

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

CEHTM

Certified Ethical Hacker

STUDY GUIDE


Exam 312-50
Exam EC0-350

Kimberly Graves



SERIOUS SKILLS.

Chapter 3. Gathering Network and Host Information: Scanning and Enumeration.....	1
Section 3.1. Scanning.....	2
Section 3.2. Enumeration.....	19
Section 3.3. Summary.....	24
Section 3.4. Exam Essentials.....	25
Section 3.5. Review Questions.....	27
Section 3.6. Answers to Review Questions.....	31



Chapter 3

Gathering Network and Host Information: Scanning and Enumeration

CEH EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ Define the terms port scanning, network scanning, and vulnerability scanning
- ✓ Understand the CEH scanning methodology
- ✓ Understand ping sweep techniques
- ✓ Understand `nmap` command switches
- ✓ Understand SYN, stealth, XMAS, NULL, IDLE, and FIN scans
- ✓ List TCP communication flag types
- ✓ Understand war-dialing techniques
- ✓ Understand banner grabbing and OS fingerprinting techniques
- ✓ Understand how proxy servers are used in launching an attack
- ✓ How do anonymizers work?
- ✓ Understand HTTP tunneling techniques
- ✓ Understand IP spoofing techniques
- ✓ What is enumeration?
- ✓ What is meant by null sessions?
- ✓ What is SNMP enumeration?
- ✓ What are the steps involved in performing enumeration?



Scanning is the first phase of active hacking and is used to locate target systems or networks for later attack. Enumeration is the follow-on step once scanning is complete and is used to identify computer names, usernames, and shares. Scanning and enumeration are discussed together in this chapter because many hacking tools perform both steps simultaneously.

Scanning

After the reconnaissance and information-gathering stages have been completed, scanning is performed. It is important that the information-gathering stage be as complete as possible to identify the best location and targets to scan. During scanning, the hacker continues to gather information regarding the network and its individual host systems. Information such as IP addresses, operating system, services, and installed applications can help the hacker determine which type of exploit to use in hacking a system.

Scanning is the process of locating systems that are alive and responding on the network. Ethical hackers use scanning to identify target systems' IP addresses. Scanning is also used to determine whether a system is on the network and available. Scanning tools are used to gather information about a system such as IP addresses, the operating system, and services running on the target computer.

Table 3.1 lists the three types of scanning.

TABLE 3.1 Types of scanning

Scanning type	Purpose
Port scanning	Determines open ports and services
Network scanning	Identifies IP addresses on a given network or subnet
Vulnerability scanning	Discovers presence of known weaknesses on target systems

Port Scanning Port scanning is the process of identifying open and available TCP/IP ports on a system. Port-scanning tools enable a hacker to learn about the services available on

a given system. Each service or application on a machine is associated with a *well-known* port number. Port Numbers are divided into three ranges:

- Well-Known Ports: 0-1023
- Registered Ports: 1024-49151
- Dynamic Ports: 49152-65535

For example, a port-scanning tool that identifies port 80 as open indicates a web server is running on that system. Hackers need to be familiar with well-known port numbers.

Common Port Numbers

On Windows systems, well-known port numbers are located in the C:\windows\system32\drivers\etc\services file. Services is a hidden file. To view it, show hidden files in Windows Explorer, and double-click the filename to open it with Notepad. The CEH exam expects you to know the well-known port numbers for common applications; familiarize yourself with the port numbers for the following applications:

- FTP, 21
- Telnet, 23
- HTTP, 80
- SMTP, 25
- POP3, 110
- HTTPS, 443

The following list contains additional port numbers not necessarily on the CEH exam but useful for real-world penetration testing:

- Global Catalog Server (TCP), 3269 and 3268
- LDAP Server (TCP/UDP), 389
- LDAP SSL (TCP/UDP), 636
- IPsec ISAKMP (UDP), 500
- NAT-T (UDP), 4500
- RPC (TCP), 135
- ASP.NET Session State (TCP), 42424
- NetBIOS Datagram Service (UDP), 137 and 138
- NetBIOS Session Service (TCP), 139

- DHCP Server (UDP), 67
- LDAP Server (TCP/UDP), 389
- SMB (TCP), 445
- RPC (TCP), 135
- DNS (TCP/UDP), 53
- IMAP (TCP), 143
- IMAP over SSL (TCP), 993
- POP3 (TCP), 110
- POP3 over SSL (TCP), 995
- RPC (TCP), 135
- RPC over HTTPS (TCP), 443 or 80
- SMTP (TCP/UDP), 25

Network Scanning Network scanning is a procedure for identifying active hosts on a network, either to attack them or as a network security assessment. Hosts are identified by their individual IP addresses. Network-scanning tools attempt to identify all the *live* or responding hosts on the network and their corresponding IP addresses.

Vulnerability Scanning Vulnerability scanning is the process of proactively identifying the vulnerabilities of computer systems on a network. Generally, a vulnerability scanner first identifies the operating system and version number, including service packs that may be installed. Then, the scanner identifies weaknesses or vulnerabilities in the operating system. During the later attack phase, a hacker can exploit those weaknesses in order to gain access to the system.

Although scanning can quickly identify which hosts are listening and active on a network, it is also a quick way to be identified by an intrusion detection system (IDS). Scanning tools probe TCP/IP ports looking for open ports and IP addresses, and these probes can be recognized by most security intrusion detection tools. Network and vulnerability scanning can usually be detected as well, because the scanner must interact with the target system over the network.

