Covers all Exam Objectives for CEHv6

Includes Real-World Scenarios, Hands-On Exercises, and Leading-Edge Exam Prep Software Featuring:

- Custom Test Engine
- Hundreds of Sample Questions
- Electronic Flashcards
- Entire Book in PDF

CEH™

Certified Ethical Hacker

STUDY GUIDE

Exam 312-50
Exam EC0-350

Kimberly Graves

SYBEX | SERIOUS SKILLS.

Table of Contents

Chapter 5. Trojans, Backdoors, Viruses, and Worms.......... 1

Section 5.1. Trojans and Backdoors.......... 2

Section 5.2. Viruses and Worms.......... 17

Section 5.3. Summary.......... 22

Section 5.4. Exam Essentials.......... 22

Section 5.5. Review Questions.......... 23

Section 5.6. Answers to Review Questions.......... 27

Chapter 5

Trojans, Backdoors, Viruses, and Worms

CEH EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ What is a Trojan?
- ✓ What is meant by overt and covert channels?
- ✓ List the different types of Trojans
- ✓ What are the indications of a Trojan attack?
- ✓ Understand how the "Netcat" Trojan works
- ✓ What is meant by "wrapping"?
- ✓ How do reverse connecting Trojans work?
- ✓ What are the countermeasure techniques in preventing Trojans?
- ✓ Understand Trojan evading techniques
- ✓ Understand the differences between a virus and a worm
- ✓ Understand the types of viruses
- ✓ How a virus spreads and infects a system
- ✓ Understand antivirus evasion techniques
- ✓ Understand virus detection methods

Trojans and backdoors are two ways a hacker can gain access to a target system. They come in many different varieties, but they all have one thing in common: they must be installed by another program, or the user must be tricked into installing the Trojan or backdoor on their system. Trojans and backdoors are potentially harmful tools in the ethical hacker's toolkit and should be used judiciously to test the security of a system or network.

Viruses and worms can be just as destructive to systems and networks as Trojans and backdoors. In fact, many viruses carry Trojan executables and can infect a system, then create a backdoor for hackers. This chapter will discuss the similarities and differences among Trojans, backdoors, viruses, and worms. All of these types of *malicious code* or *malware* are important to ethical hackers because they are commonly used by hackers to attack and compromise systems.

Trojans and Backdoors

Trojans and backdoors are types of malware used to infect and compromise computer systems. A *Trojan* is a malicious program disguised as something benign. In many cases the Trojan appears to perform a desirable function for the user but actually allows a hacker access to the user's computer system. Trojans are often downloaded along with another program or software package. Once installed on a system, they can cause data theft and loss, as well as system crashes or slowdowns. Trojans can also be used as launching points for other attacks, such as distributed denial of service (DDoS). Many Trojans are used to manipulate files on the victim computer, manage processes, remotely run commands, intercept keystrokes, watch screen images, and restart or shut down infected hosts. Sophisticated Trojans can connect themselves to their originator or announce the Trojan infection on an Internet Relay Chat (IRC) channel.

Trojans ride on the backs of other programs and are usually installed on a system without the user's knowledge. A Trojan can be sent to a victim system in many ways, such as the following:

- An instant messenger (IM) attachment
- IRC
- An email attachment
- NetBIOS file sharing
- A downloaded Internet program

Many fake programs purporting to be legitimate software such as freeware, spyware-removal tools, system optimizers, screensavers, music, pictures, games, and videos can install a Trojan on a system just by being downloaded. Advertisements on Internet sites for free programs, music files, or video files lure a victim into installing the Trojan program; the program then has system-level access on the target system, where it can be destructive and insidious.

Table 5.1 lists some common Trojans and their default port numbers.

TABLE 5.1 Common Trojan programs

Trojan	Protocol	Port
BackOrifice	UDP	31337 or 31338
Deep Throat	UDP	2140 and 3150
NetBus	TCP	12345 and 12346
Whack-a-Mole	TCP	12361 and 12362
NetBus 2	TCP	20034
GirlFriend	TCP	21544
Master's Paradise	TCP	3129, 40421, 40422, 40423, and 40426

A *backdoor* is a program or a set of related programs that a hacker installs on a target system to allow access to the system at a later time. A backdoor can be embedded in a malicious Trojan. The objective of installing a backdoor on a system is to give hackers access into the system at a time of their choosing. The key is that the hacker knows how to get into the backdoor undetected and is able to use it to hack the system further and look for important information.

Adding a new service is the most common technique to disguise backdoors in the Windows operating system. Before the installation of a backdoor, a hacker must investigate the system to find services that are running. Again the use of good information-gathering techniques is critical to knowing what services or programs are already running on the target system. In most cases the hacker installs the backdoor, which adds a new service and gives it an inconspicuous name or, better yet, chooses a service that's never used and that is either activated manually or completely disabled.

This technique is effective because when a hacking attempt occurs the system administrator usually focuses on looking for something odd in the system, leaving all existing services unchecked. The backdoor technique is simple but efficient: the hacker can get back into the machine with the least amount of visibility in the server logs. The backdoored service lets the hacker use higher privileges—in most cases, as a System account.

Remote Access Trojans (RATs) are a class of backdoors used to enable remote control over a compromised machine. They provide apparently useful functions to the user and, at the same time, open a network port on the victim computer. Once the RAT is started, it behaves as an executable file, interacting with certain Registry keys responsible for starting processes and sometimes creating its own system services. Unlike common backdoors, RATs hook themselves into the victim operating system and always come packaged with two files: the client file and the server file. The server is installed in the infected machine, and the client is used by the intruder to control the compromised system.

RATs allow a hacker to take control of the target system at any time. In fact one of the indications that a system has been exploited is unusual behavior on the system, such as the mouse moving on its own or pop-up windows appearing on an idle system.

A Word of Caution about Practicing with Trojans

I intentionally left any step-by-step exercises out of this section on Trojans and backdoors because I do not want to advocate anyone installing them on production systems and experiencing loss of data. However, the best way to learn how to use these tools and their capabilities is to install them and test them out. So here is my recommendation to learn ethical hacking skills using Trojans and backdoors.

Take an older computer that you do not have any intention of using again, or buy a second hard drive for your laptop (this is what I did). Install the Windows XP operating system with no service packs or updates enabled. Do not install any virus scanning or firewall. The next step is to really go crazy installing all the Trojans, rootkits, and backdoors tools listed in this chapter. This will give you the freedom to learn and test the tools without being blocked by a virus scan or personal firewall trying to protect your computer. Once you are finished, you can either reinstall Windows or just switch out the hard drive for your production drive.

A final suggestion if you are looking for a small, inexpensive computer to use as a test machine is to purchase an inexpensive netbook that runs Windows XP and use it to install and test tools.

Overt and Covert Channels

An *overt channel* is the normal and legitimate way that programs communicate within a computer system or network. A *covert channel* uses programs or communications paths in ways that were not intended.

Trojans can use covert channels to communicate. Some client Trojans use covert channels to send instructions to the server component on the compromised system. This sometimes makes Trojan communication difficult to decipher and understand. An unsuspecting intrusion detection system (IDS) sniffing the transmission between the Trojan client and server would not flag it as anything unusual. By using the covert channel, the Trojan can communicate or "phone home" undetected, and the hacker can send commands to the client component undetected.

