in Figure 3.6.



192.168.1.97

Host Status

State: up

Open ports: 9

Filtered ports: 0

Closed ports: 991

Scanned ports: 1000

Up time: 2285479

Last boot: Tue Aug 21 11:19:44 2018

Addresses

IPv4: 192.168.1.97

IPv6: Not available

MAC: 84:1B:5E:26:FC:54

Operating System

Name: Netgear ReadyNAS device (RAIDiator 4.2.21 - 4.2.27)

Accuracy: 100%

Ports used

OS Classes

Type	Vendor	OS Family	OS Generation	Accuracy
storage-misc	Netgear	RAIDiator	4.X	100%

TCP Sequence

IP ID Sequence

TCP TS Sequence

Comments

Figure 3.6: Zenmap host details

To save an individual scan to a file, choose the Scan menu and select Save Scan from the drop-down. If there is more than one scan, you will be asked which one to save. You have a choice of saving in `.xml` or `.txt` format. The `.xml` format can only be opened and used again by Zenmap. By default, all scans are saved automatically, but only for 60 days.

Before you install Nmap or Zenmap, you will want to make sure it isn't already installed. There are several operating systems (including most Linux systems) that have Nmap packages embedded but not installed. Type the following at a command prompt:

```
nmap --version
```

This will display the version of Nmap that is installed. If you get an error message such as `nmap: command not found`, then Nmap is not installed on your system.

Zenmap is found in the executable Windows installer. The latest stable release will be on the www.nmap.org/download page. To download the executable file, click the link shown in Figure 3.7.

Latest stable release self-installer: nmap-7.70-setup.exe

Figure 3.7: Downloading `nmap-7.70-setup.exe`

As with most executable files for Windows, the file is saved by default in the Downloads folder. Double-click the executable to start the install process. Click Next through the windows, keeping all the defaults, until you get to Finish. Once the install has completed, open the Start menu on your taskbar and begin typing **Nmap**. At the top of your menu, you should see Nmap-Zenmap GUI. Click the application, define the target assets, and click Scan to launch.

The white paper “CIS Controls Implementation Guide for Small- and Medium-Sized Enterprises (SMEs)” published at www.cisecurity.org breaks down into these three phases:

1. Know your environment.
2. Protect your assets.
3. Prepare your organization.

In phase 1, Nmap is described as a famous multipurpose network scanner, and Zenmap is described as an easy-to-use graphic user interface for Nmap. You must know your environment better than an attacker and use that attacker's mind-set in key controls to develop your security program.

CHAPTER 4
Vulnerability Management

WHAT YOU WILL LEARN IN THIS CHAPTER:

- Managing vulnerabilities
- OpenVAS
- Continuous assessment
- Remediation
- Nexpose Community

I have years of vulnerability management experience. At first, it was theoretical when I was teaching at Louisiana State University. It became a more hands-on role when I worked as an IT director for a small private school and then again when I worked for the U.S. Department of Defense (DoD) as a contractor. If you are planning to take any security certification exams—whether it's ISACA, ISC2, or CompTIA—you need to be aware that the management of the vulnerability lifecycle and risk is a key component on those exams.

Some ships are titanic, and some boats are small. Some boats, like a kayak, could represent your home network, while a Fortune 50 company would be more like the *Queen Elizabeth II*. The goal of both vessels is the same: Don't sink. If you have been tasked with vulnerability management, your task is the same: Don't sink.

Managing Vulnerabilities

As I mentioned earlier, you must know your environment better than an attacker and use that attacker's mind-set in key controls to develop your security program. Now that you have all the open-source tools to troubleshoot your network and you know what assets you have to protect, you have to be able to assess those assets for vulnerabilities. It is a cyclic endeavor, as shown in Figure 4.1.

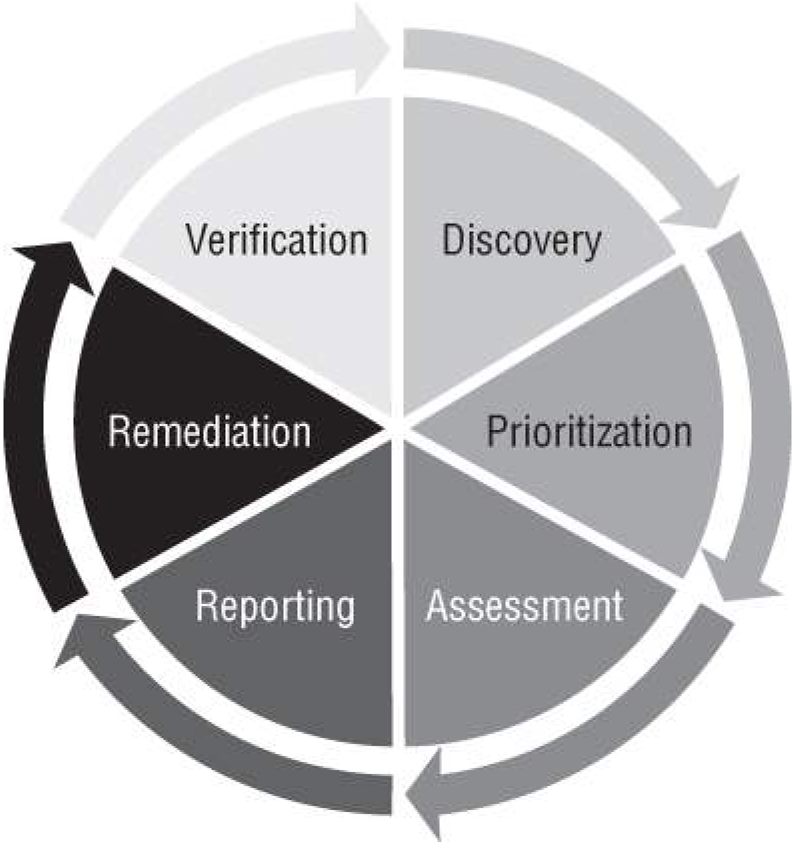


Figure 4.1: The vulnerability management lifecycle

In the discovery phase, you have to figure out what is on your network communicating to other devices. You cannot protect what you don't know you have. Once you're able to map out the assets, hosts, nodes, and intermediary devices on your network, then you're able to move to the next step.

Not all devices are created equal. A domain is a group of computers and other devices on a network that are accessed and administered with a common set of rules. A Windows domain controller (DC) is a Microsoft server that responds to login authentication requests within a network. In an enterprise environment, if a DC fails, your help desk will explode with calls because of the inability for users to log in to the domain. However, if you have a marketing department with a small file server that it backs up to once a month, if this machine fails, then it might warrant a phone call or two. After you know what machines exist on your network, you must prioritize which assets are mission critical.

Once you have identified which assets have a heartbeat and you know which assets would cause chaos through failure or compromise, the next step is to determine the assets' vulnerabilities. This is usually accomplished by analyzing the operating system, ports that are open, services running on those ports, and applications you have installed on those assets.

Now you're ready to build a report. Some reports will bubble up to upper management and require information such as trending analysis and vulnerability remediation plans. The decisions that upper management will make based on these reports could be budgetary or based on head count. The more technical reports will usually trickle down to the asset owner and contain what needs to be fixed on that device.

With the report in hand, you now have a list of vulnerabilities in your environment and on what device they reside. Some software with advanced capabilities will generate instructions on how to remediate those vulnerabilities. Most of these technical reports will give you a severity rating typically based on the Common Vulnerability Scoring System (CVSS), as listed in Table 4.1. The National Institute of Standards and Technology (NIST) maintains the National Vulnerability Database (NVD). In this database, you can see a quantitative analysis of every vulnerability based on access vector, complexity, and authentication as well as the impact to confidentiality, integrity, and availability. Basically, this means every vulnerability will have a score of 0 to 10, with 0 being good and 10 being horrendously awful.

Table 4.1: CVSS v3.0 Ratings

Source: National Institute of Standards and Technology

SEVERITY	BASE SCORE RANGE
None	0
Low	0.1–3.9
Medium	4.0–6.9
High	7.0–8.9
Critical	9.0–10.0

In the vulnerability management lifecycle, building your remediation attack plan is a critical step. After completing the asset classification and vulnerability assessment, you correlate the findings to compile your plan of action. There are some organizations I have worked with that have the goal of becoming 100 percent free of vulnerabilities, and that just isn't a realistic goal to have in our modern digital infrastructure. If you have devices connected and communicating to the world, there is a way into your network and a way out. On mission-critical devices, prioritize the repair of critical and high-severity vulnerabilities. Save the less critical devices to be remediated later.

There is nothing more frustrating than taking apart a PC, fixing what you think is the problem, putting that PC completely back together, and then realizing you didn't fix it and having to start over. Verification is vital to this process. If you do not rescan assets looking for the same vulnerability and you assume that your fix worked but it didn't, you will have a false sense of confidence in that item and leave yourself open to attack.

It has been my experience that the IT industry is one of the most dynamic, with constant change and evolution. There will be times in an enterprise environment that risky behavior will happen when change management processes and procedures are not followed. Our networks are constantly changing and evolving. The networking infrastructure staff throws a new server with no patches on the domain because the people who requested it have the authority to bypass security controls. There are people in the DoD with enough brass on their shoulders to ask for something like this without understanding the repercussions. Those assets still need to be scanned, and if they're not scanned before being added to your network, you get to scan them after.

Some organizations I have worked with have compliance needs that require they scan monthly. Some organizations have a robust security policy where they require assets to be scanned at least once a week. Either way, you vulnerability scanning is not just a one-time action. It is something that needs to be maintained to ensure your network/infrastructure is secure.

OpenVAS

The Open Vulnerability Assessment System (OpenVAS) is an open-source framework of several tools and services that offers powerful vulnerability scanning and management systems. It was designed to search for networked devices, accessible ports, and services and then test for vulnerabilities. It is a competitor to the well-known Nexpose or Nessus vulnerability scanning tool. Analyzing the results from tools like these is an excellent first step for an IT security team working to create a robust, fully developed picture of their network. These tools can also be used as part of a more mature IT platform that regularly assesses a corporate network for vulnerabilities and alerts IT professionals when a major change or new vulnerability has been introduced.

At the center of this modular service-oriented product is the OpenVAS scanner, sometimes called an *engine*. The scanner uses the Network Vulnerability Tests (NVT) maintained by Greenbone Networks based in Germany. Greenbone Networks was founded by experts for network security and free software in 2008 and provides an open-source solution for analyzing and managing vulnerabilities, assessing risk, and recommending an action plan. According to the OpenVAS website, there are more than 50,000 NVTs, and this number is growing weekly.

The OpenVAS Manager is the actual manager of the processes, controlling the scanner using OpenVAS Transfer Protocol (OTP) and OpenVAS Management Protocols (OMP). The Manager component schedules scans and manages the generation of reports. The Manager runs on a SQL database where all the scan results are stored. The Greenbone Security Manager (GSM) web application interface is the easiest alternative to the command-line client to control the scanner, schedule scans, and view reports. Once you have OpenVAS installed, you will log in through the Greenbone Security Assistant, as shown in Figure 4.2.

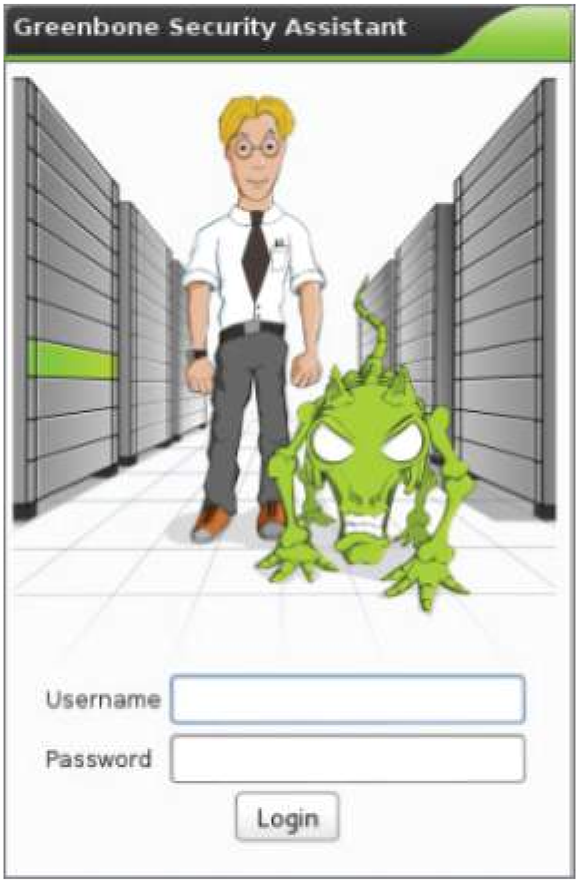


Figure 4.2: The Greenbone Security Assistant login for OpenVAS

An ISO file is a replication of an entire CD or DVD that you use to install operating systems or software. Sometimes called an *ISO image*, you will need this file to deploy the OpenVAS image. Once you have the OpenVAS `.iso` file from the website, you can install on bare metal or in a virtual environment. If you want to install this on a Linux system, I suggest 16.04. You will need a newly deployed

Ubuntu server, a nonroot user with `sudo` privileges, and a static IP address. You also need to know how to use the following commands:

```
    sudo apt-get update -y

    sudo apt-get upgrade -y

    sudo reboot
```

The `sudo` command is used on Linux systems and means "superuser do." If you are more familiar with the Windows environment, `sudo` is similar to right-clicking a program and choosing Run As Administrator. When you add the `-y` option, it will bypass any yes/no prompt with an affirmative answer.

The `apt-get update` command will update the list of available packages and versions. The `apt-get upgrade` command will install the newer versions.

A little like plug-and-play in the old days, you need to install the required dependencies using the following commands:

```
    sudo apt-get install python-software-properties

    sudo apt-get install sqlite3
```

OpenVAS is not a default in the Ubuntu repository, so to use the personal package archive (PPA), you must add it, update it, and install it using the following commands:

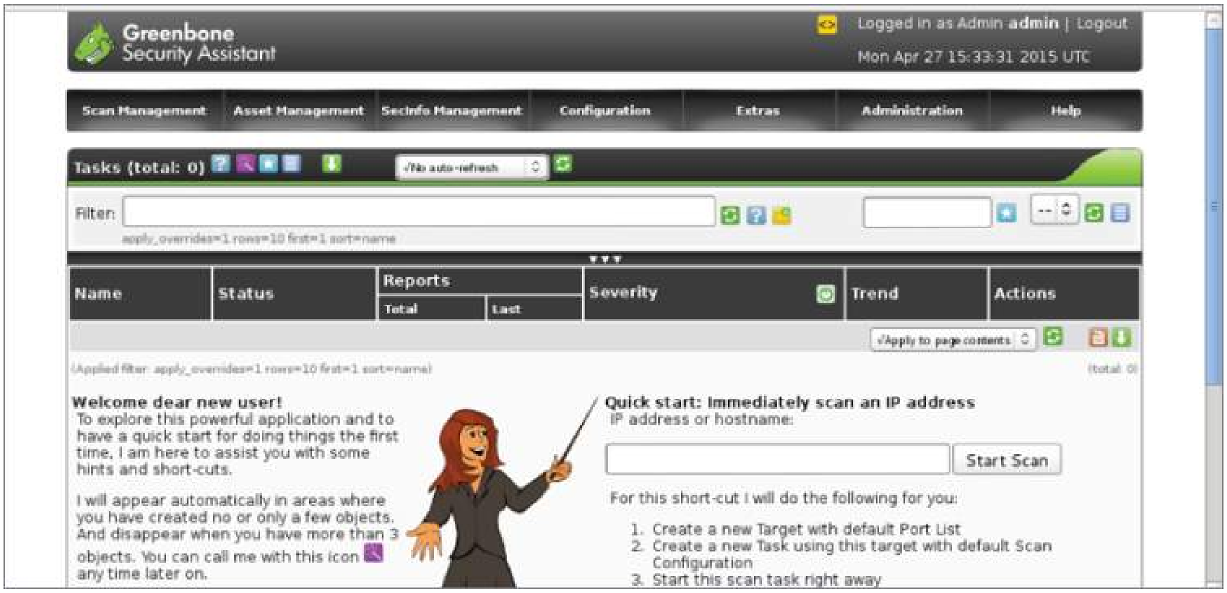
```
    sudo add-apt-repository ppa: mrazavi/openvas

    sudo apt-get update

    sudo apt-get install openvas
```

By default, OpenVAS runs on port 443, so you need to allow this through your firewalls to enable the update of the vulnerability database. The NVT database contains more than 50,000 NVTs, and this is always growing. For online synchronization, use the following command:

```
    sudo openvas-nvt-sync
```

If you skip this step, you will most likely have critical errors later. If you prefer, you can wait until you launch the program and go to the Administration feature inside the software to update the vulnerability database feed. Either way, it must be done.

Once the database is synced, use your browser (preferably Mozilla Firefox) to log into `https://`*`your static IP address`* with the default credentials *admin*/*admin*. You should then see the OpenVAS Security Assistant welcome page displayed on your screen, as shown in Figure 4.3.



Welcome dear new user!
To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.

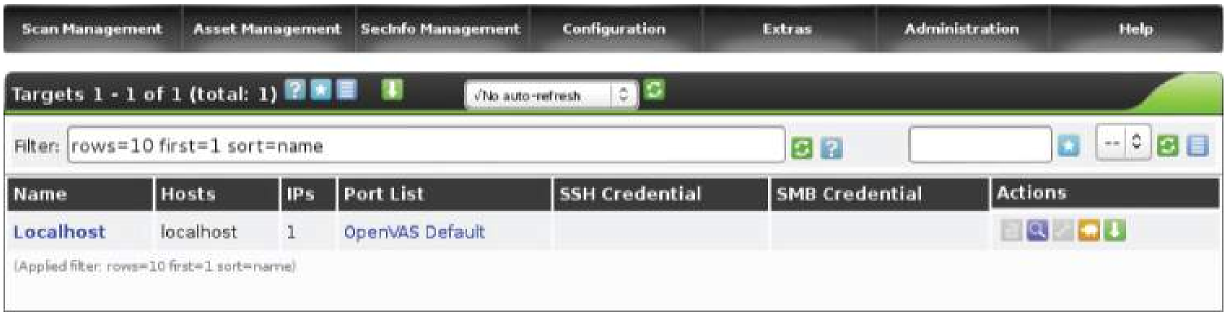
Quick start: Immediately scan an IP address
IP address or hostname:

For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away

Figure 4.3: Greenbone Security Assistant welcome screen for OpenVAS

The blue star icon is one of the most important buttons on the home page. It will allow you to add a new object such as the configuration of a scan or host list. If you are looking to scan just one IP address, you can use the super-quick Scan Now button on the home page. To get familiar with the software, start with one such as in Figure 4.4 and then branch out to many.



Targets 1 - 1 of 1 (total: 1)

Filter: rows=10 first=1 sort=name

Name	Hosts	IPs	Port List	SSH Credential	SMB Credential	Actions
Localhost	localhost	1	OpenVAS Default			

(Applied filter: rows=10 first=1 sort=name)

Figure 4.4: The default Localhost setup for launching a scan

As you may have noticed, there are multiple star icons. If you use the star icon on the right side of the program, you will create a new filter. To add a list of subnets, use the star icon in the top header of the Targets page. The process from start to finish will look like what's shown in Figure 4.5.

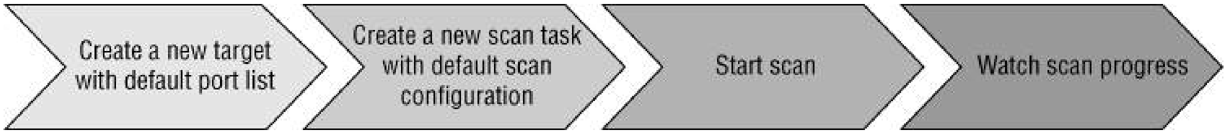

Create a new target with default port list
Create a new scan task with default scan configuration
Start scan
Watch scan progress

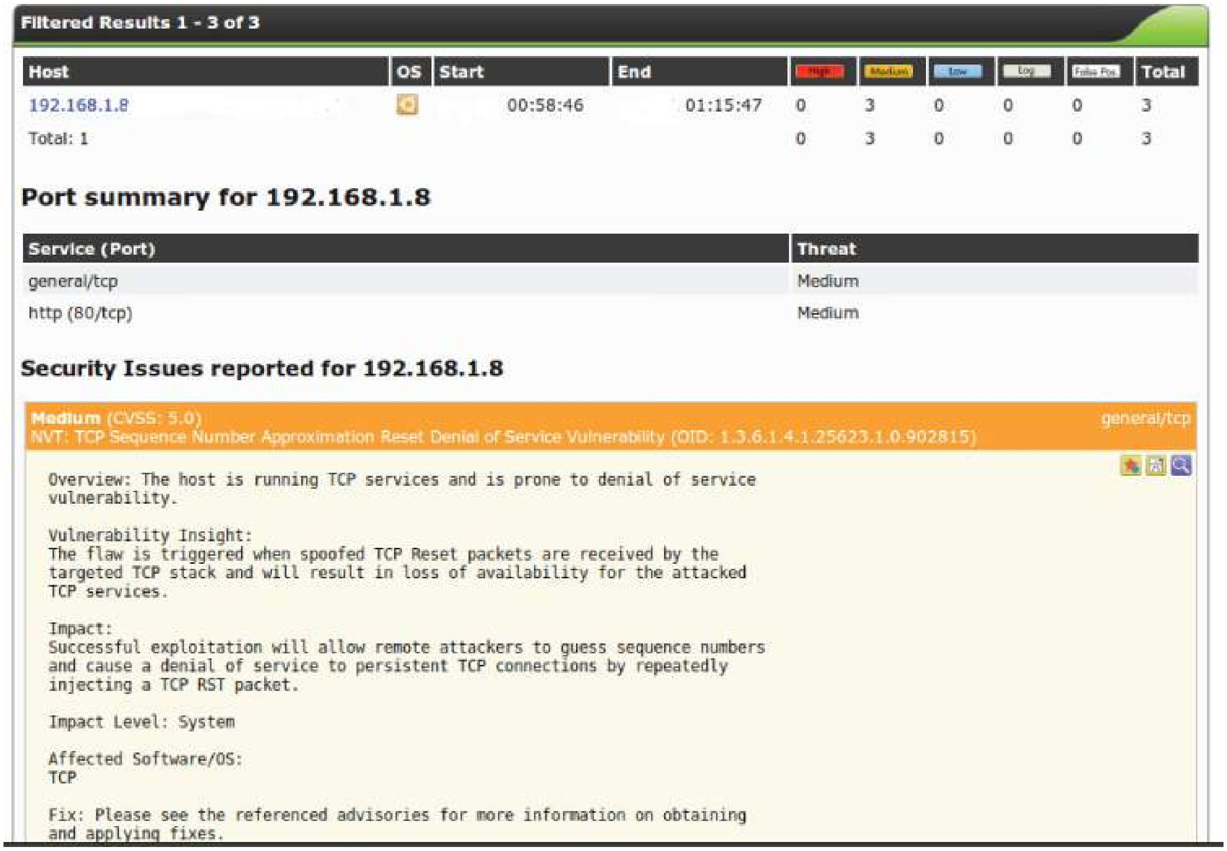
Figure 4.5: Workflow for a scan of assets for vulnerabilities

1. To configure a list of hosts after you're done with the one, navigate to the Configuration tab. Look for Targets in the header portion of the page. This is where you can add a new list of subnets of IP address ranges. Please be aware that, depending on the size of your subnets of IP address ranges, CIDR notation can occasionally error out. You may just need to itemize the list of individual IP addresses. Your local host will be listed on the home page by default.
2. Name the scan appropriately. I usually try to name the scan in a way that allows me to refer to the name and know what I scanned rather than some type of numerical name where I have to actually open the scan to know what I was thinking at the time. The scanning configuration can be left at the default of Full And Fast Ultimate. Select your targets and click Create Task. The new task will show up with a green bar next to the status of New.
3. When you're ready, click the green arrow under Actions to run this new task and start your scan.

4. This is the part I love—watching in the task details page. To watch the scan live, set the No AutoRefresh option to Refresh Every 30 Sec. It's better than television. Depending on how many targets you listed, the scan should be done within a few minutes.

Reporting is vital to your vulnerability management lifecycle. After the scan has completed, check the summary of scan results. They will be classified into High, Medium, and Low and will also contain logs. Each issue that has been discovered will be detailed into vulnerabilities, impact, affected software, and (my favorite if it's available) how to fix what is broken. You can download and export this file as a `.pdf`, `.txt`, `.xml`, or `.html` file.

Figure 4.6 is an example of filtered results to include in a report. You have the IP address of the host, what operating system is on the host, and the security issues and threat level below.



Filtered Results 1 - 3 of 3

Host	OS	Start	End	High	Medium	Low	Log	False Pos.	Total
192.168.1.8		00:58:46	01:15:47	0	3	0	0	0	3
Total: 1				0	3	0	0	0	3

Port summary for 192.168.1.8

Service (Port)	Threat
general/tcp	Medium
http (80/tcp)	Medium

Security Issues reported for 192.168.1.8

Medium (CVSS: 5.0) general/tcp
NVT: TCP Sequence Number Approximation Reset Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902815)

```
Overview: The host is running TCP services and is prone to denial of service
vulnerability.

Vulnerability Insight:
The flaw is triggered when spoofed TCP Reset packets are received by the
targeted TCP stack and will result in loss of availability for the attacked
TCP services.

Impact:
Successful exploitation will allow remote attackers to guess sequence numbers
and cause a denial of service to persistent TCP connections by repeatedly
injecting a TCP RST packet.

Impact Level: System

Affected Software/OS:
TCP

Fix: Please see the referenced advisories for more information on obtaining
and applying fixes.
```

Figure 4.6: Summary results of an asset

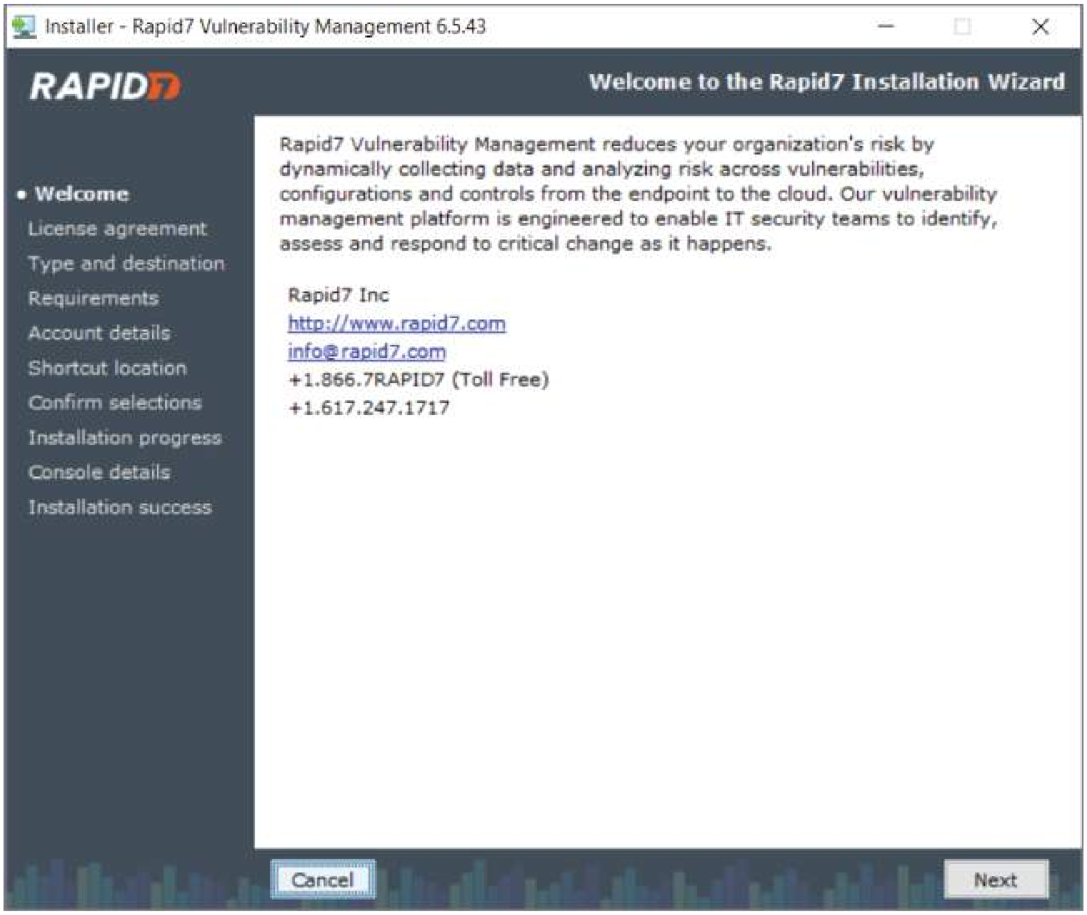
Nexpose Community

A lot of organizations offer free or community editions of their software. These editions are usually a lighter version of the paid copy with limited features. Once such community vulnerability management software is Nexpose by Rapid7. There are several versions of Nexpose but the community version is an excellent place to start learning because it's free. If you search in a browser for “Nexpose Community,” one of the first options should be the community software directly from Rapid7. You could download from other third parties but I find it safer to download and verify software directly from the vendor whenever possible.

After you complete the form to receive your community license, you will end up on a page to download either the Windows or Linux version with its MD5 sum hash. The hash will verify that your download is not corrupt. Once the download is finished, run the installer. You will notice the community version of Nexpose will only work on 64-bit architecture. To scan an enterprise for vulnerabilities takes a lot of resources including CPU and RAM. Historically, 32-bit architecture can only recognize 4GB of RAM. Nexpose Community cannot do a proper scan with only 4GB of RAM.

LAB 4.1: INSTALLING NEXPOSE COMMUNITY

1. Download and open the executable file. Click Next as you see in Figure 4.7.



Installer - Rapid7 Vulnerability Management 6.5.43

Welcome to the Rapid7 Installation Wizard

Rapid7 Vulnerability Management reduces your organization's risk by dynamically collecting data and analyzing risk across vulnerabilities, configurations and controls from the endpoint to the cloud. Our vulnerability management platform is engineered to enable IT security teams to identify, assess and respond to critical change as it happens.

Rapid7 Inc
http://www.rapid7.com
info@rapid7.com
+1.866.7RAPID7 (Toll Free)
+1.617.247.1717

Figure 4.7: Installing Nexpose Community GUI

2. You will choose Security Console with local Scan Engine. You will see the option for Scan Engine only which gives you the ability to deploy scanning engines close to the assets to do the scanning work and then bubble that information up to the scan console without compromising bandwidth. Nexpose runs on a PostgreSQL 9.4.1 database which comes included in the console. Because of the size of most environments, the recommended storage for the database is 80GB. The console will naturally bind to port 3780, which is important when we access the software through the browser through

https://youripaddress:3780. The PostgreSQL database will communicate over 5432 unless you change it at this stage of installation.

3. You will add user details including First Name, Last Name, and Company. This is done to create the SSL certificate should you ever need to request help or send data to tech support.
4. Create secure credentials and remember them. You will not be able to easily recovery them. Please do not use admin/admin in these fields. Make them as robust as possible.
5. Click Next twice to review the settings and begin extracting files to complete the installation. In Figure 4.8 you see the hyperlink that you will be using to access the program. Install will require a reboot, be sure to save anything you have open and grab a bite to eat. Nexpose loads over 130,000 vulnerability definitions at startup and can take up to 30 minutes.

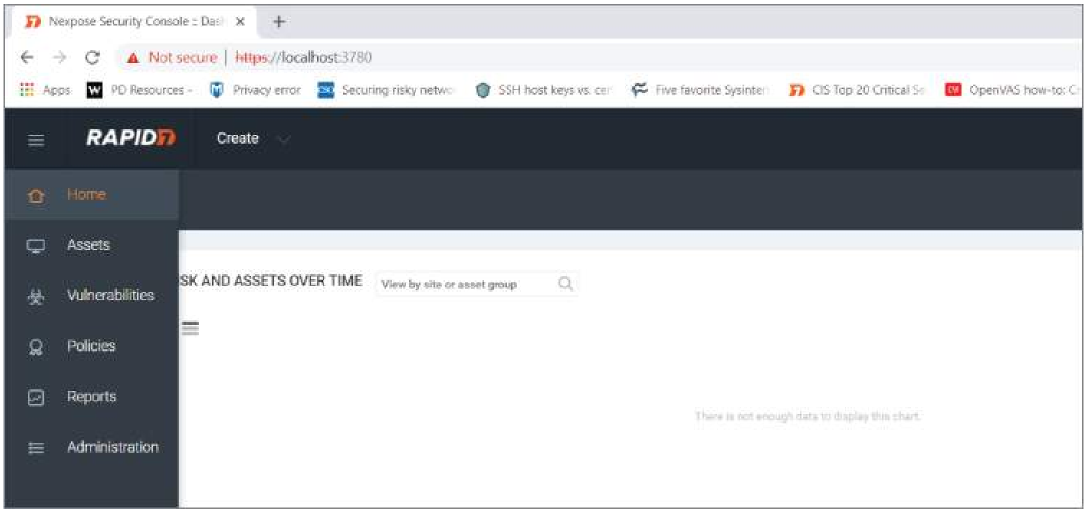


Figure 4.8: Nexpose Community Menu

6. When you come back after rebooting, you will see the orange Rapid7 logo on your desktop. You will need the license that was sent to the email you provided when you registered before you downloaded the software to complete the install

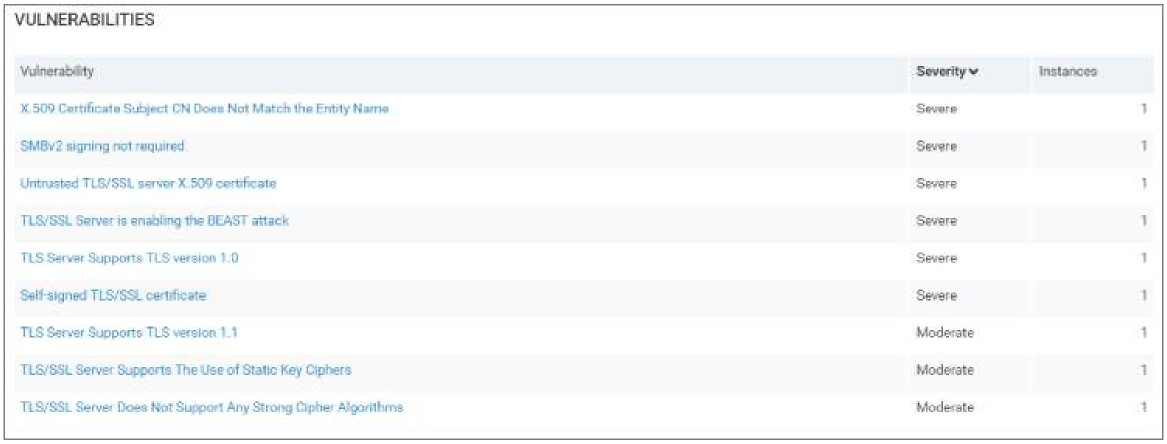
process. Use the license that was sent to you to activate the product.

7. On the left side, you will have a vertical menu shown in Figure 4.8.

The home menu gives you a summary of assets, risk scores, and asset groups. The asset page will break down individual items you have scanned and the vulnerability page will give you information on those assets from a different vantage point, where and what makes you vulnerable. The policy tab will be empty since this is the community version but in a paid-for version, you can scan an asset to CIS or a federal guideline of configuration. Reports will be below policies.

LAB 4.2: CREATE A SITE AND SCAN

1. Click on the Create button at the very top of the page. Slide down to Site. You have seven sections to consider for optimal scanning and performance.
2. The General Tab is where you can name the site for future reference and reporting. Add the name TEST.
3. The Assets Tab will allow you to enter a single name, address, or CIDR range of IP addresses you would like to scan. In the community version, it may be wise to do an nmap scan first to build an inventory and then bring in those assets individually since you're limited to 32 assets. For this TEST site, add your IP address. If you are unsure of your IP address, open up a command prompt and do an ipconfig /all.
4. The Authentication tab gives you the ability to be authorized to scan those assets listed on the Assets tab. If you would like a deeper scan, use administrator credentials on this page. Skip this the first time and you will have the ability to create a baseline comparison report in the future.
5. There are several scan templates on the next tab to choose from. The default scan template is a full audit without web spidering. This is an ideal template to use first.
6. You only have one engine available to you in the community version. This is the local scan engine you installed in Lab 4.1.
7. Alerts are configured to notify an administrator that a scan has failed.
8. The schedule tab will allow you to stay on top of your assets vulnerabilities as Nexpose is updated and new assets are added to your environment.
9. Click Save And Scan in the upper right. This test scan on a single asset will start and you can watch the progress.
10. When the scan completes, review the vulnerabilities on your host. On the asset page, they will look like Figure 4.9.