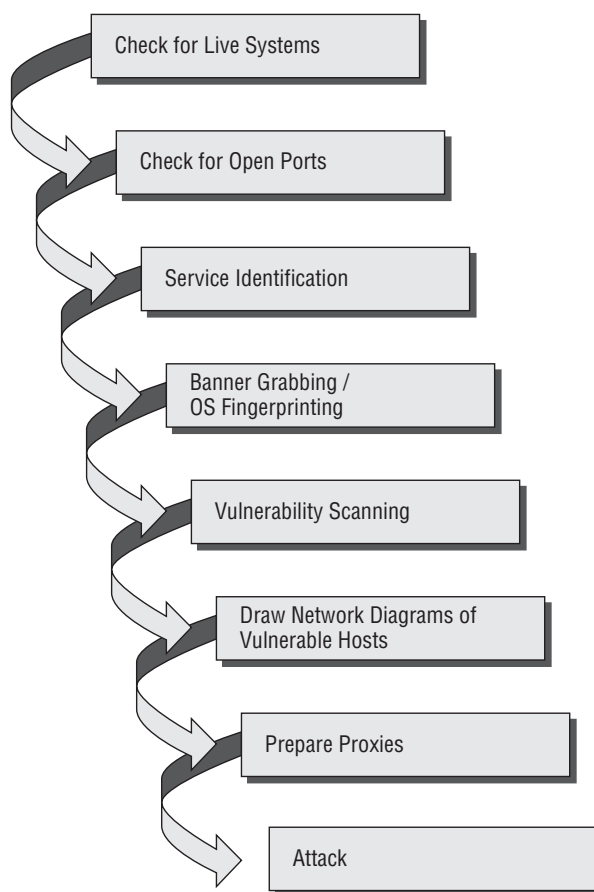
Depending on the type of scanning application and the speed of the scan, an IDS will detect the scanning and flag it as an IDS event. Some of the tools for scanning have different modes to attempt to defeat an IDS and are more likely to be able to scan undetected. As a CEH it is your job to gather as much information as possible and try and remain undetected.

The CEH Scanning Methodology

As a CEH, you're expected to be familiar with the scanning methodology presented in Figure 3.1. This methodology is the process by which a hacker scans the network. It ensures that no system or vulnerability is overlooked and that the hacker gathers all necessary information to perform an attack.

We'll look at the various stages of this scanning methodology throughout this book, starting with the first three steps—checking for systems that are live and for open ports and service identification—in the following section.

FIGURE 3.1 CEH scanning methodology



Ping Sweep Techniques

The CEH scanning methodology starts with checking for systems that are live on the network, meaning that they respond to probes or connection requests. The simplest, although not necessarily the most accurate, way to determine whether systems are live is to perform a *ping sweep* of the IP address range. All systems that respond with a ping reply are considered live on the network. A ping sweep is also known as Internet Control Message Protocol (ICMP) scanning, as ICMP is the protocol used by the `ping` command.

ICMP scanning, or a ping sweep, is the process of sending an ICMP request or ping to all hosts on the network to determine which ones are up and responding to pings. ICMP began as a protocol used to send test and error messages between hosts on the Internet. It has evolved as a protocol utilized by every operating system, router, switch or Internet Protocol (IP)-based device. The ability to use the ICMP Echo request and Echo reply as a connectivity test between hosts is built into every IP-enabled device via the `ping` command. It is a quick and dirty test to see if two hosts have connectivity and is used extensively for troubleshooting.

A benefit of ICMP scanning is that it can be run in *parallel*, meaning all systems are scanned at the same time; thus it can run quickly on an entire network. Most hacking tools include a ping sweep option, which essentially means performing an ICMP request to every host on the network. Systems that respond with a ping response are alive and listening on the network. Exercise 3.1 shows how to perform a ping sweep using built-in windows tools.

One considerable problem with this method is that personal firewall software and network-based firewalls can block a system from responding to ping sweeps. More and more systems are configured with firewall software and will block the ping attempt and notify the user that a scanning program is running on the network. Another problem is that the computer must be on to be scanned.



Real World Scenario

Indications of a Scanning Attack

Bob is working on his laptop while connected on a business trip away from the office. He is using the hotel's free wireless Internet access from his computer. As he is sending an email he notices a pop-up window on the system tray of his Windows XP computer. It says "Windows has detected and blocked an intrusion attempt to your computer." He just closes the pop-up window and goes back to finish writing his email. He then notices another pop-up window with a similar message. He begins to get concerned that his computer is being hacked. He decides to shut down his laptop so that no other connection attempts can be made to his computer.

Hacking Tools

Pinger, Friendly Pinger, and WS_Ping_Pro are all tools that perform ICMP queries. You should be familiar with all these tools for the exam.