Real World Scenario

Using a Covert Channel

Jeremiah Denton, a prisoner of war during the Vietnam War, used a covert channel to communicate without his captors' knowledge. Denton was interviewed by a Japanese TV reporter, and eventually a videotape of the interview made its way to the United States. As American intelligence agents viewed the tape, one of them noticed Denton was blinking in an unusual manner. They discovered he was blinking letters in Morse code. The letters were T-O-R-T-U-R-E, and Denton was blinking them over and over. This is a real-world example of how a covert channel can be used to send a communication message undetected.

Another example of using a computer to convey information via a covert channel is the use a characteristic of a file to deliver information rather that the file itself. A computer-based example of a covert channel is in the creation of a seemingly innocent computer file 16 bytes in size. The file can contain any data as that is not the important information. The file can then be emailed to another person. Again, it seems innocent enough but the real communication is of the number 16. The file size is the important data, not the contents of the file.

Some covert channels rely on a technique called *tunneling*, which lets one protocol be carried over another protocol. Internet Control Message Protocol (ICMP) tunneling is a method of using ICMP echo-request and echo-reply to carry any payload an attacker may wish to use, in an attempt to stealthily access or control a compromised system. The `ping` command is a generally accepted troubleshooting tool, and it uses the ICMP protocol. For that reason, many router, switches, firewalls, and other packet filtering devices allow the ICMP protocol to be passed through the device. Therefore, ICMP is an excellent choice of tunneling protocols.

Hacking Tool

Loki is a hacking tool that provides shell access over ICMP, making it much more difficult to detect than TCP- or UDP-based backdoors. As far as the network is concerned, a series of ICMP packets are being sent across the network. However, the hacker is really sending commands from the Loki client and executing them on the server.

Types of Trojans

Trojans can be created and used to perform different attacks. Here are some of the most common types of Trojans:

Remote Access Trojans (RATs) Used to gain remote access to a system.

Data-Sending Trojans Used to find data on a system and deliver data to a hacker.

Destructive Trojans Used to delete or corrupt files on a system.

Denial-of-Service Trojans Used to launch a denial-of-service attack.

Proxy Trojans Used to tunnel traffic or launch hacking attacks via other systems.

FTP Trojans Used to create an FTP server in order to copy files onto a system.

Security Software Disabler Trojans Used to stop antivirus software.

How Reverse-Connecting Trojans Work

Reverse-connecting Trojans let an attacker access a machine on the internal network from the outside. The hacker can install a simple Trojan program on a system on the internal network, such as the reverse WWW shell server. On a regular basis (usually every 60 seconds), the internal server tries to access the external master system to pick up commands. If the attacker has typed something into the master system, this command is retrieved and executed on the internal system. The reverse WWW shell server uses standard HTTP. It's dangerous because it's difficult to detect: it looks like a client is browsing the Web from the internal network.

Hacking Tools

TROJ_QAZ is a Trojan that renames the application `notepad.exe` file to `note.com` and then copies itself as `notepad.exe` to the Windows folder. This will cause the Trojan to be launched every time a user runs Notepad. It has a backdoor that a remote user or hacker can use to connect to and control the computer using port 7597. TROJ_QAZ also infects the Registry so that it is loaded every time Windows is started.

Tini is a small and simple backdoor Trojan for Windows operating systems. It listens on port 7777 and gives a hacker a remote command prompt on the target system. To connect to a Tini server, the hacker telnets to port 7777.

Donald Dick is a backdoor Trojan for Windows OSs that allows a hacker full access to a system over the Internet. The hacker can read, write, delete, or run any program on the system. Donald Dick also includes a keylogger and a Registry parser, and can perform functions such as opening or closing the CD-ROM tray. The attacker uses the client to send commands to the victim listening on a predefined port. Donald Dick uses default port 23476 or 23477.

NetBus is a Windows GUI Trojan program and is similar in functionality to Donald Dick. It adds the Registry key `HKEY_CURRENT_USER\NetBus Server` and modifies the `HKEY_CURRENT_USER\NetBus Server\General\TCPPort` key. If NetBus is configured to start automatically, it adds a Registry entry called NetBus Server Pro in `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices`.

SubSeven is a Trojan that can be configured to notify a hacker when the infected computer connects to the Internet and can tell the hacker information about the system. This notification can be done over an IRC network, by ICQ, or by email. SubSeven can cause a system to slow down, and generates error messages on the infected system.

Back Orifice 2000 is a remote administration tool that an attacker can use to control a system across a TCP/IP connection using a GUI interface. Back Orifice doesn't appear in the task list or list of processes, and it copies itself into the Registry to run every time the computer is started. The filename that it runs is configurable before it's installed. Back Orifice modifies the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices` Registry key. BackOrifice plug-ins add features to the BackOrifice program. Plug-ins include cryptographically strong Triple DES encryption, a remote desktop with optional mouse and keyboard control, drag-and-drop encrypted file transfers, Explorer-like file system browsing, graphical remote Registry editing, reliable UDP and ICMP communications protocols, and stealth capabilities that are achieved by using ICMP instead of TCP and UDP.

BoSniffer appears to be a fix for Back Orifice but is actually a Back Orifice server with the SpeakEasy plug-in installed. If `BoSniffer.exe`, the BoSniffer executable, is run on a target system, it attempts to log on to a predetermined IRC server on channel `#BO_OWNED` with a random username. It then proceeds to announce its IP address and a custom message every few minutes so that the hacker community can use this system as a zombie for future attacks.

ComputerSpy Key Logger is a program that a hacker can use to record computer activities on a computer, such as websites visited; logins and passwords for ICQ, MSN, AOL, AIM, and Yahoo! Messenger or webmail; current applications that are running or executed; Internet chats; and email. The program can even take snapshots of the entire Windows desktop at set intervals.

Beast is a Trojan that runs in the memory allocated for the `WinLogon.exe` service. Once installed, the program inserts itself into Windows Explorer or Internet Explorer. One of Beast's most distinct features is that it's an all-in-one Trojan, meaning the client, the server, and the server editor are stored in the same application.

CyberSpy is a telnet Trojan that copies itself into the Windows system directory and registers itself in the system Registry so that it starts each time an infected system is rebooted. Once this is done, it sends a notice via email or ICQ and then begins to listen to a previously specified TCP/IP port.

Subroot is a remote administration Trojan that a hacker can use to connect to a victim system on TCP port 1700.

LetMeRule! is a remote access Trojan that can be configured to listen on any port on a target system. It includes a command prompt that an attacker uses to control the target system. It can delete all files in a specific director, execute files at the remote host, or view and modify the Registry.

Firekiller 2000 disables antivirus programs and software firewalls. For instance, if Norton AntiVirus is in auto scan mode in the Taskbar, and AtGuard Firewall is activated, the program stops both on execution and makes the installations of both unusable on the hard drive. They must then be reinstalled to restore their functionality. Firekiller 2000 works with all major protection software, including AtGuard, Norton AntiVirus, and McAfee Antivirus.