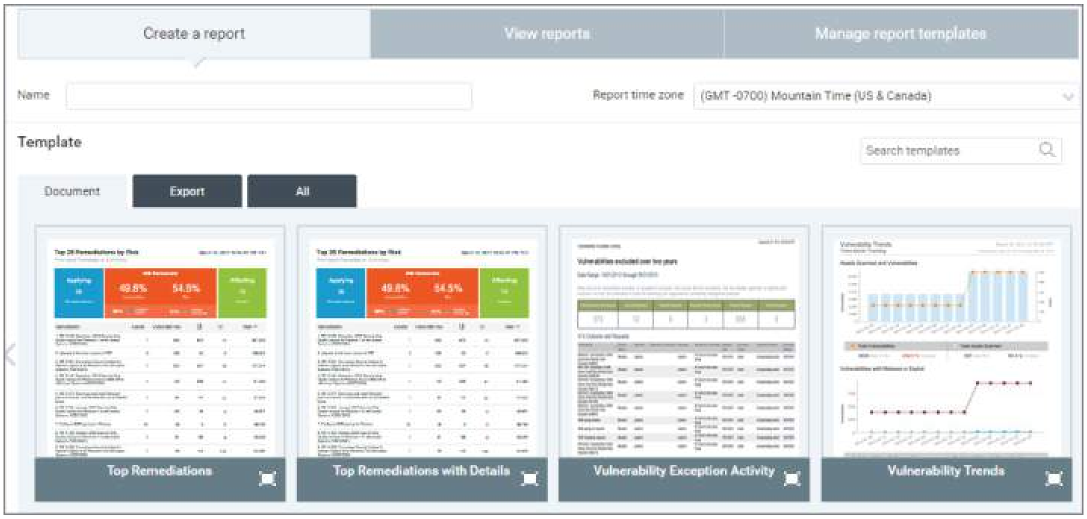
VULNERABILITIES

Vulnerability	Severity ⌄	Instances
X.509 Certificate Subject CN Does Not Match the Entity Name	Severe	1
SMBv2 signing not required	Severe	1
Untrusted TLS/SSL server X.509 certificate	Severe	1
TLS/SSL Server is enabling the BEAST attack	Severe	1
TLS Server Supports TLS version 1.0	Severe	1
Self-signed TLS/SSL certificate	Severe	1
TLS Server Supports TLS version 1.1	Moderate	1
TLS/SSL Server Supports The Use of Static Key Ciphers	Moderate	1
TLS/SSL Server Does Not Support Any Strong Cipher Algorithms	Moderate	1

Figure 4.9: List of Vulnerabilities found in Nexpose Community sorted by severity

LAB 4.3: REPORTING

1. Click on the reports menu on the left.
2. Using the carousel under the reports, navigate to the circle that displays the last four default document reports as you see in Figure 4.10.

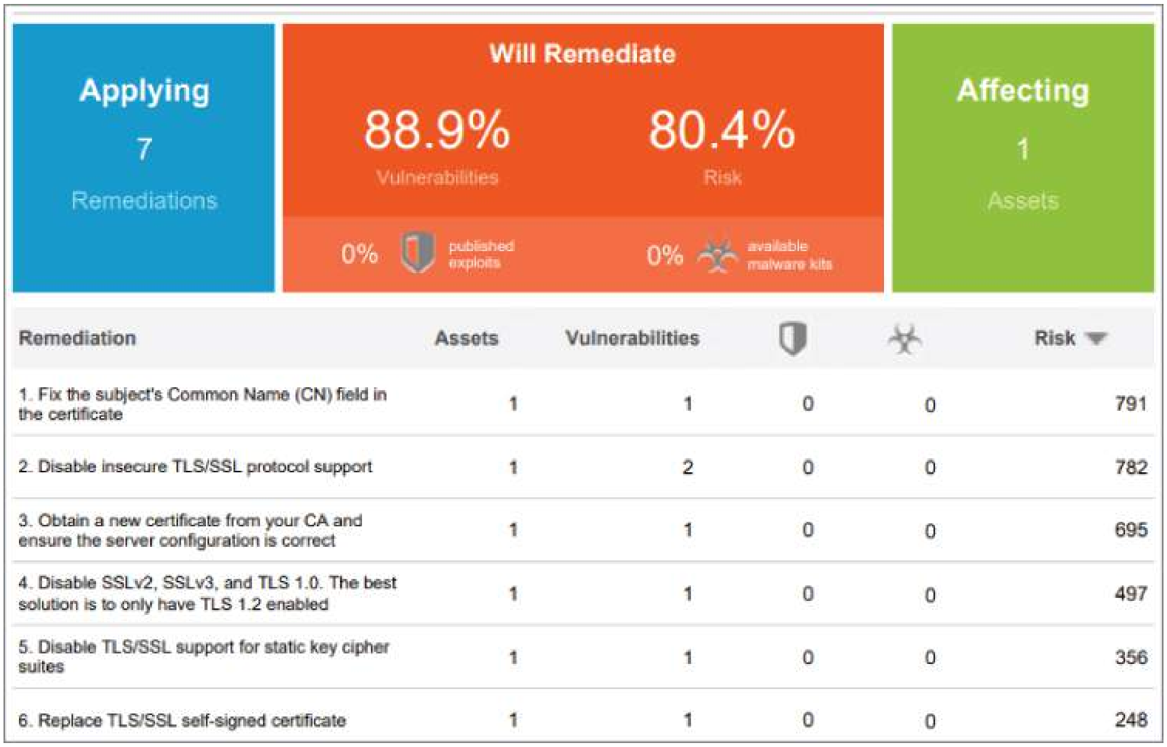


Report time zone (GMT -0700) Mountain Time (US & Canada)

Figure 4.10: Document report menu in Nexpose Community

3. At the top of the page, name this report “Best VM Report EVER.”
4. You will see the Top Remediations with Details. Single-click on the report to select.
5. Leave the file format as PDF.
6. Under Scope, choose the big plus in the center and select your test site made in Lab 4.2.
7. Choose Save And Run The Report. The report will generate and when done, you will be able to click on the report name to open.
8. Scroll down through the preview of the report to see the impact of remediated vulnerabilities, the list of vulnerabilities, and the host the vulnerability is on, as

displayed in Figure 4.11. Navigate to page two to view the instructions on how to fix the vulnerabilities listed above.



Applying
7
Remediations

Will Remediate
88.9% Vulnerabilities
80.4% Risk
0% 🛡 published exploits
0% ☣ available malware kits

Affecting
1
Assets

Remediation	Assets	Vulnerabilities	🛡	☣	Risk ▼
1. Fix the subject's Common Name (CN) field in the certificate	1	1	0	0	791
2. Disable insecure TLS/SSL protocol support	1	2	0	0	782
3. Obtain a new certificate from your CA and ensure the server configuration is correct	1	1	0	0	695
4. Disable SSLv2, SSLv3, and TLS 1.0. The best solution is to only have TLS 1.2 enabled	1	1	0	0	497
5. Disable TLS/SSL support for static key cipher suites	1	1	0	0	356
6. Replace TLS/SSL self-signed certificate	1	1	0	0	248

Figure 4.11: Top Remediations

You now have a picture of how an attacker might see you and your network. This is exactly the methodology attackers would use to find the landscape of your environment and attempt to exploit what they find. If you can thwart their efforts by closing up the vulnerabilities that are exposed to the world, you will have a much safer ecosystem.

CHAPTER 5
Monitoring with OSSEC

WHAT YOU WILL LEARN IN THIS CHAPTER:

- Log-Based Intrusion Detection Systems
- Agents
- Log Analysis

Open Source Security (OSSEC) is a free, open-source, host-based intrusion detection system (HIDS). Daniel Cid, the author of OSSEC, often refers to it in the log analysis portion of OSSEC as a *log-based intrusion detection system* (LIDS). Log analysis for intrusion detection is the process of using the recorded events to detect attacks on a specific environment.

With the proper agents installed on your assets and logs being processed by OSSEC, you meet the criteria for another CIS control. CIS Control 6 is the maintenance, monitoring, and analysis of logs. You must ensure that logging is enabled locally on your systems and it is actively being monitored. Sometimes logging is the only record or evidence of a successful attack. Without solid logs, an attack may go undetected, and damage can be ongoing for months, if not years. Not only can a LIDS protect against an external threat, it also can protect against an internal threat such as detecting a user who is violating an acceptable use policy (AUP).

Log-Based Intrusion Detection Systems

On your hosts across your network, it is vital to monitor the current state of a machine, check the files that are stored on that machine (the log files), and check to make sure that these files have not been changed. OSSEC operates on the principle that attackers who are successful at exploiting a vulnerability and have gained access to a machine will leave evidence of their activities. Once attackers gain access to a system, they of course will not want to lose access. Some attackers will establish some type of backdoor that allows them to return, bypassing all security you may have in place. A computer system should be able to detect these modifications and find persistent threats that penetrate firewalls and other network intrusion systems.

OSSEC is a security log analysis tool and is not known to be useful for log management. It will store the alerts but not every single log. You should have another mechanism for log storage if you need to store logs for your internal security policies or compliance. If you choose to use OSSEC as a HIDS, you will be using a database to monitor file system objects. OSSEC can remember size, attributes, and dates as well as a hash of contents on a machine. For example, if integrity is the most important aspect of file monitoring, an MD5sum hash will use an algorithm to create a digital fingerprint of the file.

With any new project/program implementation, there comes a need for current evaluation. Your team needs to define what success will look like, analyze your current situation, start with a few key components, and take a look at your incident response (IR) plan. An IR plan will contain policies, procedures, and guidelines surrounding processes to complete if an unplanned event occurs.

The benefits to using OSSEC is that it is an open-source free tool that doesn't require a lot of hardware. This HIDS tool will give you visibility into logs generated by firewalls, applications, servers, and routers. You also gain visibility to encrypted protocols such as SSH and SSL logs.

A challenge with OSSEC is it focuses on reactive remediation, reacting to an event that already occurred rather than proactive remediation, where you mitigate and remediate the issue before it occurs. Another challenge you may face is “alert fatigue.” This happens when a system floods you with alerts hundreds of times to an event or incident. These can be managed with log correlation and fine-tuning.

OSSEC can be used to monitor thousands of servers with OSSEC agents. These will be monitored by the OSSEC manager.

OSSEC is fairly easy to install, is easy to customize, is extremely scalable, and can use many different platforms, including Windows, Solaris, Mac, and Linux. Secure by default, there are hundreds of rules that can be used straight out of the box. One of the key benefits to OSSEC is how it helps customers meet specific compliance requirements such as those in the Payment Card Industry (PCI) and the Health Insurance Portability and Accountability Act (HIPAA). It lets users detect and alert on a file system modification that was unauthorized or if there is any malicious behavior in any log files. If your organization does have to subscribe to a compliance like PCI, you have to implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. Web servers, database servers, and DNS should be implemented on separate servers. A database, which needs to have strong security measures in place, would be at risk sharing a server with a web application, which needs to be open and directly face the Internet. Each server may generate its own unique type of logs, and that may require some configuration of OSSEC. In Figure 5.1, you see the process that OSSEC will use to gather, analyze, and possibly alert you to activity.

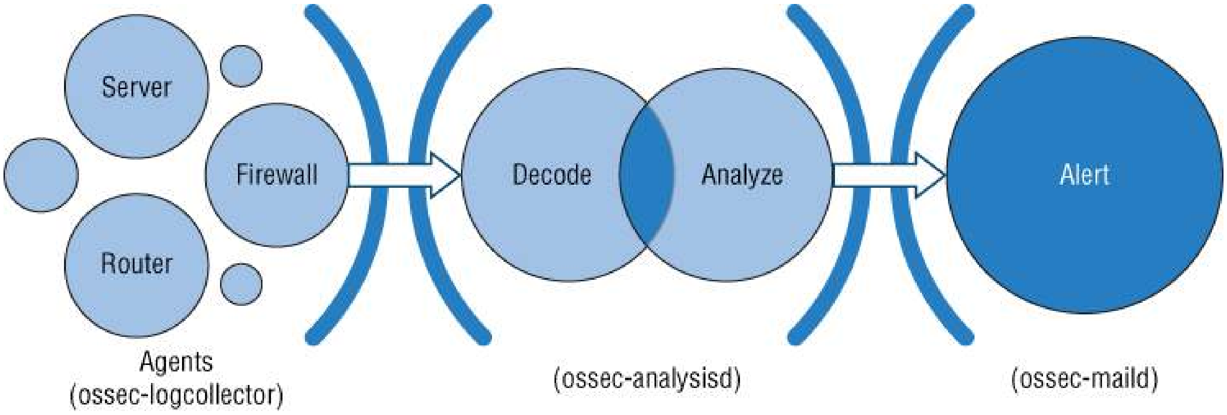


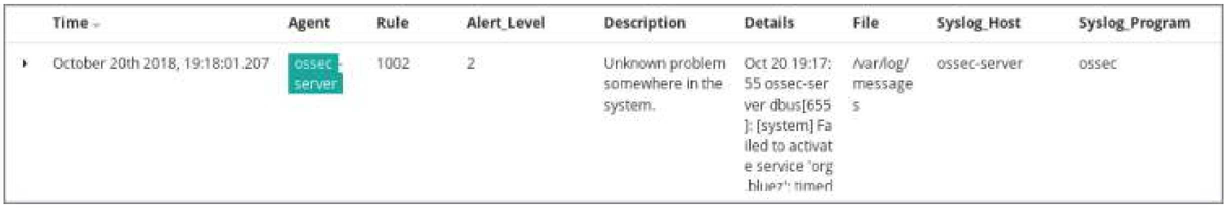
Figure 5.1: The collection of data from agents analyzed and possibly generating alerts

The log analysis flow for the client/server/agent architecture begins with the collection of logs from the assets that need monitoring. After the logs are collected, generic information is extracted such as hostname, program name, and time from the syslog header.

The OSSEC is a virtual appliance based on CentOS and includes Elastic search-Logstash-Kibana (ELK). It comes with its own library of log decoders that will be used by default. These decoders can parse or analyze the logs from Windows, SSH, or Apache using default tags within the logs that help identify what they are and where they came from. The decoders in OSSEC are written in XML and organized into libraries to make them easy to open, decode, define, and close. As you see in Figure 5.2, the virtual appliance spins up ready for you to begin interacting with the dashboard, libraries, and parsing data.

Figure 5.2: The OSSEC appliance

OSSEC must first understand what is in a log before it can tell you if something is wrong or alert you to an event. After parsing the log and normalizing the data, it will match fingerprint with fingerprint and syntax with syntax, forwarding the log file to be evaluated by the rules for processing. If OSSEC receives a log that it doesn't understand, it will generate an event 1002, “Unknown problem somewhere on the system,” as you see in Figure 5.3. One of the best solutions is to configure some type of trigger that lists a unique field in the log so it's no longer unknown.



	Time	Agent	Rule	Alert_Level	Description	Details	File	Syslog_Host	Syslog_Program
▸	October 20th 2018, 19:18:01.207	ossec-server	1002	2	Unknown problem somewhere in the system.	Oct 20 19:17:55 ossec-server dbus[655]: [system] Failed to activate service 'org.bluez': timed	/var/log/messages	ossec-server	ossec

Figure 5.3: An OSSEC 1002 alert

Straight out of the box, there is an extensive set of rules embedded in OSSEC. The rules themselves can be correlated and grouped. After decoding the log, the next step is to check the rules. The rules are internally stored in a tree-type structure and allow you to match on user-defined expressions based on the decoded information. There are more than 400 rules available by default. Please do not modify the default rules inside OSSEC as they will be written over when you upgrade.

There are two basic types of rules: atomic and composite. Atomic rules are based on a single event occurring, while a composite rule is based on patterns across multiple logs. When you're learning to write rules, it requires a rule ID, a level that is a number between 0 and 15, and a pattern. For example, if a log is decoded as SSH, generate rule 123. If you want to add a secondary rule, it will be dependent on the first. You can add more rules to be called if the second one matches; for example, you can specify whether the IP address comes from inside or outside the network. Be careful—don't write new rules dependent on composite rules. You should look at the original atomic rule that the composite rule is based on.

OSSEC can generate thousands of alerts a day and, if misconfigured, in a much shorter period of time. You must tune your instance or else you will start to ignore these alerts. Make sure your alerts are relatively rare and relevant to your environment.

Agents

To get started with these processes, OSSEC has many different options for installation. From the `www.ossec.net` website, you can choose from a server/agent `tar.gz` file, a virtual appliance, a Docker container, and an `.exe` file for the Windows agents.

The easiest install for a new user is the virtual appliance. Inside the virtual appliance, which is based on a CentOS Linux 7 distribution, you have the files needed, so getting the `.ova` file set up is fairly easy. Do not forget: When you download an `.ova` file, there is usually a `.readme` file. Be sure to open and read the file for any helpful hints such as default passwords, ports to open or connect on, or ways to bridge with your host network. Two CentOS users are predefined in the virtual appliance: `ossec` and `root`. The root password is `_0ssec_`. The `ossec` user does not have a password, so you can just press Enter to log on.

If you are working with the OSSEC Virtual Appliance 2.9.3 and downloaded it from OSSEC's GitHub, it already contains the following:

- OSSEC 2.9.3
- Elasticsearch-Logstash-Kibana (ELK) 6.1.1
- Cerebro 0.7.2
- CentOS 7.4

You can import this virtual appliance into most virtual systems. OSSEC recommends VirtualBox for creating and running the appliance, but VMware works as well. The appliance network interface is configured to NAT mode. To use this as a server, you must configure the network to use bridged mode and set a static IP. In Figure 5.4, you see the Kibana OSSEC dashboard is built to visualize alerts, including how many over time, top alerts per agent deployed, and alert data.

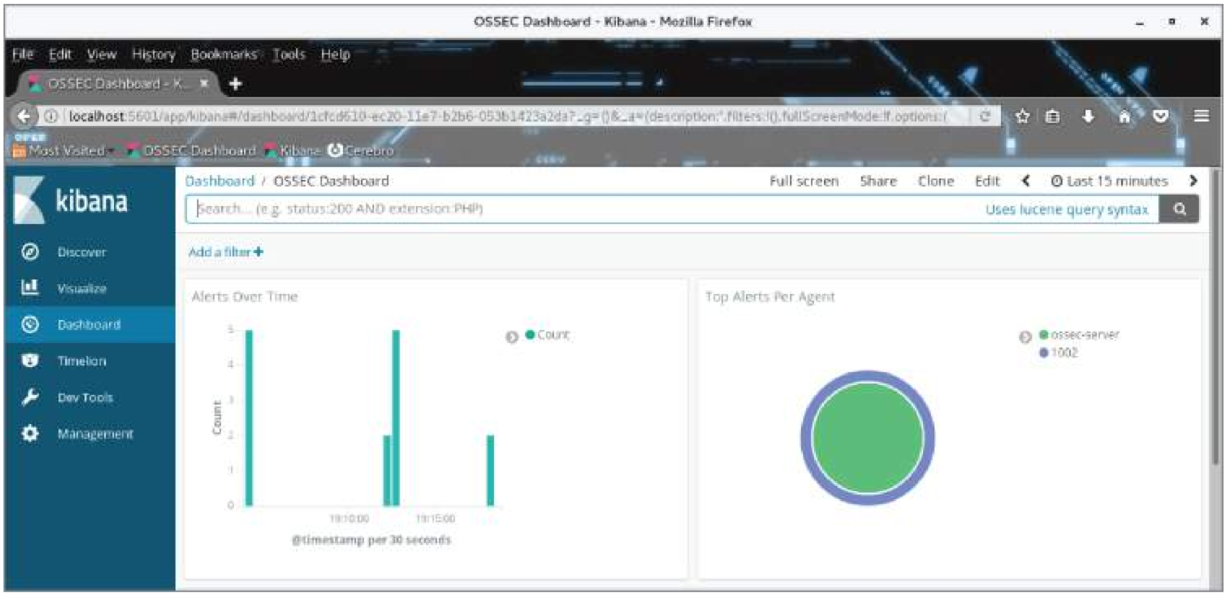

OSSEC Dashboard - Kibana - Mozilla Firefox
File Edit View History Bookmarks Tools Help
OSSEC Dashboard - K...
localhost:5601/app/kibana#/dashboard/1cfcd610-ec20-11e7-b2b6-053b1423a2da?_g=()&_a=(description:'',filters:!(),fullScreenMode:!f,options:(
Most Visited OSSEC Dashboard Kibana Cerebro
kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Dashboard / OSSEC Dashboard
Full screen Share Clone Edit Last 15 minutes
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax
Add a filter +
Alerts Over Time
Count
5
4
3
2
1
0
19:10:00
19:15:00
@timestamp per 30 seconds
Count
Top Alerts Per Agent
ossec-server
1002

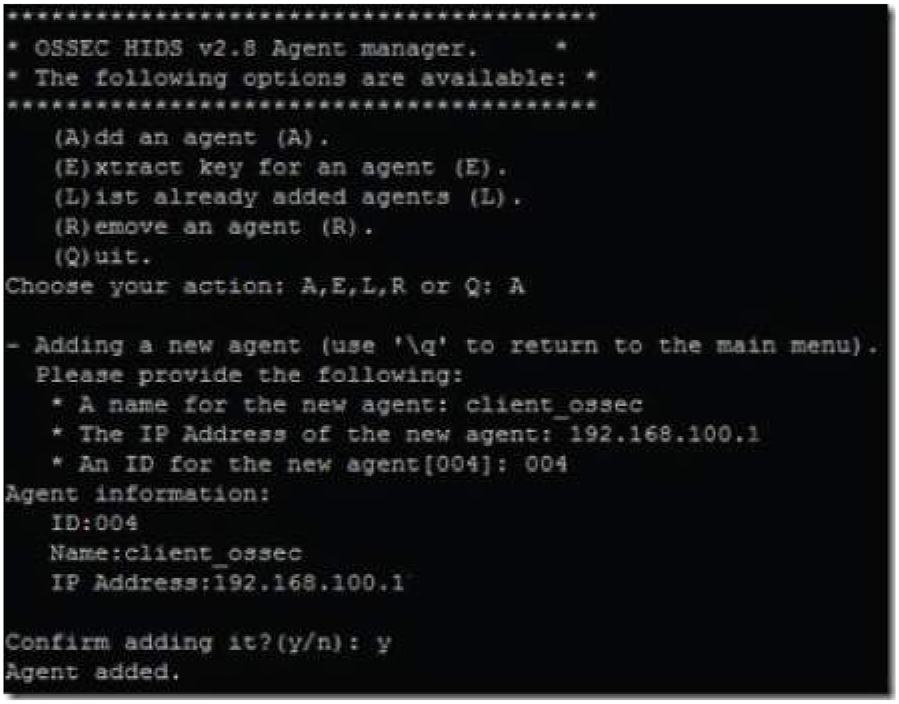
Figure 5.4: The OSSEC dashboard

Two types of agents will feed data into OSSEC: installable and agentless. Installable agents are installed on hosts, and they report to the server; agentless agents require no installation on a remote host. Both of these processes are started and maintained from the OSSEC manager. After information is gathered, it uses SSH, RDP, SNMP, or WMI to send the data to the manager for processing and decoding.

To add an agent, you will need to do the following:

1. Run `manage_agents`.
2. Add an agent.
3. Extract and copy the key for the agent.
4. Run `manage_agents` on the agent.
5. Import the key.
6. Restart the OSSEC server.
7. Start the agent.

In Figure 5.5, you can see the OSSEC agent manager. To run `manage_agents` from the terminal, ensure that you have root privileges and type in the following:



```
****************************************
* OSSEC HIDS v2.8 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: client_ossec
   * The IP Address of the new agent: 192.168.100.1
   * An ID for the new agent[004]: 004
Agent information:
   ID:004
   Name:client_ossec
   IP Address:192.168.100.1

Confirm adding it?(y/n): y
Agent added.
```

Figure 5.5: OSSEC agent manager

```
# /var/ossec/bin/manage_agents
```

Several options are available in the agent manager. You can choose to add an agent, extract a key for an agent, list existing agents, remove an agent, and quit. Each of these has a corresponding letter to those actions.

Adding an Agent

To perform this action, type **a** at the Choose Your Action prompt on the `manage_agents` screen and press Enter.

You are then prompted to provide a name for the new agent. This can be the hostname or another string to identify the system. Figure 5.6 shows an example of how to create a name for an agent. For best practice, create a constant naming convention using some type of spreadsheet that allows you to track your agents.

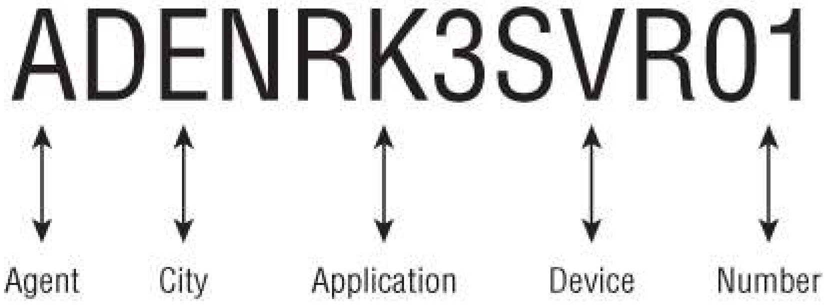


Figure 5.6: An example of a representative agent name

From this agent name, I know that it is an agent in Denver in rack 3. It's a server, and the agent sequence number is 01. Too many times organizations will name their machines what they are and give a road map to exploitation to the hacker on a silver platter. Security through obfuscation is a pillar of our industry. You wouldn't name a machine WIN2K8SQL, would you?

After you have named the agent, you have to specify the IP address for the agent. This can be either a single IP address or an entire range of IPs. If you use a specific IP address, it should be unique. If you duplicate any IP addresses, it will most definitely cause issues in the future.

Using a network range is preferable when the IP of an agent changes frequently because of DHCP or if different systems appear to come from the same IP address (NAT). For ease of use, you can use CIDR notation when specifying ranges.

After you specify the ID you want to assign to the agent, `manage_agents` will suggest a value for the ID. This value will be the lowest number that is not already assigned to another agent. The ID `000` is assigned to the OSSEC server. To accept the suggestion, simply press Enter. To choose another value, type it in and then press Enter.

As the final step in creating an agent, you have to confirm adding the agent. For example, you would enter the values shown in bold here:

```
ID: 001
Name: ADENRK3SVR01
IP Address: 192.168.100.1
Confirm adding it?(y/n): y
Agent added.
```

After that, `manage_agents` appends the agent information to `/var/ossec/etc/client.keys` and goes back to the start screen. If this is the first agent added to this server, the server's OSSEC processes should be restarted by running the command `/var/ossec/bin/ossec-control restart`.

Extracting the Key for an Agent

Each agent shares a key pair with the manager. If you have 100 agents, you need 100 keys. After you add an agent, a key is created. To extract the key, type **e** at the Choose Your Action prompt on the `manage_agents` screen. You will be given a list of all agents on the server. To extract the key for an agent, simply type in the agent ID as shown in bold in the following code snippet (note that you have to enter all digits of the ID):

```
Available agents:
   ID: 001, Name: ADENRK3SVR01, IP: 192.168.100.1
Provide the ID of the agent to extract the key (or '\q' to
quit): 001

Agent key information for '001' is:
WERifgh50weCbNwiohg'oixjHOIIWIsdv1437i82370skdfosdFrghhbdfQWE33
2dJ234
```

The key is encoded in the string and includes information about the agent. This string can be added to the agent through the agent version of `manage_agents`, and the best approach is to cut and paste it.

Removing an Agent

If you want to remove an OSSEC agent from the server, type **r** at the Choose Your Action prompt on the `manage_agents` screen. You will be given a list of all agents already added to the server. Type in the ID of the agent, press Enter, and then confirm the deletion when prompted to do so. It is important to note that you have to enter all digits of the ID. Here's an example:

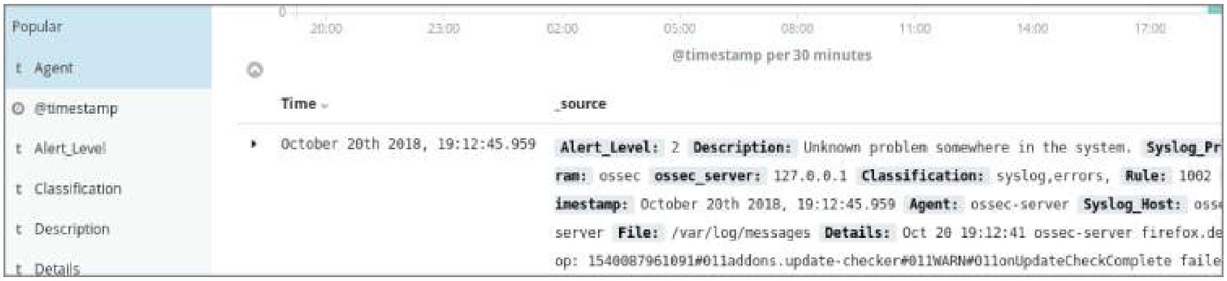
```
Choose your action: A,E,L,R or Q: r
Available agents:
   ID: 001, Name: ADENRK3SVR01, IP: 192.168.100.1
Provide the ID of the agent to be removed (or '\q' to quit):
```

```
001
Confirm deleting it?(y/n): y
```

There is no secondary confirmation. Please double-check that you are removing the proper agent because once `manage_agents` invalidates the agent information in `/var/ossec/etc/client.keys`, you will have to start all over again if you have made a mistake. Yes, I have done it. Learn from my mistakes. Only the values for ID and the key are kept to avoid conflicts when adding agents. The deleted agent can no longer communicate with the OSSEC server.

When you have installed your agents on Windows and Linux machines, they should automatically start checking in with the manager. When you open up the Kibana OSSEC dashboard, you will see there are three major panels.

- OSSEC Alerts Over Time—There is a bar graph that displays the number of events by a unit of time.
- Top Alerts Per Agent—This pie chart shows the top alerts for each active agent.
- OSSEC Alert Data—This table displays the individual alerts and the fields being alerted on, as you see in Figure 5.7.



```
October 20th 2018, 19:12:45.959   Alert_Level: 2 Description: Unknown problem somewhere in the system. Syslog_Pr
                                  ram: ossec ossec_server: 127.0.0.1 Classification: syslog,errors, Rule: 1002
                                  imestamp: October 20th 2018, 19:12:45.959 Agent: ossec-server Syslog_Host: oss
                                  server File: /var/log/messages Details: Oct 20 19:12:41 ossec-server firefox.de
                                  op: 1540087961091#011addons.update-checker#011WARN#011onUpdateCheckComplete faile
```

Figure 5.7: OSSEC individual agent alert

Log Analysis

Now that you have your agents gathering logs and bringing them into your OSSEC server, it is time for decoding, inspecting, filtering, classifying, and analyzing. The goal of LIDS is to find any attacks, misuse, or errors that systems are generating using the logs.

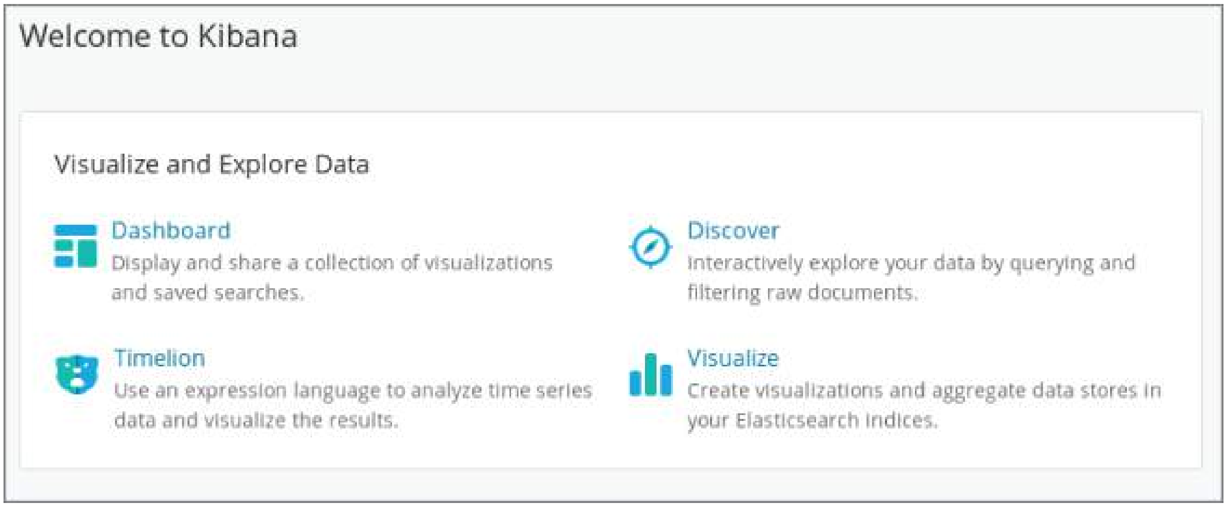
Logs are monitored in real time by the manager. By default, log messages from host agents are not retained. Once analyzed, OSSEC deletes these logs unless the `<logall>` option is included in the OSSEC manager's `ossec.conf` file. If this option is enabled, OSSEC stores the incoming logs from agents in a text file that is rotated daily. The resources used by the agent are minimal, but the resources used by the manager can fluctuate depending on the events per second (EPS). There are two major ways you can analyze your logs: either by the processes that are running or by the files you are monitoring.

When you are monitoring processes on an asset with OSSEC, the logs that are generated are parsed with the rules contained within the database. Even if some information is not readily available in the logs, OSSEC can still monitor it by examining the output of commands and treating the output as if it was a log file. File log monitoring will monitor log files for new events. When a new log arrives, it forwards the log for processing and decoding.

Configuring a log to be monitored can be pretty easy if you are familiar with Extensible Markup Language (XML). XML is a programming markup language that defines a set of rules used to make a document that is both human readable and machine readable. The design of XML makes it simple and applicable in many scenarios. All you have to do is provide the name of the file to be monitored and the format of the log. For example, the XML may look like this:

```
<localfile>
       <location>/var/log/messages</location>
       <log_format>syslog</log_format>
</localfile>
```

On a virtual machine, you will have the ability to display the dashboard, visualizations, and searches; query the logs; and filter the raw data as well as use data stores for other indexing, as you see in Figure 5.8.



Welcome to Kibana

Visualize and Explore Data

Dashboard
Display and share a collection of visualizations and saved searches.

Discover
Interactively explore your data by querying and filtering raw documents.

Timelion
Use an expression language to analyze time series data and visualize the results.

Visualize
Create visualizations and aggregate data stores in your Elasticsearch indices.

Figure 5.8: Kibana dashboard

CHAPTER 6
Protecting Wireless Communication

WHAT YOU WILL LEARN IN THIS CHAPTER:

- 802.11
- inSSIDer
- Wireless Network Watcher
- Hamachi
- TOR

The wireless technology that we use today can trace its origin to radiotelegraphy, which transmitted information using electromagnetic waves. Wireless communication today travel over the same electromagnetic waves including radio frequencies, infrared, cellular, and satellite. The Federal Communications Commission (FCC) regulates how the wireless spectrum is used in the United States to ensure stability and reliability. It is up to the users to protect their data at rest as well as their data in transit.

802.11

The Institute of Electrical and Electronics Engineers Standards Association (IEEE) is an organization that develops standards for wireless communication gathering information from subject-matter experts (SME). IEEE is not an institution formed by a specific government but is a community of recognized leaders who follow the principle of "one country, one vote."

The IEEE 802.11 is a set of specifications on implementing wireless over several frequencies. As technology has evolved, so has the need for more revisions. If you were to go shopping for wireless equipment, you would see the array of choices you have based on those revisions of 802.11. Most consumer and enterprise wireless devices conform to 802.11a, 802.11b/g/n, and 802.11ac standards. These standards are better known as Wi-Fi. Bluetooth and wireless personal area networks (WPANs) are specialized wireless technologies, and they are defined by IEEE 802.15.

In Figure 6.1, you see a simple wireless topology; you have a laptop, a printer, and a mobile device all connecting through one wireless access point (WAP) via a router that connects directly to the Internet service provider (ISP), giving the end devices access to the Internet all at the same time.

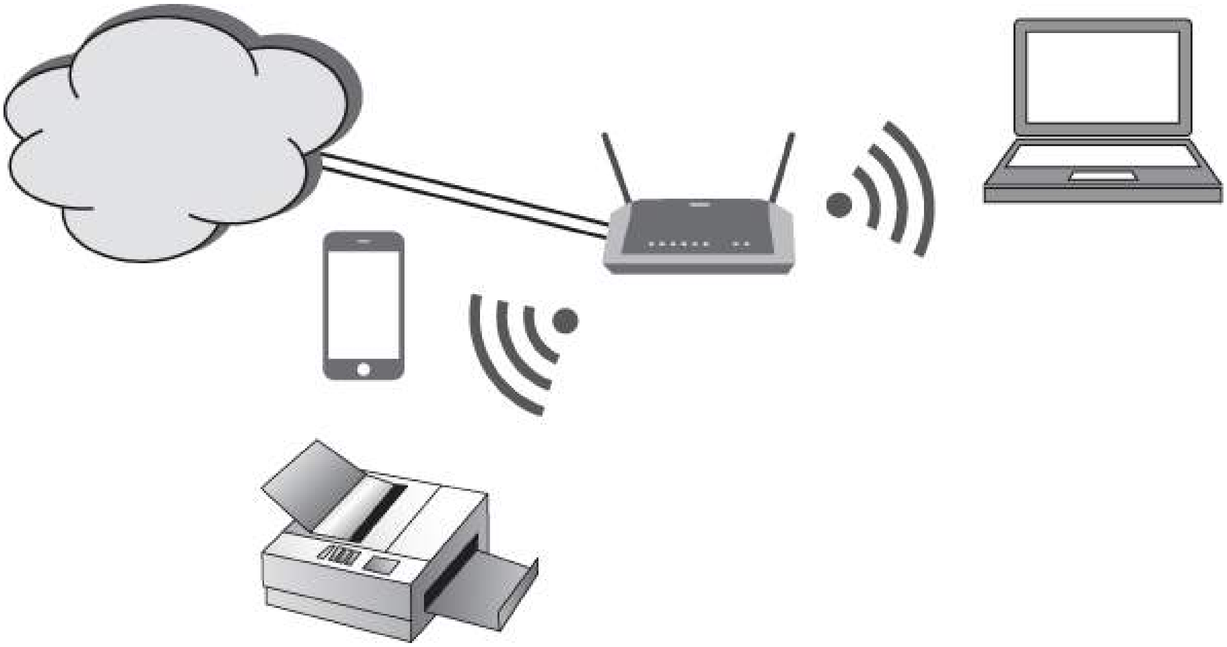


Figure 6.1: Simple star wireless topology

To best utilize and protect this wireless environment, you need to understand how it works. If you can control electromagnetic waves, you can use them to communicate. Information is sent from one component called a *transmitter* and picked up by another called a *receiver*. The transmitter sends electrical signals through an antenna to create waves that spread outward. The receiver with another antenna in the path of those waves picks up the signal and amplifies it so it can be processed. A wireless router is simply a router that uses radio waves instead of cables. It contains a low-power radio transmitter and receiver, with a range of about 90 meters or 300 feet, depending on what your walls are made of. The router can send and receive Internet data to any computer in your environment that is also equipped with wireless access. Each computer on the wireless network has to have a transmitter and receiver in it as well. A router becomes an access point for the Internet, creating an invisible "cloud" of wireless connectivity called as a *hotspot*.