EXERCISE 3.1

Using a Windows Ping

To use the built-in ping command in Windows to test connectivity to another system:

1. Open a command prompt in Windows.
2. Type **ping www.microsoft.com**.

```
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\kimberly>ping www.microsoft.com

Pinging lbf.wsu.ne.akadnc.net [207.46.19.198] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 207.46.19.198:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

A timeout indicates that the remote system is not responding or turned off or that the ping was blocked. A reply indicates that the system is alive and responding to ICMP requests.

Detecting Ping Sweeps

Almost any IDS or intrusion prevention system (IPS) system will detect and alert the security administrator to a ping sweep occurring on the network. Most firewall and proxy servers block ping responses so a hacker can't accurately determine whether systems are available using a ping sweep alone. More intense port scanning must be used if systems don't respond to a ping sweep. Just because a ping sweep doesn't return any active hosts on the network doesn't mean they aren't available—you need to try an alternate method of identification. Remember, hacking takes time, patience, and persistence.

Scanning Ports and Identifying Services

Checking for open ports is the second step in the CEH scanning methodology. *Port scanning* is the method used to check for open ports. The process of port scanning involves probing each port on a host to determine which ports are open. Port scanning generally yields more valuable information than a ping sweep about the host and vulnerabilities on the system.

Service identification is the third step in the CEH scanning methodology; it's usually performed using the same tools as port scanning. By identifying open ports, a hacker can usually also identify the services associated with that port number. Remember the well-known port numbers discussed earlier in this chapter.

Port-Scan Countermeasures

Countermeasures are processes or toolsets used by security administrators to detect and possibly thwart port scanning of hosts on their network. The following list of countermeasures should be implemented to prevent a hacker from acquiring information during a port scan:

- Proper security architecture, such as implementation of IDS and firewalls, should be followed.
- Ethical hackers use their toolset to test the scanning countermeasures that have been implemented. Once a firewall is in place, a port-scanning tool should be run against hosts on the network to determine whether the firewall correctly detects and stops the port-scanning activity.
- The firewall should be able to detect the probes sent by port-scanning tools. The firewall should carry out *stateful inspections*, which means it examines the data of the packet and not just the TCP header to determine whether the traffic is allowed to pass through the firewall.
- Network IDS should be used to identify the OS-detection method used by some common hackers tools.
- Only needed ports should be kept open. The rest should be filtered or blocked.
- The staff of the organization using the systems should be given appropriate training on security awareness. They should also know the various security policies they're required to follow.

nmap Command Switches

Nmap is a free, open source tool that quickly and efficiently performs ping sweeps, port scanning, service identification, IP address detection, and operating system detection. Nmap has the benefit of scanning a large number of machines in a single session. It's supported by many operating systems, including Unix, Windows, and Linux.

The state of the port as determined by an nmap scan can be open, filtered, or unfiltered. *Open* means that the target machine accepts incoming request on that port. *Filtered* means a firewall or network filter is screening the port and preventing nmap from discovering whether it's open. *Unfiltered* mean the port is determined to be closed, and no firewall or filter is interfering with the nmap requests.

Nmap supports several types of scans. Table 3.2 details some of the common scan methods.

TABLE 3.2 Nmap scan types

Nmap scan type	Description
TCP connect	The attacker makes a full TCP connection to the target system. The most reliable scan type but also the most detectable. Open ports reply with a SYN/ACK while closed ports reply with a RST/ACK.
XMAS tree scan	The attacker checks for TCP services by sending XMAS-tree packets, which are named as such because all the “lights” are on, meaning the FIN, URG, and PSH flags are set (the meaning of the flags will be discussed later in this chapter). Closed ports reply with a RST flag.
SYN stealth scan	This is also known as <i>half-open scanning</i> . The hacker sends a SYN packet and receives a SYN-ACK back from the server. It’s stealthy because a full TCP connection isn’t opened. Open ports reply with a SYN/ACK while closed ports reply with a RST/ACK.
Null scan	This is an advanced scan that may be able to pass through firewalls undetected or modified. Null scan has all flags off or not set. It only works on Unix systems. Closed ports will return a RST flag.
Windows scan	This type of scan is similar to the ACK scan and can also detect open ports.
ACK scan	This type of scan is used to map out firewall rules. ACK scan only works on Unix. The port is considered filtered by firewall rules if an ICMP destination unreachable message is received as a result of the ACK scan.

The nmap command has numerous switches to perform different types of scans. The common command switches are listed in Table 3.3.

TABLE 3.3 Common nmap command switches

nmap command switch	Scan performed
-sT	TCP connect scan
-sS	SYN scan
-sF	FIN scan
-sX	XMAS tree scan
-sN	Null scan
-sP	Ping scan
-sU	UDP scan

TABLE 3.3 Common nmap command switches (*continued*)

nmap command switch	Scan performed
-sO	Protocol scan
-sA	ACK scan
-sW	Windows scan
-sR	RPC scan
-sL	List/DNS scan
-sI	Idle scan
-Po	Don't ping
-PT	TCP ping
-PS	SYN ping
-PI	ICMP ping
-PB	TCP and ICMP ping
-PB	ICMP timestamp
-PM	ICMP netmask
-oN	Normal output
-oX	XML output
-oG	Greppable output
-oA	All output
-T Paranoid	Serial scan; 300 sec between scans
-T Sneaky	Serial scan; 15 sec between scans
-T Polite	Serial scan; .4 sec between scans
-T Normal	Parallel scan
-T Aggressive	Parallel scan, 300 sec timeout, and 1.25 sec/probe
-T Insane	Parallel scan, 75 sec timeout, and .3 sec/probe

To perform an nmap scan, at the Windows command prompt type **Nmap IPaddress** followed by any command switches used to perform specific type of scans. For example, to scan the host with the IP address 192.168.0.1 using a TCP connect scan type, enter this command:

```
Nmap 192.168.0.1 -sT
```



Make sure you're familiar with the different types of nmap scans, the syntax to run nmap, and how to analyze nmap results. The syntax and switches used by the nmap command will be tested on the CEH exam.

Scan Types

As a CEH, you need to be familiar with the following scan types and uses:

SYN A SYN or stealth scan is also called a half-open scan because it doesn't complete the TCP three-way handshake. (The TCP/IP three-way handshake will be covered in the next section.) A hacker sends a SYN packet to the target; if a SYN/ACK frame is received back, then it's assumed the target would complete the connect and the port is listening. If an RST is received back from the target, then it's assumed the port isn't active or is closed. The advantage of the SYN stealth scan is that fewer IDS systems log this as an attack or connection attempt.

XMAS XMAS scans send a packet with the FIN, URG, and PSF flags set. If the port is open, there is no response; but if the port is closed, the target responds with a RST/ACK packet. XMAS scans work only on target systems that follow the RFC 793 implementation of TCP/IP and don't work against any version of Windows.

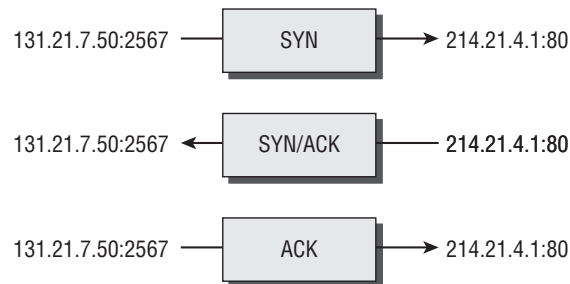
FIN A FIN scan is similar to an XMAS scan but sends a packet with just the FIN flag set. FIN scans receive the same response and have the same limitations as XMAS scans.

NULL A NULL scan is also similar to XMAS and FIN in its limitations and response, but it just sends a packet with no flags set.

IDLE An IDLE scan uses a spoofed IP address to send a SYN packet to a target. Depending on the response, the port can be determined to be open or closed. IDLE scans determine port scan response by monitoring IP header sequence numbers.

TCP Communication Flag Types

TCP scan types are built on the *TCP three-way handshake*. TCP connections require a three-way handshake before a connection can be made and data transferred between the sender and receiver. Figure 3.2 details the steps of the TCP three-way handshake.

FIGURE 3.2 TCP three-way handshake

To complete the three-way handshake and make a successful connection between two hosts, the sender must send a TCP packet with the synchronize (SYN) bit set. Then, the receiving system responds with a TCP packet with the synchronize (SYN) and acknowledge (ACK) bit set to indicate the host is ready to receive data. The source system sends a final packet with the ACK bit set to indicate the connection is complete and data is ready to be sent.

Because TCP is a connection-oriented protocol, a process for establishing a connection (three-way handshake), restarting a failed connection, and finishing a connection is part of the protocol. These protocol notifications are called *flags*. TCP contains ACK, RST, SYN, URG, PSH, and FIN flags. The following list identifies the function of the TCP flags:

SYN Synchronize. Initiates a connection between hosts.

ACK Acknowledge. Established connection between hosts.

PSH Push. System is forwarding buffered data.

URG Urgent. Data in packets must be processed quickly.

FIN Finish. No more transmissions.

RST Reset. Resets the connection.

A hacker can attempt to bypass detection by using flags instead of completing a normal TCP connection. The TCP scan types in Table 3.4 are used by some scanning tools to elicit a response from a system by setting one or more flags.

TABLE 3.4 TCP scan types

XMAS scan	Flags sent by hacker
XMAS scan	All flags set (ACK, RST, SYN, URG, PSH, FIN)
FIN scan	FIN
NULL scan	No flags set

TABLE 3.4 TCP scan types (*continued*)

XMAS scan	Flags sent by hacker
TCP connect/full-open scan	SYN, then ACK
SYN scan / half-open scan	SYN, then RST

Hacking Tools

IPEye is a TCP port scanner that can do SYN, FIN, Null, and XMAS scans. It's a command-line tool.

IPEye probes the ports on a target system and responds with closed, reject, drop, or open. Closed means there is a computer on the other end, but it doesn't listen at the port. Reject means a firewall is rejecting the connection to the port (sending a reset back). Drop means a firewall is dropping everything to the port, or there is no computer on the other end. Open means some kind of service is listening at the port. These responses help a hacker identify what type of system is responding.

IPSecScan is a tool that can scan either a single IP address or a range of addresses looking for systems that are IPSec enabled.

NetScan Tools Pro, hping2, KingPingicmpenum, and SNMP Scanner are all scanning tools and can also be used to fingerprint the operating system (discussed later).

Icmpenum uses not only ICMP Echo packets to probe networks, but also ICMP Timestamp and ICMP Information packets. Furthermore, it supports spoofing and sniffing for reply packets. Icmpenum is great for scanning networks when the firewall blocks ICMP Echo packets but fails to block Timestamp or Information packets.

The hping2 tool is notable because it contains a host of other features besides OS fingerprinting such as TCP, User Datagram Protocol (UDP), ICMP, and raw-IP ping protocols, traceroute mode, and the ability to send files between the source and target system.

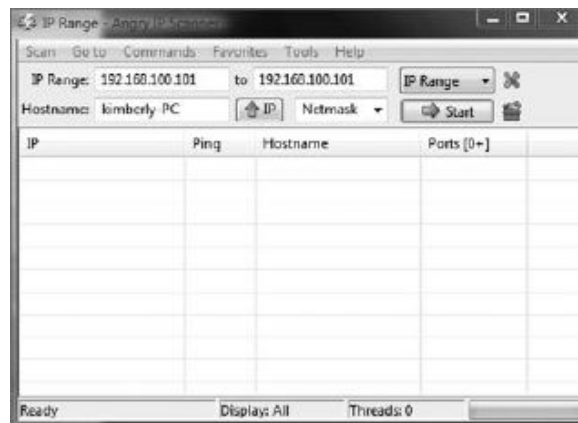
SNMP Scanner allows you to scan a range or list of hosts performing ping, DNS, and Simple Network Management Protocol (SNMP) queries.

Exercise 3.2 shows how to use AngryIP scanner to perform a port scan.

EXERCISE 3.2**Free IPTools Port Scan**

To use a port scan tool to determine listening ports of active hosts:

1. Download Angry IP Scanner from www.angryip.org/w/Download.
2. Enter the IP address of the target system in the Host or IP Address field or enter a range or IP address for your lab systems and click Start to perform a conventional (full connect) scan of standard ports.

**War-Dialing Techniques**

War dialing is the process of dialing modem numbers to find an open modem connection that provides remote access to a network for an attack to be launched against the target system. The term *war dialing* originates from the early days of the Internet when most companies were connected to the Internet via dial-up modem connections. War dialing is included as a scanning method because it finds another network connection that may have weaker security than the main Internet connection. Many organizations set up remote-access modems that are now antiquated but have failed to remove those remote-access servers. This gives hackers an easy way into the network with much weaker security mechanisms. For example, many remote-access systems use the Password Authentication Protocol (PAP), which send passwords in cleartext, rather than newer virtual private networking (VPN) technology that encrypts passwords.

War-dialing tools work on the premise that companies don't control the dial-in ports as strictly as the firewall, and machines with modems attached are present everywhere even if those modems are no longer in use. Many servers still have modems with phone lines connected as a backup in case the primary Internet connection fails. These available modem

connections can be used by a war-dialing program to gain remote access to the system and internal network.



Real World Scenario

Using a Forgotten Modem Connection for War Dialing

I was performing a network security audit for a financial services firm a few years ago. They asked me to do a walkthrough of the site for the purposes of a physical security audit. As I was passing one of the desks in the marketing department I noticed a phone line coming out from around the desk and connecting to a wall jack. I asked about the use of modems as I was trying to ascertain the reason for the phone line cable. I was told that they used to use dial-up on some of the computers for Internet access but that two years ago they switched to a high-speed T1 connection for the entire office. As we explored further, it was revealed that the employee who used that computer still used AOL on the dial-up connection to check her personal email account. Quite surprising to everyone, when the new Internet connection was installed no one ever checked to ensure all the dial-up connections were removed. Here is a prime example of why war dialing still works in some cases.

Hacking Tools

THC-Scan, PhoneSweep, and TeleSweep are tools that identify phone numbers and can dial a target to make a connection with a computer modem. These tools generally work by using a predetermined list of common usernames and passwords in an attempt to gain access to the system. Most remote-access dial-in connections aren't secured with a password or use very rudimentary security.

Banner Grabbing and OS Fingerprinting Techniques