The Hard Drive Killer Pro programs offer the ability to fully and permanently destroy all data on any given DOS or Windows system. The program, once executed, deletes files and infects and reboots the system within a few seconds. After rebooting, all hard drives attached to the system are formatted in an unrecoverable manner within only one to two seconds, regardless of the size of the hard drive.

How the Netcat Trojan Works

Netcat is a Trojan that uses a command-line interface to open TCP or UDP ports on a target system. A hacker can then telnet to those open ports and gain shell access to the target system. Exercise 5.1 shows you how to use Netcat.

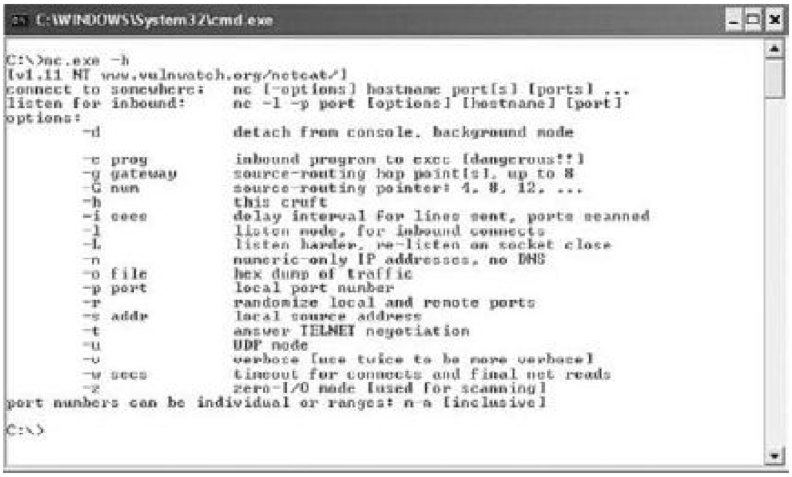
NOTE

For the CEH exam, it's important to know how to use Netcat. Make sure you download the Netcat tool and practice the commands before attempting the exam.

EXERCISE 5.1

Using Netcat

Download a version of Netcat for your system. There are many versions of Netcat for all Windows OSs. Also, Netcat was originally developed for the Unix system and is available in many Linux distributions, including BackTrack.



```
C:\>nc.exe -h
[v1.11 NT www.vulnwatch.org/netcat/]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [options] [hostname] [port]
options:
        -d              detach from console, background mode

        -e prog         inbound program to exec [dangerous!!]
        -g gateway      source-routing hop point[s], up to 8
        -G num          source-routing pointer: 4, 8, 12, ...
        -h              this cruft
        -i secs         delay interval for lines sent, ports scanned
        -l              listen mode, for inbound connects
        -L              listen harder, re-listen on socket close
        -n              numeric-only IP addresses, no DNS
        -o file         hex dump of traffic
        -p port         local port number
        -r              randomize local and remote ports
        -s addr         local source address
        -t              answer TELNET negotiation
        -u              UDP mode
        -v              verbose [use twice to be more verbose]
        -w secs         timeout for connects and final net reads
        -z              zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]

C:\>
```

Netcat needs to run on both a client and the server. The server side of the connection in enabled by the `-l` attribute and is used to create a listener port. For example, use the following command to enable the Netcat listener on the server:

```
nc -L -p 123 -t -e cmd.exe
```

On the Netcat client, run the following command to connect to the Netcat listener on the server:

```
nc <ip address of the server> <listening port on the server>
```

The client should then have a command prompt shell open from the server.

Unusual system behavior is usually an indication of a Trojan attack. Actions such as programs starting and running without the user's initiation; CD-ROM drawers opening or closing; wallpaper, background, or screen saver settings changing by themselves; the screen display flipping upside down; and a browser program opening strange or unexpected websites are all indications of a Trojan attack. Any action that is suspicious or not initiated by the user can be an indication of a Trojan attack.

Real World Scenario

Indications of a Virus or Trojan Infection

Carrie was using her computer at work and noticed that her computer seemed to be running slowly. When she tried to open files in Microsoft Word, her system would give an error message and then she was unable to use certain functions in the program. She had not received any new email messages in the last 24 hours; she usually received 50 or so messages per day, so this seemed a bit unusual. Lastly, a client of hers had said he received duplicate emails from her last week, which seemed odd.

So, Carrie called John, the company network administrator, and asked him to look at her computer to determine what was causing the computer slowdown and other issues with Microsoft Outlook. John looked at Carrie's computer and noticed that the virus definitions were 6 months old. The antivirus program kept popping up with windows indicating that the virus definitions were out of date, but Carrie just ignored them and kept closing the pop-up windows. John updated the antivirus definitions and ran a full system scan. The antivirus program determined that the system had been infected with 114 viruses and Trojans. The antivirus program was able to clean the infections and restore the computer to its previous uninfected state. John was testing Microsoft Outlook to ensure that it was indeed working when he noticed several emails from online horoscope services, entertainment websites, and online gaming websites. John removed several questionable programs from her computer. Apparently, Carrie did not realize that these types of downloads could cause harm to her computer.

Network software to push virus updates to all workstations, network controls to prevent installation of unauthorized software, and user security awareness training could have prevented this incident from occurring.

Wrappers are software packages that can be used to deliver a Trojan. The wrapper binds a legitimate file to the Trojan file. Both the legitimate software and the Trojan are combined into a single executable file and installed when the program is run.

Generally, games or other animated installations are used as wrappers because they entertain the user while the Trojan in being installed. This way, the user doesn't notice the slower processing that occurs while the Trojan is being installed on the system—the user only sees the legitimate application being installed.

Hacking Tools

Graffiti is an animated game that can be wrapped with a Trojan. It entertains the user with an animated game while the Trojan is being installed in the background.

Silk Rope 2000 is a wrapper that combines the BackOrifice server and any other specified application.

ELiTeWrap is an advanced EXE wrapper for Windows used for installing and running programs. ELiTeWrap can create a setup program to extract files to a directory and execute programs or batch files that display help menus or copy files on to the target system.

Icon Converter Plus is a conversion program that translates icons between various formats. An attacker can use this type of application to disguise malicious code or a Trojan so that users are tricked into executing it, thinking it is a legitimate application.

Trojan Construction Kit and Trojan Makers

Several Trojan-generator tools enable hackers to create their own Trojans. Such toolkits help hackers construct Trojans that can be customized. These tools can be dangerous and can backfire if not executed properly. New Trojans created by hackers usually have the added benefit of passing undetected through virus-scanning and Trojan-scanning tools because they don't match any known signatures.