There are advantages and disadvantages to communicating wirelessly. Networks are pretty easy to set up and rather inexpensive, with several choices of frequencies to communicate over. Disadvantages can include keeping this communication secure, the range of the wireless devices, reliability, and, of course, speed. The transmitter and the receiver need to be on the same frequency, and each 802.11 standard has its own set of pros and cons. Table 6.1 describes the IEEE 802.11 standards for wireless devices. As with any technology, wireless devices have evolved to become faster with more range depending on the standard. 802.11ac is sometimes referred to as Wi-Fi 5 and is what most current wireless routers are compliant with. These devices will have multiple antennas to send and receive data reducing errors and boosting speed. There is a new Wi-Fi technology coming in the near future called 802.11ax or Wi-Fi 6. 802.11ax will be anywhere from four to ten times faster than existing Wi-Fi with wider channels available and promises to be less congested and improve battery life on mobile devices since data is transmitted faster.

Table 6.1: IEEE 802.11 standards

FEATURE	802.11A	802.11B	802.11G	802.11N	802.11AC
Frequency	5 GHz	2.4 GHz	5 GHz	2.4/5 GHz	5 GHz
Maximum data rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Mbps
Range indoors	100 feet	100 feet	125 feet	225 feet	90 feet
Range outdoors	400 feet	450 feet	450 feet	825 feet	1,000 feet

As with any technology, as it evolves, you will start making decisions on what scenario is best for you and your organization. There may be trade-offs on frequency used, speed, or the range of a device from a Wi-Fi hotspot. A hotspot is merely an area with an accessible network.

When building a typical wireless small office or home office (SOHO) environment, after you identify what technology and design is best for your situation, you configure the settings of your router using a web interface. You can select the name of the network you want to use, known as the *service set identifier* (SSID). You can choose the channel. By default, most routers use channel 6 or 11. You will also choose security options, such as setting up your own username and password as well as encryption.

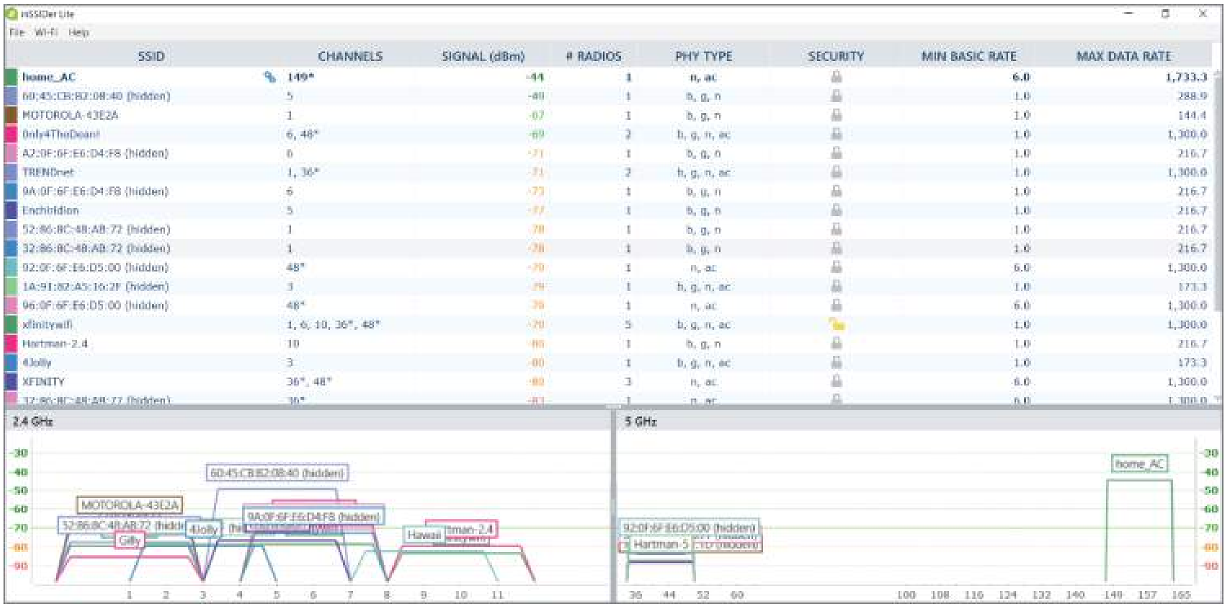
As a best practice, when you configure security settings on your router, choose Wi-Fi Protected Access version 2 (WPA2). WPA2 is the recommended security standard for Wi-Fi networks. It can use either TKIP or AES encryption, depending on the choices you make during setup. AES is considered more secure.

Another best practice is configuring MAC filtering on your router. This doesn't use a password to authenticate. It uses the MAC address of the device itself. Each device that connects to a router has its own MAC address. You can specify which MAC addresses are allowed on your network as well as set limitations to how many devices can join your network. If you set up your router to use MAC filtering, one drawback is every time you need to add a device, you have to grant network permission. You sacrifice convenience for better protection. After reading this book, the more advanced user will know how to capture packets, examine the data, and possibly identify the MAC address of a device in the list of permitted devices. MAC filtering with WPA2 encryption will be the best way to protect your data.

inSSIDer

One of my favorite tools is called inSSIDer by MetaGeek. inSSIDer is a wireless network scanner. It was meant to replace NetStumbler, which was a Microsoft Windows Wi-Fi scanner. There is a free version with limited features called inSSIDer Lite, and you can download it from https://www.metageek.com/products/inssider/free/.

inSSIDer intercepts information from wireless devices and will report all of the wireless networks that are nearby. It will report details such as the SSID of the WAP and what channels the device is using, as well as signal strength, the physical type of the WAP, if it's secured, and the minimum/maximum data rate. You also get a graph of the WAPs divided up by channels 2.4 and 5 GHz. In Figure 6.2, you see that inSSIDer Lite captures the SSID of the broadcasting router, channel, signal, 802.11 type, and kind of security that is being used as well as minimum and maximum data rates.



SSID	CHANNELS	SIGNAL (dBm)	# RADIOS	PHY TYPE	SECURITY	MIN BASIC RATE	MAX DATA RATE
home_AC	149*	-44	1	n, ac	🔒	6.0	1,733.3
60:45:CB:82:08:40 (hidden)	5	-40	1	b, g, n	🔒	1.0	288.9
MOTOROLA-43E2A	1	-67	1	b, g, n	🔒	1.0	144.4
Only4TheDean!	6, 48*	-69	2	b, g, n, ac	🔒	1.0	1,300.0
A2:0F:6F:E6:D4:F8 (hidden)	6	-71	1	b, g, n	🔒	1.0	216.7
TRENDnet	1, 36*	-71	2	b, g, n, ac	🔒	1.0	1,300.0
9A:0F:6F:E6:D4:F8 (hidden)	6	-73	1	b, g, n	🔒	1.0	216.7
Enchiridion	5	-77	1	b, g, n	🔒	1.0	216.7
52:86:8C:48:AB:72 (hidden)	1	-78	1	b, g, n	🔒	1.0	216.7
32:86:8C:48:AB:72 (hidden)	1	-78	1	b, g, n	🔒	1.0	216.7
92:0F:6F:E6:D5:00 (hidden)	48*	-79	1	n, ac	🔒	6.0	1,300.0
1A:91:82:A5:16:2F (hidden)	3	-79	1	b, g, n, ac	🔒	1.0	173.3
96:0F:6F:E6:D5:00 (hidden)	48*	-79	1	n, ac	🔒	6.0	1,300.0
xfinitywifi	1, 6, 10, 36*, 48*	-79	5	b, g, n, ac	🔓	1.0	1,300.0
Hartman-2.4	10	-80	1	b, g, n	🔒	1.0	216.7
4Jolly	3	-80	1	b, g, n, ac	🔒	1.0	173.3
XFINITY	36*, 48*	-82	3	n, ac	🔒	6.0	1,300.0
32:86:8C:48:AB:72 (hidden)	36*	-83	1	n, ac	🔒	6.0	1,300.0

Figure 6.2: inSSIDer capture of Wi-Fi

If you know what is happening around you, you can use this data to fix problems you might be having or improve your network performance. Most people will use inSSIDer to pick the best channel that no one else is using for the best reception and no interference. You can check to see whether your network is secure and what other networks have been discovered.

If there is a lot of traffic on wireless devices around you, you will see this displayed in the visualizations of what channel each access point is on. They can overlap and basically compete for airspace. Using inSSIDer, you can make sure your router is using the best channel.

Looking at Figure 6.2, notice that there is a router in the 5 GHz channel all the way over to the right that is not sharing airspace with anyone. Yes, that's me.

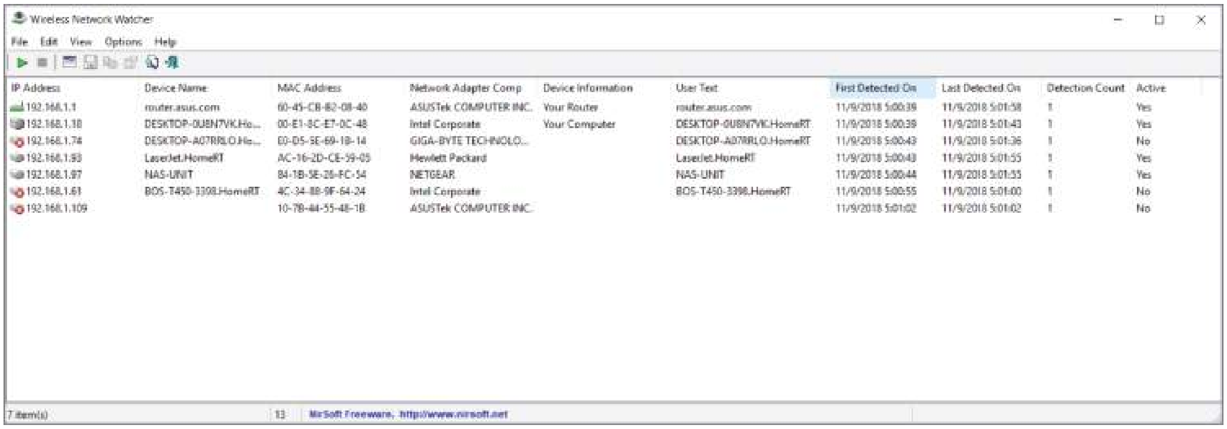
One issue everyone experiences from time to time are dead spots. They are one of the most common pain points of Wi-Fi technology. Depending on which version of inSSIDer you use, there is an option to change from Physical to Logical mode. If you change to Physical mode, you can walk around your work or home environment to evaluate whether your router is in the correct spot. If signal strength dips below -70 dBm, you have a weak area. If it falls below -80 dBm, you have a dead spot.

Wireless Network Watcher

inSSIDer will help you manage the wireless connections around you for a stable, reliable connection. Now that you have that stable connection, you may want to monitor who else is attached to the network you are connected to. Wireless Network Watcher by NirSoft is a small program that scans the wireless network you are attached to and displays the list of all computers and devices that are connected to the same network. You can download the latest version from `https://www.nirsoft.net/utils/wireless_network_watcher.html`.

For every computer or network device attached, you will see the IP address, the MAC address, the company that manufactured the network interface card, and the computer name. You can take that list and export the connected devices into an HTML, XML, CSV, or TXT file. You can even copy the list and paste it into Excel or another spreadsheet application where you can use tools to list, sort, and pivot the information depending on the volume of data.

This program works well when hosted on a Windows machine but can find other platforms such as Linux or Cisco. Wireless Network Watcher will only find assets connected to the network you are currently connected to, not other wireless networks. In some cases, if your network adapter is not found, you can go to Advanced Options and choose the correct network adapter. Under the View tab, you can add gridlines or shaded odd/even rows. If you're actively monitoring the status of your wireless networks, you can even have the program beep when a new device is found. Figure 6.3 shows a list of IP addresses, the device name, MAC address, and other information including whether the device is active on the current network.



IP Address	Device Name	MAC Address	Network Adapter Comp	Device Information	User Text	First Detected On	Last Detected On	Detection Count	Active
192.168.1.1	router.asus.com	60-45-CB-82-08-40	ASUSTek COMPUTER INC.	Your Router	router.asus.com	11/9/2018 5:00:39	11/9/2018 5:01:58	1	Yes
192.168.1.18	DESKTOP-0U8N7VK.Ho...	00-E1-8C-E7-0C-48	Intel Corporate	Your Computer	DESKTOP-0U8N7VK.HomeRT	11/9/2018 5:00:39	11/9/2018 5:01:43	1	Yes
192.168.1.74	DESKTOP-A07RRLO.Ho...	E0-D5-5E-69-18-14	GIGA-BYTE TECHNOLO...		DESKTOP-A07RRLO.HomeRT	11/9/2018 5:00:43	11/9/2018 5:01:36	1	No
192.168.1.93	LaserJet.HomeRT	AC-16-2D-CE-59-05	Hewlett Packard		LaserJet.HomeRT	11/9/2018 5:00:43	11/9/2018 5:01:55	1	Yes
192.168.1.97	NAS-UNIT	84-1B-5E-26-FC-54	NETGEAR		NAS-UNIT	11/9/2018 5:00:44	11/9/2018 5:01:33	1	Yes
192.168.1.61	BOS-T450-3398.HomeRT	4C-34-88-9F-64-24	Intel Corporate		BOS-T450-3398.HomeRT	11/9/2018 5:00:55	11/9/2018 5:01:00	1	No
192.168.1.109		10-7B-44-55-48-1B	ASUSTek COMPUTER INC.			11/9/2018 5:01:02	11/9/2018 5:01:02	1	No

7 item(s) 13 NirSoft Freeware. http://www.nirsoft.net

Figure 6.3: Wireless Network Watcher capture

In Table 6.2, there are command-line options for scanning and saving in specific file types while using Wireless Network Watcher.

Table 6.2: Wireless Network Watcher command-line options

OPTION	RESULT
`/stext <filename>`	Scan the network; save in TXT file
`/stab <filename>`	Scan the network; save in tab-delimited file
`/scomma <filename>`	Scan the network; save in CSV file

Hamachi

Hamachi by LogMeIn is a cloud-based, professional-level application that allows you to easily create a virtual private network (VPN) in minutes. A VPN seems complicated, but Hamachi is not. Unlike traditional software-based VPNs, Hamachi is on-demand, giving you secure access remotely to your business anywhere you have an Internet connection. Without protection, the information you send will be out in the open, and anyone interested in intercepting your data can capture it. Figure 6.4 shows an example of a laptop sending an email using VPN to secure transmission over the Internet.

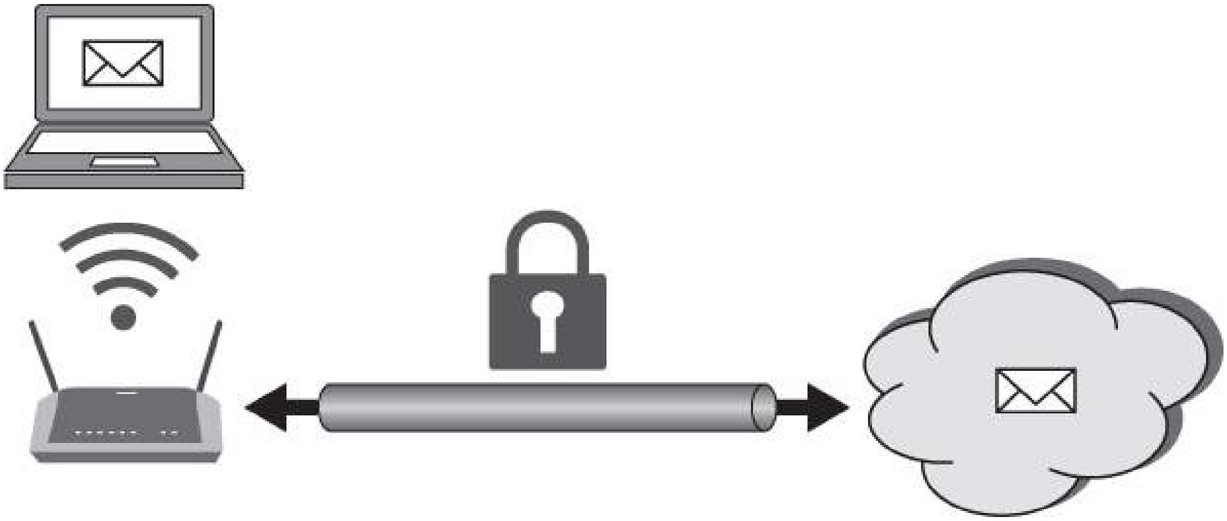


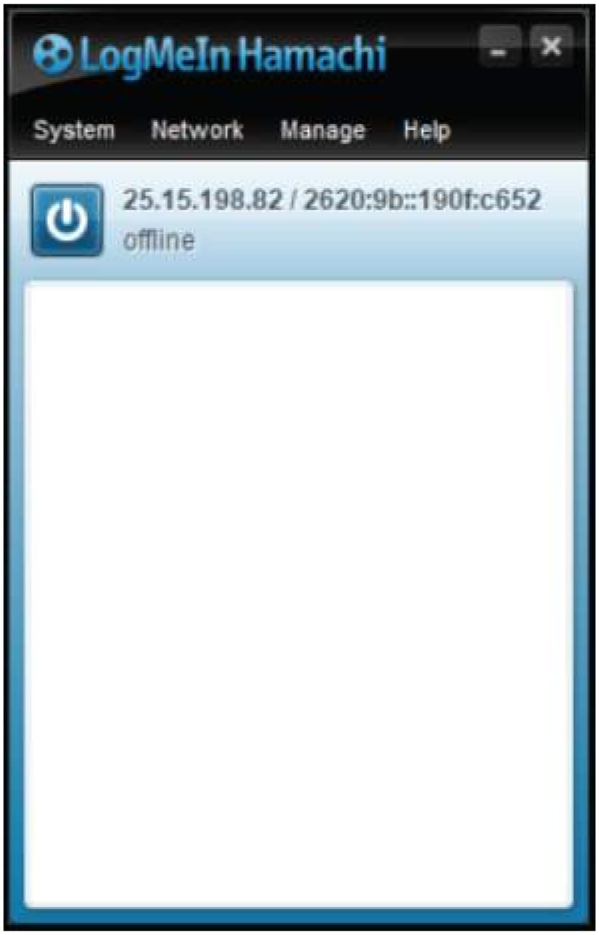
Figure 6.4: Securing the transmission of data using a VPN

Based on the fact that you are reading this book, I would probably bet you are the tech support for your friends and family. I've used Hamachi to help friends who are not technically savvy to install printers, troubleshoot issues, and share files and games with other friends around the globe. If you have remote computers that you would like to access, this software gives you access to that remote machine, imitating a local area network.

Using Hamachi, you can add friends, family, and mobile employees to a virtual network where you share resources. Your foundational network configuration does not change. With the VPN connection, information you send to your bank, business email, or other sensitive data is protected. When you use a VPN service, the data is encrypted when it gets to the Internet. The destination site sees the VPN server as the origin of the data. It is extremely difficult to identify the source of the data, what websites you visit, or money you are transferring. The data is encrypted, so even if it is intercepted, no one gets the raw data.

To use Hamachi to create a VPN, you must first download the executable file that will allow you to be a client. The term *client* refers to both the software and any device you've installed the software on.

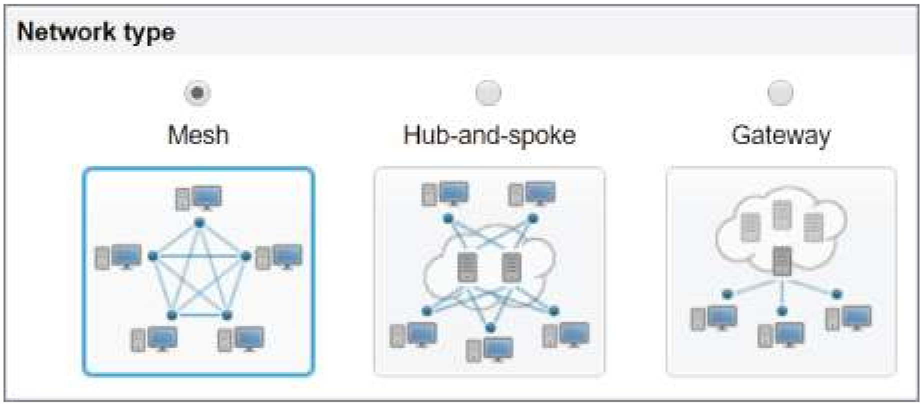
With the correct permission, your client can become a member of any network. The client can be used only with a LogMeIn ID that you create as part of your LogMeIn account when you open and power up the client for the first time. There is no obligation and no credit card required. This ID provides a single sign-on login experience. Once you're logged in to Hamachi, as you see in Figure 6.5, you have your IPv4 and IPv6 address.



25.15.198.82 / 2620:9b::190f:c652
offline

Figure 6.5: Hamachi VPN management console

Every client will have one IPv4 address in the 25.X.X.X range and one IPv6 address. This virtual IP address is globally unique and is used to access any other Hamachi network. As shown in Figure 6.6, when you set up your network, you will have an option to choose Mesh, Hub-And-Spoke, or Gateway.



Network type

● Mesh ○ Hub-and-spoke ○ Gateway

Figure 6.6: Hamachi network type options

In a meshed network, every single member of the network is connected to every other member, which makes it easier to relay data. A mesh topology can handle high amounts of network traffic since every device is considered a node. Interconnected devices can transfer data at the same time, and data moves smoothly, which makes this an ideal choice for gaming. The hub-and-spoke topology provides more control than the meshed network topology. Hubs are connected to everyone, and you have spokes connected to hubs but not to each other. This is a typical choice for a corporate environment where you have workstations connecting to a server. A gateway network will integrate well with a physical network, giving members access to the physical network. There will be only one gateway, and there can many members.

You must sign up for a free account with LogMeIn to complete the install process, and you will need an email address. When you register, you have improved network management, administration, and the ability to create networks. When you have entered an email and password, you will need to create a client-owned network. This will include a unique network ID and password so you can manage your new VPN. This peer-to-peer VPN is using AES 256-bit encryption to secure your data. You can share the network ID with up to five people for free, and they can install the client, use the network ID you created, and join your network. If you need more than five members per network, you may want to look at standard or premium packages.

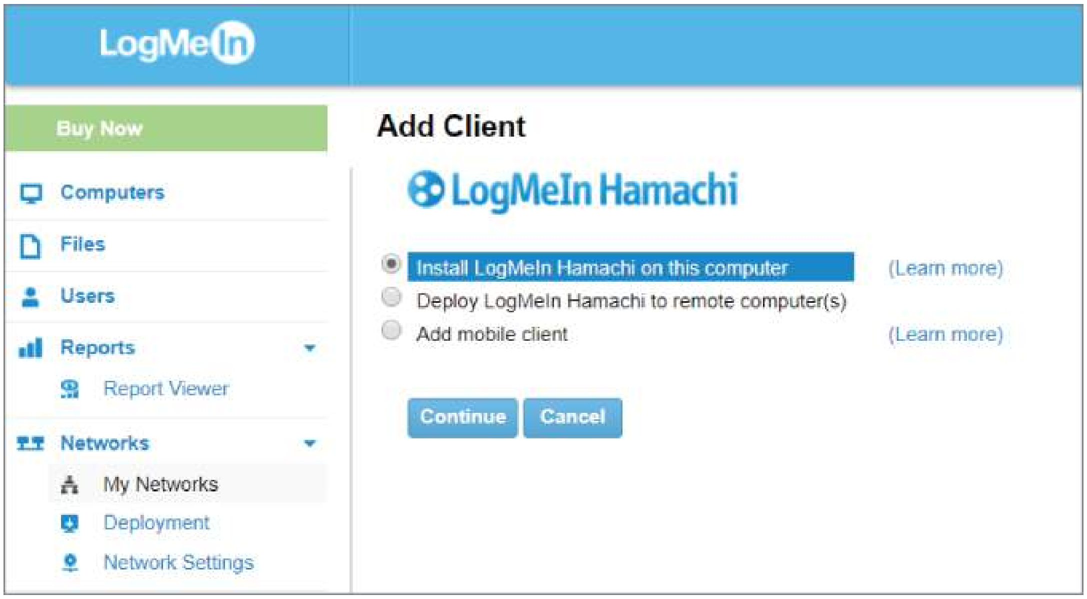
LogMeIn has been tested with many operating systems, and the most current version supports the following:

- Windows Vista (all versions)
- Windows Server 2008 R2 Standard, Business Editions
- Windows 7, 8.1, and 10
- Windows Server 2012
- Mac OS 10.6 (Snow Leopard) and above
- Ubuntu 16.04 and above
- CentOS 7.2 and above

Depending on the topology you have chosen, keep in mind that you cannot assign the Gateway Node functionality to a Mac or Small Business Server.

LAB 6.1: INSTALLING AND USING HAMACHI

1. On the LogMeIn website, you will you see the download link that attaches your networks to your login *only after you have created a user account and logged in*. If you attempt to download the client without being signed in, any network you create will be unable to be joined by anyone else but you.
2. In the menu on the left in Figure 6.7, there's a Networks menu item. Click Add Clients, and your options will be to install the software on your current machine or a remote machine or add this client to a mobile device. Leave the default of adding LogMeIn Hamachi on this computer and click Continue.



● Install LogMeIn Hamachi on this computer (Learn more)
○ Deploy LogMeIn Hamachi to remote computer(s)
○ Add mobile client (Learn more)

Figure 6.7: LogMeIn Hamachi client menu

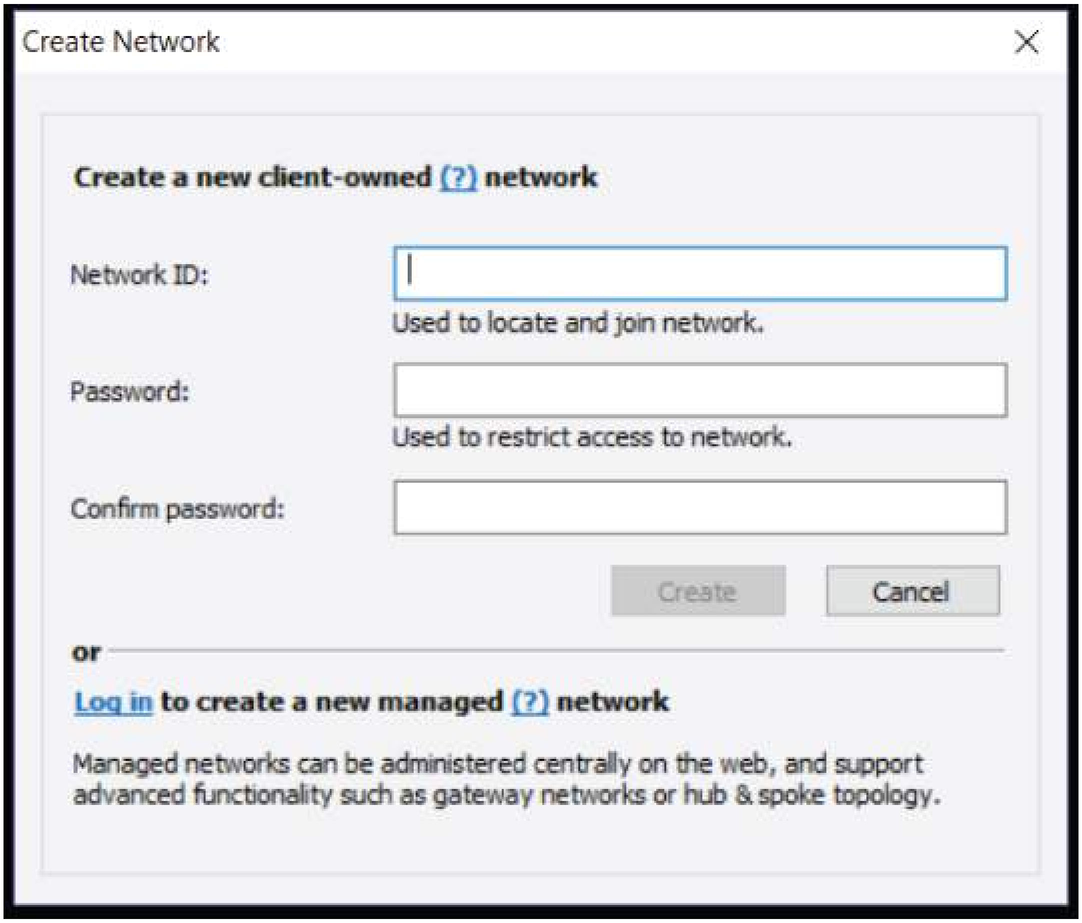
3. Click the Download Now button to allow the installer to download, and follow all the setup wizard's on-screen instructions. You're now ready to configure your first network.

NOTE

The welcome screen will show you which LogMeIn Account this client will be attached to.

LAB 6.2: CREATING A CLIENT-OWNED NETWORK

1. From the LogMeIn Hamachi menu in Figure 6.5, click Network and then Create Network.
2. As you see in Figure 6.8, create a unique network ID. This is the ID that others will use to join your network. An error message will be displayed if the network ID you've entered is already taken.



Create Network

Create a new client-owned (?) network

Network ID:

Used to locate and join network.

Password:

Used to restrict access to network.

Confirm password:

Log in to create a new managed (?) network

Managed networks can be administered centrally on the web, and support advanced functionality such as gateway networks or hub & spoke topology.

Figure 6.8: Creating a new client network

3. Choose and confirm a password that others will use to access your network.
4. Click Create. The new network will appear in your client.

LAB 6.3: CREATING A MANAGED NETWORK

1. From the LogMeIn website, sign in with your ID.
2. From the menu on the left in Figure 6.9, choose My Networks.

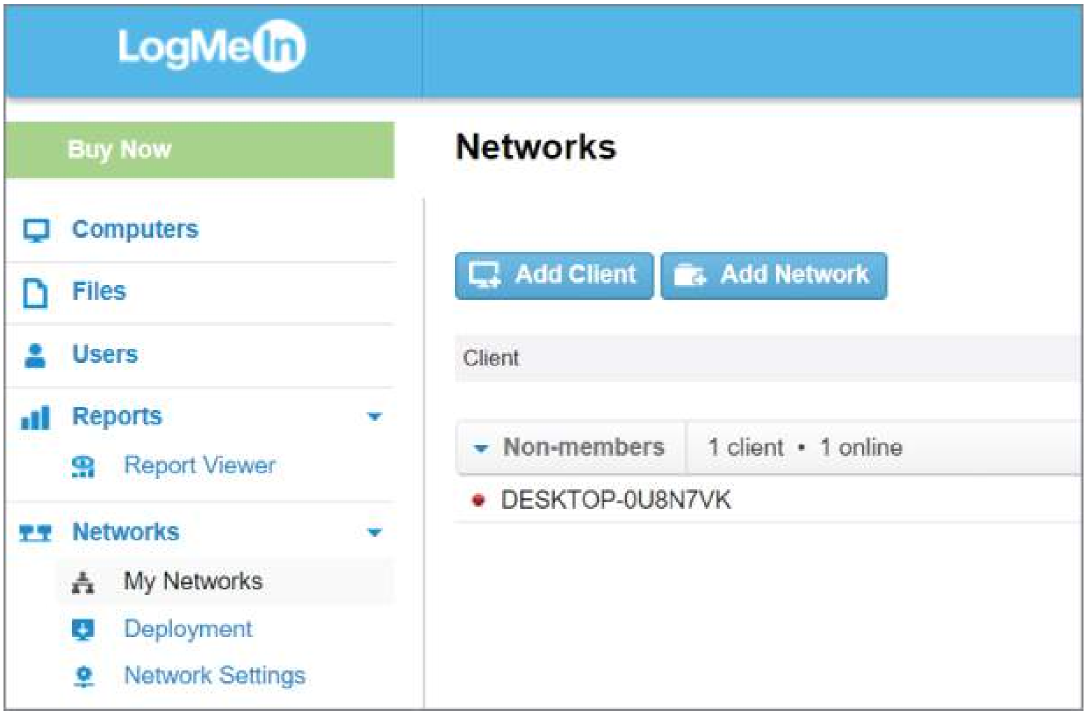
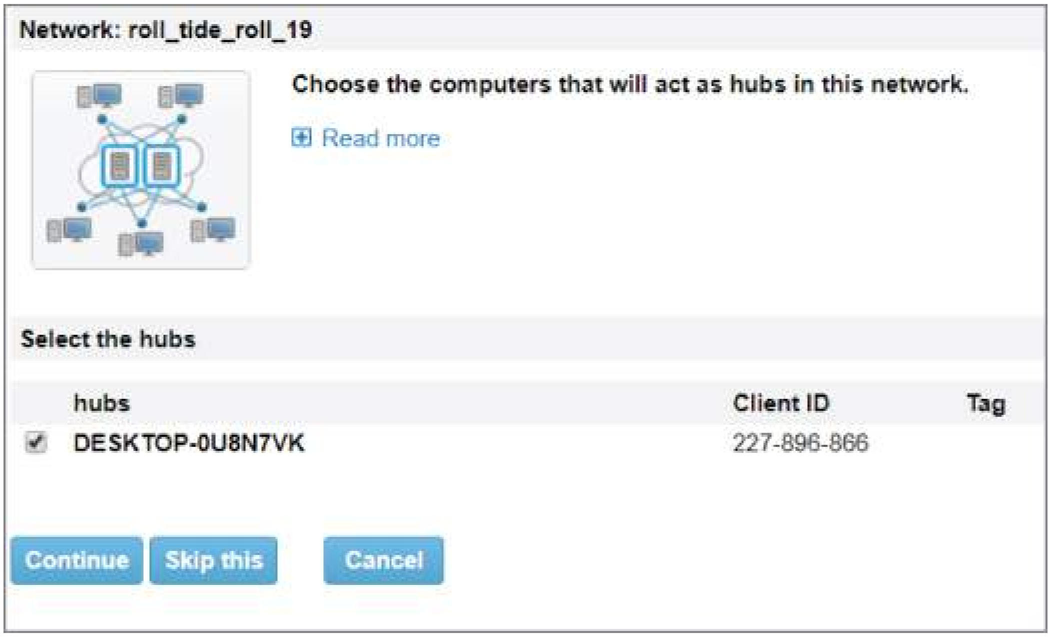


Figure 6.9: Creating a managed network

3. Click Add Network. Choose a network name, description, and type, and then click Continue. After you click Continue, you cannot change the network type—you will have to delete it.
4. You have an option to accept or approve join requests as well as give the network a password.
5. Click Continue.
6. If you chose the hub-and-spoke topology, you will now choose the computer that will act as the hub, as shown in Figure 6.10. If you chose a gateway topology, choose the computer that will act as the gateway computer. The gateway

computer cannot be a member of any other VPN. It is typically a server on the physical network. You can change the gateway at any time.



Network: roll_tide_roll_19

Choose the computers that will act as hubs in this network.