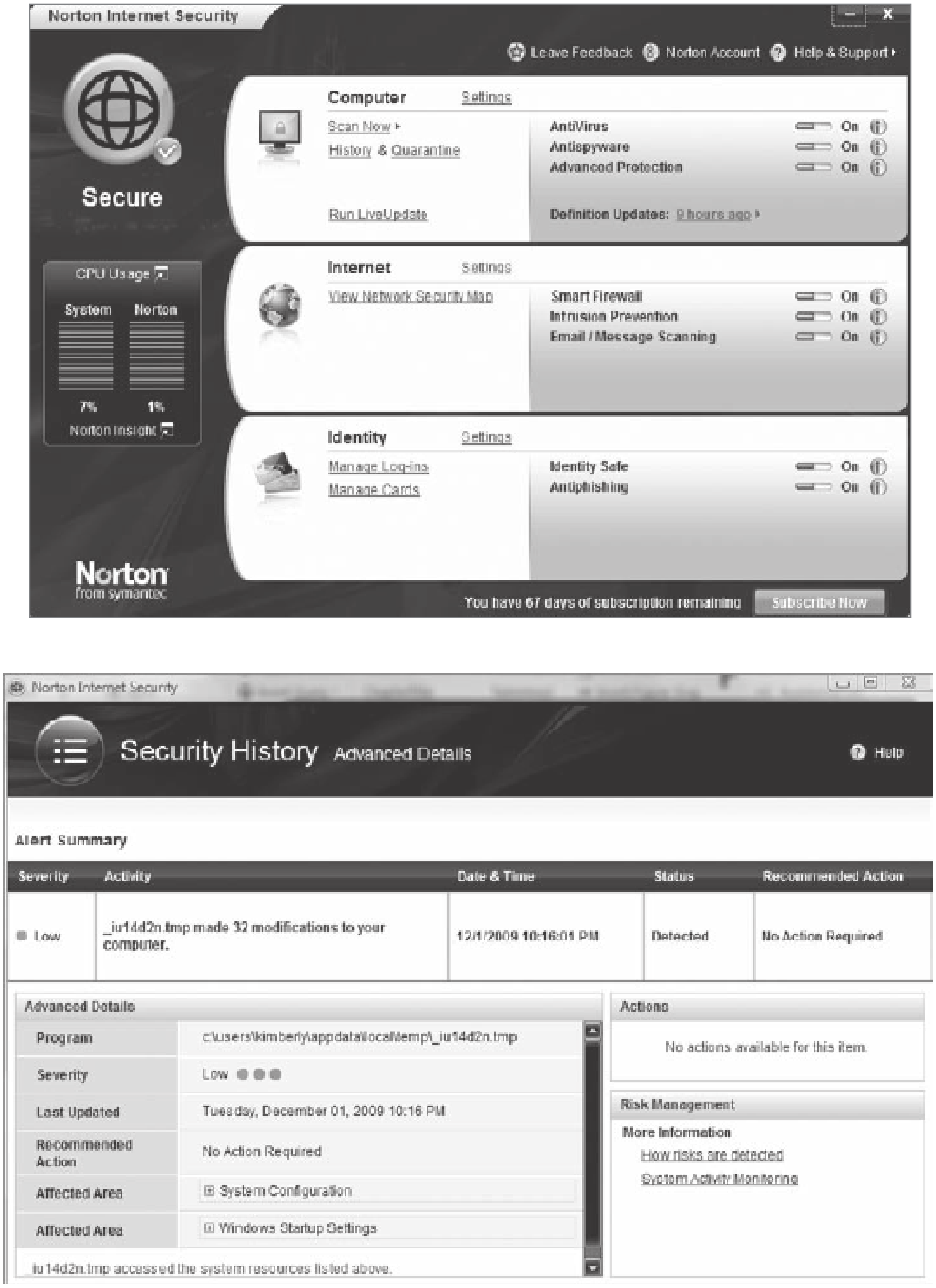
Some of the Trojan kits available in the wild are Senna Spy Generator, the Trojan Horse Construction Kit v2.0, Progenic Mail Trojan Construction Kit, and Pandora's Box.

Trojan Countermeasures

Most commercial antivirus program have anti-Trojan capabilities as well as spyware detection and removal functionality. These tools can automatically scan hard drives on startup to detect backdoor and Trojan programs before they can cause damage. Once a system is infected, it's more difficult to clean, but you can do so with commercially available tools.

Although several commercially antivirus or Trojan removal tools are available, my personal recommendation is Norton Internet Security (Figure 5.1). Norton Internet Security includes a personal firewall, intrusion detection system, antivirus, antispyware, antiphishing, and email scanning. Norton Internet Security will clean most Trojans from a system as well.

FIGURE 5.1 Norton Internet Security



Norton Internet Security

Leave Feedback | Norton Account | Help & Support ▸

Secure

Computer Settings

Scan Now ▸

History & Quarantine

Run LiveUpdate

AntiVirus On

Antispyware On

Advanced Protection On

Definition Updates: 9 hours ago ▸

Internet Settings

View Network Security Map

Smart Firewall On

Intrusion Prevention On

Email / Message Scanning On

Identity Settings

Manage Log-ins

Manage Cards

Identity Safe On

Antiphishing On

CPU Usage

System 7%

Norton 1%

Norton Insight

You have 67 days of subscription remaining

Norton Internet Security

Security History Advanced Details

Alert Summary

Severity	Activity	Date & Time	Status	Recommended Action
● Low	_iu14d2n.tmp made 32 modifications to your computer.	12/1/2009 10:16:01 PM	Detected	No Action Required

Advanced Details

Program	c:\users\kimberly\appdata\local\temp_iu14d2n.tmp
Severity	Low ● ● ●
Last Updated	Tuesday, December 01, 2009 10:16 PM
Recommended Action	No Action Required
Affected Area	⊞ System Configuration
Affected Area	⊞ Windows Startup Settings

_iu14d2n.tmp accessed the system resources listed above.

Actions

No actions available for this item.

Risk Management

More Information

How risks are detected

System Activity Monitoring

The security software works by having known signatures of malware, such as Trojans and viruses. The repair for the malware is made through the use of definitions of the malware. When installing and using any personal security software or antivirus and anti-Trojan software, you must make sure that the software has all the current definitions. To ensure the latest patches and fixes are available, you should connect the system to the Internet so the software can continually update the malware definitions and fixes.

It's important to use commercial applications to clean a system instead of freeware tools, because many freeware removal tools can further infect the system. In addition, a lot of commercial security software includes an intrusion detection component that will perform port monitoring and can identify ports that have been opened or files that have changed.

The key to preventing Trojans and backdoors from being installed on a system is to educate users not to install applications downloaded from the Internet or open email attachments from parties they don't know. Many system administrators don't give users the system permissions necessary to install programs on their system for that very reason. Proper use of Internet technologies should be included in regular employee security awareness training.

Port-Monitoring and Trojan-Detection Tools

Fport reports all open TCP/IP and UDP ports and maps them to the owning application. You can use fport to quickly identify unknown open ports and their associated applications.

TCPView is a Windows program that shows detailed listings of all TCP and UDP endpoints on the system, including the local and remote addresses and state of TCP connections. When TCPView runs, it enumerates all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions.

PrcView is a process viewer utility that displays detailed information about processes running under Windows. PrcView comes with a command-line version you can use to write scripts that check whether a process is running and, if so, kill it.

Inzider is a useful tool that lists processes in the Windows system and the ports on which each one listens. Inzider may pick up some Trojans. For instance, BackOrifice injects itself into other processes, so it isn't visible in the Task Manager as a separate process, but it does have an open port that it listens on.

Tripwire verifies system integrity. It automatically calculates cryptographic hashes of all key system files or any file that is to be monitored for modifications. The Tripwire software works by creating a baseline snapshot of the system. It periodically scans those files, recalculates the information, and sees whether any of the information has changed. If there is a change, the software raises an alarm.

Dsniff is a collection of tools used for network auditing and penetration testing. Dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and WebSpy passively monitor a network for interesting data such as passwords, email, and file transfers. Arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker due to Layer 2 switching. Sshmitm and webmitm implement active man-in-the-middle attacks against redirected Secure Shell (SSH) and HTTP Over SSL (HTTPS) sessions by exploiting weak bindings in ad hoc Public Key Infrastructure (PKI). These tools will be discussed in further detail in Chapter 6, "Gathering Data from Networks: Sniffers."

Checking a System with System File Verification

Windows 2003 includes a feature called Windows File Protection (WFP) that prevents the replacement of protected files. WFP checks the file integrity when an attempt is made to overwrite a SYS, DLL, OCX, TTF, or EXE file. This ensures that only Microsoft-verified files are used to replace system files.

Another tool, sigverif, checks to see what files Microsoft has digitally signed on a system. In Exercise 5.2, we will use this tool.

EXERCISE 5.2

Signature Verification

We will run sigverif, a signature verification checker, and compare the results to the currently running processes in Task Manager:

1. Press Ctrl+Alt+Del and select Start Task Manager.
2. Click the Processes tab. Note any unusual processes and the amount of CPU time they are using. Any processes using a consistently high percentage of CPU time may indicate a virus or Trojan infection.

EXERCISE 5.2 *(continued)*

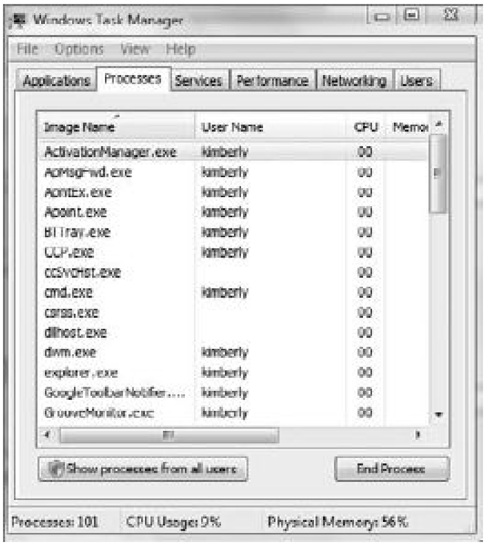
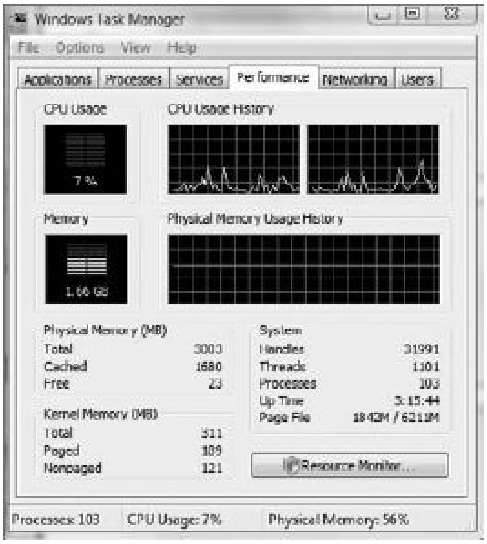


Image Name	User Name	CPU	Memor
ActivationManager.exe	kimberly	00	
AOMsgFwd.exe	kimberly	00	
AOntEx.exe	kimberly	00	
Apoint.exe	kimberly	00	
BTTray.exe	kimberly	00	
CCP.exe	kimberly	00	
ccSvcHst.exe		00	
cmd.exe	kimberly	00	
csrss.exe		00	
dllhost.exe		00	
dwm.exe	kimberly	00	
explorer.exe	kimberly	00	
GoogleToolbarNotifier....	kimberly	00	
GrooveMonitor.exe	kimberly	00	

Processes: 101 CPU Usage: 9% Physical Memory: 56%

3. Click the Performance tab in Task Manager to view the current CPU usage.



Physical Memory (MB)	
Total	3003
Cached	1680
Free	23

Kernel Memory (MB)	
Total	311
Paged	109
Nonpaged	121

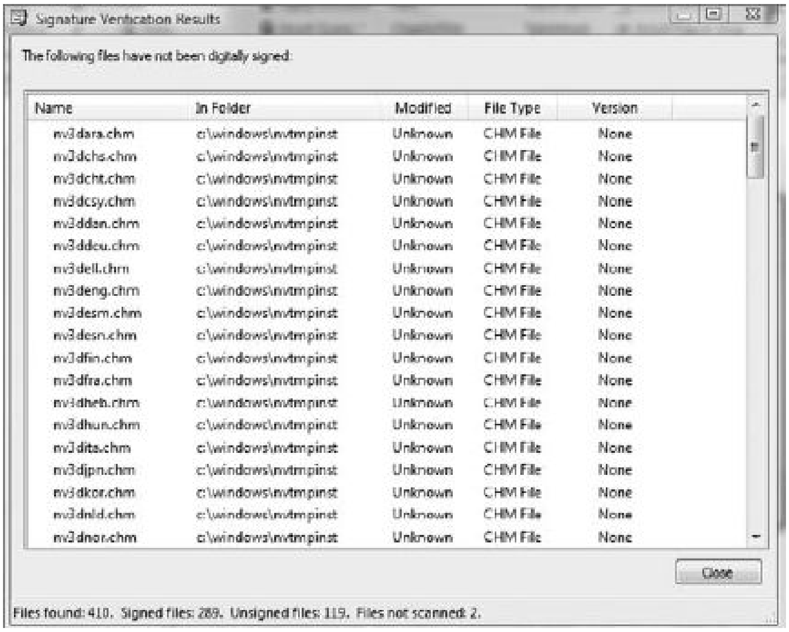
System	
Handles	31991
Threads	1101
Processes	103
Up Time	3:15:44
Page File	1842M / 6211M

Processes: 103 CPU Usage: 7% Physical Memory: 56%

4. Click Start ➢ Run.

EXERCISE 5.2 ***(continued)***

5. Type **`sigverif`**, and click Start.

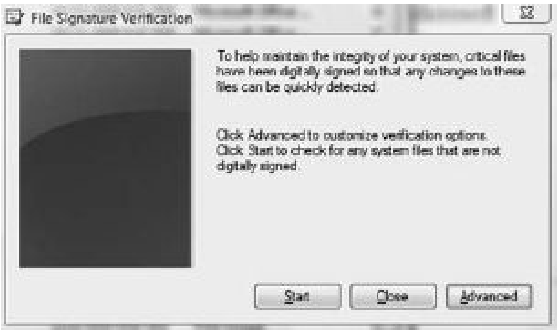


The following files have not been digitally signed:

Name	In Folder	Modified	File Type	Version
nv3dara.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3dchs.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3dcht.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3dcsy.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3ddan.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3ddeu.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3dell.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3deng.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3desm.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3desn.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3dfin.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3dfra.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3dheb.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3dhun.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3dita.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3djpn.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3dkor.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3dnld.chm	c:\windows\nvtmpinst	Unknown	CHM File	None
nv3dnor.chm	c:\windows\nvtmpinst	Unknown	CHM File	None

Files found: 410. Signed files: 289. Unsigned files: 119. Files not scanned: 2.