Select the hubs

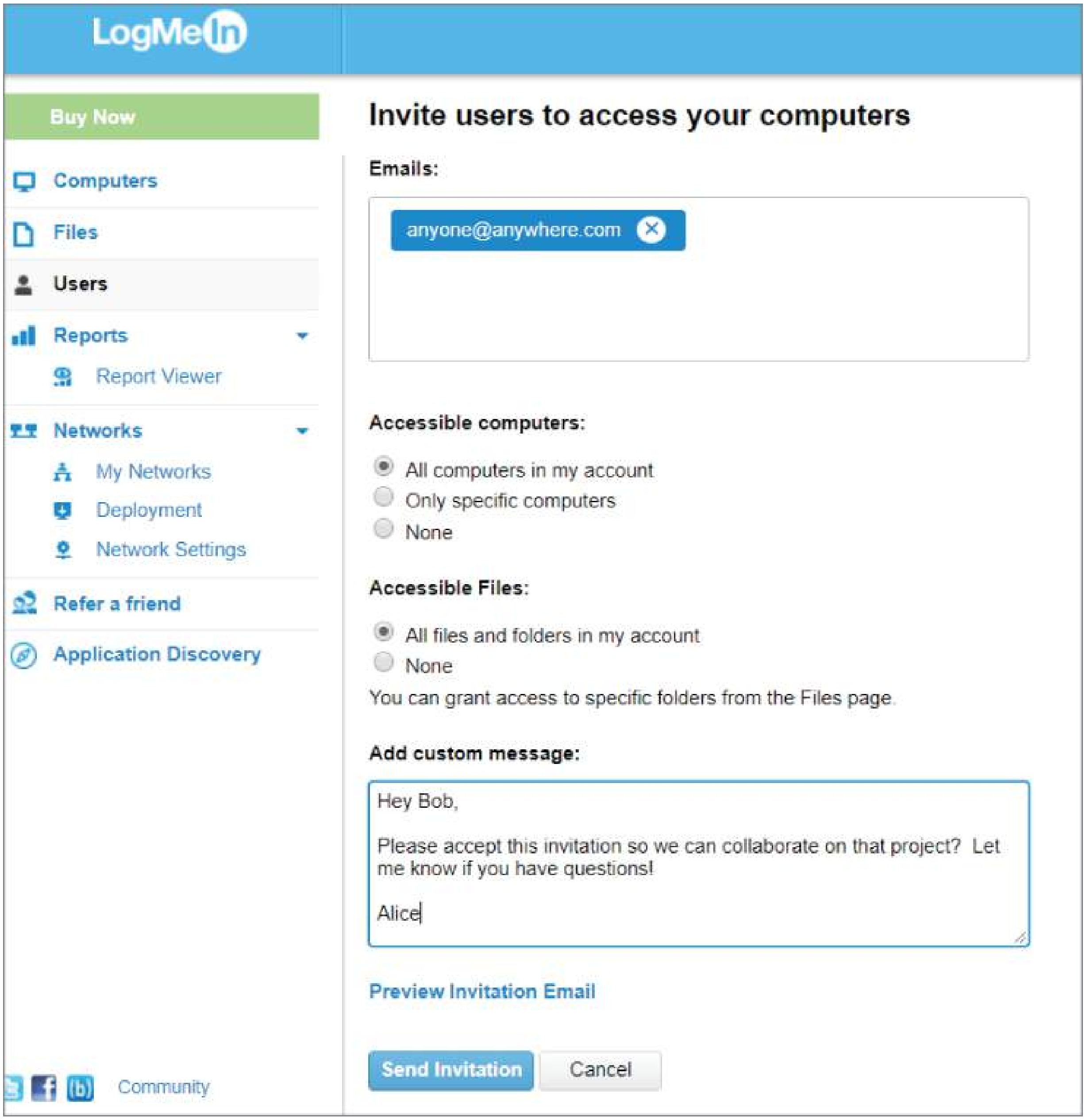
	hubs	Client ID	Tag
☑	DESKTOP-0U8N7VK	227-896-866	

Figure 6.10: Selecting the hub for your network

7. Under Add Network, step 3, you select the hub for your network. Click Continue, and on the next screen, step 4, choose the spokes of your network and then click Finish.

To join a network that has been created by someone else, from the Hamachi client, go to Network ➪ Join Network. You will need to know the network ID and the password if one was added.

One of the tools inside the Hamachi web interface gives you the ability to manage computers, files, and users and run reports on sessions occurring in the last 30 days. Under Computers in your web browser, you can add different computers by opening the Computers page and click Add Computer. To add the computer you're sitting at, just download the installer and follow the on-screen instructions to download and install LogMeIn. To add a computer other than the one you are using, click Add Different Computer ➪ Generate Link. Follow the on-screen instructions, but be aware this link does expire after 24 hours. This is where others can download and install the software for the client. With the Files menu, you can upload files, share links, and connect storage space for easy access. Figure 6.11 shows the Users section where you can choose to add users to an account and select which computers you want them to have access to.



Invite users to access your computers

Emails:

anyone@anywhere.com

Accessible computers:

● All computers in my account
○ Only specific computers
○ None

Accessible Files:

● All files and folders in my account
○ None

You can grant access to specific folders from the Files page.

Add custom message:

Hey Bob,

Please accept this invitation so we can collaborate on that project? Let me know if you have questions!

Alice

Figure 6.11: Adding users to your computer, granting access to files and folders

Tor

The more you learn about cybersecurity, the more paranoid you may seem to those who do not understand the interworking of the Internet. Monitoring of traffic on the Internet is widespread, and there are many organizations, including governments, corporations, and criminals, that can monitor your traffic covertly. In 2003, a program called Total/Terrorism Information Awareness was established by the United States Information Awareness Office to gather detailed information about individuals in an attempt to prevent crimes before they happened. They called this *predictive policing*.

Many civil rights organizations and privacy groups like Reporters Without Borders and the American Civil Liberties Union have expressed concern that with ever-increasing surveillance, we will end up with limited political or personal freedoms. There are hacktivist organizations such as Anonymous, Lizard Squad, Morpho, and APT28 that all have their own modus operandi and moral code.

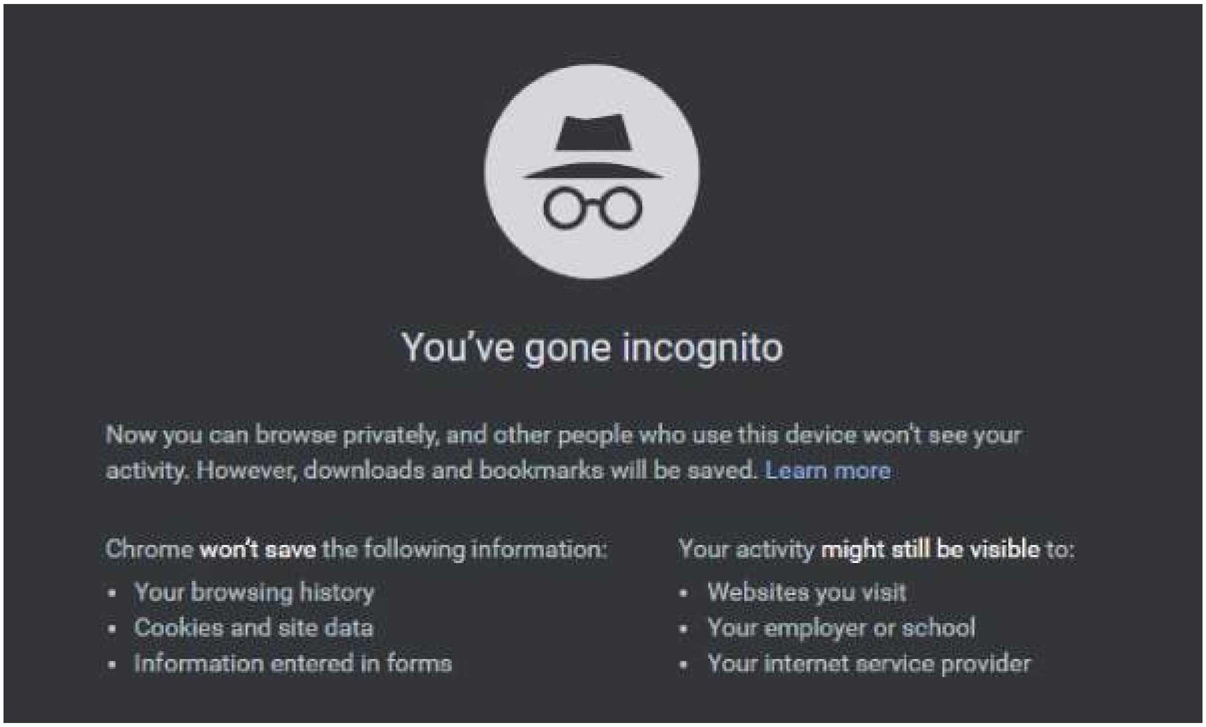
Edward Snowden, whether you believe what he did was right or wrong, showed us how the NSA is using tailored access operation (TAO) to compromise common computer systems and force companies to purposefully insert vulnerabilities into their own systems for TAO to exploit. An example of this is WARRIOR PRIDE, which is iPhone and Android software that can turn on a phone remotely, turn on the microphone, and activate geolocation. The modules of this kit have cartoon names, including Dreamy Smurf, which handles power management; Nosey Smurf, which can turn on the microphone; and Tracker Smurf, which turns on high-precision geolocation.

According to `www.statistica.com`, Google had more than 2 billion users in 2017. There are a little more than 7 billion people on the planet. One of the first things I do when teaching a Metasploit class or an open-source intelligence (OSINT) class is to have my students Google themselves. When you get to the My Activity page in Google, depending on your privacy settings, you'll see a timeline of activity, websites you've visited, and images you've viewed. Have you ever had a conversation with a friend and the very next ad you see on your PC or your phone is in direct correlation to the conversation you had?

Tor (also called The Onion Router) is the answer to much of this. Tor is a network that enables you to stay anonymous on the Internet. Tor is based on "onion routing" developed at the U.S. Naval Research Laboratory and was launched in 2002. The Tor Project (`www.torproject.org`) is a nonprofit organization that currently maintains and develops the free Tor Browser client. The U.S. government funds it with some support by the Swedish government and some individual contributors.

Is Tor illegal? No. Is engaging in activities that are illegal in your country on Tor illegal? Yes.

Some cyber professionals believe that using Incognito mode in Chrome is the same thing as running Tor. Browsing the Internet in Incognito mode only keeps the browser from saving your history, cookies, or form data. It does not hide your browsing from your ISP, employer, spouse, or the NSA. To activate Incognito mode in a Chrome browser, press the Ctrl+Shift+N. In Figure 6.12, you see Chrome in Incognito mode.



You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome **won't save** the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity **might still be visible** to:

- Websites you visit
- Your employer or school
- Your internet service provider

Figure 6.12: Chrome in Incognito mode

By contrast, Tor reduces the risk of traffic analysis by distributing it so that no single point can link you to your destination. To create a private network path, the users of the Tor Browser client will incrementally build a circuit of encrypted connections through different relays on the network. In Figure 6.13, you see the route that data takes from your Tor Browser client to the destination. The circuit is built one hop at a time so that each relay only knows to whom it's giving data and where it is sending that data. No individual relay knows the entire path. For security, after 10 minutes, a new circuit is created to keep anyone from attempting to figure out the path through the nodes.

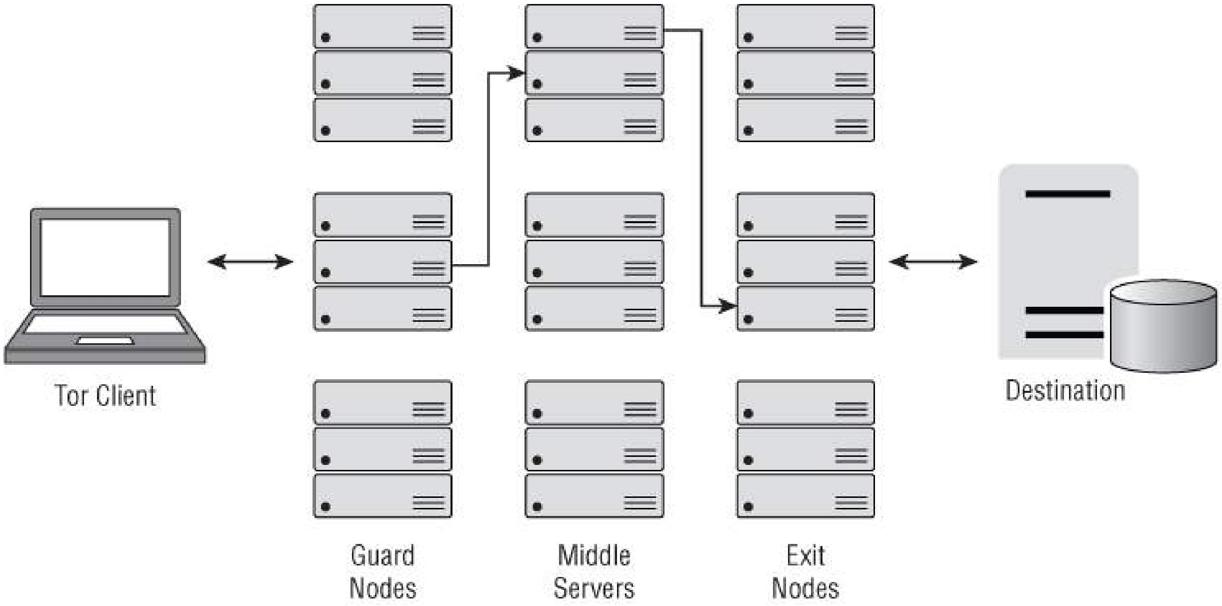
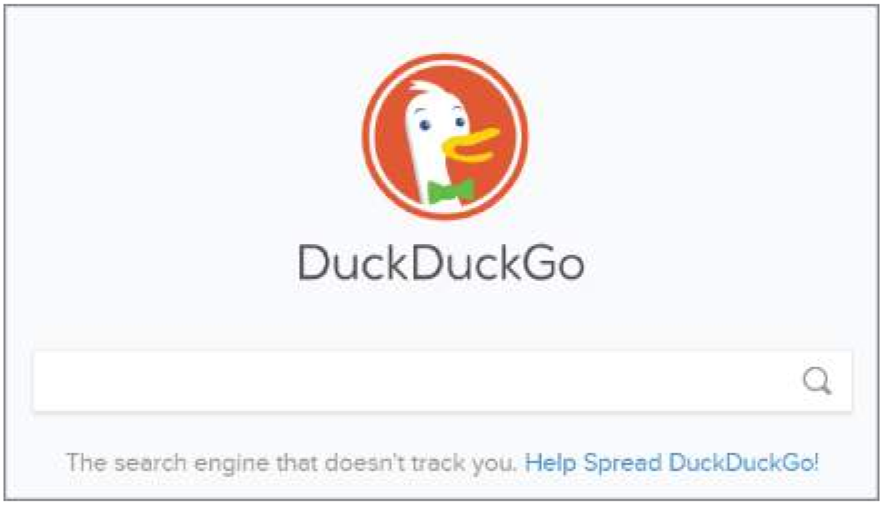


Figure 6.13: Tor routing data for anonymity

To use the Tor Browser client, download the install file from `www.torproject.org`, run the setup program, choose your desired language, choose a destination folder (I usually choose the Desktop), and click Install.

Open your Tor folder and double-click the Tor Browser client. You will have an option to configure the tool to work with a proxy. Click the Connect button to create the first encrypted relay and open the tool. If you are used to a quick response, you may need to take a deep breath. Because of the architecture of Tor, be prepared for slight delays. It's the exchange you make for privacy. In Figure 6.14, you see the default search engine that Tor uses is DuckDuckGo, layering even more protection of your privacy.



DuckDuckGo

The search engine that doesn't track you. Help Spread DuckDuckGo!

Figure 6.14: DuckDuckGo browser

Now you have end-to-end protection for your wireless communications. You know which networks around you are encrypted; what assets are on your network; which users, devices, and data you're sharing on your virtual private network; and that your browser cannot be traced.

CHAPTER 7
Wireshark

WHAT YOU WILL LEARN IN THIS CHAPTER:

- Wireshark
- OSI Model
- Capture
- Filters and Colors
- Inspection

Wireshark

My first real experience using Wireshark was in a forensics class with Sherri Davidoff, CEO of LMG Security. Sherri walked us through many tools to investigate a case study where money had been stolen. Wireshark was the tool we kept returning to time and time again to prove what had been planned and executed, and eventually we were able to prove who the threat actors were.

Wireshark is a tool that every network or security administrator should know. It is an open-source tool used for capturing network traffic and analyzing packets at an extremely granular level. Sometimes Wireshark is called a *network analyzer* or a *sniffer*. Packet capturing can tell you about transmit time, source, destination, and protocol type. This can be critical information for evaluating events that are happening or troubleshooting devices across your network. It can also help a security analyst determine whether network traffic is a malicious attack, what type of attack, the IP addresses that were targeted, and where the attack originated from. As a result, you will be able to create rules on a firewall to block the IP addresses where the malicious traffic originated.

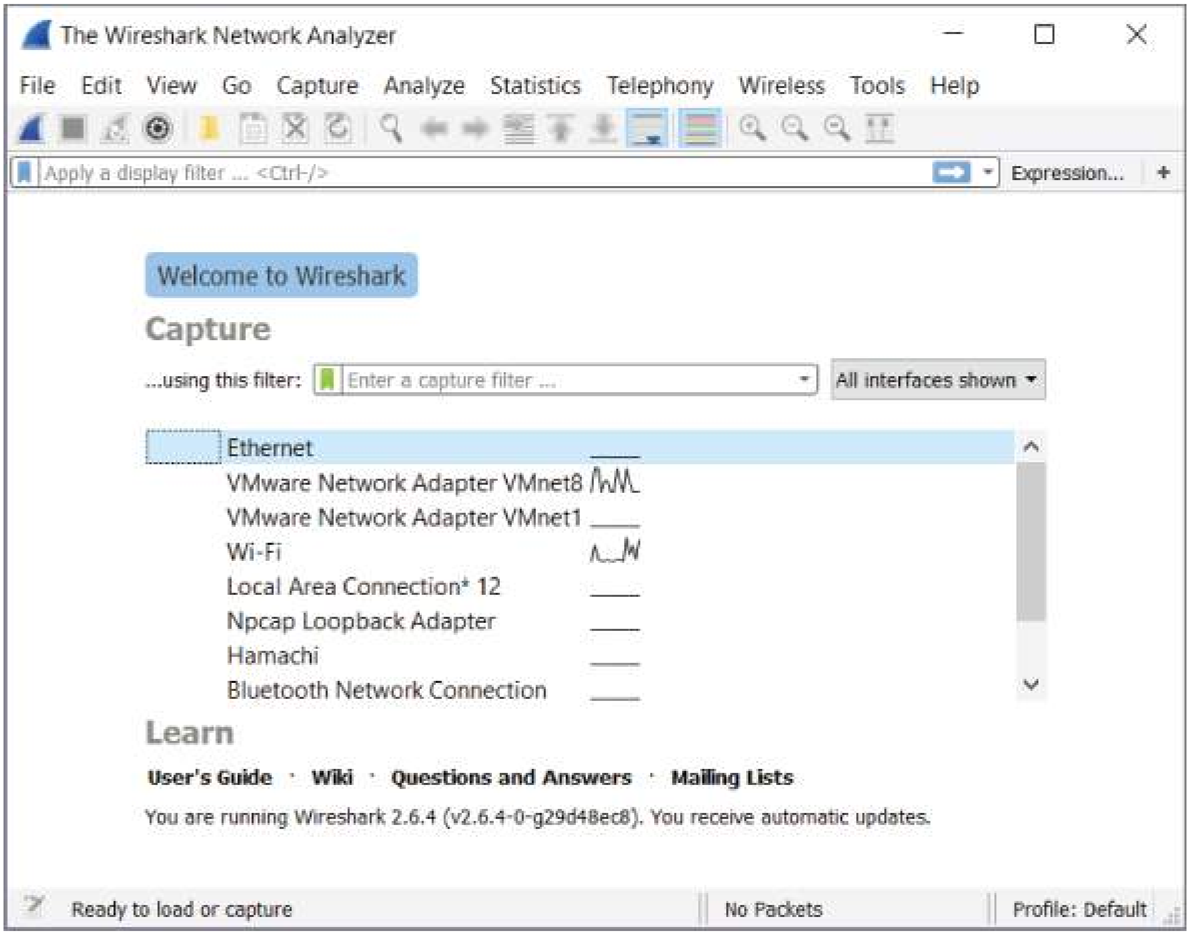
Wireshark shows packet details captured from different network media, breaking down the Open Systems Interconnection (OSI) model into the data link, network, transport, and application layers. At the bottom of the workspace, you have an option to open the hexadecimal with corresponding ASCII values on the right.

Wireshark is a powerful tool and technically can be used for eavesdropping. When you plan to use this in a business environment, you will want to get written permission to use it and make sure your organization has a clearly defined security privacy policy that specifies the rights of individuals using the network. Stories abound of network administrators capturing usernames, passwords, email addresses, and other sensitive user data. Wireshark is legal to use, but it can become illegal if you attempt to monitor a network that you do not have explicit authorization to monitor.

Determining the resources that Wireshark needs depends on the size of the `.pcap` file you are examining. If you have a busy network, then the files will be large. Wireshark can run on Windows and Linux machines. You will need a supported network card for capturing data, such as an Ethernet card or a wireless adapter. To get the latest copy of Wireshark, visit `www.wireshark.org`. The download page will have the proper version for your computers architecture and version operating system. A new version typically comes out every other month.

To install Wireshark, double-check the name of the file you have downloaded. If you have downloaded `Wireshark-win64-2.6.4.exe`, you will be installing Wireshark 2.6.4 for Windows 64-bit architecture. The download will include WinPcap, which allows you to capture live network traffic, not just examine saved packet captures (`.pcap` files).

Once you have installed the Wireshark executable, you will see the list of the different network interfaces that are functioning on the device as well as a graph to the right of current network activity on each interface. It reminds me of an electrocardiogram (EKG) that measures heart rhythms. As you see in Figure 7.1, if you have peaks and valleys, then you have traffic on that interface. If the line is flat, then that interface is not active.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+
Welcome to Wireshark
Capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

Apply a display filter ... <Ctrl-/>

...using this filter: Enter a capture filter ...

All interfaces shown

Ethernet
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Wi-Fi
Local Area Connection* 12
Npcap Loopback Adapter
Hamachi
Bluetooth Network Connection

You are running Wireshark 2.6.4 (v2.6.4-0-g29d48ec8). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

Figure 7.1: Choosing a network interface card for capture

When you double-click a network interface that is displaying activity, the main window will open to display all the traffic on that network. The major components of this page include the menu; the packet list, details, and bytes panes; and the status bar at the bottom, which can give you a great deal of detail regarding your capture.

The packet list pane is located in the top third of the window and by default shares information from the headers of each packet captured. Summary information includes source IP address, destination IP address, protocol in use, length of the packet, and information about the packet. By clicking the individual packets, you control what is shown in the bottom two panes. To drill down into each packet, select the packet in the packet list pane to view more details in the middle window, which feeds data into the bottom window.

In the packet details pane, you see individual packet size, both on the wire and bytes captured. You also see the transmission medium, protocol, source port, and destination port, and then depending on the type of packet, you may see flags or queries. You can click the > sign on the left to reveal different levels of detail about each packet in human-readable language.

At the bottom is a packet bytes pane. This displays data in hexadecimal code, which makes up the actual digital contents of the packet. It highlights the field selected above in the packet details pane. When you click any line in the middle pane, the hexadecimal code at bottom will be highlighted, giving you an extremely granular view of the data such as a URL that someone visited or contents of an email that was sent.

Under Preferences on the Edit menu, you can change the default layout of Wireshark, choosing exactly what columns you want listed; the fonts, colors, and position/direction of the panes; and what is displayed in each column. Since I learned how to use Wireshark in the default configuration, other than making the font larger and the colors more contrasting, I usually leave all of these preferences alone.

There are also quite a few keyboard navigation shortcuts. Table 7.1 describes the common ones.

Table 7.1: Keyboard shortcuts for Wireshark

KEY COMBINATION	DESCRIPTION
Tab	Moves between packet panes
Ctrl+F8	Moves to the next packet
Ctrl+F7	Moves to the previous packet
Ctrl+.	Moves to the next packet in the same conversation (TCP, UDP)
Ctrl+,	Moves to the previous packet in the same conversation (TCP, UDP)
Backspace	In packet details, jumps to the parent node
Enter	In packet details, toggles the selected tree item
Ctrl+L	Opens capture interfaces to start a new capture
Ctrl+E	Begins a capture from Ethernet

OSI Model

The OSI model was created by the International Organization for Standardization (ISO) to give architects, engineers, and manufacturers a modular way to troubleshoot issues. Certain protocols work at certain layers of OSI. As illustrated in Figure 7.2, the OSI moves in both directions depending on whether someone is either sending or receiving data.

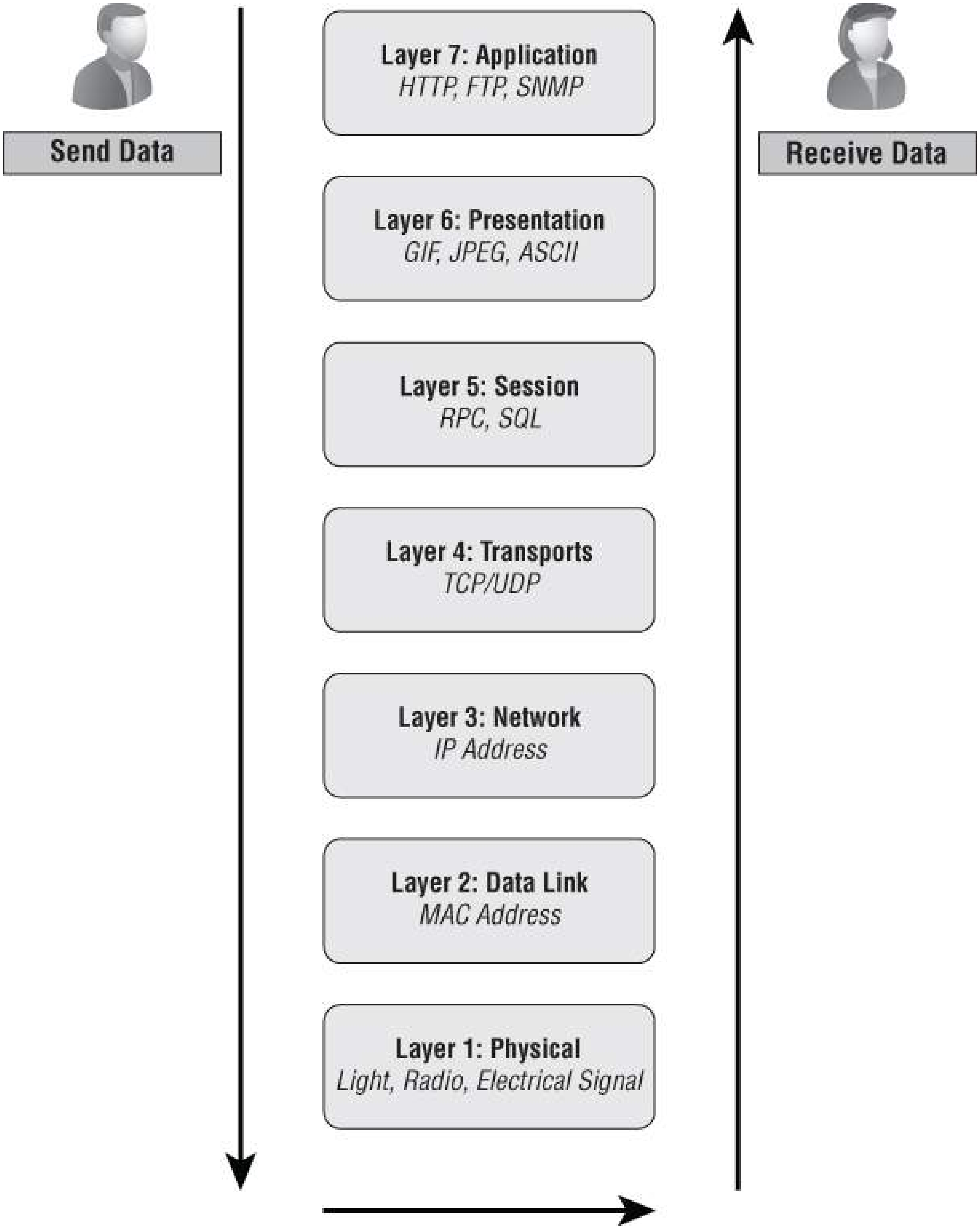


Figure 7.2: The OSI model sending and receiving data

When data is sent across a network, the information is encapsulated as it travels down the OSI layers. When the data is received, it travels up the seven layers and is demultiplexed and delivered to the end user at the upper layers. This process is often likened to using the post office. You write a letter, fold it and put it in an envelope, address it with a destination and receiving address, pay postage, and drop it off at the post office. The post office delivers it to its destination address and the intended person.

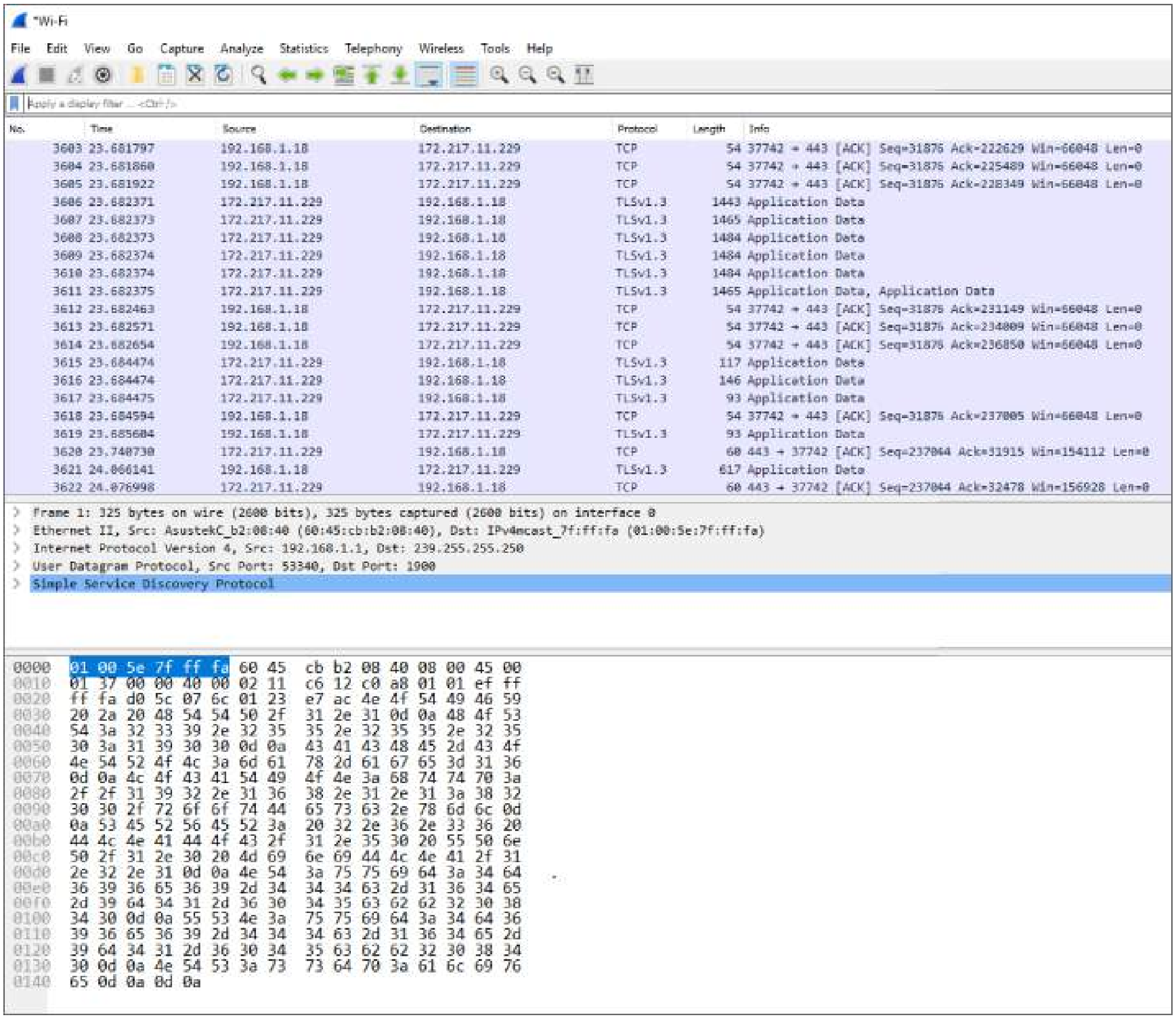
Complex problems can be more easily solved when you take this huge process and break it into smaller pieces. Nontechnical end users will turn on their system, log in, open a browser, type in a URL, and enter a username and password to read and compose their email with no clue how it works or what it looks like from a digital point of view. For any type of analysis, it's important to understand what is happening at the different layers of the OSI model. Wireshark will capture and filter traffic on specific fields within supported protocols in manageable-sized `.pcap` files in real time.

The physical layer is where you start. This is where the transmission of data using electrical signals, light, or radio occurs. Typically you can think of this as being the hardware layer. Devices such as hubs, the actual cables, and Ethernet work at this layer. When forming a hypothesis for correcting issues in your network, the physical layer is the equivalent of “Have you turned it on?” If there is no power, you have no communication, so start troubleshooting the physical layer.

The data link layer (or layer 2) is responsible for the encoding and decoding the electrical signals from the physical layer into bits and bytes and into frames. The data link layer can be subdivided into two sublayers: MAC and Logical Link Control (LLC). The MAC layer controls how a computer on the network gains access to data, and the LLC layer controls flow and error checking. Think of MAC as the MAC address that is burned into the network interface card.

The network layer is where the switching and routing take place using IP addresses. This is where the logical path gets plotted across the World Wide Web, taking the data packet to its final destination.