6. In the sigverif program, choose Advanced to see the signature verification report.

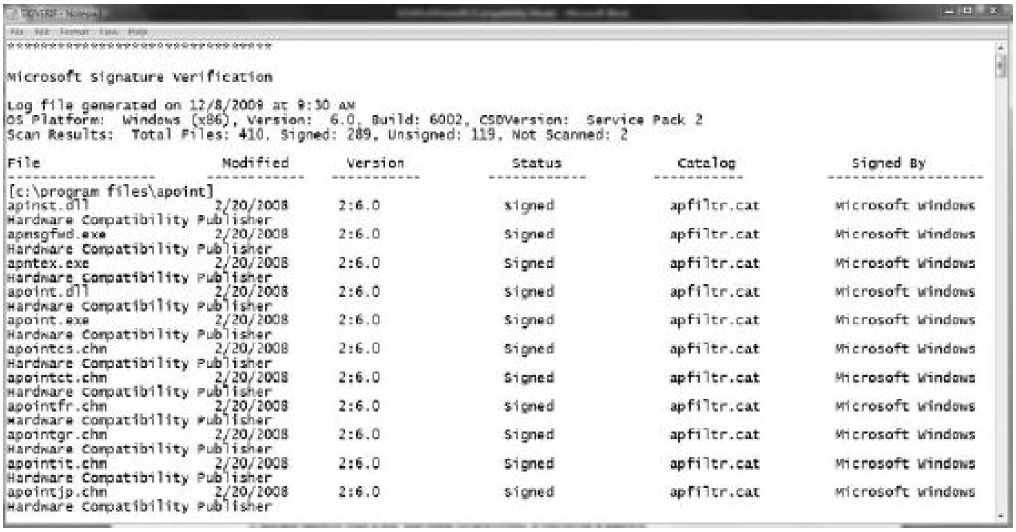


To help maintain the integrity of your system, critical files have been digitally signed so that any changes to these files can be quickly detected.

Click Advanced to customize verification options.
Click Start to check for any system files that are not digitally signed.

EXERCISE 5.2 *(continued)*

7. Click the View Log button to see the report.



```
**********************************

Microsoft Signature Verification

Log file generated on 12/8/2009 at 9:30 AM
OS Platform:  Windows (x86), Version:  6.0, Build: 6002, CSDVersion:  Service Pack 2
Scan Results:  Total Files: 410, Signed: 289, Unsigned: 119, Not Scanned: 2

File                      Modified      Version          Status          Catalog          Signed By
------------------      ------------  ------------    ------------    -----------    -------------------
[c:\program files\apoint]
apinst.dll                 2/20/2008     2:6.0            Signed          apfiltr.cat      Microsoft Windows
Hardware Compatibility Publisher
apmsgfwd.exe               2/20/2008     2:6.0            Signed          apfiltr.cat      Microsoft Windows
Hardware Compatibility Publisher
apntex.exe                 2/20/2008     2:6.0            Signed          apfiltr.cat      Microsoft Windows
Hardware Compatibility Publisher
apoint.dll                 2/20/2008     2:6.0            Signed          apfiltr.cat      Microsoft Windows
Hardware Compatibility Publisher
apoint.exe                 2/20/2008     2:6.0            Signed          apfiltr.cat      Microsoft Windows
Hardware Compatibility Publisher
apointcs.chm               2/20/2008     2:6.0            Signed          apfiltr.cat      Microsoft Windows
Hardware Compatibility Publisher
apointct.chm               2/20/2008     2:6.0            Signed          apfiltr.cat      Microsoft Windows
Hardware Compatibility Publisher
apointfr.chm               2/20/2008     2:6.0            Signed          apfiltr.cat      Microsoft Windows
Hardware Compatibility Publisher
apointgr.chm               2/20/2008     2:6.0            Signed          apfiltr.cat      Microsoft Windows
Hardware Compatibility Publisher
apointit.chm               2/20/2008     2:6.0            Signed          apfiltr.cat      Microsoft Windows
Hardware Compatibility Publisher
apointjp.chm               2/20/2008     2:6.0            Signed          apfiltr.cat      Microsoft Windows
Hardware Compatibility Publisher
```

System File Checker is another command line–based tool used to check whether a Trojan program has replaced files. If System File Checker detects that a file has been overwritten, it retrieves a known good file from the `Windows\system32\dllcache` folder and overwrites the unverified file. The command to run the System File Checker is `sfc/scannow`.

Viruses and Worms

Viruses and worms can be used to infect a system and modify a system to allow a hacker to gain access. Many viruses and worms carry Trojans and backdoors. In this way, a virus or worm is a carrier and allows malicious code such as Trojans and backdoors to be transferred from system to system much in the way that contact between people allows germs to spread.

A *virus* and a *worm* are similar in that they're both forms of malicious software (*malware*). A virus infects another executable and uses this carrier program to spread itself. The virus code is injected into the previously benign program and is spread when the program is run. Examples of virus carrier programs are macros, games, email attachments, Visual Basic scripts, and animations.

A worm is similar to a virus in many ways but does not need a carrier program. A worm can self-replicate and move from infected host to another host. A worm spreads from system to system automatically, but a virus needs another program in order to spread. Viruses and worms both execute without the knowledge or desire of the end user.

Types of Viruses

Viruses are classified according to two factors: what they infect and how they infect. A virus can infect the following components of a system:

- System sectors
- Files
- Macros (such as Microsoft Word macros)
- Companion files (supporting system files like DLL and INI files)
- Disk clusters
- Batch files (BAT files)
- Source code

A virus infects through interaction with an outside system. Viruses need to be carried by another executable program. By attaching itself to the benign executable a virus can spread fairly quickly as users or the system runs the executable. Viruses are categorized according to their infection technique, as follows:

Polymorphic Viruses These viruses encrypt the code in a different way with each infection and can change to different forms to try to evade detection.

Stealth Viruses These viruses hide the normal virus characteristics, such as modifying the original time and date stamp of the file so as to prevent the virus from being noticed as a new file on the system.

Fast and Slow Infectors These viruses can evade detection by infecting very quickly or very slowly. This can sometimes allow the program to infect a system without detection by an antivirus program.

Sparse Infectors These viruses infect only a few systems or applications.

Armored Viruses These viruses are encrypted to prevent detection.

Multipartite Viruses These advanced viruses create multiple infections.

Cavity (Space-Filler) Viruses These viruses attach to empty areas of files.

Tunneling Viruses These viruses are sent via a different protocol or encrypted to prevent detection or allow it to pass through a firewall.

Camouflage Viruses These viruses appear to be another program.

NTFS and Active Directory Viruses These viruses specifically attack the NT file system or Active Directory on Windows systems.

An attacker can write a custom script or virus that won't be detected by antivirus programs. Because virus detection and removal is based on a signature of the program, a hacker just needs to change the signature or look of the virus to prevent detection. The virus signature or definition is the way an antivirus program is able to determine if a system is infected by a virus. Until the virus is detected and antivirus companies have a chance to update virus definitions, the virus goes undetected. Additional time may elapse before a user updates the antivirus program, allowing the system to be vulnerable to an infection. This allows an attacker to evade antivirus detection and removal for a period of time. A critical countermeasure to virus infection is to maintain up-to-date virus definitions in an antivirus program.

One of the most longstanding viruses was the Melissa virus, which spread through Microsoft Word Macros. Melissa infected many users by attaching to the Word doc and then when the file was copied or emailed, the virus spread along with the file.

Virus Hoaxes are emails sent to users usually with a warning about a virus attack. The Virus Hoax emails usually make outlandish claims about the damage that will be caused by a virus and then offer to download a remediation patch from well-known companies such as Microsoft or Norton. Other Hoaxes recommend users delete certain critical systems files in order to remove the virus. Of course, should a user follow these recommendations they will most certainly have negative consequences. Some of the most common virus hoaxes are shown in Table 5.1:

TABLE 5.1 Common Virus Hoaxes

Name	Executable	Description
Antichrist	(none)	This is a hoax that warned about a supposed virus discovered by Microsoft and McAfee named "Antichrist", telling the user that it is installed via an email with the subject line: "SURPRISE?!!!!!!!!!!" after which it destroys the zeroth sector of the hard disk, rendering it unusable.
Budweiser Frogs	BUDSAVER.EXE	Supposedly would erase the user's hard drive and steal the user's screen name and password.
Goodtimes virus	(none)	Warnings about a computer virus named "Good Times" began being passed around among Internet users in 1994. The Goodtimes virus was supposedly transmitted via an email bearing the subject header "Good Times" or "Goodtimes," hence the virus's name, and the warning recommended deleting any such email unread. The virus described in the warnings did not exist, but the warnings themselves, were, in effect, virus-like.

TABLE 5.1 Common Virus Hoaxes *(continued)*

Name	Executable	Description
Invitation attachment (computer virus hoax)	Allright now/ I'm just sayin	The invitation virus hoax involved an email spam in 2006 that advised computer users to delete an email, with any type of attachment that stated "invitation" because it was a computer virus.
Jdbgmgr.exe	bear.a	The jdbgmgr.exe virus hoax involved an email spam in 2002 that advised computer users to delete a file named jdbgmgr.exe because it was a computer virus. jdbgmgr.exe, which had a little teddy bear-like icon (The Microsoft Bear), was actually a valid Microsoft Windows file, the Debugger Registrar for Java (also known as Java Debug Manager, hence jdbgmgr).
Life is beautiful	Life is wonderful	The hoax was spread through the Internet around January 2001 in Brazil. It told of a virus attached to an email, which was spread around the Internet. The attached file was supposedly called "Life is beautiful.pps" or "La vita è bella.pps".
Olympic Torch	Postcard or Postcard from Hallmark	Olympic Torch is a computer virus hoax sent out by email. The hoax emails first appeared in February 2006. The "virus" referred to by the email does not actually exist. The hoax email warns recipients of a recent outbreak of "Olympic Torch" viruses, contained in emails titled "Invitation," which erase the hard disk of the user's computer when opened.
SULFNBK.EXE Warning	none	SULFNBK.EXE (short for Setup Utility for Long File Name Backup) is an internal component of the Microsoft Windows operating system (in Windows 98 and Windows Me) for restoring long file names. The component became famous in the early 2000s as the subject of an email hoax. The hoax claimed that SULFNBK.EXE was a virus, and contained instructions to locate and delete the file. While the instructions worked, they were needless and (in some rare cases, for example, when the long file names are damaged and need to be restored) can cause disruptions, as SULFNBK.EXE is not a virus, but instead an operating system component.

To find out whether an email regarding a virus is legitimate, review the list of virus hoaxes on the website `home.mcafee.com/virusinfo`.

Virus Detection Methods

The following techniques are used to detect viruses:

- Scanning
- Integrity checking with checksums
- Interception based on a virus signature

The process of virus detection and removal is as follows:

1. Detect the attack as a virus. Not all anomalous behavior can be attributed to a virus.
2. Trace processes using utilities such as `handle.exe`, `listdlls.exe`, `fport.exe`, `netstat.exe`, and `pslist.exe`, and map commonalities between affected systems.
3. Detect the virus payload by looking for altered, replaced, or deleted files. New files, changed file attributes, or shared library files should be checked.
4. Acquire the infection vector and isolate it. Then, update your antivirus definitions and rescan all systems.

In Exercise 5.3, we will create a test virus.

EXERCISE 5.3

Creating a Test Virus

A test virus can be created by typing the following code in Notepad and saving the file as `EICAR.COM`. Your antivirus program should respond when you attempt to open, run, or copy it.

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Worms can be prevented from infecting systems in much the same way as viruses. Worms can be more difficult to stop because they spread on their own, meaning they do not need user intervention to install and continue to propagate the malware. Worms can be detected with the use of antimalware software that contains definitions for worms. Worms, most importantly, need to be stopped from spreading. In order to do this, an administrator may need to take systems off line. The best practice for cleaning worms off networked systems is to first remove the computer from the network and then run the security software to clean the worm.

Summary

Trojans, backdoors, viruses, and worms are all forms of malware used to infect systems and either cause data damage or infect the system so a hacker can gain further access to a system. The types of viruses, ways they infect, and how they are used are exam objectives for the CEH exam.

The best way to prevent malware from infecting systems is to ensure Internet security software is installed and up-to-date with virus and Trojans signatures and definitions. Additionally, malware can be avoided with security awareness training of users to prevent them from opening and running any files they are not familiar with or can verify.

Exam Essentials

Understand the definition of a Trojan. Trojans are malicious pieces of code that are carried by software to a target system.

Understand what a covert channel is. A covert channel uses communications in a way that was not intended. ICMP tunneling, reverse WWW shell, and man-in-the-middle attacks are common covert channels.

Understand the definition of a backdoor. A backdoor is usually a component of a Trojan. It's used to maintain access after the initial system weakness has been discovered and removed. It usually takes the form of a port being opened on a compromised system.

Understand what a Trojan is and how it works. Trojans are used primarily to gain and retain access on the target system. A Trojan often resides deep in the system and makes Registry changes that allow it to meet its purpose as a remote administration tool.

Know the best Trojan countermeasures. Awareness and preventive measures are the best defenses against Trojans.

Understand how a virus is different from a worm. Viruses must attach themselves to other programs, whereas worms spread automatically.

Understand the different types of viruses. Polymorphic, stealth, fast infectors, slow infectors, sparse infectors, armored, multipartite, cavity, tunneling, camouflage, NTFS, and AD viruses are all types of viruses.