The transport layer is responsible for end-to-end error recovery. TCP and UDP work to get the data where it is supposed to go, but in very different ways. Using the post office analogy again, TCP is like using return receipt requested, and UDP is the marketing material that may or may not get placed in your mailbox. TCP is connection-oriented architecture where you will see SYN, SYN-ACK, and ACK. TCP's three-way handshaking technique is often referred to as “SYN, SYN-ACK, ACK” because there are three messages transmitted. SYN is synchronize, and ACK is acknowledge. You send a packet, which is the SYN, and the receiver acknowledges the receipt of said packet, which is the SYN-ACK. You acknowledge receivers’ acknowledgment that they did indeed receive that packet, which is the ACK. TCP is used to make sure systems get all the pieces they need to reassemble a message. This is called a *three-way handshake*. UDP doesn't care in the least if you receive their data. Think of a video or voice stream. Nothing gets resent if the connection breaks, and nothing is ever acknowledged that it was received. Figure 7.3 shows the ACK of packets and their number so they can be rebuilt properly by the receiver.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.     Time          Source           Destination      Protocol  Length Info
   3603 23.681797     192.168.1.18     172.217.11.229   TCP           54 37742 → 443 [ACK] Seq=31876 Ack=222629 Win=66048 Len=0
   3604 23.681860     192.168.1.18     172.217.11.229   TCP           54 37742 → 443 [ACK] Seq=31876 Ack=225489 Win=66048 Len=0
   3605 23.681922     192.168.1.18     172.217.11.229   TCP           54 37742 → 443 [ACK] Seq=31876 Ack=228349 Win=66048 Len=0
   3606 23.682371     172.217.11.229   192.168.1.18     TLSv1.3     1443 Application Data
   3607 23.682373     172.217.11.229   192.168.1.18     TLSv1.3     1465 Application Data
   3608 23.682373     172.217.11.229   192.168.1.18     TLSv1.3     1484 Application Data
   3609 23.682374     172.217.11.229   192.168.1.18     TLSv1.3     1484 Application Data
   3610 23.682374     172.217.11.229   192.168.1.18     TLSv1.3     1484 Application Data
   3611 23.682375     172.217.11.229   192.168.1.18     TLSv1.3     1465 Application Data, Application Data
   3612 23.682463     192.168.1.18     172.217.11.229   TCP           54 37742 → 443 [ACK] Seq=31876 Ack=231149 Win=66048 Len=0
   3613 23.682571     192.168.1.18     172.217.11.229   TCP           54 37742 → 443 [ACK] Seq=31876 Ack=234009 Win=66048 Len=0
   3614 23.682654     192.168.1.18     172.217.11.229   TCP           54 37742 → 443 [ACK] Seq=31876 Ack=236850 Win=66048 Len=0
   3615 23.684474     172.217.11.229   192.168.1.18     TLSv1.3      117 Application Data
   3616 23.684474     172.217.11.229   192.168.1.18     TLSv1.3      146 Application Data
   3617 23.684475     172.217.11.229   192.168.1.18     TLSv1.3       93 Application Data
   3618 23.684594     192.168.1.18     172.217.11.229   TCP           54 37742 → 443 [ACK] Seq=31876 Ack=237005 Win=66048 Len=0
   3619 23.685604     192.168.1.18     172.217.11.229   TLSv1.3       93 Application Data
   3620 23.740730     172.217.11.229   192.168.1.18     TCP           60 443 → 37742 [ACK] Seq=237044 Ack=31915 Win=154112 Len=0
   3621 24.066141     192.168.1.18     172.217.11.229   TLSv1.3      617 Application Data
   3622 24.076998     172.217.11.229   192.168.1.18     TCP           60 443 → 37742 [ACK] Seq=237044 Ack=32478 Win=156928 Len=0
```

```
> Frame 1: 325 bytes on wire (2600 bits), 325 bytes captured (2600 bits) on interface 0
> Ethernet II, Src: AsustekC_b2:08:40 (60:45:cb:b2:08:40), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 53340, Dst Port: 1900
> Simple Service Discovery Protocol
```

```
0000  01 00 5e 7f ff fa 60 45  cb b2 08 40 08 00 45 00
0010  01 37 00 00 40 00 02 11  c6 12 c0 a8 01 01 ef ff
0020  ff fa d0 5c 07 6c 01 23  e7 ac 4e 4f 54 49 46 59
0030  20 2a 20 48 54 54 50 2f  31 2e 31 0d 0a 48 4f 53
0040  54 3a 32 33 39 2e 32 35  35 2e 32 35 35 2e 32 35
0050  30 3a 31 39 30 30 0d 0a  43 41 43 48 45 2d 43 4f
0060  4e 54 52 4f 4c 3a 6d 61  78 2d 61 67 65 3d 31 36
0070  0d 0a 4c 4f 43 41 54 49  4f 4e 3a 68 74 74 70 3a
0080  2f 2f 31 39 32 2e 31 36  38 2e 31 2e 31 3a 38 32
0090  30 30 2f 72 6f 6f 74 44  65 73 63 2e 78 6d 6c 0d
00a0  0a 53 45 52 56 45 52 3a  20 32 2e 36 2e 33 36 20
00b0  44 4c 4e 41 44 4f 43 2f  31 2e 35 30 20 55 50 6e
00c0  50 2f 31 2e 30 20 4d 69  6e 69 44 4c 4e 41 2f 31
00d0  2e 32 2e 31 0d 0a 4e 54  3a 75 75 69 64 3a 34 64
00e0  36 39 36 65 36 39 2d 34  34 34 63 2d 31 36 34 65
00f0  2d 39 64 34 31 2d 36 30  34 35 63 62 62 32 30 38
0100  34 30 0d 0a 55 53 4e 3a  75 75 69 64 3a 34 64 36
0110  39 36 65 36 39 2d 34 34  34 63 2d 31 36 34 65 2d
0120  39 64 34 31 2d 36 30 34  35 63 62 62 32 30 38 34
0130  30 0d 0a 4e 54 53 3a 73  73 64 70 3a 61 6c 69 76
0140  65 0d 0a 0d 0a
```

Figure 7.3: Wireshark acknowledgment traffic

The session layer is layer 5 of the OSI model. It's responsible for making, managing, and terminating connections. Layer 6 is the presentation layer, which is in charge of what gets presented to your screen. Encryption and decryption of data happen at layer 6 as well. Finally, the seventh layer is the application layer, which supports the end users and their processes. Quality of service (QoS) works at layer 7 as well as application services such as email and HTTP. QoS is the ability of a network to provide better service to certain network traffic. The primary goal is to give priority to that traffic by dedicating bandwidth to control latency.

Each layer of the OSI model ensures the delivery of data from one place to another. If a layer fails, you end up with an error. With

Wireshark's help to diagnos the failing protocol, you can pinpoint where the problem is occurring so you can fix the error.

Capture

One of my favorite ways to teach Wireshark to beginners is to have students download and install Wireshark, bring up a terminal window, and capture the traffic after they launch Nmap. As you learned in Chapter 3, “Nmap: The Network Mapper,” good guys as well as bad guys use it. If you can recognize what Nmap traffic looks like and you know that you're not the one running it, then odds are it is someone attempting to map out your network.

LAB 7.1:ZENMAP AND WIRESHARK

NOTE

You will need to use three tools to make this lab work: a terminal window, Zenmap, and Wireshark. I am running this lab on a Windows 10 machine where I can open a command shell. You used Zenmap in Chapter 3. You can download Wireshark from `www.wireshark.org`.

1. Open a terminal window. Run the following command: **`ipconfig /all`**. Look for the IP address on your Wi-Fi network interface card.
2. Open Zenmap. In the Target field, add the IP address identified in the previous step. In the Profile field, leave the default of Intense scan.
3. Open Wireshark. On the welcome page as you saw in Figure 7.1, identify the Wi-Fi interface that corresponds with step 2. Double-click the Wi-Fi connection. It will start capturing data.
4. Go back to Zenmap and click the Scan button. On a single asset, the Nmap scan may last a to 2 minutes.
5. When the Nmap scan is done, return to Wireshark and click the red box under the word Edit. This will stop the capture, and you now have data to save and analyze.
6. With the Nmap window next to the Wireshark window, you will see traffic in Wireshark you can identify as the Nmap scan. During an Intense scan, Nmap will attempt to resolve DNS.
7. In Wireshark, look at the Protocol column for any DNS traffic. If you cannot find it by scrolling, try clicking the word

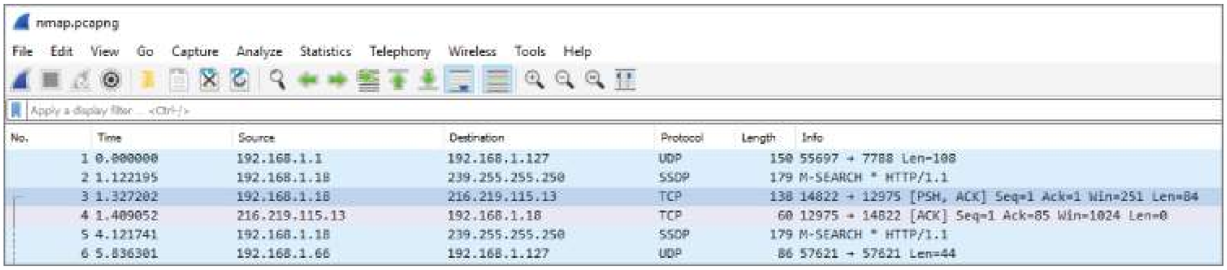
protocol in the top pane. Each column can be sorted in ascending and then descending order just by clicking the column headings.

8. To save the network traffic you just sniffed in Wireshark, go to File ➪ Save, name the file **nmap**, and click Save.

In any Wireshark menu, items will be grayed out if the feature isn't available. You cannot save a file if you haven't captured any data. Most of the Wireshark menu has the standard File, Edit, View, and Capture options. The Analyze menu allows you to manipulate filters, enable or disable dissection of protocols, or follow a particular stream of data. The Telephony menu is my favorite for analysis of voice traffic. In the Telephony menu, you can build flow diagrams and display statistics.

Capture filters are set before starting a packet capture. Display filters are not. In the Welcome To Wireshark window, you can find the capture filter just above the interfaces list. For instance, if you want to capture traffic only from a specific IP address, the filter would look like this: host 192.168.1.0. To capture traffic over a specific port, the filter would look like this: port 53. Double-click an interface to begin the capture.

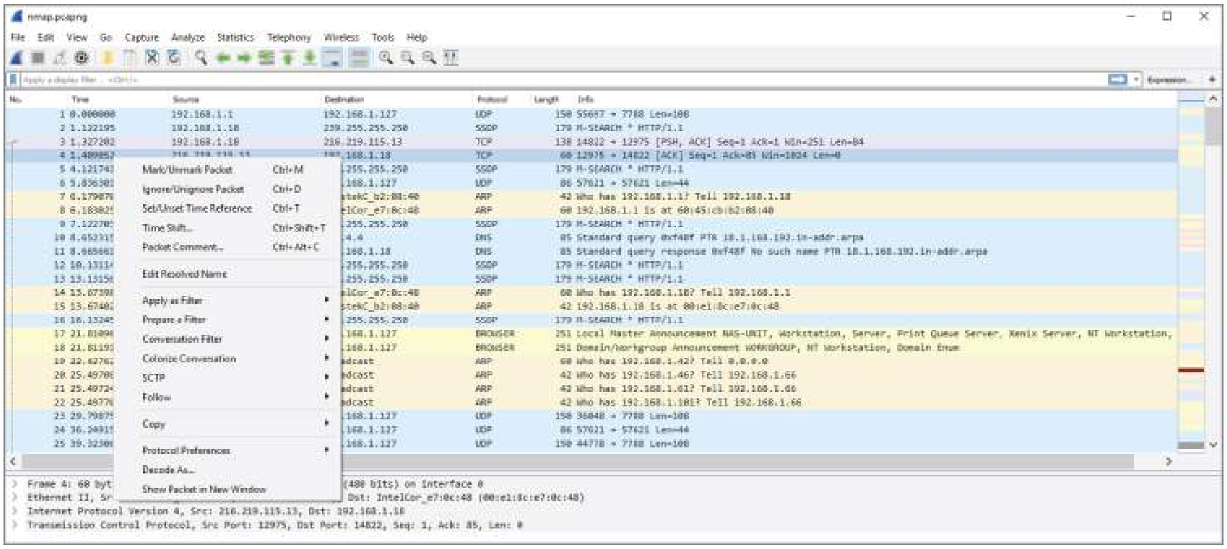
Now that you have your first capture started, the top pane is the packet list. The first column shows relationships between packets. Figure 7.4 shows the relationships between the selected packet and other “conversations” you captured. In line 3 under the No. column, you see the first packet of a conversation represented by a right angle, and line 4 continues with a solid line. Lines 5 and 6 start with a dotted line, which signifies that these two captured packets are not part of the conversation started in lines 3 and 4.


nmap.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time        Source           Destination      Protocol  Length Info
    1 0.000000    192.168.1.1      192.168.1.127    UDP          150 55697 → 7788 Len=108
    2 1.122195    192.168.1.18     239.255.255.250  SSDP         179 M-SEARCH * HTTP/1.1
    3 1.327202    192.168.1.18     216.219.115.13   TCP          138 14822 → 12975 [PSH, ACK] Seq=1 Ack=1 Win=251 Len=84
    4 1.409052    216.219.115.13   192.168.1.18     TCP           60 12975 → 14822 [ACK] Seq=1 Ack=85 Win=1024 Len=0
    5 4.121741    192.168.1.18     239.255.255.250  SSDP         179 M-SEARCH * HTTP/1.1
    6 5.836301    192.168.1.66     192.168.1.127    UDP           86 57621 → 57621 Len=44
```

Figure 7.4: Showing conversation relationships

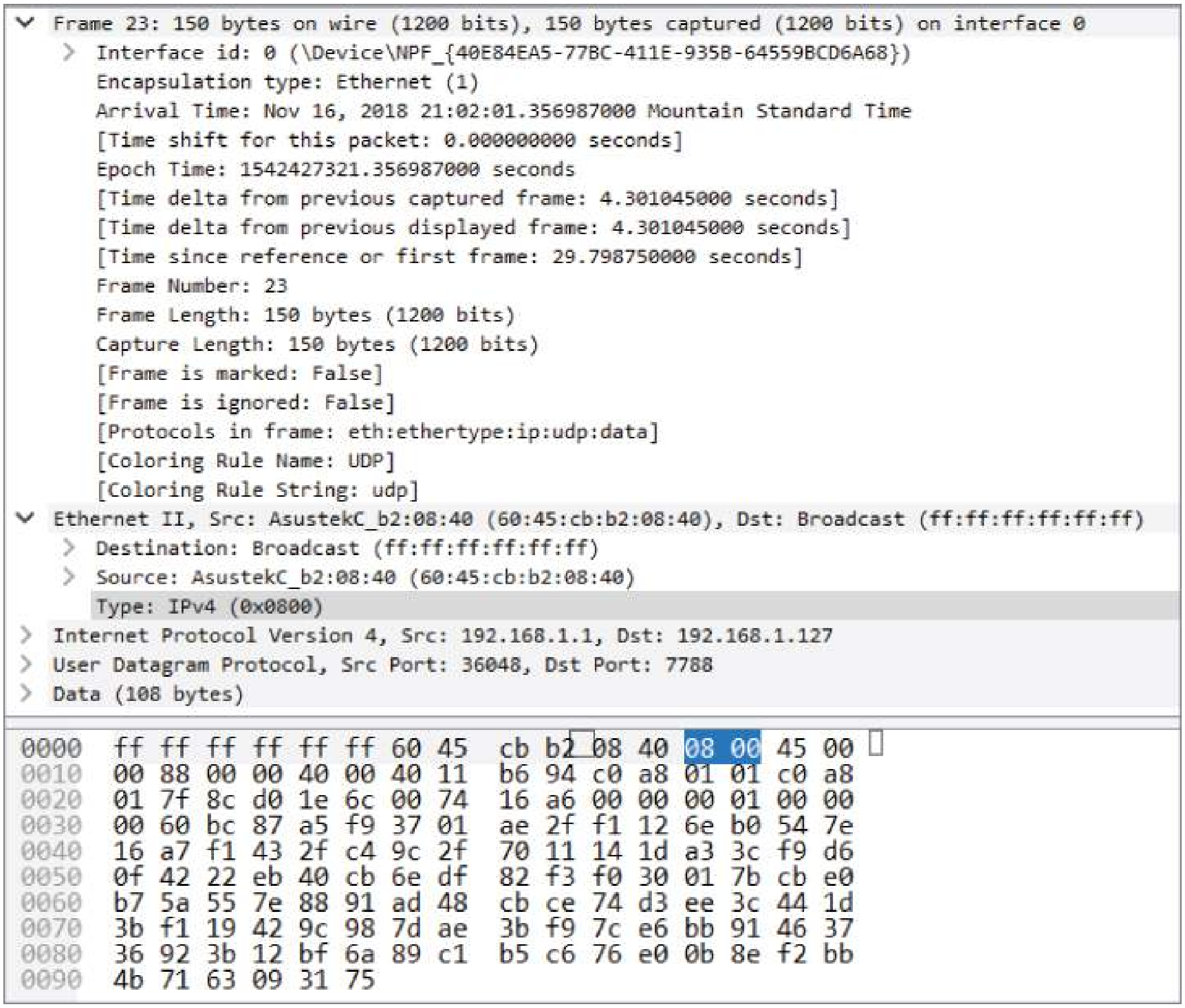
The next pane under the packet traffic is the packet details pane. This pane shows the protocols and fields of the packet selected in the pane above. The protocols and fields can be expanded and collapsed as needed. As you see in Figure 7.5, you can also right-click a packet for options in the packet list pane. Some fields have special generated fields such as additional information that isn't presented in the captured data, which is shown in square brackets. There will be links between packets if a relationship is found. These will be blue and underlined, and you can move from packet to packet.


nmap.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift… Ctrl+Shift+T
Packet Comment… Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As…
Show Packet in New Window

```
No.   Time        Source           Destination      Protocol  Length Info
    1 0.000000    192.168.1.1      192.168.1.127    UDP          150 55697 → 7788 Len=108
    2 1.122195    192.168.1.18     239.255.255.250  SSDP         179 M-SEARCH * HTTP/1.1
    3 1.327202    192.168.1.18     216.219.115.13   TCP          138 14822 → 12975 [PSH, ACK] Seq=1 Ack=1 Win=251 Len=84
    4 1.409052    216.219.115.13   192.168.1.18     TCP           60 12975 → 14822 [ACK] Seq=1 Ack=85 Win=1024 Len=0
    5 4.121741                     .255.255.250     SSDP         179 M-SEARCH * HTTP/1.1
    6 5.836301                     .168.1.127       UDP           86 57621 → 57621 Len=44
    7 6.179876                     tekC_b2:08:40    ARP           42 Who has 192.168.1.1? Tell 192.168.1.18
    8 6.183825                     elCor_e7:0c:48   ARP           60 192.168.1.1 is at 60:45:cb:b2:08:40
    9 7.122705                     .255.255.250     SSDP         179 M-SEARCH * HTTP/1.1
   10 8.652315                     .4.4             DNS           85 Standard query 0xf48f PTR 18.1.168.192.in-addr.arpa
   11 8.665661                     .168.1.18        DNS           85 Standard query response 0xf48f No such name PTR 18.1.168.192.in-addr.arpa
   12 10.1311                      .255.255.250     SSDP         179 M-SEARCH * HTTP/1.1
   13 13.1315                      .255.255.250     SSDP         179 M-SEARCH * HTTP/1.1
   14 13.6739                      elCor_e7:0c:48   ARP           60 Who has 192.168.1.18? Tell 192.168.1.1
   15 13.6748                      tekC_b2:08:40    ARP           42 192.168.1.18 is at 00:e1:8c:e7:0c:48
   16 16.1324                      .255.255.250     SSDP         179 M-SEARCH * HTTP/1.1
   17 21.8109                      .168.1.127       BROWSER      251 Local Master Announcement NAS-UNIT, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation,
   18 21.8119                      .168.1.127       BROWSER      251 Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum
   19 22.6276                      dcast            ARP           60 Who has 192.168.1.42? Tell 0.0.0.0
   20 25.4970                      dcast            ARP           42 Who has 192.168.1.46? Tell 192.168.1.66
   21 25.4972                      dcast            ARP           42 Who has 192.168.1.61? Tell 192.168.1.66
   22 25.4977                      dcast            ARP           42 Who has 192.168.1.181? Tell 192.168.1.66
   23 29.7987                      .168.1.127       UDP          150 36048 → 7788 Len=108
   24 36.2491                      .168.1.127       UDP           86 57621 → 57621 Len=44
   25 39.3230                      .168.1.127       UDP          150 44778 → 7788 Len=108

> Frame 4: 60 byt                         (480 bits) on interface 0
> Ethernet II, Sr                         Dst: IntelCor_e7:0c:48 (00:e1:8c:e7:0c:48)
> Internet Protocol Version 4, Src: 216.219.115.13, Dst: 192.168.1.18
> Transmission Control Protocol, Src Port: 12975, Dst Port: 14822, Seq: 1, Ack: 85, Len: 0
```

Figure 7.5: Right-clicking a packet

The packets bytes pane at the bottom of the window contains all the hexadecimal code of each packet. Each line of text contains 16 bytes. Each byte (8 bits) of packet capture is represented as a two-digit hexadecimal. In Figure 7.6, you can see the direct relationship between the IP type and the hexadecimal code.



```
v Frame 23: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
    > Interface id: 0 (\Device\NPF_{40E84EA5-77BC-411E-935B-64559BCD6A68})
      Encapsulation type: Ethernet (1)
      Arrival Time: Nov 16, 2018 21:02:01.356987000 Mountain Standard Time
      [Time shift for this packet: 0.000000000 seconds]
      Epoch Time: 1542427321.356987000 seconds
      [Time delta from previous captured frame: 4.301045000 seconds]
      [Time delta from previous displayed frame: 4.301045000 seconds]
      [Time since reference or first frame: 29.798750000 seconds]
      Frame Number: 23
      Frame Length: 150 bytes (1200 bits)
      Capture Length: 150 bytes (1200 bits)
      [Frame is marked: False]
      [Frame is ignored: False]
      [Protocols in frame: eth:ethertype:ip:udp:data]
      [Coloring Rule Name: UDP]
      [Coloring Rule String: udp]
v Ethernet II, Src: AsustekC_b2:08:40 (60:45:cb:b2:08:40), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    > Source: AsustekC_b2:08:40 (60:45:cb:b2:08:40)
      Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.127
> User Datagram Protocol, Src Port: 36048, Dst Port: 7788
> Data (108 bytes)

0000   ff ff ff ff ff ff 60 45  cb b2 08 40 08 00 45 00
0010   00 88 00 00 40 00 40 11  b6 94 c0 a8 01 01 c0 a8
0020   01 7f 8c d0 1e 6c 00 74  16 a6 00 00 00 01 00 00
0030   00 60 bc 87 a5 f9 37 01  ae 2f f1 12 6e b0 54 7e
0040   16 a7 f1 43 2f c4 9c 2f  70 11 14 1d a3 3c f9 d6
0050   0f 42 22 eb 40 cb 6e df  82 f3 f0 30 01 7b cb e0
0060   b7 5a 55 7e 88 91 ad 48  cb ce 74 d3 ee 3c 44 1d
0070   3b f1 19 42 9c 98 7d ae  3b f9 7c e6 bb 91 46 37
0080   36 92 3b 12 bf 6a 89 c1  b5 c6 76 e0 0b 8e f2 bb
0090   4b 71 63 09 31 75
```

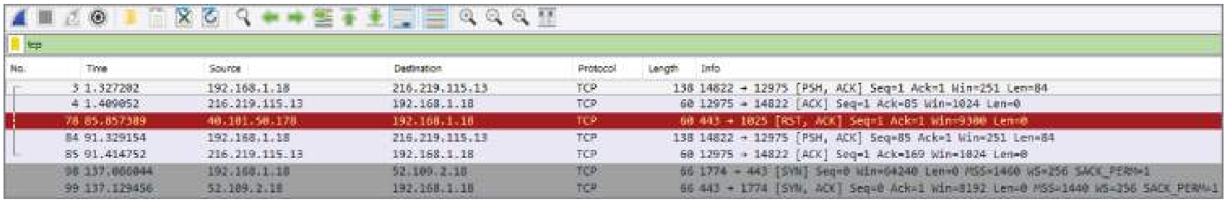
Figure 7.6: Hexadecimal representation

For your second capture, repeat the steps in the preceding lab but instead of doing an Nmap scan, open the browser of your choice and navigate to `www.example.com`. The Nmap capture was slow compared to this. The second you open the browser, you see an explosion of packets as your home page loads. Navigate to another site that you usually log into, like an email account or a bank. Log in as you usually do, but watch your Wireshark traffic as you complete that task.

Since I have explained how to take a capture, it is important for me to discuss where to take a capture. If you are in a large enterprise environment and there was an issue with network performance, the placement of the network sniffer is important. Place Wireshark as close to the employees and/or customers to identify any traffic issues from their perspectives. If people are complaining about a certain server on the network, you can move Wireshark in proximity to that server to find the problem. One best practice is to put Wireshark on a laptop and move around your location while you're tracking down these problems.

Filters and Colors

Wireshark uses display filters to concentrate on interesting packets while hiding the boring ones. You can select packets based on protocol, value, or comparison. To filter packets based on protocol, type in the protocol you want to narrow down to, as shown in Figure 7.7. Press Enter to accept the filter selection. When you're using a filter, it only changes the view, not the contents. The capture file remains intact. To remove a filter, click the clear button, which is the X to the right of the filter.



tcp

No.	Time	Source	Destination	Protocol	Length	Info
3	1.327202	192.168.1.18	216.219.115.13	TCP	138	14822 → 12975 [PSH, ACK] Seq=1 Ack=1 Win=251 Len=84
4	1.409052	216.219.115.13	192.168.1.18	TCP	60	12975 → 14822 [ACK] Seq=1 Ack=85 Win=1024 Len=0
78	85.857389	40.101.50.178	192.168.1.18	TCP	60	443 → 1025 [RST, ACK] Seq=1 Ack=1 Win=9300 Len=0
84	91.329154	192.168.1.18	216.219.115.13	TCP	138	14822 → 12975 [PSH, ACK] Seq=85 Ack=1 Win=251 Len=84
85	91.414752	216.219.115.13	192.168.1.18	TCP	60	12975 → 14822 [ACK] Seq=1 Ack=169 Win=1024 Len=0
98	137.060044	192.168.1.18	52.109.2.18	TCP	66	1774 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
99	137.129456	52.109.2.18	192.168.1.18	TCP	66	443 → 1774 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_PERM=1

Figure 7.7: Sorting packet capture based on TCP traffic

You can compare the values inside packets as well as combine expressions into far more specific expressions. Every field inside a packet can be used as a string, such as `tcp`. A `tcp` string will show all packets containing the TCP protocol. Once you have chosen the strings you want to knit together, you choose the appropriate operator. Table 7.2 lists commonly used filters.

Table 7.2: Filter operators

ENGLISH	OPERATOR	DESCRIPTION	EXAMPLE
eq	`==`	Equal	`ip.src==192.168.1.0`
ne	`!=`	Not equal	`Ip.src!=192.168.1.0`
gt	`>`	Greater than	`frame.len>16`
lt	`<`	Less than	`frame.len<64`
match	`~`	Field match	`http.host matches`
contains		Field contains	`tcp contains traffic`

Colorizing the traffic can be an effective filter to locate and highlight packets you may be searching for. You can choose to color packets that indicate errors, anomalies, breaches, or evidence. Wireshark has predefined coloring rules in the Edit menu under Preferences. Your coloring rules are placed at the top of the list by default, so your rules will trump any that come after.

For temporary colors, right-click a packet, go to Colorize Conversation, and slide down the list of types of traffic. To colorize the conversation, choose the protocol and select the color you would like that conversation to be. For example, you can color all IPv4 traffic blue and all Ethernet traffic red. This color rule will stay in effect until you restart Wireshark. You can also mark packets by right-clicking them. They will be shown with a black background, regardless of coloring rules. Marking a packet is helpful while analyzing a large capture, almost like a bookmark holding your place.

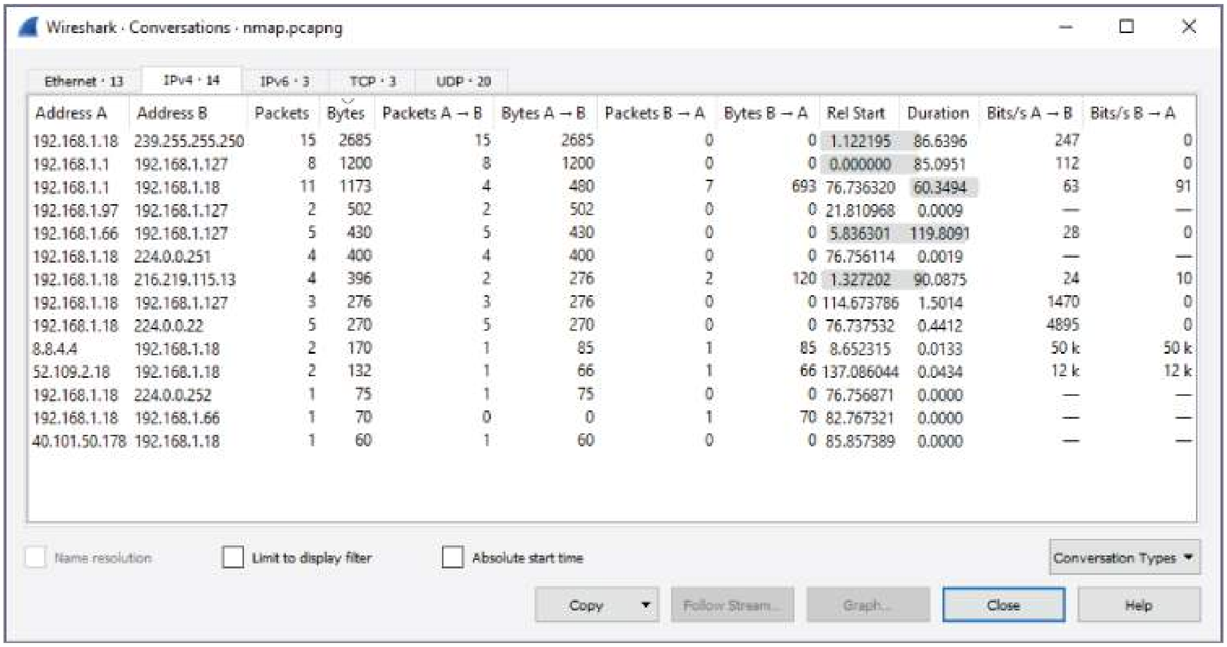
If you right-click a packet, you also have the ability to create packet comments. This is an excellent way to leave information that you have discovered, document a hypothesis, or communicate with other team members about network traffic you suspect is causing an issue.

Inspection

When you start inspecting and comparing packets in a packet capture, you'll notice the second column is based on time. Most computer systems start counting at 0, and Wireshark is no different.

The first column is set to a time value of 0, and all other timestamps base their times on that first packet capture. To view statistics for a number of packets, select Statistics on the menu. The statistics vary according to protocols, address, port, streams, or conversations.

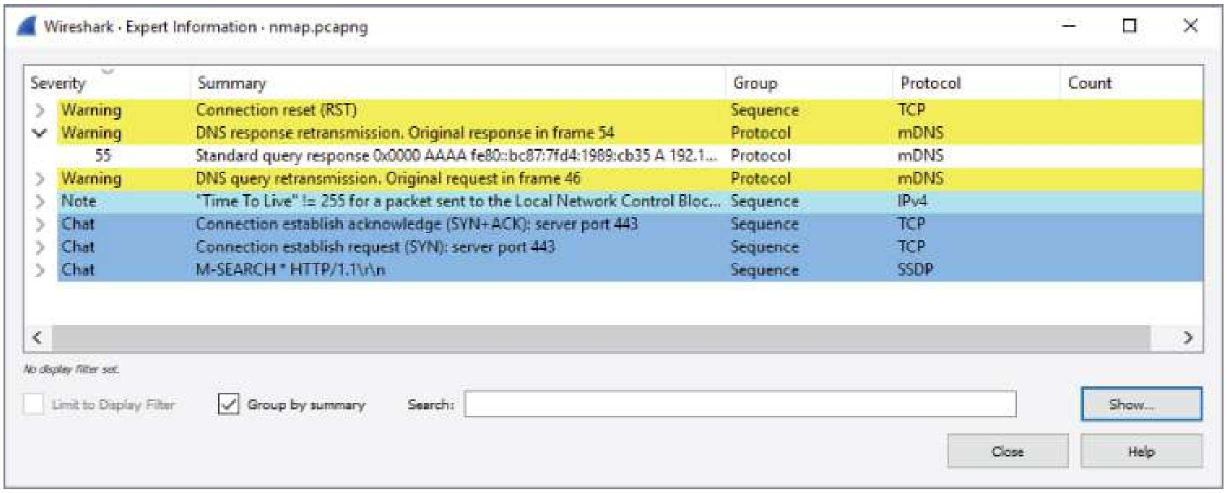
A conversation is a pair of physical or logical entities communicating. Conversations can include MAC, ARP, ICMP pings, or port numbers. To compare the conversations in the packet capture, go to the Statistics tab, and then inside that menu, go to Conversations. The default tabs across the top of the Conversation dialog box will show you the data broken down into Ethernet, IPv4, IPv6, TCP, and UDP. Each line shows the values for exactly one conversation. To add other conversation statistics, click Conversation Types in the lower-right corner. When working with a large file, sorting on the bytes transferred between hosts enables you to find the most active communication based on packets or duration of conversation. In Figure 7.8, notice the column for IPv4 conversations has been sorted to show the most active conversation between source and destinations.



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.18	239.255.255.250	15	2685	15	2685	0	0	1.122195	86.6396	247	0
192.168.1.1	192.168.1.127	8	1200	8	1200	0	0	0.000000	85.0951	112	0
192.168.1.1	192.168.1.18	11	1173	4	480	7	693	76.736320	60.3494	63	91
192.168.1.97	192.168.1.127	2	502	2	502	0	0	21.810968	0.0009	—	—
192.168.1.66	192.168.1.127	5	430	5	430	0	0	5.836301	119.8091	28	0
192.168.1.18	224.0.0.251	4	400	4	400	0	0	76.756114	0.0019	—	—
192.168.1.18	216.219.115.13	4	396	2	276	2	120	1.327202	90.0875	24	10
192.168.1.18	192.168.1.127	3	276	3	276	0	0	114.673786	1.5014	1470	0
192.168.1.18	224.0.0.22	5	270	5	270	0	0	76.737532	0.4412	4895	0
8.8.4.4	192.168.1.18	2	170	1	85	1	85	8.652315	0.0133	50 k	50 k
52.109.2.18	192.168.1.18	2	132	1	66	1	66	137.086044	0.0434	12 k	12 k
192.168.1.18	224.0.0.252	1	75	1	75	0	0	76.756871	0.0000	—	—
192.168.1.18	192.168.1.66	1	70	0	0	1	70	82.767321	0.0000	—	—
40.101.50.178	192.168.1.18	1	60	1	60	0	0	85.857389	0.0000	—	—

Figure 7.8: Wireshark conversations sorted by IPv4 protocol

There is another tool in Wireshark that logs anomalies found in a capture file: the Expert Info tool. The idea behind this tool is to provide a better understanding and display of notable network behavior. Both novice and expert users can solve issues quickly rather than combing through every packet manually. Expert info, as you see in Figure 7.9, is considered a hint.



Wireshark · Expert Information · nmap.pcapng

Severity	Summary	Group	Protocol	Count
Warning	Connection reset (RST)	Sequence	TCP	
Warning	DNS response retransmission. Original response in frame 54	Protocol	mDNS	
55	Standard query response 0x0000 AAAA fe80::bc87:7fd4:1989:cb35 A 192.1...	Protocol	mDNS	
Warning	DNS query retransmission. Original request in frame 46	Protocol	mDNS	
Note	"Time To Live" != 255 for a packet sent to the Local Network Control Bloc...	Sequence	IPv4	
Chat	Connection establish acknowledge (SYN+ACK): server port 443	Sequence	TCP	
Chat	Connection establish request (SYN): server port 443	Sequence	TCP	
Chat	M-SEARCH * HTTP/1.1\r\n	Sequence	SSDP	

No display filter set.

Figure 7.9: Expert Info tool color-coded "hints"

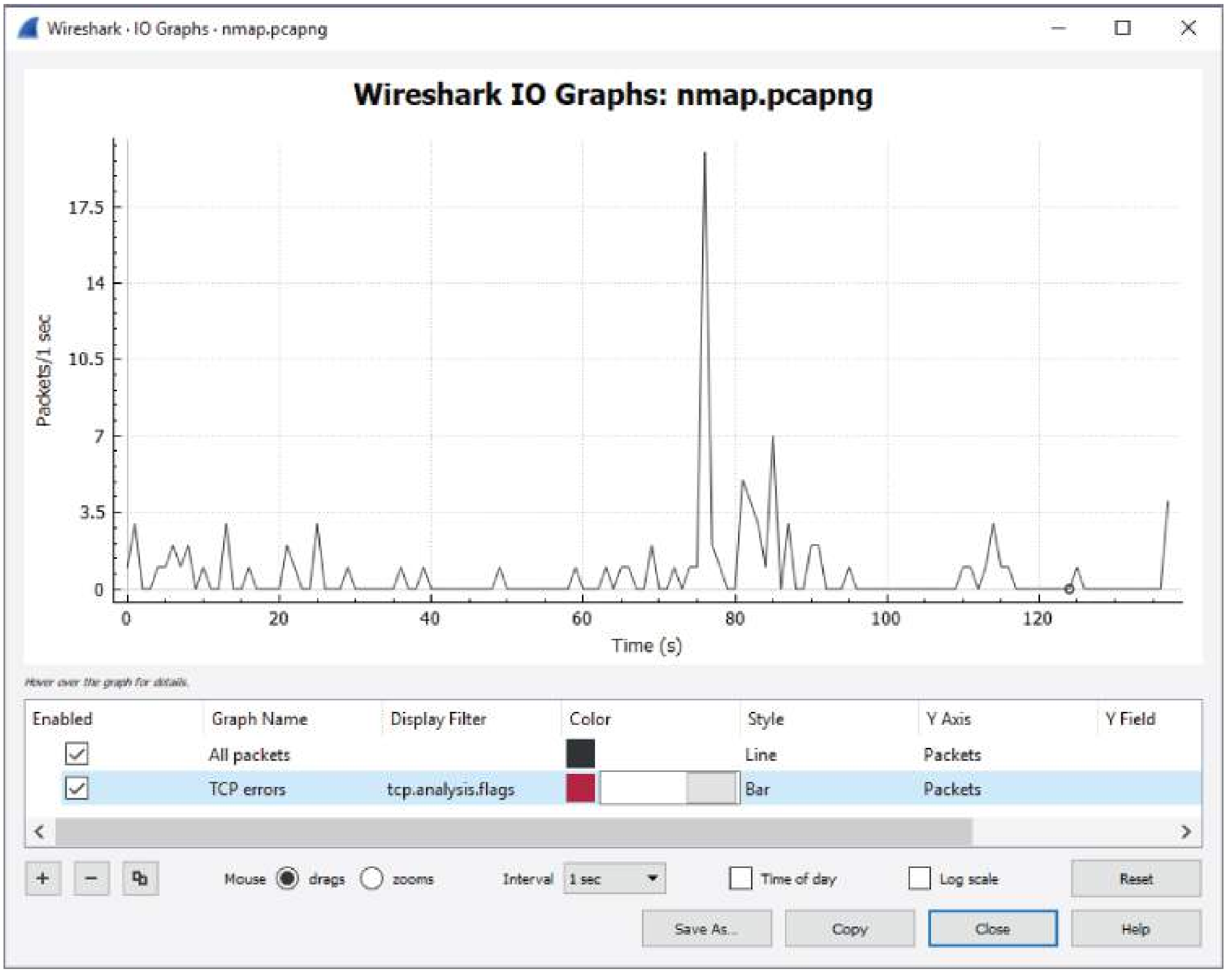
Every Expert Info type has a specific severity level. Table 7.3 lists the different Expert Info severity levels.

Table 7.3: Expert Info severity levels

LEVEL	COLOR	EXPLANATION
Chat	Blue	Informational, usual workflow
Note	Cyan	Normal errors
Warning	Yellow	Unusual errors
Error	Red	Serious problem

You can configure a graph of the captured network packets. You can configure the I/O graph to see the overall traffic as well as highs and lows in your traffic, which is typically based on a per-second, per-packet rate. You can use this to rectify problems, and you can even use it for monitoring. By default, the y-axis will set the interval to 1 second, and the y-axis will be packets like you see in Figure 7.10. Click any point on the graph to focus on that packet in the background. There are three different styles of graphs you can use:

line, impulse, and dots. If you are graphing multiple items, you can choose different styles for each graph.


Wireshark · IO Graphs · nmap.pcapng
Wireshark IO Graphs: nmap.pcapng
Packets/1 sec
17.5
14
10.5
7
3.5
0
0
20
40
60
80
100
120
Time (s)
Hover over the graph for details.
+
−
Reset
Save As...
Copy
Close
Help

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field
☑	All packets		■	Line	Packets	
☑	TCP errors	tcp.analysis.flags	🟥	Bar	Packets	

Mouse ● drags ○ zooms Interval 1 sec □ Time of day □ Log scale

Figure 7.10: Graphing all packets versus just TCP errors

After capturing network traffic on your own system, the Nmap scan, and web browser traffic, if you want to branch out and look at other, more-complicated traffic but you don't have access to a more complicated network, there is a link inside Wireshark that will help you build a strong skill set with this tool. Under the Help menu are sample captures that can be interesting to dissect. On the page that lists the sample captures, one of the simplest to begin with is `HTTP.cap`, which is a simple HTTP request and response.

CHAPTER 8
Access Management

WHAT YOU WILL LEARN IN THIS CHAPTER:

- Authentication, Authorization, and Auditing
- Least Privilege
- Single Sign-On
- JumpCloud

Let's take a trip through an airport. You have to produce identification to authenticate you are who you say you are. Then you have to provide a ticket to an agent to access the boarding area. Your belongings are screened to make sure you're not bringing any malicious contraband with you into a secured area. When you board the plane, they scan your ticket to prove you gained access to the aircraft. Now the airline can track and audit if and when you traveled. This is fundamental access management. Now take the same concept and apply it to a networked environment.

With all these layers of access management, how often do we hear of people getting past security? What other layers of security are in place at an airport that you have not even considered? As a security professional, you become acutely aware of those layers of defense in depth. You always have to be thinking strategically and protectively and asking targeted questions. What if someone is impersonating another on my network? What if someone has too much access? What if someone does access the network but has brought ransomware along?

Access management makes system or network administrators think about how people log into their computers and network. Most users don't realize there is a difference between logging in with domain credentials versus logging directly into an asset. Many users don't realize there are different levels of access. They believe what you see is what you get (WYSIWYG).

Access management is the process of identifying, controlling, managing, and auditing authorized users' access to any asset you manage. Typically in IT, asset management (AM) is used in conjunction with identity management (IM). IM creates and provisions different users, roles, groups, and policies where AM ensures that the security guidelines, procedures, and policies are followed.

There are many different organizations selling IM/AM solutions today. Picking a solution is not easy. You have to keep in mind scalability, performance, and usability. Close-sourced solutions can hamper your ability to adapt applications to your specific requirements and total cost of ownership becomes high. Open-source management can give you freedom to make good business decisions, customize it for unique situations, and have low or no maintenance fees, but it can be difficult to implement. Not only do you have to manage IM/AM, you have to add least privilege into the equation. The practice of least privilege is limiting access rights of users to only what they need to get the job done. Josh Franz, a security consultant at Rapid7, says, “Simply put, if you don't have identity access management in your company, you do not have security. All the security controls in the world won't stop an attacker if everyone on your network is a domain admin.”

AAA

Authentication, authorization, and auditing (AAA) are often used together in cybersecurity when it comes to how someone gains access to a system. Authentication and authorization are critical topics often confused, but they are different from each other. Authentication is confirming who you are, while authorization means verifying what you have access to. Authentication is usually a username or ID and a password but could also be something you have like a token or something you are like a fingerprint.

Based on your security policies, you and your organization may need different levels of authentication.

- Single-factor—easiest authentication, usually a simple password to grant access to a system or domain.
- Two-factor—two-step verification that results in more security. When you visit the bank to withdraw money from an ATM, you need both a physical card and a personal identification number (PIN).
- Multifactor—the most secure type of authentication to grant access, using two or more techniques from different categories.

Authorization happens after you have been authenticated. In the two-factor analogy, after using the ATM card and PIN, you get access to your money, and only your money. Authorization determines your ability to access what systems and which accounts are you able to withdraw money from. This is a key component to access policy.

Auditing (some say the third *A* is accounting) is used to make sure the controls put in place are working. Auditing is used to support accounting. Auditing is the logging of events that have significance such as who has logged in and logged out or who attempted some type of privileged action. Monitoring can help make sure that there are no malicious activities happening in the environment. If you are looking to prove someone did something on your network, audit and security logs are the absolute best files to maintain that someone or something performed an action in a networked environment.

Another important part of auditing and accounting is nonrepudiation. Nonrepudiation means that the person authenticated and authorized cannot deny the performance of an action. You do not want a situation where one person claims an action happened and another is in total opposition to the story. A traditional example of nonrepudiation is a signature you received a document. In cybersecurity, nonrepudiation requires the creation of certain artifacts such as the following:

- An identity

- Authentication of that identity
- Evidence connecting that identity to an action

Least Privilege

If you ever take a certification exam, you may see this as principle of least privilege (PoLP) and even principle of least authority (PoLA). It is a concept that reduces the accidental or purposeful attack surface of an organization. There are several ways through access management you can use this concept to protect your ecosystem. In IT, we learn from others' mistakes.

About a decade ago, I was an administrator on a network with about 12,000 machines and 9,000 users. We used Group Policy in Windows to control the working environment. It was a way to centralize management of users' settings, applications, and operating systems in an Active Directory environment. We had someone new to the organization who was full of great ideas but was not aware of or willing to follow the change management procedures we had put in place to safeguard the network.

He changed a major feature in Group Policy that had catastrophic results. In the Event Viewer on a Windows machine you can configure your security logs. He checked the box to not overwrite security logs and pushed it out to 12,000 machines using Group Policy objects. If you've been IT for a while, you might be cringing. Within 24 hours, he had locked out 9,000 users on our network by filling up the allotted log space for successful and failed logon/logoff events. Thankfully, we were able to fix the problem within about 30 minutes after we had figured out what had happened. At first, we had thought we were under attack. Through nonrepudiation, we knew which admin had been logged into the system when the change occurred.

Here are the morals of this story:

- If you're not sure what you're doing, then ask.
- Just because you can doesn't mean you should.

- If you limit who has access to critical systems, you reduce your attack surface.

Most devices have mechanisms built in where you have standard end-user and administrator accounts. Administrator accounts are for users who need full access to all areas of the machine where user accounts are restricted; users can run applications but do not have full administrative access.

One reason this principle works so well is that it will make you do internal research on what privileges at what level are actually needed. Unfortunately, the path of least resistance in many organizations has been the overuse of accounts with deep and far-reaching privilege. The consequences of a network administrator opening an email attachment that launches malware while logged into the domain administrator's account are that the malware will have administrator's privilege on the domain and unrestricted access to the network. If the network administrator is logged into a standard end-user account, the malware only has access to the user's data, and the potential compromise scope is much smaller.

You should default to creating a separate standard user account for every user including administrators, and every account should use at least single-factor authentication. This enables you to control what the users can install and websites they can visit. Too many organizations allow all users on their network administrative privileges, and it creates a massive attack surface. Administrators should always log in using their standard user account and then use the Run As Administrator feature to run those programs they need elevated privileges to use. There are far too many breaches that get traced back to administrators opening email and clicking a link that leads to a malicious download that compromises an asset that spreads through a network and steals everything. Not only do organizations lose intellectual property, but they end up fined for violations of compliance, which can lead to a loss of millions in a single breach.

One of the best ways to start implementing the PoLP is to start with a privileged audit. A user account created to use a database does not need admin rights like a programmer building the database. You do not want to hinder your end users; you want to give them only enough access to perform their required job.

Do an audit of privilege on a regular basis. This is not a one-and-done exercise. It is operational. Who has access to what, and who has changed jobs and retained access to their old permissions?

Start every account as low as possible. Only add higher permissions if needed/requested and only for the time needed. An auditor may need elevated privileges but only for the duration of the audit.

Separation of duties (SoD) is a strategic function of least privilege. You have one person write the check and one person sign the check. By having more than one person accomplish a task, it can help prevent fraud or errors. In the Group Policy story earlier, SoD was part of that process. If the employee had followed procedures for change management, I could have told him why it was a really bad idea.

By implementing least privilege, you can even improve operational performance, reduce the chance of unauthorized behavior, reduce the attack surface, and reduce the chances of malicious software propagating since it might need elevated processes to run. One of the biggest benefits of implementing least privilege is that it makes it easier to meet compliance requirements. Many compliance regulations such as PCI-DSS, HIPAA, FISMA, and SOX require that organizations apply least privilege to ensure proper data management and security.

The Federal Desktop Core Configuration requirements by the National Institute of Standards and Technologies (NIST) say that federal employees must log into PCs with standard privileges. PCI-DSS 3.0 7.2.2 requires assignment of privileges to individuals based on job classification and function.

Single Sign-On

Working in our modern-day environments requires us to log into multiple programs to get our jobs done. We have to log into customer management databases, share resources in cloud applications, check email, and create documentation online. It can be a headache for the average user to remember all those usernames and passwords. To alleviate that issue, we use single sign-on (SSO) applications. SSO is another form of access control between multiple, interrelated software systems.

Benefits of single sign-on can include the reduction of password fatigue or having end users write their passwords on sticky notes and put them on their monitor or under the keyboard. It can save time typing in passwords over and over and ideally reduce help-desk issues of people calling in because they went on vacation and forgot their password and locked themselves out. One of the big criticisms of SSO is the access to many different resources from just one login. To combat this issue, we have to focus on protecting the "keys to the kingdom" and combine this with strong verification like multifactor authentication.

The CIA triad shown in Figure 8.1 is used to find the right balance for an organization based on priorities. Some organizations like the military's preference toward confidentiality, where organizations such as Amazon might lean toward availability. After all, the military does not want its secrets leaked, and you cannot purchase from a website if the site is down.

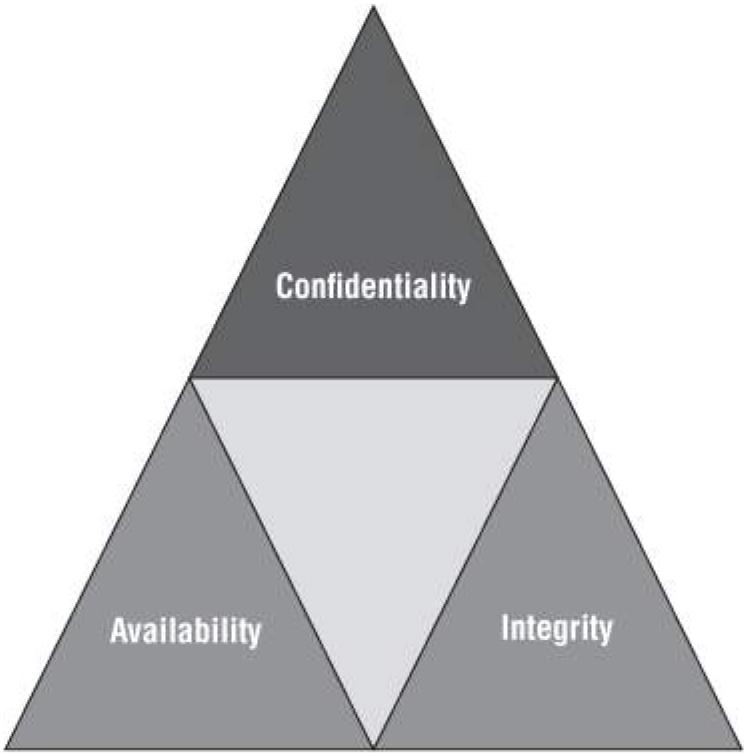


Figure 8.1: CIA triad

Confidentiality is a set of rules that limit access to information, integrity is the assurance that the information is accurate, and availability is giving the right information access to the right people. Network and security IT administrators have to find a balance between protecting the environment and meeting compliance without hindering the workflow of the end users. If you tighten controls too tight, users cannot do their job, but if controls are too lax, it results in a vulnerability. If you're not careful, end users will start saving their credentials in their browser for easy login into their favorite banking or shopping websites. They may even save their corporate credentials, which could be catastrophic if the machine is ever accessed by non-authorized individuals.

As a security leader in your organization, you have decisions to make. The problem with making decisions today is your enterprise will mostly likely change tomorrow. Most of the processes we use in IT are cyclic, always subject to reevaluation. When your security maturity model reaches the point where building and documenting AAA, least privilege, and SSO into your management process, every individual from CEO to the security administrator needs his or her access configuration audited. In Figure 8.2, you see a simple matrix of users' needs when it comes to accessing their network. Once you know what users need to perform their role, it becomes easy to build that role for them.

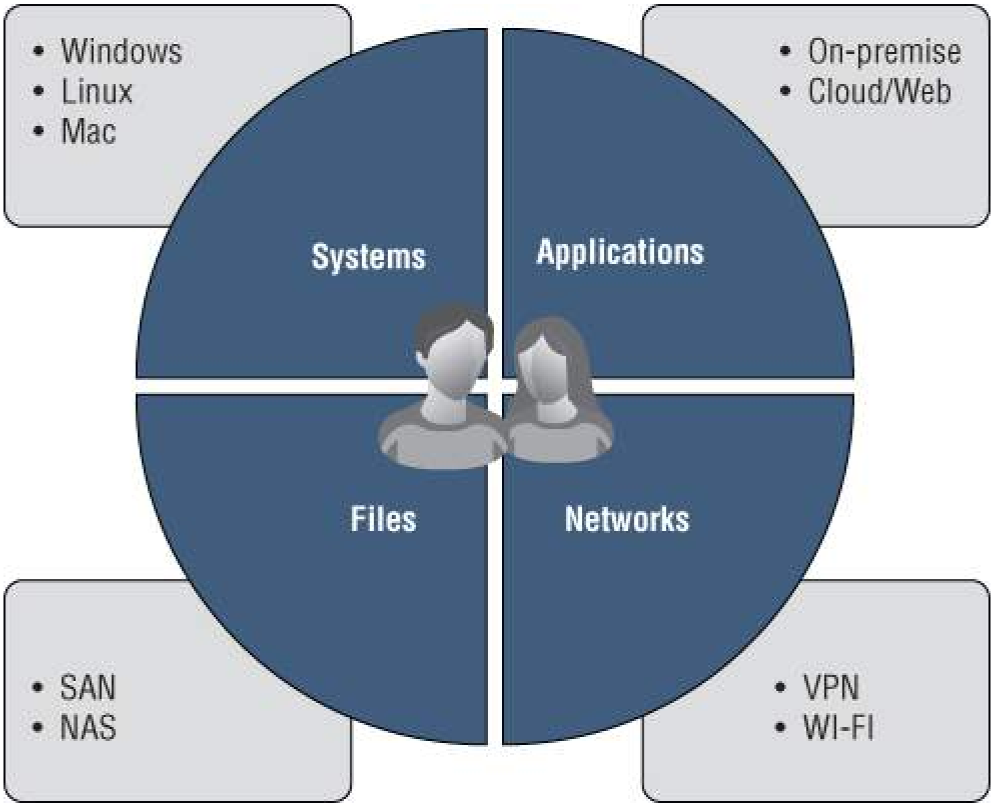


Figure 8.2: Evaluating users' needs in your network

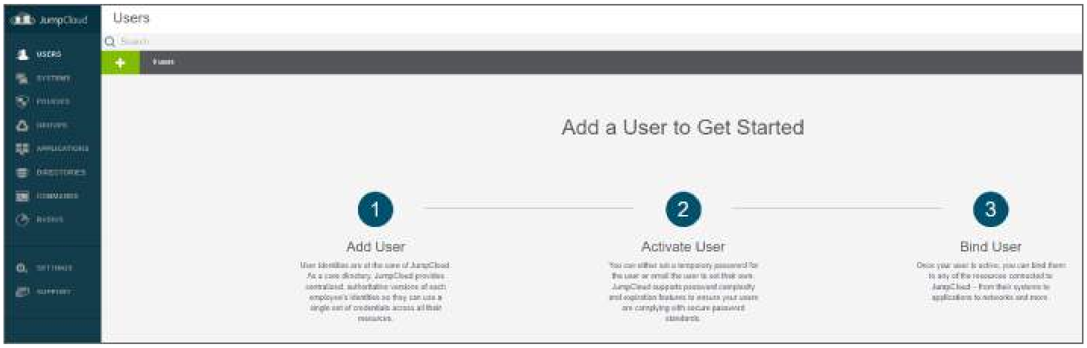
JumpCloud

According to Zach DeMeyer at JumpCloud, “Generally endpoint management solutions have focused solely on managing the system, not including identities and access.” JumpCloud is a cutting-edge blend of SSO and management of permissions in a network. Users' identities are at the core of JumpCloud as a directory as a service. You create a central, authoritative version of each identity so employees can use a single set of credentials throughout all the resources they need to access. You can set up password complexity and expiration features to ensure policies are met and then, once set up, bind those users to any of the resources connected to JumpCloud from their host system to applications to networks.

To get started, go to jumpcloud.com and create your user account. Your first ten users are completely free, forever. After that, there is a small charge per user. Once your user account is validated through your email, you have access to the central console where you can set up credentials for platform, protocol, or location. You can use JumpCloud to enforce policies, set password requirements including multifactor authentication, and streamline access to most IT resources. Lab 8.1 shows how to create a user, and Lab 8.2 shows how to create a system.

LAB 8.1: CREATING A USER

1. Open your browser and log into the JumpCloud web interface.
2. On the Users tab, click the green box with the plus sign (see Figure 8.3).



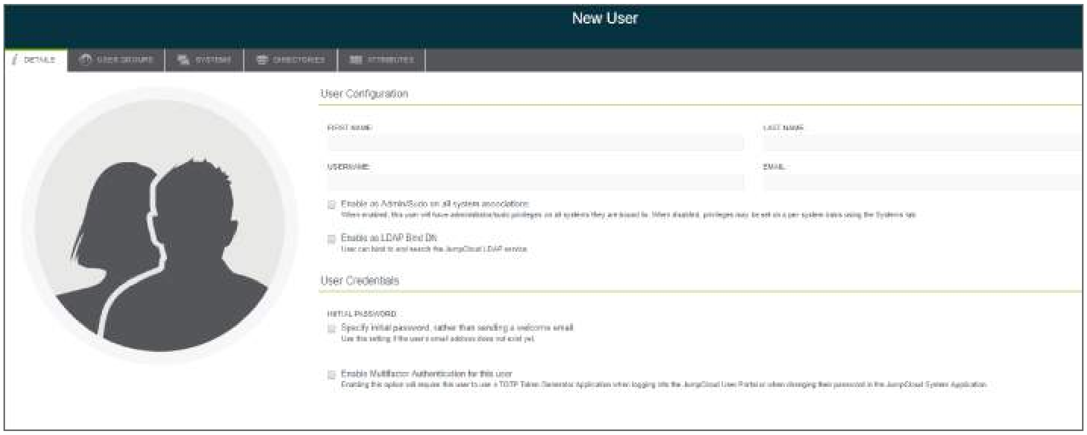
User identities are at the core of JumpCloud. As a core directory, JumpCloud provides centralized, authoritative versions of each employee's identities so they can use a single set of credentials across all their resources.

You can either set a temporary password for the user or email the user to set their own. JumpCloud supports password complexity and expiration features to ensure your users are complying with secure password standards.

Once your user is active, you can bind them to any of the resources connected to JumpCloud – from their systems to applications to networks and more.

Figure 8.3: How to create a user in JumpCloud

3. Define the new user's first name, last name, username, and email address. If you have audited this user's needs, then you will know if you need to enable admin/sudo permissions or require multifactor authentication. In Figure 8.4, you see the New User dialog box. This is where you can add the initial password for the user.



☐ Enable as Admin/Sudo on all system associations
When enabled, this user will have administrative/sudo privileges on all systems they are bound to. When disabled, privileges may be set on a per system basis using the Systems tab.

☐ Enable as LDAP Bind DN
User can bind to and search the JumpCloud LDAP service

☐ Specify initial password, rather than sending a welcome email
Use this setting if the user's email address does not exist yet.

☐ Enable Multifactor Authentication for this user
Enabling this option will require this user to use a TOTP Token Generator Application when logging into the JumpCloud User Portal or when changing their password in the JumpCloud System Application.

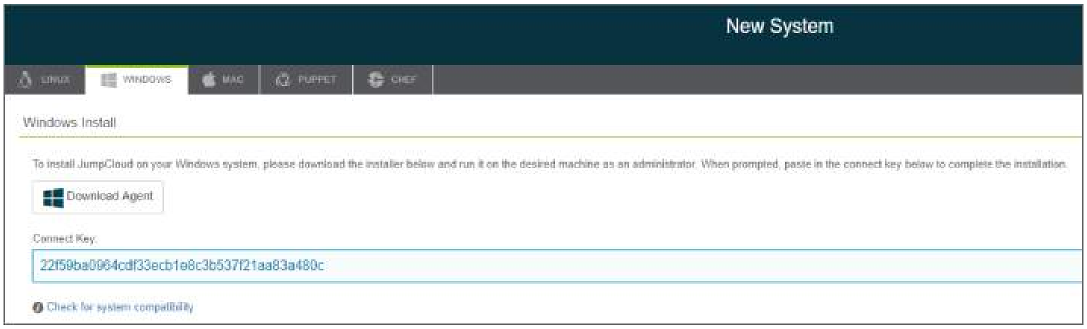
Figure 8.4: The New User dialog box

4. For each user, you have the ability to add that person to user groups for access permissions, what systems each has

permission to sign into, and what directories each needs access to. You will have to build these next to tie them together.

LAB 8.2: CREATING A SYSTEM

1. Open the systems menu, second from the top. Click the green box with the plus sign to open the New System instructions.
2. Mac, Windows, and Linux systems are bound to the JumpCloud platform when you install the system agent. Once it is installed, you can remotely and securely manage a system and the accounts on those systems and set policies. The agent is small and checks in through port 443 and reports event data. *Align the system you need to manage with the platform at the type of New System.*
3. Each of these will have specific instructions and connection keys. In the case of Windows, you have an agent to download as well as a connect key (see Figure 8.5). When you double-click the Windows executable, you will be asked for the key during the install process.



Windows Install

To install JumpCloud on your Windows system, please download the installer below and run it on the desired machine as an administrator. When prompted, paste in the connect key below to complete the installation.

Download Agent

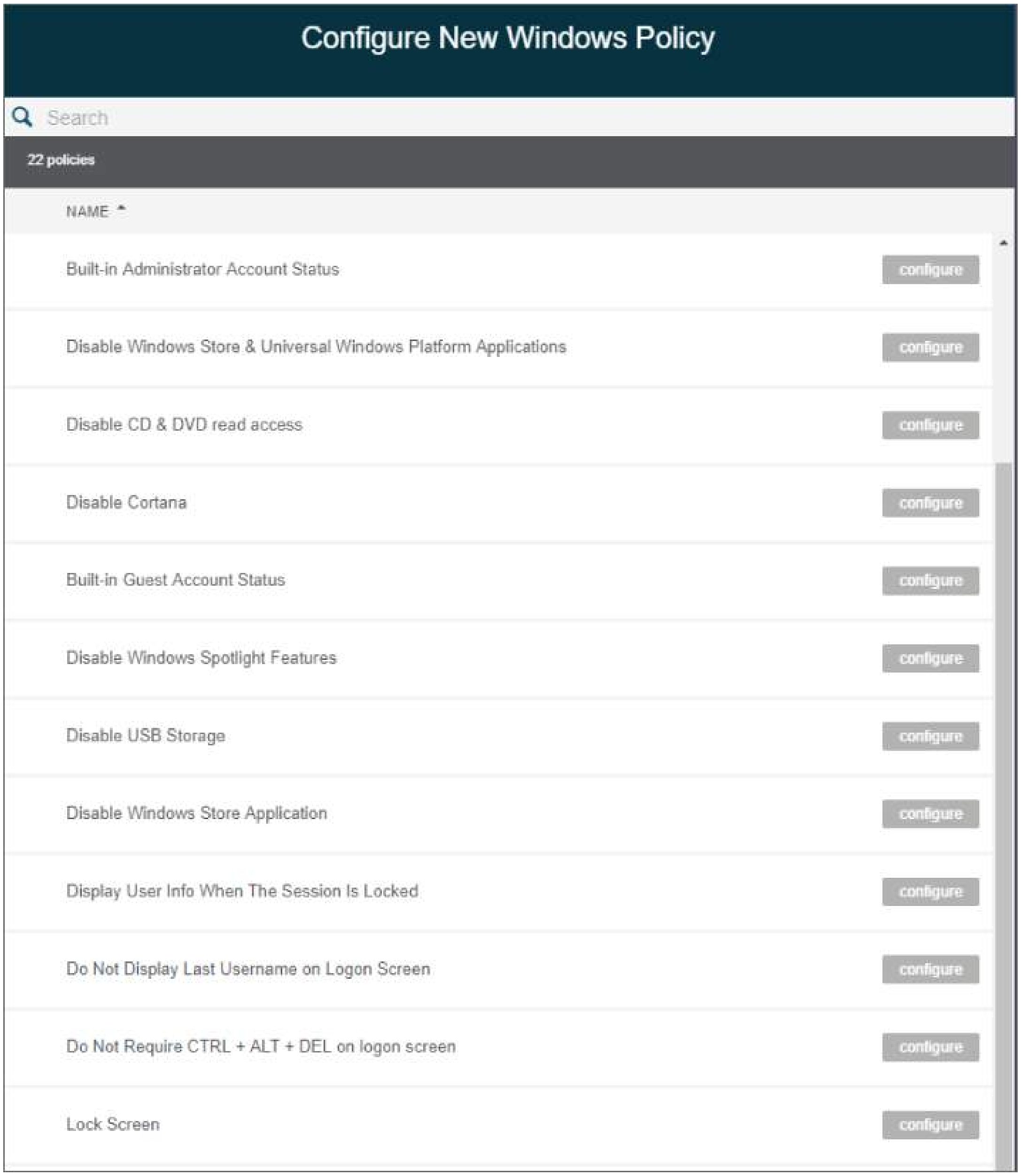
Connect Key:

22f59ba0964cdf33ecb1e8c3b537f21aa83a480c

Check for system compatibility

Figure 8.5: Download the Windows Agent and use the connect key to complete the installation.

4. Copy and paste the connect key into the install file to bind the JumpCloud agent to your system. In a few moments, you will see the hostname displayed in Systems page.
5. After the asset has successfully checked in, you can apply policies to that asset. By default, Windows has 22 policies you can configure. Figure 8.6 shows a few of them. One best practice is to set up a lock screen.



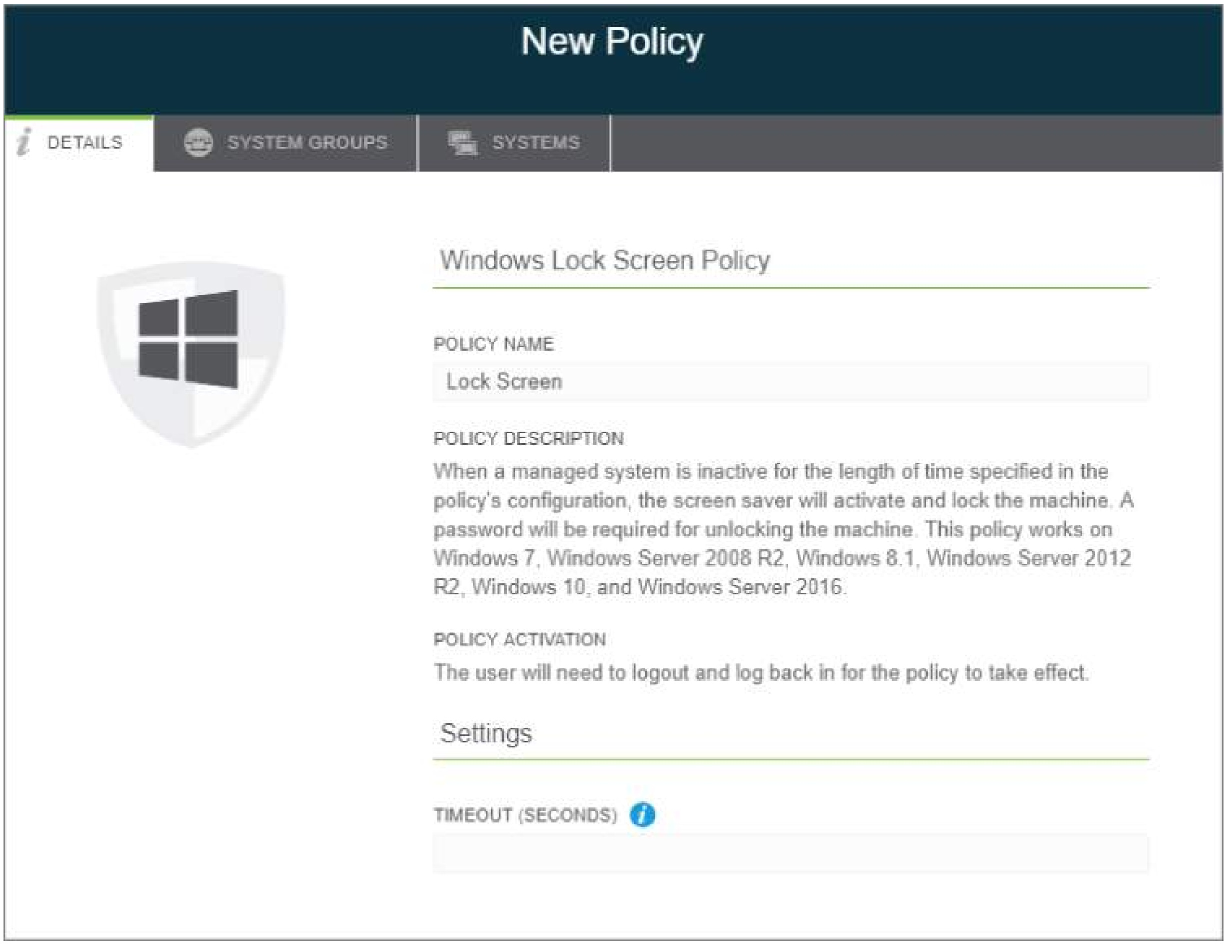
Configure New Windows Policy

22 policies

NAME
Built-in Administrator Account Status
Disable Windows Store & Universal Windows Platform Applications
Disable CD & DVD read access
Disable Cortana
Built-in Guest Account Status
Disable Windows Spotlight Features
Disable USB Storage
Disable Windows Store Application
Display User Info When The Session Is Locked
Do Not Display Last Username on Logon Screen
Do Not Require CTRL + ALT + DEL on logon screen
Lock Screen

Figure 8.6: Configuring Windows policies

The lock screen can help you not fall victim to donut day. *Donut day* is when you leave your computer unlocked, step away or turn your back for a moment, and someone takes advantage of you being logged in. That person will send an email to everyone saying, “I'm bringing the donuts tomorrow!” Everyone knows you left the machine unlocked. Some organizations I've worked for had a prank where they would change our wallpaper to My Little Pony and called it getting *pwned*. You must lock your computer, and if you forget, a policy can do it for you. It can be an expensive lesson to bring donuts for 250 people. In Figure 8.7, you see the Windows Lock Screen policy and the ability to set the timeout in seconds. Again, you have to balance the CIA triad with usability. I have seen an executive, frustrated with the lockout policy, place a “perpetual drinking bird” next to his keyboard to peck his keyboard and simulate activity so he didn't have to type in his password every 60 seconds.



Windows Lock Screen Policy

POLICY NAME

Lock Screen

POLICY DESCRIPTION

When a managed system is inactive for the length of time specified in the policy's configuration, the screen saver will activate and lock the machine. A password will be required for unlocking the machine. This policy works on Windows 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012 R2, Windows 10, and Windows Server 2016.

POLICY ACTIVATION

The user will need to logout and log back in for the policy to take effect.

Settings

TIMEOUT (SECONDS)

Figure 8.7: Windows Lock Screen policy

Now that you have a user, a system, and a policy, it's time to evaluate groups, applications, and directories. Each of these will have its own impact on the security posture of your organization. With groups, you have the ability to provide your users and admins access to resources while pulling them into a central management portal. To add another layer of security, giving users the ability to use SSO to sign into an application will enhance these processes. Finally, building a directory will allow you to synchronize user accounts and enable JumpCloud to act as a single authoritative directory of users.

The goal is to work your way through the CIS controls. CIS Control 5 is controlling IM and AM. With controlled use of the correct privileges on computers, networks, and applications, you protect information and assets from theft and misuse. It becomes even more important because you have to deal with the monumental outside threat but also insiders doing things they shouldn't be doing. It can be a daunting task, but it is essential.

CHAPTER 9
Managing Logs

WHAT YOU WILL LEARN IN THIS CHAPTER:

- Windows Event Viewer
- PowerShell
- BareTail
- Syslog
- Solarwinds Kiwi

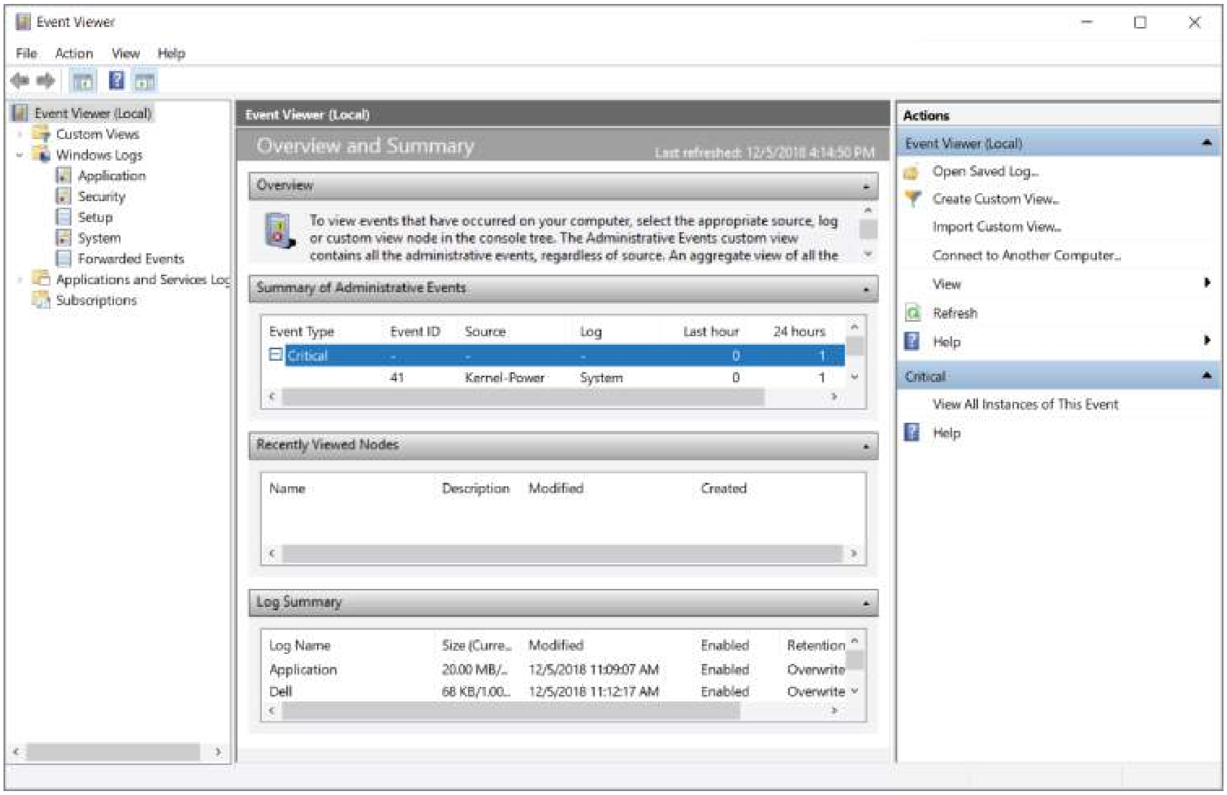
When I was growing up, my older brother was a Trekkie, a *Star Trek* fan. James T. Kirk, the captain of the U.S.S. *Enterprise*, would make entries into a captain's log. The captain's log has been a form of record keeping since the first captains sailed the seas. The log was used to inform the captain's superiors, either owners of the ship or governmental entities, what was happening while exploring or completing a mission or to record historical facts for future generations. Our networks work the same way. Every device on your network generates some type of log-in some type of language. Some of it is human readable, and some looks like gibberish. Some logs are more useful than others, and we should understand which ones need to be preserved for future analysis. You don't need to log everything, but what you do log should be purposely collected and managed.

CIS Control 6 is the maintenance, monitoring, and analysis of audit logs. Our organizations are evolving quickly, and we have to learn to deal with log data in the big data cloud era. Analyzing audit logs is a vital part of security, not just for system security but for processes and compliance. Part of the process of log analysis is reconciling logs from different sources and correlation even if those devices are in different time zones. If you look at a basic network topology, you will have many types of devices, including routers, switches, firewalls, servers, and workstations. Each of these devices that helps connect you to the rest of the world will generate logs based on its operating systems, configuration, and software. Examining logs is one of the most effective ways of looking for issues and troubleshooting issues occurring on a system or an application.

Synchronization and the ability to correlate the data between these devices are vital to a healthy environment. When I first started in IT, you could get away with occasionally using logs for troubleshooting. Attackers can hide their activities on machines if logging is not done correctly; therefore, you need a strategic method of consolidating and auditing all your logs. Without solid audit log analysis, an attack can go unnoticed for a long time. According to the 2018 Verizon Data Breach Investigations Report, 87 percent of compromises took minutes or less to occur, and 68 percent went undiscovered for months. The full report was based on detailed analysis of more than 53,000 security incidents, including 2,216 data breaches. You can download the full details at `verizonenterprise.com/DBIR2018`.

Windows Event Viewer

A Windows event log is one of the first tools to use to learn to analyze problems. As a security administrator, you must ensure that local logging is enabled on systems and networking devices. The process that can create an audit log is usually required to run in privileged mode so that users cannot stop or change it. To view logs on a Windows asset through a graphic user interface (GUI) like you see in Figure 9.1, you have to open the Event Viewer.



To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative events, regardless of source. An aggregate view of all the

Event Type	Event ID	Source	Log	Last hour	24 hours
⊟ Critical	-	-	-	0	1
	41	Kernel-Power	System	0	1

Name	Description	Modified	Created

Log Name	Size (Curre...	Modified	Enabled	Retention
Application	20.00 MB/...	12/5/2018 11:09:07 AM	Enabled	Overwrite
Dell	68 KB/1.00...	12/5/2018 11:12:17 AM	Enabled	Overwrite

Figure 9.1: Windows Event Viewer displaying logs

Events are placed into three different categories, each of which is related to a log that Windows keeps. While there are a lot of categories, the majority of troubleshooting and investigation happens in the application, system, or security log.

Application The application log records events related to Windows components like drivers.