Review Questions

1. What is a wrapper?
   - **A.** A Trojaned system
   - **B.** A program used to combine a Trojan and legitimate software into a single executable
   - **C.** A program used to combine a Trojan and a backdoor into a single executable
   - **D.** A way of accessing a Trojaned system
2. What is the difference between a backdoor and a Trojan?
   - **A.** A Trojan usually provides a backdoor for a hacker.
   - **B.** A backdoor must be installed first.
   - **C.** A Trojan is not a way to access a system.
   - **D.** A backdoor is provided only through a virus, not through a Trojan.
3. What port does Tini use by default?
   - **A.** 12345
   - **B.** 71
   - **C.** 7777
   - **D.** 666
4. Which is the best Trojan and backdoor countermeasure?
   - **A.** Scan the hard drive on network connection, and educate users not to install unknown software.
   - **B.** Implement a network firewall.
   - **C.** Implement personal firewall software.
   - **D.** Educate systems administrators about the risks of using systems without firewalls.
   - **E.** Scan the hard drive on startup.
5. How do you remove a Trojan from a system?
   - **A.** Search the Internet for freeware removal tools.
   - **B.** Purchase commercially available tools to remove the Trojan.
   - **C.** Reboot the system.
   - **D.** Uninstall and reinstall all applications.
6. What is ICMP tunneling?
   - **A.** Tunneling ICMP messages through HTTP
   - **B.** Tunneling another protocol through ICMP
   - **C.** An overt channel
   - **D.** Sending ICMP commands using a different protocol

7. What is reverse WWW shell?

A. Connecting to a website using a tunnel

B. A Trojan that connects from the server to the client using HTTP

C. A Trojan that issues commands to the client using HTTP

D. Connecting through a firewall

8. What is a covert channel?

A. Using a communications channel in a way that was not intended

B. Tunneling software

C. A Trojan removal tool

D. Using a communications channel in the original, intended way

9. What is the purpose of system file verification?

A. To find system files

B. To determine whether system files have been changed or modified

C. To find out if a backdoor has been installed

D. To remove a Trojan

10. Which of the following is an example of a covert channel?

A. Reverse WWW shell

B. Firewalking

C. SNMP enumeration

D. Steganography

11. What is the difference between a virus and a worm?

A. A virus can infect the boot sector but a worm cannot.

B. A worm spreads by itself but a virus must attach to an email.

C. A worm spreads by itself but a virus must attach to another program.

D. A virus is written in C++ but a worm is written in shell code.

12. What type of virus modifies itself to avoid detection?

A. Stealth virus

B. Polymorphic virus

C. Multipartite virus

D. Armored virus

13. Which virus spreads through Word macros?
    - **A.** Melissa
    - **B.** Slammer
    - **C.** Sobig
    - **D.** Blaster

14. Which worm affects SQL servers?
    - **A.** Sobig
    - **B.** SQL Blaster
    - **C.** SQL Slammer
    - **D.** Melissa

15. Which of the following describes armored viruses?
    - **A.** Hidden
    - **B.** Tunneled
    - **C.** Encrypted
    - **D.** Stealth

16. What are the three methods used to detect a virus?
    - **A.** Scanning
    - **B.** Integrity checking
    - **C.** Virus signature comparison
    - **D.** Firewall rules
    - **E.** IDS anomaly detection
    - **F.** Sniffing

17. What components of a system do viruses infect? (Choose all that apply.)
    - **A.** Files
    - **B.** System sectors
    - **C.** Memory
    - **D.** CPU
    - **E.** DLL files

18. Which of the following are the best indications of a virus attack? (Choose all that apply.)
    - **A.** Any anomalous behavior
    - **B.** Unusual program opening or closing
    - **C.** Strange pop-up messages
    - **D.** Normal system operations as most viruses run in the background

19. A virus that can cause multiple infections is known as what type of virus?

A. Multipartite

B. Stealth

C. Camouflage

D. Multi-infection

20. Which of the following is a way to evade an antivirus program?

A. Write a custom virus script.

B. Write a custom virus signature.

C. Write a custom virus evasion program.

D. Write a custom virus detection program.

Answers to Review Questions

1. B. A wrapper is software used to combine a Trojan and legitimate software into a single executable so that the Trojan is installed during the installation of the other software. After a Trojan has been installed, a system is considered "Trojaned." A backdoor is a way of accessing a Trojaned system and can be part of the behavior of a Trojan.

2. A. A Trojan infects a system first and usually includes a backdoor for later access. The backdoor is not installed independently, but is part of a Trojan. A Trojan is one way a hacker can access a system.

3. C. Tini uses port 7777 by default. Doom uses port 666.

4. A. The best prevention is to scan the hard drive for known Trojans on network connections and backdoors and to educate users not to install any unknown software. Scanning the hard drive at startup is a good method for detecting a Trojan, but will not prevent its installation. User education is an important component of security but will not always and consistently prevent a Trojan attack.

5. B. To remove a Trojan, you should use commercial tools. Many freeware tools contain Trojans or other malware. Rebooting the system alone will not remove a Trojan from the system. Uninstalling and reinstalling applications will not remove a Trojan as it infects the OS.

6. B. ICMP tunneling involves sending what appear to be ICMP commands but really are Trojan communications. An overt channel sends data via a normal communication path such as via email. Sending or tunneling ICMP within another protocol such as HTTP is not considered ICMP tunneling.

7. B. Reverse WWW shell is a connection from a Trojan server component on the compromised system to the Trojan client on the hacker's system. Connecting to a website using tunneling or through a firewall is not considered a reverse WWW shell.

8. A. A covert channel is the use of a protocol or communications channel in a nontraditional way. Tunneling software is one way of using a covert channel but does not necessarily define all covert channels. Using a communications channel in the original intended way is considered an overt channel.

9. B. System file verification tracks changes made to system files and ensures that a Trojan has not overwritten a critical system file. System files and backdoors are not located using system file verification. To remove a Trojan, you should use commercial removal tools.

10. A. Reverse WWW shell is an example of a covert channel. Firewalking is enumerating a firewall for firewall rules, allowed traffic, and open ports. Steganography is hiding information in text or graphics. SNMP enumeration is used to identify SNMP MIB settings on networking devices.

11. C. A worm can replicate itself automatically, but a virus must attach to another program. Viruses are not always spread via email but can also be attached to other programs or installed directly by tricking the user. Both viruses and worms can infect the boot sector. The programming language is not used to categorize malware as either viruses or worms.

12. B. A polymorphic virus modifies itself to evade detection. Stealth viruses hide the normal virus characteristics to prevent detection. Multipartite viruses are viruses that create multiple infections or infect multiple files or programs. Armored viruses use encryption to evade detection.

13. A. Melissa is a virus that spreads via Word macros. Slammer and Blaster are actually worm infections, not viruses. Sobig is another type of virus.

14. C. SQL Slammer is a worm that attacks SQL servers. Melissa affects Word files through the use of macros. There is no such worm as SQL Blaster.

15. C. Armored viruses are encrypted. They are not by nature tunneled and do not change characteristics, as do stealth viruses. Also, armored viruses are not hidden in any other way.

16. A, B, C. Scanning, integrity checking, and virus signature comparison are three ways to detect a virus infection. Firewalls, IDS anomaly detection, and sniffing all work at lower layers of the OSI model and are not able to detect viruses.

17. A, B, E. A virus can affect files, system sectors, and DLL files. Memory and CPU cannot be infected by viruses.

18. B, C. Trojans, backdoors, spyware, and other malicious software can cause a system to not act normally. Any indications of programs opening or closing without user intervention, unresponsive programs, unusual error messages, or pop-ups *could* indicate any type of malware has infected the system. But not all anomalous behavior can be attributed to a virus.

19. A. A multipartite virus can cause multiple infections. Stealth viruses hide the normal virus characteristics to prevent detection. Camouflage and multi-infection are not categories of viruses.

20. A. A custom virus script can be used to evade detection because the script will not match a virus signature.