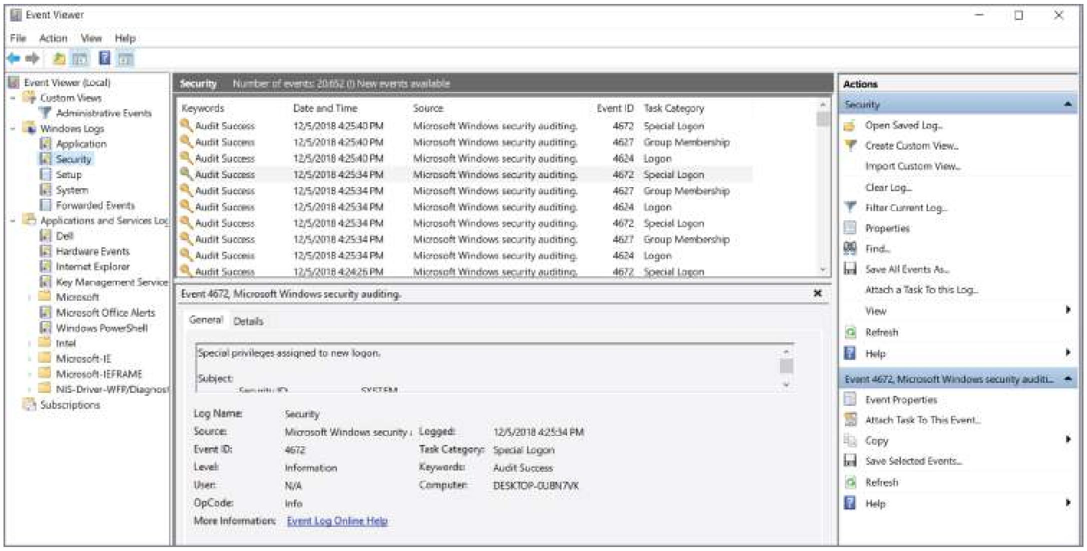
System The system log records events about programs installed.

Security When security logging is enabled, this log records events related to security, such as logon attempts and resources accessed.

In Lab 9.1 you'll learn how to examine the Windows security logs.

LAB 9.1: EXAMINING WINDOWS SECURITY LOGS

1. On a Windows system, use the Windows+R key combination to open the Run menu.
2. Type **eventvwr** in the Open field and press Enter.
3. There are three panes on the Event Viewer screen. The pane to the left is the hierarchy of log files. The pane to the right shows the actions you can take. For a granular view of the logs, you use the large center pane. Open each level of logs by clicking the arrow to the left of the folder or file in the left pane.
4. Under Windows Logs, click Security. In the center of the page, a list of all security events that have been recorded on this machine is displayed. As you see in Figure 9.2, these are audit successes recorded on this host. To the left, you see actions you can take on these logs, including filtering them for critical events or warnings as well as examining the log properties.



Security Number of events: 20,652 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	12/5/2018 4:25:40 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	12/5/2018 4:25:40 PM	Microsoft Windows security auditing.	4627	Group Membership
Audit Success	12/5/2018 4:25:40 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	12/5/2018 4:25:34 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	12/5/2018 4:25:34 PM	Microsoft Windows security auditing.	4627	Group Membership
Audit Success	12/5/2018 4:25:34 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	12/5/2018 4:25:34 PM	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	12/5/2018 4:25:34 PM	Microsoft Windows security auditing.	4627	Group Membership
Audit Success	12/5/2018 4:25:34 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	12/5/2018 4:24:26 PM	Microsoft Windows security auditing.	4672	Special Logon

Event 4672, Microsoft Windows security auditing.

Special privileges assigned to new logon.

Subject:

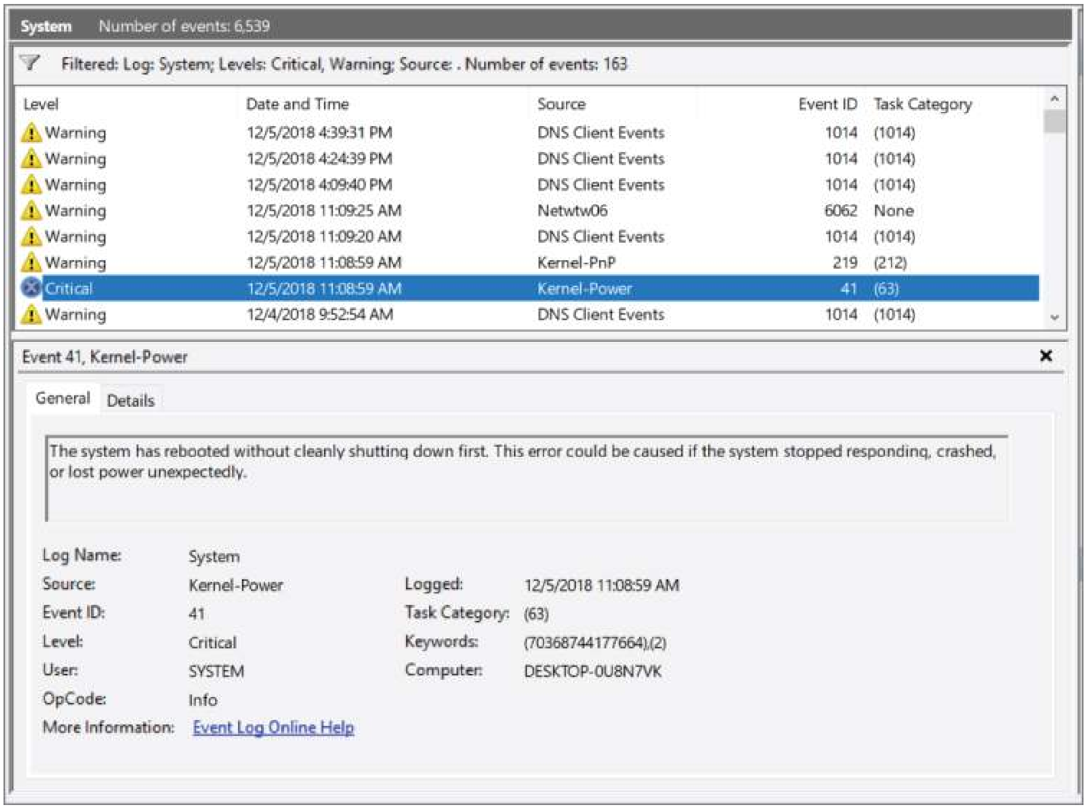
Security ID: SYSTEM

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	12/5/2018 4:25:34 PM
Event ID:	4672	Task Category:	Special Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-0UBN7VK
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 9.2: Security logs on a Windows machine

5. When you're familiar with the security logs, open the Application and System folders. These logs will help you understand what applications are running on your machine,

what they are doing, and whether they are having difficulties. The System folder is an excellent place to filter critical events such as configuration changes or power loss, as displayed in Figure 9.3.



System Number of events: 6,539

Filtered: Log: System; Levels: Critical, Warning; Source: . Number of events: 163

Level	Date and Time	Source	Event ID	Task Category
⚠ Warning	12/5/2018 4:39:31 PM	DNS Client Events	1014	(1014)
⚠ Warning	12/5/2018 4:24:39 PM	DNS Client Events	1014	(1014)
⚠ Warning	12/5/2018 4:09:40 PM	DNS Client Events	1014	(1014)
⚠ Warning	12/5/2018 11:09:25 AM	Netwtw06	6062	None
⚠ Warning	12/5/2018 11:09:20 AM	DNS Client Events	1014	(1014)
⚠ Warning	12/5/2018 11:08:59 AM	Kernel-PnP	219	(212)
⊗ Critical	12/5/2018 11:08:59 AM	Kernel-Power	41	(63)
⚠ Warning	12/4/2018 9:52:54 AM	DNS Client Events	1014	(1014)

Event 41, Kernel-Power

General Details

The system has rebooted without cleanly shutting down first. This error could be caused if the system stopped responding, crashed, or lost power unexpectedly.

Log Name:	System		
Source:	Kernel-Power	Logged:	12/5/2018 11:08:59 AM
Event ID:	41	Task Category:	(63)
Level:	Critical	Keywords:	(70368744177664),(2)
User:	SYSTEM	Computer:	DESKTOP-0U8N7VK
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 9.3: Critical warning on a Windows machine

Windows PowerShell

A *shell* is typically a user interface that accesses the tools behind the GUI of an operating system. It uses a command-line interface (CLI) rather than moving and clicking a mouse. It's called a shell because it is the layer outside the operating system's kernel. To use a CLI successfully, you have to be familiar with the proper syntax and commands.

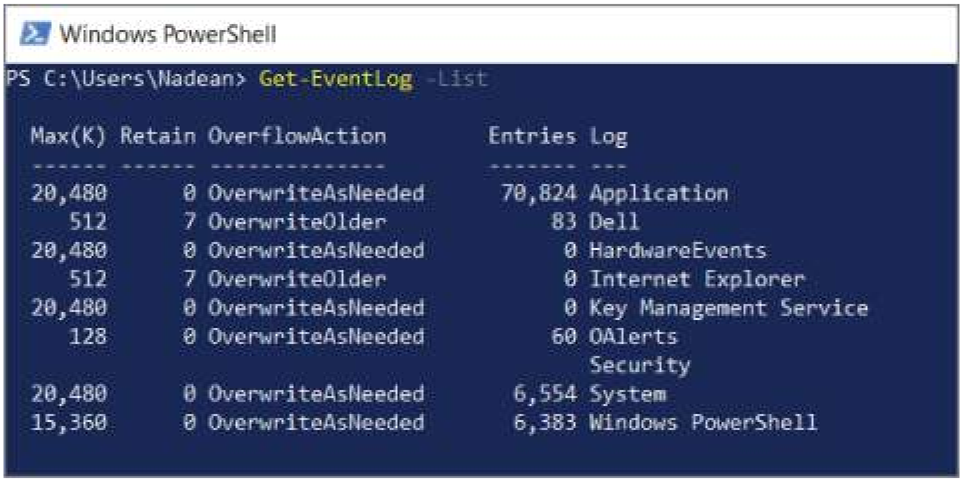
Windows PowerShell is a proprietary Windows command-line shell designed specifically for administrators. My favorite feature of a command shell is the ability to speed up the processes by using command-line completion, a lifesaver for those of us who are horrible typists. In the command shell, type a few characters of a command and press the Tab key a couple of times until the item you want appears. Another feature of PowerShell is the ability to save sequences of commands that you might want to reuse in the future. This feature allows you to press the up arrow to cycle through previous commands.

PowerShell introduced the *cmdlet* (pronounced “command-let”). It is a simple, single-function command-line tool built into the shell. A cmdlet is a specific order you give the OS to perform an action like “run this program.” There are more than 200 cmdlets that are written as a verb-noun pair. For example, you can type the command **`Get-Help`**, and this will give you a description of a cmdlet.

Searching logs using PowerShell has an advantage over Windows Event Viewer. You can check for events on remote computers much quicker, which is extremely valuable if you ever do server management. PowerShell will help you generate reports, and since we are all so busy, any automation can help. In Lab 9.2, you'll use Windows PowerShell to review logs.

LAB 9.2: USING WINDOWS POWERSHELL TO REVIEW LOGS

1. On a Windows system, use the Windows+R key combination to open the Run menu. Type in `powershell` and press Enter.
2. To get a list of event logs on the local machine, as shown in Figure 9.4, type the following command:



```
PS C:\Users\Nadean> Get-EventLog -List

  Max(K) Retain OverflowAction        Entries Log
  ------ ------ --------------        ------- ---
  20,480      0 OverwriteAsNeeded      70,824 Application
     512      7 OverwriteOlder             83 Dell
  20,480      0 OverwriteAsNeeded           0 HardwareEvents
     512      7 OverwriteOlder              0 Internet Explorer
  20,480      0 OverwriteAsNeeded           0 Key Management Service
     128      0 OverwriteAsNeeded          60 OAlerts
                                              Security
  20,480      0 OverwriteAsNeeded       6,554 System
  15,360      0 OverwriteAsNeeded       6,383 Windows PowerShell
```

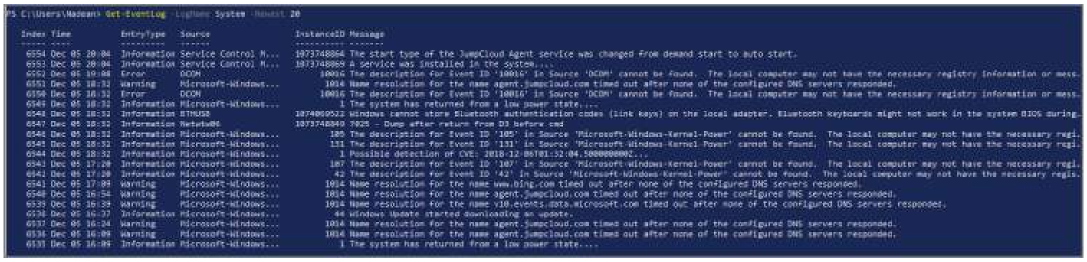
Figure 9.4: Getting a list in PowerShell of available locations of logs

```
Get-EventLog -List
```

3. To get the system log in its entirety on the local computer, type in the following command:

```
Get-EventLog -LogName System
```

4. The `Get-EventLog` command generates a massive list. To narrow down the view, you can display only the last 20 entries in the system log, as shown in Figure 9.5, by pressing the up arrow and adding the following syntax:

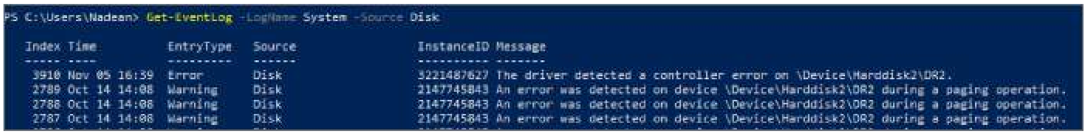


```
PS C:\Users\Nadean> Get-EventLog -LogName System -Newest 20

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
    6554 Dec 05 20:04  Information Service Control M...   1073748864 The start type of the JumpCloud Agent service was changed from demand start to auto start.
    6553 Dec 05 20:04  Information Service Control M...   1073748869 A service was installed in the system....
    6552 Dec 05 19:08  Error       DCOM                        10016 The description for Event ID '10016' in Source 'DCOM' cannot be found.  The local computer may not have the necessary registry information or mess...
    6551 Dec 05 18:32  Warning     Microsoft-Windows...         1014 Name resolution for the name agent.jumpcloud.com timed out after none of the configured DNS servers responded.
    6550 Dec 05 18:32  Error       DCOM                        10016 The description for Event ID '10016' in Source 'DCOM' cannot be found.  The local computer may not have the necessary registry information or mess...
    6549 Dec 05 18:32  Information Microsoft-Windows...            1 The system has returned from a low power state....
    6548 Dec 05 18:32  Information BTHUSB                 1074069522 Windows cannot store Bluetooth authentication codes (link keys) on the local adapter. Bluetooth keyboards might not work in the system BIOS during...
    6547 Dec 05 18:32  Information Netwtw06               1073748840 7025 - Dump after return from D3 before cmd
    6546 Dec 05 18:32  Information Microsoft-Windows...          105 The description for Event ID '105' in Source 'Microsoft-Windows-Kernel-Power' cannot be found.  The local computer may not have the necessary regi...
    6545 Dec 05 18:32  Information Microsoft-Windows...          131 The description for Event ID '131' in Source 'Microsoft-Windows-Kernel-Power' cannot be found.  The local computer may not have the necessary regi...
    6544 Dec 05 18:32  Information Microsoft-Windows...            1 Possible detection of CVE: 2018-12-06T01:32:04.5000000Z...
    6543 Dec 05 17:20  Information Microsoft-Windows...          107 The description for Event ID '107' in Source 'Microsoft-Windows-Kernel-Power' cannot be found.  The local computer may not have the necessary regi...
    6542 Dec 05 17:20  Information Microsoft-Windows...           42 The description for Event ID '42' in Source 'Microsoft-Windows-Kernel-Power' cannot be found.  The local computer may not have the necessary regis...
    6541 Dec 05 17:09  Warning     Microsoft-Windows...         1014 Name resolution for the name www.bing.com timed out after none of the configured DNS servers responded.
    6540 Dec 05 16:54  Warning     Microsoft-Windows...         1014 Name resolution for the name agent.jumpcloud.com timed out after none of the configured DNS servers responded.
    6539 Dec 05 16:39  Warning     Microsoft-Windows...         1014 Name resolution for the name v10.events.data.microsoft.com timed out after none of the configured DNS servers responded.
    6538 Dec 05 16:37  Information Microsoft-Windows...           44 Windows Update started downloading an update.
    6537 Dec 05 16:24  Warning     Microsoft-Windows...         1014 Name resolution for the name agent.jumpcloud.com timed out after none of the configured DNS servers responded.
    6536 Dec 05 16:09  Warning     Microsoft-Windows...         1014 Name resolution for the name agent.jumpcloud.com timed out after none of the configured DNS servers responded.
    6535 Dec 05 16:09  Information Microsoft-Windows...            1 The system has returned from a low power state....
```

Figure 9.5: Retrieving the index, time, type, source, and message of the last 20 system logs

```
Get-EventLog -LogName System -Newest 20
```

5. You can specify system log entries related to disk source, as shown in Figure 9.6, by entering the following command:



```
PS C:\Users\Nadean> Get-EventLog -LogName System -Source Disk

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
    3910 Nov 05 16:39  Error       Disk                   3221487627 The driver detected a controller error on \Device\Harddisk2\DR2.
    2789 Oct 14 14:08  Warning     Disk                   2147745843 An error was detected on device \Device\Harddisk2\DR2 during a paging operation.
    2788 Oct 14 14:08  Warning     Disk                   2147745843 An error was detected on device \Device\Harddisk2\DR2 during a paging operation.
    2787 Oct 14 14:08  Warning     Disk                   2147745843 An error was detected on device \Device\Harddisk2\DR2 during a paging operation.
```

Figure 9.6: Disk errors and warnings in system logs

```
Get-EventLog -LogName System  -Source Disk
```

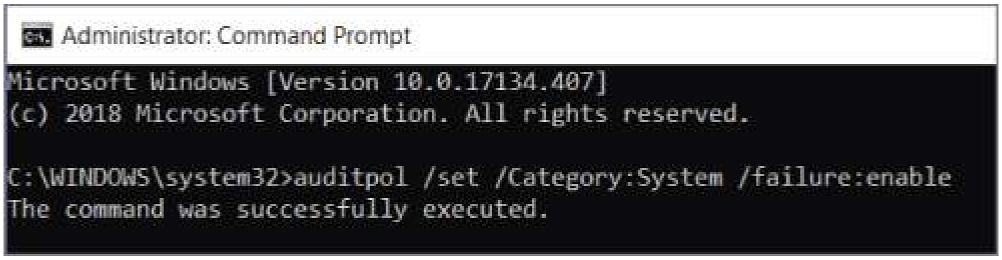
Windows enables most log files by default, although you might need to define what level of logging you need. Turning on verbose logging, the most detail possible should be done only during a specific event or while trying to track an active, known security incident. If you aren't careful, the volume of logs can take up many terabytes of disk space. Systems have been known to crash because well-meaning system administrators enabled verbose logging for all systems and then forgot to disable it when troubleshooting was completed. Be sure to put a sticky note on your monitor to remind yourself to revert logging levels after you're done troubleshooting.

Great logging is about pulling out the necessary critical events and alerts from an otherwise overwhelming amount of information. The problem for most admins is not about getting enough information, but getting useful information out of an overwhelming deluge of data.

To enable a security audit policy to capture load failures in the audit logs, open an elevated Command Prompt window by right-clicking the `Cmd.exe` shortcut and selecting Run As Administrator. You could also press Windows+R to open the Run box. Type **`cmd`** and then press Ctrl+Shift+Enter to run the command as an administrator. In the elevated Command Prompt window, run the following command:

```
Auditpol /set /Category:System /failure:enable
```

As you see in Figure 9.7, you should get a success message that you are now logging all security audit logs. You will have to restart the computer for the changes to take effect.



```
Microsoft Windows [Version 10.0.17134.407]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>auditpol /set /Category:System /failure:enable
The command was successfully executed.
```

Figure 9.7: Elevated command prompt turning on security audit logs

After you have collected the logs you need and so you do not fill up all the storage on your asset, do not forget to run the following command:

```
Auditpol /set /Category:System /failure:disable
```

Searching logs using PowerShell has an advantage over Windows Event Viewer. You can check for events on remote computers much quicker, which is extremely valuable if you ever do server management. There is no need to physically connect to a computer to collect the logs. By using the PowerShell parameter `-ComputerName`, you can connect and pass a command to the remote computer you choose and collect the information you want. If you want to pull all system logs off the computer named PC1, you can by using the following command:

```
Get-EventLog -ComputerName PC1 -LogName System
```

One of the integral parts of understanding these logs and their access to remote regions of your network is their IP address. The Internet has run out of IPv4 addresses, and the landscape of the Internet is quickly evolving. IPv4 is the technology that allows us to connect our devices to the web with a unique, numerical IP address consisting of 4 octets separated by a decimal with no number over 255. It looks like 192.168.1.0. Sending data from one computer to another and generating logs while doing so requires an IP address on both devices.

But we are in transition. With so many applications and with the evolution of the Internet of Things (IoT), we are starting to see more and more IPv6 addresses in our logging. Google collects statistics surrounding IPv6 adoption globally, and the latest numbers indicate that more than 25 percent of Google users access their resources with IPv6. For home users and small businesses, this may take another few years to become an issue, but nearly all modern devices support this new technology.

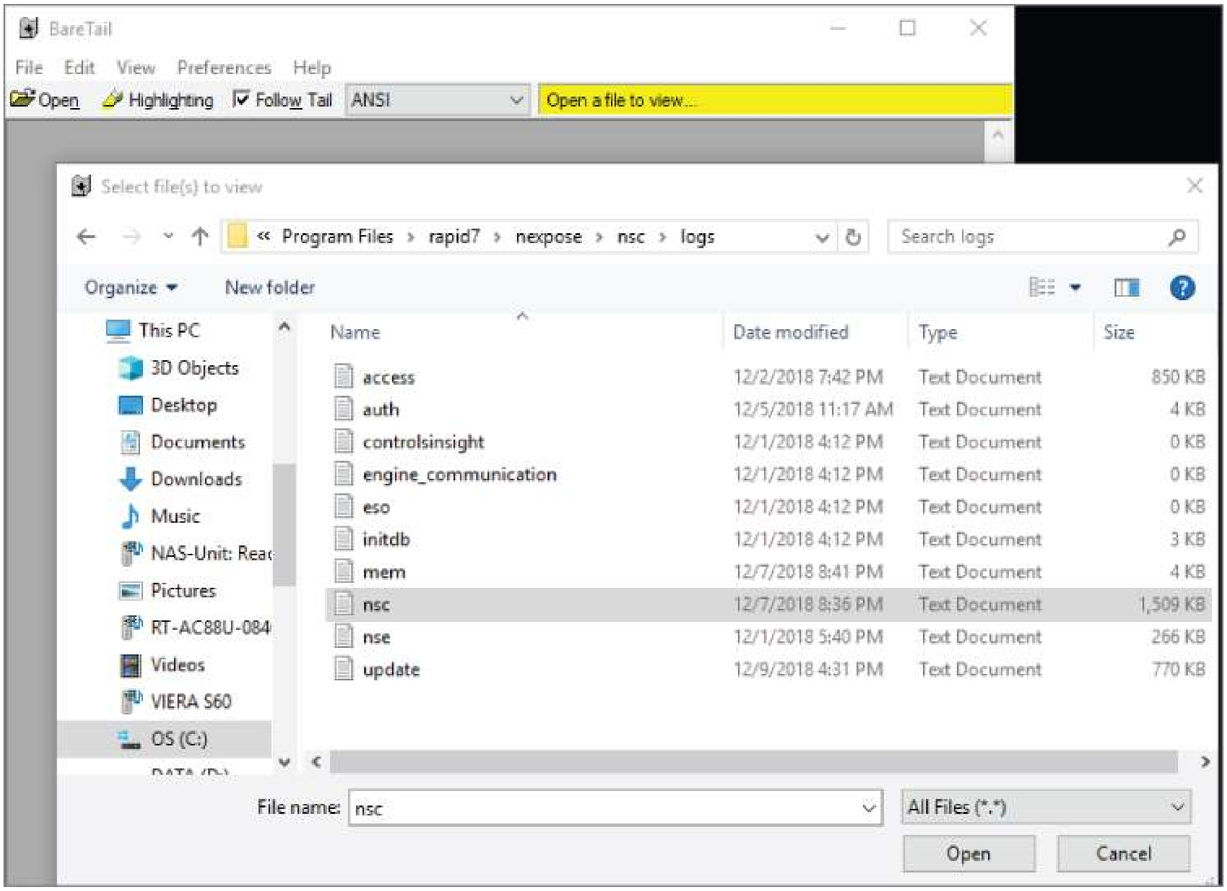
What you will start seeing in your logs will be a logical network IPv6 address of 128 bits as opposed to the 32 bits in an IPv4 address. IPv6 is written in hexadecimal as opposed to dotted decimal, and the numbers are grouped together in eight groups of four instead of four groups of three. There are some shortening techniques. For example, if the IPv6 address has a grouping of 0000, it will display as `::`. Just be aware, if you ever start to see your source address of your logs displaying 32 hexadecimal characters instead of your usual 12, something on your network is using IPv6.

BareTail

Historically, system administrators would drop down into a shell to run `tail -f` to follow logs in real time. Developed by Bare Metal Software, BareTail is an amazing, free, tiny tool that packs quite an impact. You can monitor your logs in real time in a GUI that allows you to navigate between multiple tabs to organize your streams of logs, highlighting and filtering those parts that are important. You can leave it running, and it refreshes constantly.

When you decide you need a tool to watch the flow of your logs, go to www.baremetalsoft.com/baretail to grab the tool. It downloads as `baretail.exe`, but it does not "install" as a permanent file. You can move this file and run it from any location with extremely flexible configuration options. I usually keep it on a USB.

Once you open BareTail, the first option under the main menu is Open. Click the Open File option to open a dialog box to navigate to the program logs you want to monitor. In Figure 9.8, you see the path to Nexpose to troubleshoot issues or verify confirmed vulnerabilities on your system.



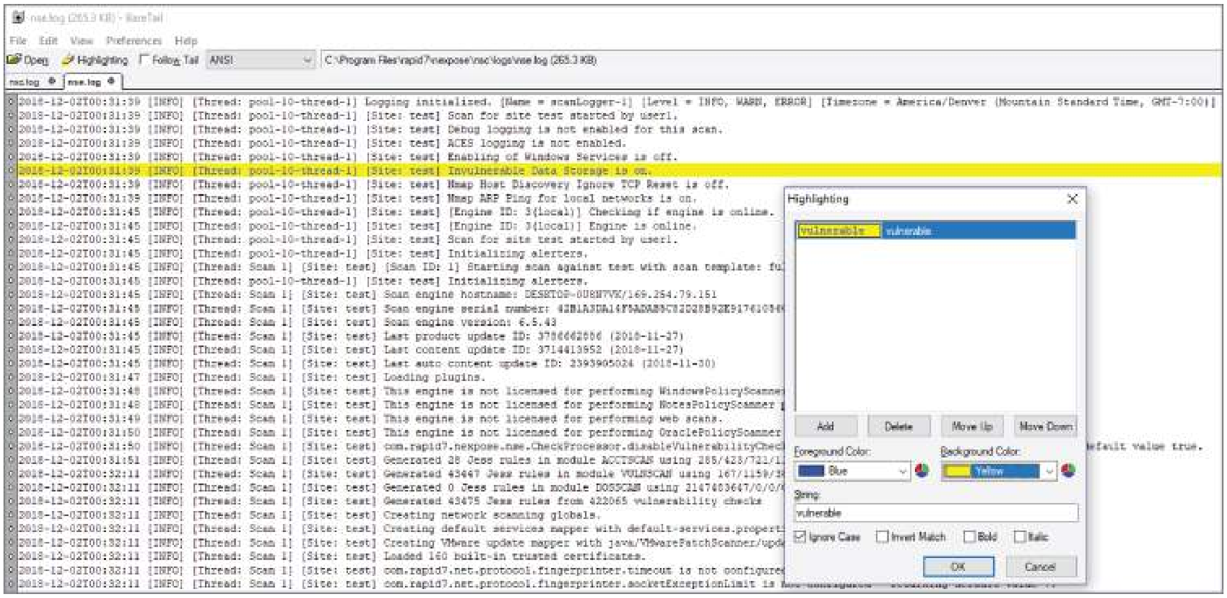
Name	Date modified	Type	Size
access	12/2/2018 7:42 PM	Text Document	850 KB
auth	12/5/2018 11:17 AM	Text Document	4 KB
controlsinsight	12/1/2018 4:12 PM	Text Document	0 KB
engine_communication	12/1/2018 4:12 PM	Text Document	0 KB
eso	12/1/2018 4:12 PM	Text Document	0 KB
initdb	12/1/2018 4:12 PM	Text Document	3 KB
mem	12/7/2018 8:41 PM	Text Document	4 KB
nsc	12/7/2018 8:36 PM	Text Document	1,509 KB
nse	12/1/2018 5:40 PM	Text Document	266 KB
update	12/9/2018 4:31 PM	Text Document	770 KB

File name: nsc

All Files (*.*)

Figure 9.8: Opening a file location to view the log

To look for specific words or *strings*, open the Highlighting menu next to the Open menu. You have the ability to filter, change the foreground color and/or background color, and type into the string location the keywords you are most interested in. In Figure 9.9, you see that in `nse.log`, I have targeted the word *vulnerable*, and I am ignoring if it is displayed in uppercase or lowercase. In this log, if you scroll down some, you may see Vulnerable or Not Vulnerable when it examines a possible vulnerability on an asset. It will find the word you are searching for inside other words if necessary. When you click OK, the highlighted filters you create will stay activated in the log for as long as you have it open.


nse.log (265.3 KB) - BareTail
File Edit View Preferences Help
Open Highlighting Follow Tail ANSI
C:\Program Files\rapid7\nexpose\nsc\logs\nse.log (265.3 KB)
nsc.log nse.log

```
2018-12-02T00:31:39 [INFO] [Thread: pool-10-thread-1] Logging initialized. [Name = scanLogger-1] [Level = INFO, WARN, ERROR] [Timezone = America/Denver (Mountain Standard Time, GMT-7:00)]
2018-12-02T00:31:39 [INFO] [Thread: pool-10-thread-1] [Site: test] Scan for site test started by user1.
2018-12-02T00:31:39 [INFO] [Thread: pool-10-thread-1] [Site: test] Debug logging is not enabled for this scan.
2018-12-02T00:31:39 [INFO] [Thread: pool-10-thread-1] [Site: test] ACES logging is not enabled.
2018-12-02T00:31:39 [INFO] [Thread: pool-10-thread-1] [Site: test] Enabling of Windows Services is off.
2018-12-02T00:31:39 [INFO] [Thread: pool-10-thread-1] [Site: test] Invulnerable Data Storage is on.
2018-12-02T00:31:39 [INFO] [Thread: pool-10-thread-1] [Site: test] Nmap Host Discovery Ignore TCP Reset is off.
2018-12-02T00:31:39 [INFO] [Thread: pool-10-thread-1] [Site: test] Nmap ARP Ping for local networks is on.
2018-12-02T00:31:45 [INFO] [Thread: pool-10-thread-1] [Site: test] [Engine ID: 3(local)] Checking if engine is online.
2018-12-02T00:31:45 [INFO] [Thread: pool-10-thread-1] [Site: test] [Engine ID: 3(local)] Engine is online.
2018-12-02T00:31:45 [INFO] [Thread: pool-10-thread-1] [Site: test] Scan for site test started by user1.
2018-12-02T00:31:45 [INFO] [Thread: pool-10-thread-1] [Site: test] Initializing alerters.
2018-12-02T00:31:45 [INFO] [Thread: Scan 1] [Site: test] [Scan ID: 1] Starting scan against test with scan template: fu
2018-12-02T00:31:45 [INFO] [Thread: pool-10-thread-1] [Site: test] Initializing alerters.
2018-12-02T00:31:45 [INFO] [Thread: Scan 1] [Site: test] Scan engine hostname: DESKTOP-0U8N7VK/169.254.79.151
2018-12-02T00:31:45 [INFO] [Thread: Scan 1] [Site: test] Scan engine serial number: 42B1A3DA14F5ADAB9C82D28B92E917610846
2018-12-02T00:31:45 [INFO] [Thread: Scan 1] [Site: test] Scan engine version: 6.5.43
2018-12-02T00:31:45 [INFO] [Thread: Scan 1] [Site: test] Last product update ID: 3786662886 (2018-11-27)
2018-12-02T00:31:45 [INFO] [Thread: Scan 1] [Site: test] Last content update ID: 3714413952 (2018-11-27)
2018-12-02T00:31:45 [INFO] [Thread: Scan 1] [Site: test] Last auto content update ID: 2393905024 (2018-11-30)
2018-12-02T00:31:47 [INFO] [Thread: Scan 1] [Site: test] Loading plugins.
2018-12-02T00:31:48 [INFO] [Thread: Scan 1] [Site: test] This engine is not licensed for performing WindowsPolicyScanner
2018-12-02T00:31:48 [INFO] [Thread: Scan 1] [Site: test] This engine is not licensed for performing NotesPolicyScanner
2018-12-02T00:31:49 [INFO] [Thread: Scan 1] [Site: test] This engine is not licensed for performing web scans.
2018-12-02T00:31:50 [INFO] [Thread: Scan 1] [Site: test] This engine is not licensed for performing OraclePolicyScanner
2018-12-02T00:31:50 [INFO] [Thread: Scan 1] [Site: test] com.rapid7.nexpose.nse.CheckProcessor.disableVulnerabilityCheck                    efault value true.
2018-12-02T00:31:51 [INFO] [Thread: Scan 1] [Site: test] Generated 28 Jess rules in module ACCTSCAN using 285/423/721/1
2018-12-02T00:32:11 [INFO] [Thread: Scan 1] [Site: test] Generated 43447 Jess rules in module VULNSCAN using 167/1159/3
2018-12-02T00:32:11 [INFO] [Thread: Scan 1] [Site: test] Generated 0 Jess rules in module DOSSCAN using 2147483647/0/0/0
2018-12-02T00:32:11 [INFO] [Thread: Scan 1] [Site: test] Generated 43475 Jess rules from 422065 vulnerability checks
2018-12-02T00:32:11 [INFO] [Thread: Scan 1] [Site: test] Creating network scanning globals.
2018-12-02T00:32:11 [INFO] [Thread: Scan 1] [Site: test] Creating default services mapper with default-services.properti
2018-12-02T00:32:11 [INFO] [Thread: Scan 1] [Site: test] Creating VMware update mapper with java/VMwarePatchScanner/upda
2018-12-02T00:32:11 [INFO] [Thread: Scan 1] [Site: test] Loaded 160 built-in trusted certificates.
2018-12-02T00:32:11 [INFO] [Thread: Scan 1] [Site: test] com.rapid7.net.protocol.fingerprinter.timeout is not configured
2018-12-02T00:32:11 [INFO] [Thread: Scan 1] [Site: test] com.rapid7.net.protocol.fingerprinter.socketExceptionLimit is
```

vulnerable vulnerable

Foreground Color: Blue

Background Color: Yellow

String: vulnerable

☑ Ignore Case ☐ Invert Match ☐ Bold ☐ Italic

Figure 9.9: Applying a filter to `nse.log` to find “vulnerable” assets

Syslog

The amount of digital data we produce is astounding. According to `www.internetlivestats.com`, Google alone processes more than 40,000 searches every single second. When you click a link, you generate a log. Around the globe, every second of the day, computer networks are generating logs. According to the same website, we create 2.5 quintillion bytes of data every single day. Honestly, without searching Google to define *quintillion*, I don't know how many digits that is. So I just Googled it. It's a billion billion, or 18 zeros after the 1.

Some of these logs are routine, and some of these indicate poor network health or a malicious attempt to breach your network. Log files contain a wealth of information to reduce exposure to intruders, malware, and legal issues. Log data needs to be collected, stored, analyzed, and monitored to meet and report on regulatory compliance standards such as HIPAA, FISMA, FERPA, PCI DSS, or the newest global compliance standard focused on privacy, GDPR. This is an incredible and overwhelming task.

Syslog is a way for network devices to send a message to a logging server. It is supported by a wide range of devices. It can be used to log different types of events. Syslog is an awesome way to consolidate logs from many different sources, in different formats, and in massive volumes into a single location. If you don't have a log management strategy in place to monitor and secure connected devices, the results can be difficult to overcome if at all.

Using a syslog server to collect and store syslog messages provides a reliable central repository for log data. Syslog uses UDP communication to send messages to a central collector, also known as a *syslog server*. Syslog messages are used to troubleshoot network problems, establish forensic evidence, and prove compliance. Forwarding syslog messages to a central syslog server helps you correlate events across your network.

Typically, most Syslog servers have the following components:

> **Syslog Listener** A Syslog server needs to receive messages sent over the network. A listener process gathers syslog data sent over UDP port 514. UDP is not connection oriented, so messages aren't acknowledged. In some cases, network devices will send Syslog data over connection-oriented TCP 1468 to ensure and confirm delivery.
>
> **Database** Large networks can generate a huge amount of Syslog data. Most Syslog servers will use a database to store syslog data to search and query.
>
> **Management Software** With so much data, it is like looking for a specific needle in a haystack. Use a syslog server that automates part of the work. Syslog servers should be able to generate alerts, notifications, and alarms in response to select messages. If you read the Verizon report, you know you have 16 minutes from compromise before the first click on a phishing

> campaign. As a security administrator, you need to be able to work quickly.

A log management solution aggregates, indexes, parses, and generates metrics. Syslog messages are generated by operating systems and applications—as well as processes on printers, routers, and switches—and are configured to be sent to your syslog server. If your network includes Windows systems, the syslog server can help you manage Windows event log information.

Logs where there are many login attempts on a single account from diverse geographic locations or other suspicious system activities is a situation any administrator will want to investigate. Proactive, automated detection of unusual activity is critical. Cybersecurity is incredibly dynamic, and we do not know every single potential attack pattern in advance, so monitoring for this type of activity is not an easy task. If you don't analyze your logs to see what's going on, you'll never be able to detect suspicious activity.

A baseline is a starting point you can use for comparisons. Create a baseline that represents normal activity on your system so you're aware when there are anomalies occurring. A few failed login attempts by a user might be considered normal, but hundreds or thousands of failed login attempts might point to a brute-force or malicious attack.

Consolidating and centrally managing all your logs is different from logging each and every event. The big question of what events to record and how much you need to log is a problem best addressed by an audit. With the right coordination, an auditor along with your legal department focused on compliance with a technical CISO's perspective can give consideration as to what the right level of information is. These questions typically need to be answered for every component of your system and be well documented so you are able to easily scale in the future. For most assets, you will probably stick with their defaults. The only major operating system that does not have built-in support for sending syslog is Microsoft Windows. Windows includes PowerShell, and PowerShell can use the .NET Framework to send UDP packets to a syslog server.

Another crucial thing to think about is your data retention needs. How long do you need to keep the logs? Do you need them for troubleshooting? Are there regulatory or audit requirements that require you to keep the logs for a certain period of time?

When I was teaching CISSP for ISC², one of the best tools they gave us to teach with was 250 retired questions. I remember one specifically concerning logs:

> **“You are a system administrator. Your organization's security policy states that you keep logs for 3 years. You have kept logs for 5 years. You have been subpoenaed for 5 years of logs. What do you legally have to give the authorities?”**

The answer is you have to turn over everything you have. We have to trust that the management team has put security policies in place for a reason. If we disagree with the policy, it is our responsibility as cyber professionals to pursue a discussion with the chain of command until either we understand why the policy is in place or we change the policy. Otherwise, the violation of keeping records too long could open up potential damaging and sometimes legal issues.

Your daily log volume might already be substantial, but it can increase exponentially when a device fails. The resulting log messages could easily quintuple the number of log messages that get generated.

Log files come in a variety of formats. Some formats follow more traditional standards, while others are completely custom. Your log solution should be able to parse and present the data in a comprehensive form in near real time, and it should allow you to define custom parsing rules. Parsing is breaking down a log into smaller, better digestible messages and putting them into their own groups so that you can analyze and even visualize them in order to identify data inconsistencies.

SolarWinds Kiwi

SolarWinds Kiwi Syslog Server has a free edition where you can collect, view, and archive syslog messages. It is easy to set up and configure how it receives, logs, displays, and forwards syslog messages from network devices, such as routers, switches, Unix hosts, and other syslog-enabled devices.

The free version of Kiwi will allow you to get statistics in real time from five sources, with summaries available in the console. You will also be able to receive and manage syslog messages from network devices and view syslog messages in multiple windows.

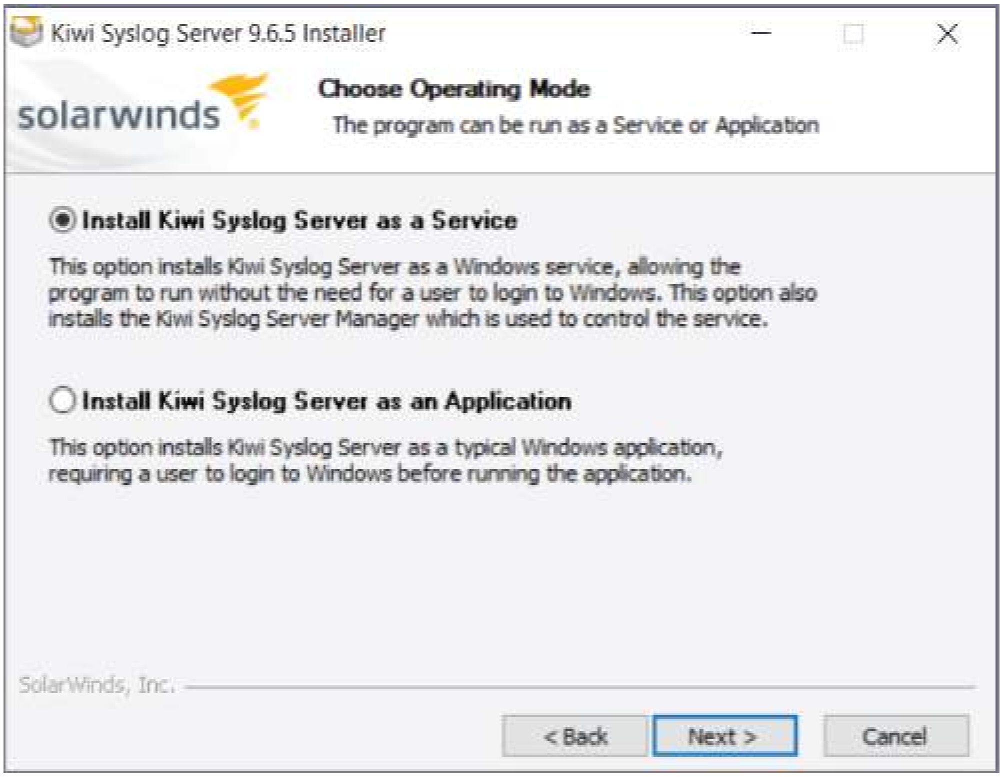
Just like any other software, you will want to make sure that your system meets the hardware and software requirements and that you've opened the appropriate ports so communication can occur. In Kiwi Syslog Server, you will need Windows 7 or newer, Internet access, and at least 4 GB of disk space. Kiwi Syslog Server uses the ports listed in Table 9.1.

Table 9.1: Ports used by Kiwi Syslog Server

Source: https://support.solarwinds.com

PORT	PROTOCOL	PURPOSE
514 (default)	UDP	Incoming UDP messages
1468 (default)	TCP	Incoming TCP messages
162 for IPv4	UDP	Incoming SNMP traps
163 for IPv6		
6514	TCP	Incoming secure TCP messages
3300	TCP	Internal communication between Syslog service and Syslog Manager
8088 (default)	TCP	Kiwi Syslog Web Access

To download and install this syslog server solution, search in your browser for ***Solarwinds kiwi syslog server free***, and it will easily take you to the download file. You will need to supply some information to create an account, and then you will receive the link to download the software. As you see in Figure 9.10, you have a choice to make when you start installing the software. You can choose either Install Kiwi Syslog Server As A Service on your Windows machine or Install Kiwi Syslog Server As An Application on your Windows machine. If you choose to install it as an application, you will be required to log in as a user before you can use the product. I have installed it as a service because it also installs the Kiwi Syslog Server Manager, which you will use to control the service.



Kiwi Syslog Server 9.6.5 Installer

Choose Operating Mode

The program can be run as a Service or Application

● **Install Kiwi Syslog Server as a Service**

This option installs Kiwi Syslog Server as a Windows service, allowing the program to run without the need for a user to login to Windows. This option also installs the Kiwi Syslog Server Manager which is used to control the service.

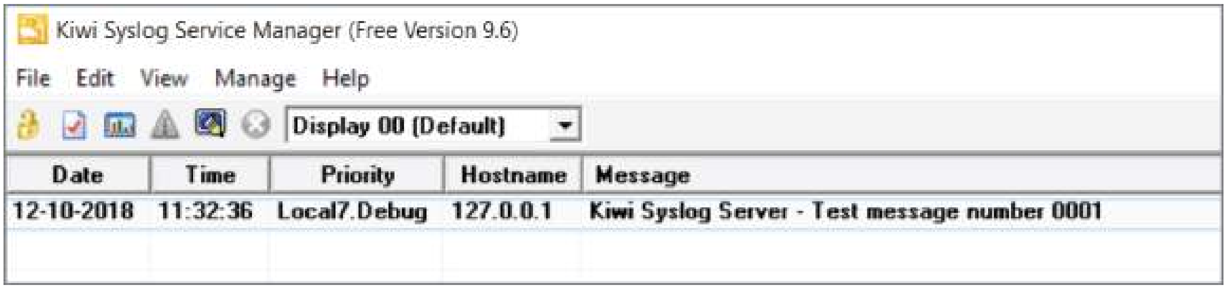
○ **Install Kiwi Syslog Server as an Application**

This option installs Kiwi Syslog Server as a typical Windows application, requiring a user to login to Windows before running the application.

Figure 9.10: Choosing a service or application operating mode with Kiwi Syslog Server

The road map to begin collecting syslog data starts with configuring devices on your network to send the proper logs so that you can start to save, digest, analyze, and be alerted to issues in your environment. In my example, I have collected syslog off a router to give you an idea of what this will look like in Kiwi Syslog Server. In your environment, it will be dependent on what devices you want to send syslog from. You will have to access your device product guide to find out whether enabling syslog can be accomplished through the application GUI or the hardware CLI. Either way, you configure the asset to send logs to one central location.

If you have configured the Kiwi Syslog Server and no logs can be detected from an asset you are attempting to collect logs from, as shown in Figure 9.11, you can test the server to make sure it is actually running.



Date	Time	Priority	Hostname	Message
12-10-2018	11:32:36	Local7.Debug	127.0.0.1	Kiwi Syslog Server - Test message number 0001

Figure 9.11: Successful test message on Kiwi Syslog Server

If the syslog server does not display the success message, then you'll want to check to see whether the service has initiated properly. Go to the Manage menu to start, stop, or ping the service and see whether it is running. As you learned in Chapter 1, "Fundamental Networking and Security Tools," you can run the `netstat -ano` command to see whether there are any active network ports using UDP 514, the default port that syslog will use to communicate. If a different process is consuming UDP 514, open your Task Manager by pressing Ctrl+Alt+Delete and ending that task. Return to the Manage menu in Kiwi Syslog Server and restart the service, and it will take its place on UDP port 514.

According to Request for Comments (RFC) 5424, the document provided by the Internet Engineering Task Force (IETF) that specifies and defines the syslog protocol, syslog will convey event notification messages using an architecture that supports different transport protocols. This RFC defines syslog as having three layers: content, application, and transport. There is no rule on how long a syslog will be, but it will contain at least a timestamp, a hostname or IP address of the device sending the message, and the message data itself. The message data is usually human readable like you see in the example in Figure 9.12.

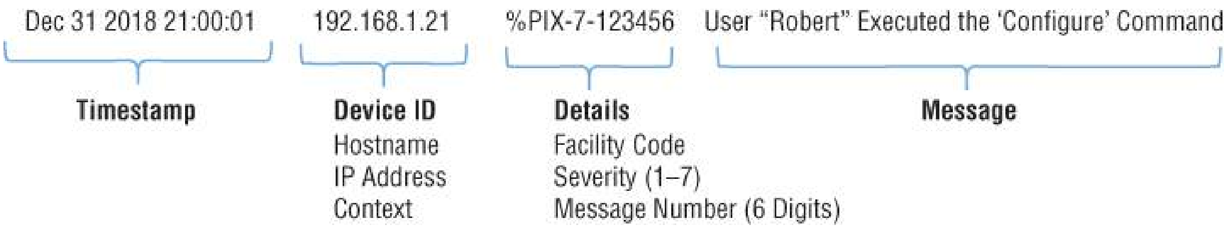


Figure 9.12: Anatomy of a syslog message

Once you have logs flowing into the syslog server, it is time to consider what rules will be applied to the log information. The rules determine what happens when the syslog server sees certain items in a log and what action it takes. You can create rules to log all messages, send an email if something critical occurs, and even run a script if a log contains a certain word. When you begin building your rules, as you saw in Figure 9.12, you will be using filters and actions. In Kiwi Syslog Server, you can have up to 100 rules, and each rule has up to 100 possible filters and 100 possible actions.

If you have ever built rules on a firewall, building rules in a syslog server is similar. When the server sees a message and that message meets the criteria for the first rule, it is then passed to the second rule, if there is one. You must build the rules in the order in which you want them to apply. When a rule applies to a message, the filters will start matching TRUE or FALSE. If the first filter returns TRUE, it will attempt to match the second filter. If the filter returns FALSE, the next message is processed. For example, Figure 9.13 shows the workflow of a rule matching the first filter but not matching the second.

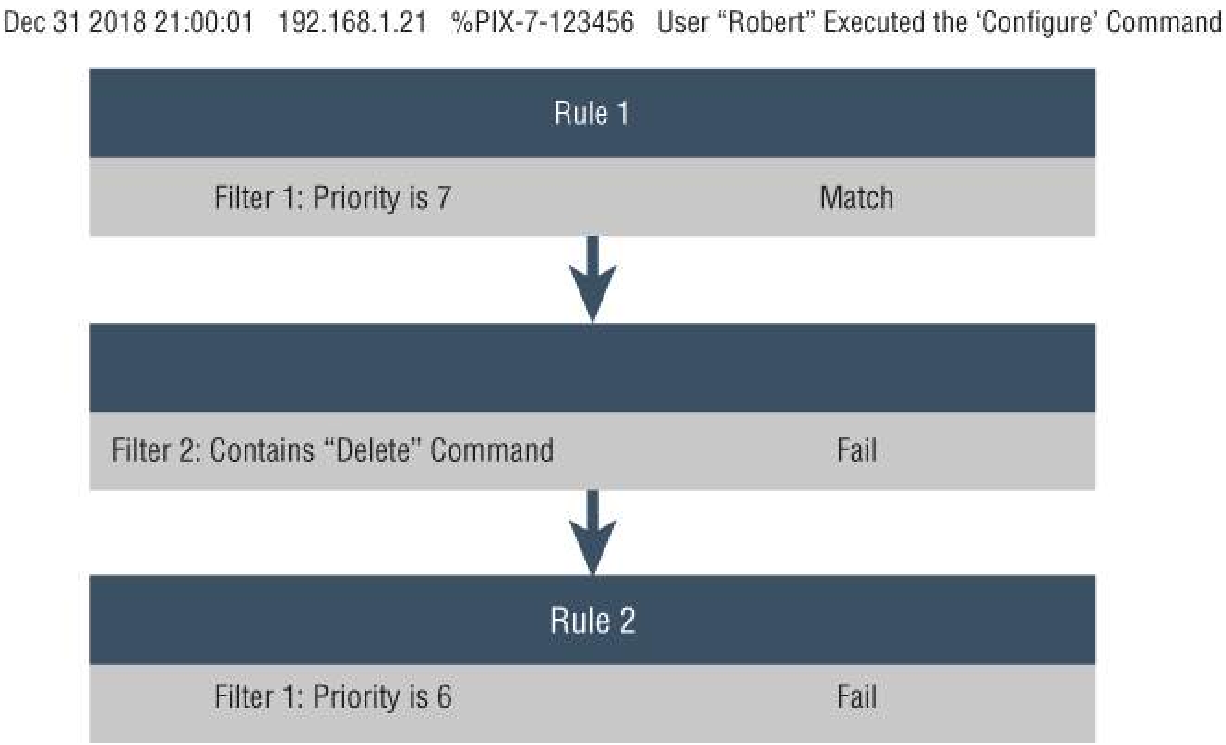

Dec 31 2018 21:00:01 192.168.1.21 %PIX-7-123456 User "Robert" Executed the 'Configure' Command
Rule 1
Filter 1: Priority is 7
Match
Filter 2: Contains "Delete" Command
Fail
Rule 2
Filter 1: Priority is 6
Fail

Figure 9.13: Syslog message being filtered by rules

The default rule in Kiwi Syslog Server applies two actions to all messages flowing into the server.

- Display each message on the console
- Log each message to the `SyslogCatchAll.txt` file

Figure 9.14 shows the same message being filtered by a different rule where both filters match so an action is performed. When all actions are performed, the server applies the next rule to the message.

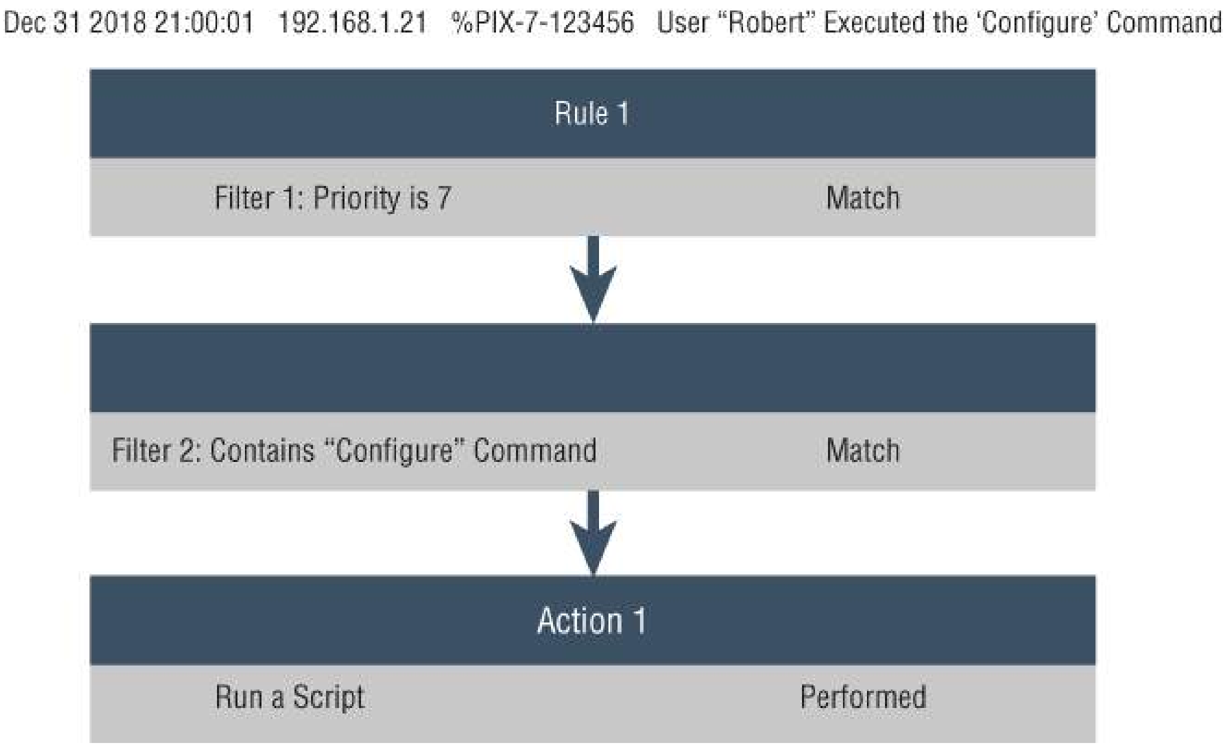
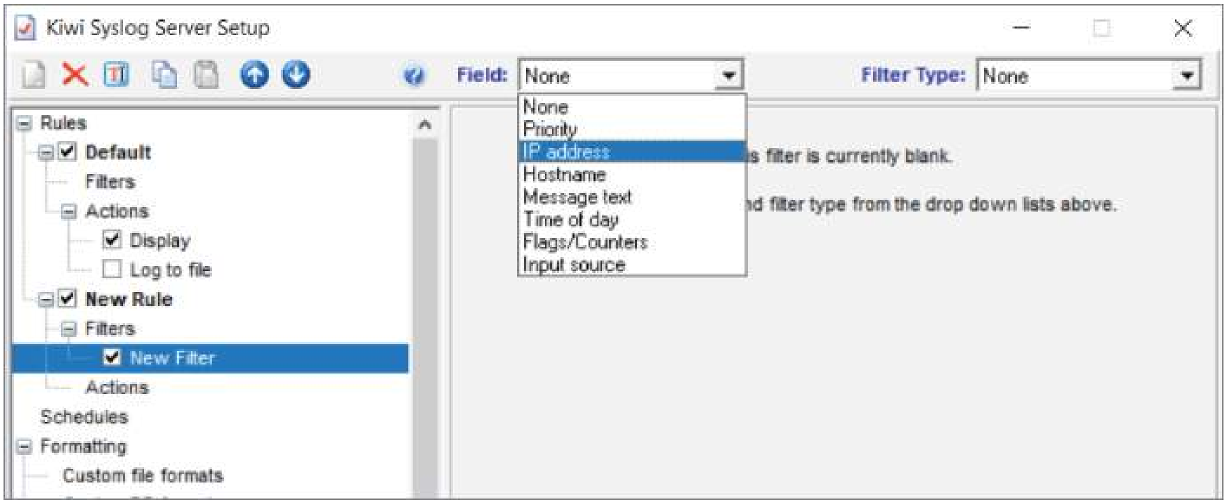

Dec 31 2018 21:00:01 192.168.1.21 %PIX-7-123456 User "Robert" Executed the 'Configure' Command
Rule 1
Filter 1: Priority is 7
Match
Filter 2: Contains "Configure" Command
Match
Action 1
Run a Script
Performed

Figure 9.14: Syslog message being filtered by rules and initiating an action

To create a rule, choose the File menu and go to Setup. Click the New button, and a new rule is added to the hierarchical tree. You can replace New Rule with a name that will make sense to the filter and action you want to create. When the new filter is selected as shown in Figure 9.15, you will see several options to filter on, including priority, IP address, or hostname. Each field you choose will have its own unique identifiers to be defined. Once you have defined the logged event you want to be alerted for, you can create an action to play a sound, send an email, run another program, or do all of these things. Multiple actions can be staged for each rule.



Field: None

Filter Type: None

s filter is currently blank.

nd filter type from the drop down lists above.

Figure 9.15: Creating a filter in Kiwi Syslog Server

One consideration while building a program with ongoing operational mechanisms is to visit the possibility of alert fatigue. In grade school, we learned about Peter and the wolf. He was the little boy who enjoyed the attention he received when he alerted everyone to a wolf outside the village when one wasn't really there. After a while, no one would pay attention to him. Eventually, he did have a confrontation with the wolf and got eaten. Logs can have the same effect with their alerting. If you have system administrators who are constantly bombarded with a large number of alarms and alerts, they do become desensitized, which can lead to longer response times or missing something important. Lastly, consider having a roundtable discussion with all the stakeholders in this process. Include your network administrators as well as your security team. Decide what your retention policy should be, whether it's dictated to you by an auditor because of your compliance needs or your industry best practices. Retention policies that you put in place will ensure that these messages will be there when you need them. Utilize the scheduling tool inside Kiwi Syslog Server to take advantage of automation. We are all busy with a focus on securing our infrastructure, and forgetting to back up our files can have severe consequences.

CHAPTER 10
Metasploit

WHAT YOU WILL LEARN IN THIS CHAPTER:

- Reconnaissance
- Installation
- Gaining Access
- Metasploitable2
- Vulnerable Web Services

Software is developed to be the solution for a problem. Metasploit Framework was developed by HD Moore in 2003 when he was only 22 years old. Originally written in Perl with a total of 11 exploits, Metasploit Framework was the answer to a problem he was having. He was spending most of his time validating and sanitizing exploit code. I imagine that for someone as brilliant as HD, this was redundant and boring. He knew there must be an easier way. He couldn't get the project he had in mind approved by the organization he worked for, so he decided to develop it in his free time. Today, we use Metasploit Framework as a platform for creating security tools and exploits, and there is a huge open-source community that supports the effort. In 2009, Rapid7 acquired the project, and HD Moore joined the team as chief security officer.

Now Metasploit Framework is written in Ruby with many, many exploits. In fact, at the time of this publishing, there are more than 3,700. Metasploit Framework is the penetration testing tool of choice of blue teamers and red teamers alike. Blue teamers are the good guys defending the network against malicious intent. Red teamers are the malicious intent. Red teamers are often called *penetration testers*, and they enjoy proving where there are vulnerabilities that can be exploited. For clarification, red teamers are very different than the criminals who use this tool for profit or hacktivism. It is all about intent. In fact, as cybersecurity has matured, there are some people, like me, who consider themselves to be purple. A blend of red and blue, I can defend a network and then periodically hack it as necessary to use this compromised viewpoint of your network as a bad actor would.

Metasploit Framework is not a destination but a journey. That journey begins before you even install the software. Before you get started, you must know that the tools in this chapter are for your personal use on your personal devices. These tools can be used in your business environment only if you have secured permission to do so. Using any of these tools to compromise machines that you do not own is illegal. You must have documentation scoping the range of your penetration test signed by the appropriate entities. This is not the type of scenario where you pass your manager in the hallway and tell him you're about to start this process. If something goes wrong and he doesn't remember the conversation, it could be time to update your résumé and start looking for a new job.

The U.S. federal government has some of the oldest and sometimes problematic cybersecurity laws around the globe. The purpose of cybersecurity regulation is to force companies to protect their systems from cyberattacks like the ones you can create and distribute in Metasploit Framework. Unless you have explicit and written permission to access a computer network or system, do not do it. You must make sure your documentation is correct and signed by the proper authority.

The Computer Fraud and Abuse Act makes it illegal to intentionally access a computer without authorization or in excess of authorization. The original law was passed in 1984 as a reaction to a 1983 movie starring Matthew Broderick called *War Games*. However, the law does not define “without authorization” or “exceeds authorized access,” which makes it easy to prosecute and sometimes difficult to defend. The law was crafted to crack down on hacking, and the repercussions can be harsh. First-time offenses of one singular incident of insufficient authorization can result in 5 years in prison and fines.

One of my favorite organizations I have been lucky enough to work with and take classes from is SANS. SANS is an organization of the best-of-the-best instructors teaching a variety of technical and sometimes nontechnical classes. If you search for SANS documentation to use as a template for your penetration test, you'll find a resources download page that has everything from a Metasploit Framework cheat sheet to a rules of engagement worksheet. Inside the scoping worksheet, you will be asked to define security concerns, the scope of what should be tested and not tested, and some type of escalation process should you break something or find evidence of a prior exploit or a currently active compromise.

Reconnaissance

Before you start this Metasploit journey, you have to do your homework. After you have gained permission to legally explore a network, you need to gain as much information about that network. This includes information such as DNS, domains, ports, and services. Start a physical or digital folder for this process. It makes life so much easier when you have to create a report. It also works as a great resource when you start expanding your reach deeper into a network. I use Microsoft OneNote because it is so versatile and keeps everything together in a single location.

Reconnaissance is gathering intelligence about an organization and can take two forms: passive and active. Passive reconnaissance is done to gather as much information as possible without any type of active engagement. The information you gather will be used to attempt successful exploitation of targets. The more information you learn, the better crafted the attacks will be. Passive reconnaissance is completely and totally legal. You can browse the company website just like you were a typical user.

It amazes me how much information is shared on social media websites. Professional social media websites are excellent places to discover employees' names and possibly email structures. If you do decide to conduct a social engineering campaign, it is helpful to know if the employees email accounts are set up using a `first.lastname@companyname.com` structure.

You can visit the websites that most companies use to advertise the jobs they currently have available. When you go to the technical positions section, if organizations are looking for an Active Directory administrator, you can surmise they are using Microsoft infrastructure. If they are looking for someone with a CCNA certification, they are using Cisco network devices. Sometimes organizations will get very specific in their advertisements, and as a red teamer, if I know you're looking for a DBA with Microsoft SQL experience, I know exactly what exploit I will be using against you as soon as I get a foothold in your environment. I mention this since I am making the assumption we are all the good guys or “blue team”—you can work with your human resources department in crafting technical position listings as generically as possible without compromising any company information.

The groundwork you lay when using all the passive reconnaissance will make your penetration test that much smoother and give you strategic options. Nothing you do in passive recon shows up in a security log or an alert, and it cannot be traced back to your IP address. It is completely legal and done every single day by good guys and bad guys alike.

Active reconnaissance involves doing something that can be seen in a security log or an alert, and it can possibly be traced back to you. This is why written permission (or a “Get Out of Jail Free card” as it is sometimes called) is so incredibly important. You start edging close to violating terms of service or even breaking the law when you run a port scan or launch a vulnerability scan on assets you do not personally own. Your goal with active reconnaissance is to build a robust four-dimensional picture of the environment you are concerned with protecting. With active recon, if you can establish a possible a point of entry and gain access, you know where to point your exploits and establish persistence.

Installation

You have many options when it comes to installing Metasploit. There is the Metasploit Framework Open Source, the Framework for Linux or Windows, Metasploit Community, and Metasploit Pro. When you navigate to `www.metasploit.com`, there is a link on this Rapid7 site to `github.com` where you can download either the Linux/Mac OS version or the Windows 32-bit version. These installers are rebuilt every single night. These installers also include the dependent software needed like Ruby and the PostgreSQL database that will manage all the information you collect during a penetration test. It will integrate seamlessly with the package manager, so they are easy to update on Linux.

Another option is to download a new operating system called Kali Linux. Kali is an evolution of Debian Linux that is designed and maintained by an organization called Offensive Security. Kali has more than 600 penetration testing programs, including Metasploit Framework as well as some I have already covered in this book, such as Nmap and Wireshark. It also has some tools yet to be covered in this book (like Burp, which is covered in Chapter 11). Kali can run on bare metal as an operating system on a hard drive, or you can boot from it on a USB drive. The most popular way of running Kali is in a virtual environment. I have done all of these, and my personal favorite is running it in a virtual environment. The benefit of deploying Kali in a virtual machine is the ability to take a snapshot. A snapshot is when you preserve the state of a machine at a specific moment in time. It is cyber time travel and a safeguard should you make a mistake. You are able to return to that specific moment in time over and over again.

I covered Nmap in Chapter 3, "Nmap: The Network Mapper," and the Nexpose Community as a vulnerability scanner in Chapter 4, "OpenVAS: Vulnerability Management." Both of these products give you data that can be imported into Metasploit. In this chapter, I cover installing Metasploit Community on a bare-metal Windows machine. The two reasons we are going to be using Metasploit Community are it is free and this is the GUI version.

As security practitioners, we know that practice makes perfect. Once you have Metasploit installed, you have an option of downloading vulnerable systems from the Open Web Application Security Project (OWASP) or Rapid7 to practice different types of exploitation. The Open Web Application Security Project is a not-for-profit organization that focuses on improving security in software. It has many different vulnerable machine downloads so that you can explore exploiting different types of web applications. In future labs and examples in this book, I will be using a vulnerable system called Metasploitable2. Metasploitable2 was purposefully crafted for training Metasploit and has many vulnerabilities to experiment with.

In Lab 10.1, you'll install Metasploit Community on a Windows system.

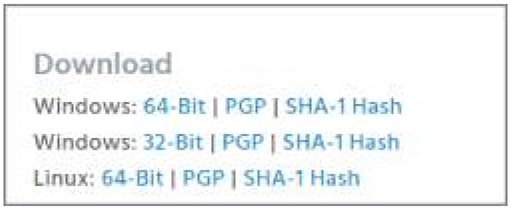
LAB 10.1: INSTALLING METASPLOIT COMMUNITY

1. Download Metasploit Community from the following website:

   `www.rapid7.com/products/metasploit/download/community`

   > **NOTE**
   >
   > If that link does not work, you can search for *Metasploit community free download*.

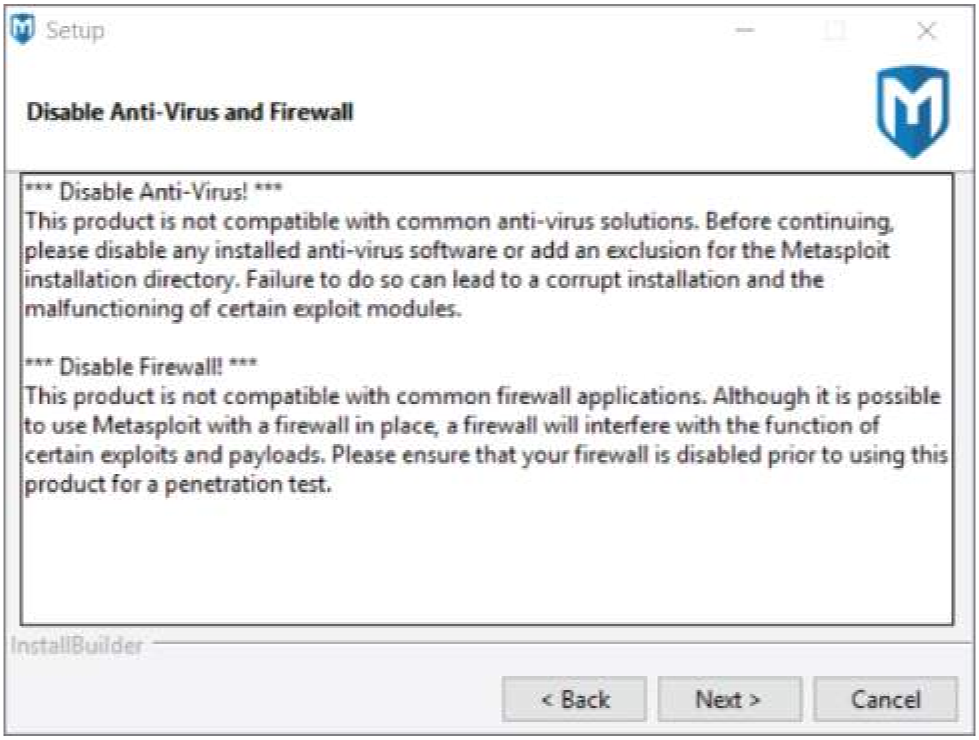
2. After you fill out and submit the form for the free license, you will have an option to download the Windows 32-bit, 64-bit, or Linux 64-bit version (see Figure 10.1). Download the appropriate architecture for your Windows or Linux machine. An email containing your license key will be sent to the email you provided on the registration page.

   Download
   Windows: 64-Bit | PGP | SHA-1 Hash
   Windows: 32-Bit | PGP | SHA-1 Hash
   Linux: 64-Bit | PGP | SHA-1 Hash

   Figure 10.1: Select the correct version of Metasploit Community for your platform and architecture.

3. Find and double-click the Metasploit Community `.exe` file. During the installation, you will get a warning regarding your antivirus and firewall settings, like you see in Figure 10.2. When you are pen testing with Metasploit, it is best practice to use a dedicated asset if at all possible. Do not put Metasploit on a system that you use for personal email, social media, or any financial accounting. It is a bad idea to put QuickBooks financials on a machine you are hacking with. I mention this because I've seen it.



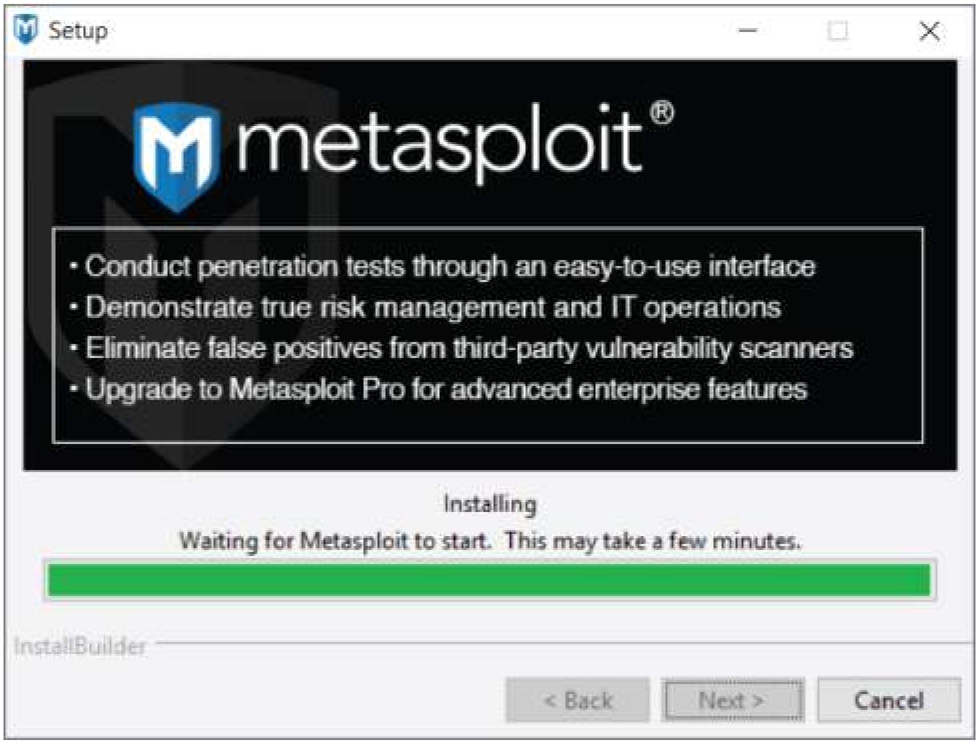
Disable Anti-Virus and Firewall

*** Disable Anti-Virus! ***
This product is not compatible with common anti-virus solutions. Before continuing, please disable any installed anti-virus software or add an exclusion for the Metasploit installation directory. Failure to do so can lead to a corrupt installation and the malfunctioning of certain exploit modules.

*** Disable Firewall! ***
This product is not compatible with common firewall applications. Although it is possible to use Metasploit with a firewall in place, a firewall will interfere with the function of certain exploits and payloads. Please ensure that your firewall is disabled prior to using this product for a penetration test.

Figure 10.2: You must disable the antivirus function, or the install process might be corrupted.

4. Metasploit Community naturally binds to port 3790. Leave the defaults for generating a certificate for accessing the software through a browser and complete the install. As the message in Figure 10.3 says, it will take a few minutes for the Metasploit services to start.



- Conduct penetration tests through an easy-to-use interface
- Demonstrate true risk management and IT operations
- Eliminate false positives from third-party vulnerability scanners
- Upgrade to Metasploit Pro for advanced enterprise features

Installing

Waiting for Metasploit to start. This may take a few minutes.

Figure 10.3: Waiting for Metasploit to start

Welcome to Metasploit! The splash screen you see makes for very informative reading. In Figure 10.4, there is an explanation of why there might be a warning regarding an insecure SSL certificate. It also explains that the Metasploit service can take upward of 10 minutes to initialize, and if you get a 404 error, just keep hitting the Refresh button. The URL you will navigate to in your browser is `https://localhost:3790/`. You can use your Start menu and navigate down to the Metasploit folder to open the Metasploit Web UI. You will also have access to updating, starting, and stopping services as well as resetting your password.