Banner grabbing and operating system identification—which can also be defined as *fingerprinting* the TCP/IP stack—is the fourth step in the CEH scanning methodology. The process of fingerprinting allows the hacker to identify particularly vulnerable or high-value targets on the network. Hackers are looking for the easiest way to gain access to a system or network. Banner grabbing is the process of opening a connection and reading the banner or response sent by the application. Many email, FTP, and web servers will respond to a telnet connection with the name and version of the software. This aids a hacker in fingerprinting

the OS and application software. For example, a Microsoft Exchange email server would only be installed on a Windows OS.

Active stack fingerprinting is the most common form of fingerprinting. It involves sending data to a system to see how the system responds. It's based on the fact that various operating system vendors implement the TCP stack differently, and responses will differ based on the operating system. The responses are then compared to a database to determine the operating system. Active stack fingerprinting is detectable because it repeatedly attempts to connect with the same target system.

Passive stack fingerprinting is stealthier and involves examining traffic on the network to determine the operating system. It uses sniffing techniques instead of scanning techniques. Passive stack fingerprinting usually goes undetected by an IDS or other security system but is less accurate than active fingerprinting.

Drawing Network Diagrams of Vulnerable Hosts

Although it isn't a CEH exam objective, understanding the tools used in step 6 of the CEH scanning methodology—drawing a network diagram of vulnerable hosts—is a must. A number of network management tools can assist you with this step. Such tools are generally used to manage network devices but can be turned against security administrators by enterprising hackers.

SolarWinds Toolset, Queso, Harris Stat, and Cheops are network management tools that can be used for detecting operating systems, mapping network diagrams, listing services running on a network, performing generalized port scanning, and so on.

These tools diagram entire networks in a GUI interface, including routers, servers, hosts, and firewalls. Most of these tools can discover IP addresses, hostnames, services, operating systems, and version information.

Netcraft and HTTrack are tools that fingerprint an operating system. Both are used to determine the OS and web server software version numbers.

Netcraft is a website that periodically polls web servers to determine the operating system version and the web server software version. Netcraft can provide useful information the hacker can use in identifying vulnerabilities in the web server software. In addition, Netcraft has an antiphishing toolbar and web server verification tool you can use to make sure you're using the actual web server rather than a spoofed web server. Exercise 3.3 shows how to use Netcraft to identify the OS or a web server.

HTTrack arranges the original site's relative link structure. You open a page of the mirrored website in your browser, and then you can browse the site from link to link as if you were viewing it online. HTTrack can also update an existing mirrored site and resume interrupted downloads.

EXERCISE 3.3**Use Netcraft to Identify the OS of a Web Server**

1. Open a web browser to the Netcraft website, www.netcraft.com.



2. Type a website name in the What's That Site Running? field in the upper-left corner of the screen.
3. Scroll down to Hosting History to see what OS and web server software are running on the server.

Scanning Anonymously

Preparing proxy servers is the last step in the CEH scanning methodology. A *proxy server* is a computer that acts as an intermediary between the hacker and the target computer.

Using a proxy server can allow a hacker to become anonymous on the network. The hacker first makes a connection to the proxy server and then requests a connection to the target computer via the existing connection to the proxy. Essentially, the proxy requests access to the target computer, not the hacker's computer. This lets a hacker surf the Web anonymously or otherwise hide their attack.

Hacking Tools

SocksChain is a tool that gives a hacker the ability to attack through a chain of proxy servers. The main purpose of doing this is to hide the hacker's real IP address and therefore minimize the chance of detection. When a hacker works through several proxy servers in series, it's much harder to locate the hacker. Tracking the attacker's IP address through the logs of several proxy servers is complex and tedious work. If one of the proxy servers' log files is lost or incomplete, the chain is broken, and the hacker's IP address remains anonymous.

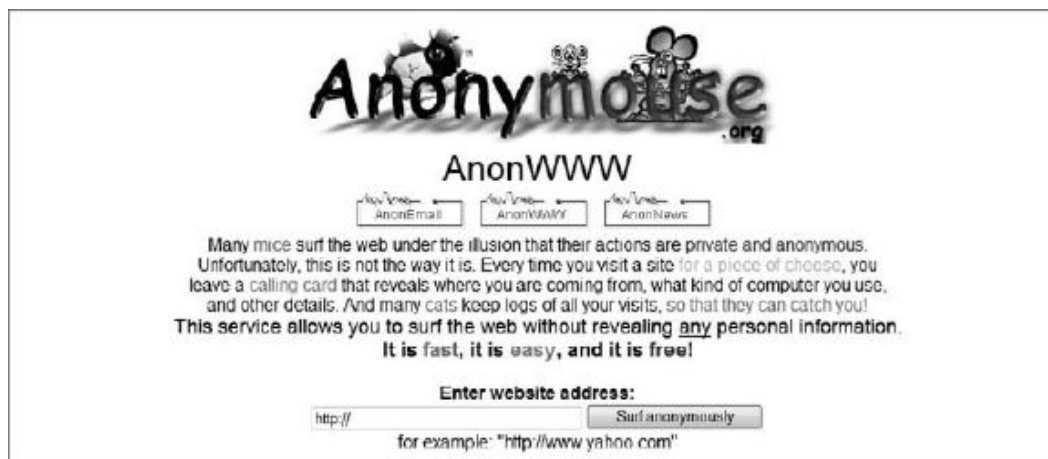
Anonymizers are services that attempt to make web surfing anonymous by utilizing a website that acts as a proxy server for the web client. The first anonymizer software tool was developed by Anonymizer.com; it was created in 1997 by Lance Cottrell. The anonymizer removes all the identifying information from a user's computers while the user surfs the Internet, thereby ensuring the privacy of the user.

To visit a website anonymously, the hacker enters the website address into the anonymizer software, and the anonymizer software makes the request to the selected site. All requests and web pages are relayed through the anonymizer site, making it difficult to track the actual requester of the web page. Use Anonymouse to web surf anonymously in Exercise 3.4.

EXERCISE 3.4

Use Anonymouse to Surf Websites Anonymously

1. Open a web browser to the <http://anonymouse.org> website and select English at the top of the page.



2. Type a website address in the Enter Website Address field and click the Surf Anonymously button.

This works especially well if you know certain websites are blocked.

A popular method of bypassing a firewall or IDS is to tunnel a blocked protocol (such as SMTP) through an allowed protocol (such as HTTP). Almost all IDS and firewalls act as a proxy between a client's PC and the Internet and pass only the traffic defined as being allowed.

Most companies allow HTTP traffic because it's usually benign web access. However, a hacker using an HTTP tunneling tool can subvert the proxy by hiding potentially destructive protocols, such as IM or chat, within an innocent-looking protocol packet.

Hacking Tools

HTTPPort, TunnelD, and BackStealth are tools to tunnel traffic through HTTP. They allow the bypassing of an HTTP proxy, which blocks certain protocols from accessing the Internet. These tools allow the following potentially dangerous software protocols to be used from behind an HTTP proxy:

- Email
- IRC
- ICQ
- News
- AIM
- FTP

A hacker can *spoof* an IP address when scanning target systems to minimize the chance of detection. One drawback of spoofing an IP address is that a TCP session can't be successfully completed.

Source routing lets an attacker specify the route that a packet takes through the Internet. This can also minimize the chance of detection by bypassing IDS and firewalls that may block or detect the attack. Source routing uses a reply address in the IP header to return the packet to a spoofed address instead of the attacker's real address. The use of source routing to bypass an IDS will be covered in more detail in Chapter 13, "Evading IDSs, Honeypots, and Firewalls."

To detect IP address spoofing, you can compare the time to live (TTL) values: the attacker's TTL will be different from the spoofed address's real TTL.

Enumeration

Enumeration occurs after scanning and is the process of gathering and compiling usernames, machine names, network resources, shares, and services. It also refers to actively querying or connecting to a target system to acquire this information.

Hackers need to be methodical in their approach to hacking. The following steps are an example of those a hacker might perform in preparation for hacking a target system:

1. Extract usernames using enumeration.
2. Gather information about the host using null sessions.
3. Perform Windows enumeration using the SuperScan tool.
4. Acquire the user accounts using the tool GetAcct.
5. Perform SNMP port scanning.

The object of enumeration is to identify a user account or system account for potential use in hacking the target system. It isn't necessary to find a system administrator account, because most account privileges can be escalated to allow the account more access than was previously granted.



The process of privilege escalation is covered in the next chapter.

Many hacking tools are designed for scanning IP networks to locate NetBIOS name information. For each responding host, the tools list IP address, NetBIOS computer name, logged-in username, and MAC address information.

On a Windows 2000 domain, the built-in tool `net view` can be used for NetBIOS enumeration. To enumerate NetBIOS names using the `net view` command, enter the following at the command prompt:

```
net view / domain
nbtstat -A IP address
```

Hacking Tools

DumpSec is a NetBIOS enumeration tool. It connects to the target system as a null user with the `net use` command. It then enumerates users, groups, NTFS permissions, and file ownership information.

Hyena is a tool that enumerates NetBIOS shares and additionally can exploit the null session vulnerability to connect to the target system and change the share path or edit the Registry.

The SMB Auditing Tool is a password-auditing tool for the Windows and Server Message Block (SMB) platforms. Windows uses SMB to communicate between the client and server. The SMB Auditing Tool is able to identify usernames and crack passwords on Windows systems.

The NetBIOS Auditing Tool is another NetBIOS enumeration tool. It's used to perform various security checks on remote servers running NetBIOS file sharing services.

Null Sessions

A null session occurs when you log in to a system with no username or password. NetBIOS null sessions are a vulnerability found in the Common Internet File System (CIFS) or SMB, depending on the operating system.



Microsoft Windows uses SMB, and Unix/Linux systems use CIFS.

Once a hacker has made a NetBIOS connection using a null session to a system, they can easily get a full dump of all usernames, groups, shares, permissions, policies, services, and more using the Null user account. The SMB and NetBIOS standards in Windows include APIs that return information about a system via TCP port 139.

One method of connecting a NetBIOS null session to a Windows system is to use the hidden Inter-Process Communication share (IPC\$). This hidden share is accessible using the `net use` command. As mentioned earlier, the `net use` command is a built-in Windows command that connects to a share on another computer. The empty quotation marks ("") indicate that you want to connect with no username and no password. To make a NetBIOS null session to a system with the IP address 192.21.7.1 with the built-in anonymous user account and a null password using the `net use` command, the syntax is as follows:

```
C: \> net use \\192.21.7.1 \IPC$ "" /u: ""
```

Once the `net use` command has been successfully completed, the hacker has a channel over which to use other hacking tools and techniques.

As a CEH, you need to know how to defend against NetBIOS enumeration and null sessions. We'll discuss that in the following section.

NetBIOS Enumeration and Null Session Countermeasures

The NetBIOS null session uses specific port numbers on the target machine. Null sessions require access to TCP ports 135, 137, 139, and/or 445. One countermeasure is to close these ports on the target system. This can be accomplished by disabling SMB services on individual hosts by unbinding the TCP/IP WINS client from the interface in the network connection's properties. To implement this countermeasure, perform the following steps:

1. Open the properties of the network connection.
2. Click TCP/IP and then the Properties button.
3. Click the Advanced button.
4. On the WINS tab, select **Disable NetBIOS Over TCP/IP**.

A security administrator can also edit the Registry directly to restrict the anonymous user from login. To implement this countermeasure, follow these steps:

1. Open `regedt32` and navigate to `HKLM\SYSTEM\CurrentControlSet\LSA`.
2. Choose **Edit** ➔ **Add Value**. Enter these values:
 - Value Name: **RestrictAnonymous**
 - Data Type: **REG_WORD**
 - Value: **2**

Finally, the system can be upgraded to Windows XP and the latest Microsoft security patches, which mitigates the NetBIOS null session vulnerability from occurring.

SNMP Enumeration

SNMP enumeration is the process of using SNMP to enumerate user accounts on a target system. SNMP employs two major types of software components for communication: the SNMP agent, which is located on the networking device, and the SNMP management station, which communicates with the agent.

Almost all network infrastructure devices, such as routers and switches and including Windows systems, contain an SNMP agent to manage the system or device. The SNMP management station sends requests to agents, and the agents send back replies. The requests and replies refer to configuration variables accessible by agent software. Management stations can also send requests to set values for certain variables. Traps let the management station know that something significant has happened in the agent software, such as a reboot or an interface failure. Management Information Base (MIB) is the database of configuration variables that resides on the networking device.

SNMP has two passwords you can use to access and configure the SNMP agent from the management station. The first is called a *read community string*. This password lets you view the configuration of the device or system. The second is called the *read/write community string*; it's for changing or editing the configuration on the device. Generally, the default read community string is public and the default read/write community string is private. A common security loophole occurs when the community strings are left at the default settings: a hacker can use these default passwords to view or change the device configuration.



If you have any questions about how easy it is to locate the default passwords of devices, look at the website www.defaultpassword.com.

Hacking Tools

SNMPUtil and IP Network Browser are SNMP enumeration tools.

SNMPUtil gathers Windows user account information via SNMP in Windows systems. Some information—such as routing tables, ARP tables, IP addresses, MAC addresses, TCP and UDP open ports, user accounts, and shares—can be read from a Windows system that has SNMP enabled using the SNMPUtil tools.

IP Network Browser from the SolarWinds Toolset also uses SNMP to gather more information about a device that has an SNMP agent.

SNMP Enumeration Countermeasures

The simplest way to prevent SNMP enumeration is to remove the SNMP agent on the potential target systems or turn off the SNMP service. If shutting off SNMP isn't an option, then change the default read and read/write community names.

In addition, an administrator can implement the Group Policy security option Additional Restrictions For Anonymous Connections, which restricts SNMP connections.



Group Policy is implemented on a Windows domain controller. Network administrators should be familiar with how to do this. It's outside the scope of this book, because many steps are involved in performing this task.

Windows 2000 DNS Zone Transfer

In a Windows 2000 domain, clients use service (SRV) records to locate Windows 2000 domain services, such as Active Directory and Kerberos. This means every Windows 2000 Active Directory domain must have a DNS server for the network to operate properly.

A simple zone transfer performed with the `nslookup` command can enumerate lots of interesting network information. The command to enumerate using the `nslookup` command is as follows:

```
nslookup ls -d domainname
```

Within the `nslookup` results, a hacker looks closely at the following records, because they provide additional information about the network services:

- Global Catalog service (`_gc._tcp_`)
- Domain controllers (`_ldap._tcp`)
- Kerberos authentication (`_kerberos._tcp`)

As a countermeasure, zone transfers can be blocked in the properties of the Windows DNS server.

An Active Directory database is a Lightweight Directory Access Protocol (LDAP)-based database. This allows the existing users and groups in the database to be enumerated with a simple LDAP query. The only thing required to perform this enumeration is to create an authenticated session via LDAP. A Windows 2000 LDAP client called the Active Directory Administration Tool (`ldp.exe`) connects to an Active Directory server and identifies the contents of the database. You can find `ldp.exe` on the Windows 2000 CD-ROM in the `Support\Reskit\Netmgmt\Dstool` folder.

To perform an Active Directory enumeration attack, a hacker performs the following steps:

1. Connect to any Active Directory server using `ldp.exe` on port 389. When the connection is complete, server information is displayed in the right pane.
2. On the Connection menu, choose Authenticate. Type the username, password, and domain name in the appropriate boxes. You can use the Guest account or any other domain account.

3. Once the authentication is successful, enumerate users and built-in groups by choosing the Search option from the Browse menu.

Hacking Tools

User2SID and SID2User are command-line tools that look up Windows service identifiers (SIDs from username input and vice versa).

Enum is a command-line enumeration utility. It uses null sessions and can retrieve usernames, machine names, shares, group and membership lists, passwords, and Local Security policy information. Enum is also capable of brute-force dictionary attacks on individual accounts.

UserInfo is a command-line tool that's used to gather usernames and that can also be used to create new user accounts.

GetAcct is a GUI-based tool that enumerates user accounts on a system.

SMBBF is a SMB brute-force tool that tries to determine user accounts and accounts with blank passwords.

Summary

Scanning and enumeration are the next steps in the hacking process after the information-gathering phase has been completed. Scanning and enumeration tools are most often active information-gathering tools and therefore allow the hacker to be detected. For this reason, many tools and techniques exist to minimize the opportunity for detection and reduce the chance of the hacker being identified.

It is during the scanning and enumeration phase that information about the host and target network is discovered. As a next step, the host and network information enumerated will be used to begin to hack the target system or network. The next chapter will focus on system hacking and gaining access to a target system.

Exam Essentials

Know the three types of scanning and scanning countermeasures. Port, network, and vulnerability scanning are the three types of scanning. Implement firewalls that prevent internal systems from being scanned by blocking ping sweeps and port-scanning tools such as nmap. IDSs and IPSs can alert an administrator to a scan taking place on the network.

Know how to determine which systems are alive on the network. Know how to use ICMP query tools to perform ping sweeps to determine which systems are responding. Ping sweeps have limitations, and some systems may not respond to the ICMP queries.

Know how to perform port scanning using nmap. Learn the switches for performing nmap scanning using the nmap command. For example, `nmap -sS` performs a SYN scan.

Understand the uses and limitations of different scan types. Make sure you're familiar with TCP connect, SYN, NULL, IDLE, FIN, and XMAS scans and when each type should be used.

Understand the process of the TCP three-way handshake. The TCP connection process starts with a SYN packet sent to the target system. The target system responds with a SYN+ACK packet, and the source system sends back an ACK packet to the target. This completes a successful TCP connection.

Know the uses of war dialing. War dialing is used to test dial-in remote access system security. Phone numbers are dialed randomly in an attempt to make an unsecured modem connection and gain access to the network.

Understand how to perform operating system fingerprinting using active and passive methods. Active fingerprinting means sending a request to a system to see how it responds (banner grabbing, for example). Passive fingerprinting is examining traffic sent to and from the system to determine the operating system.

Know how to become anonymous using an anonymizer, HTTP tunneling, and IP spoofing. Use a website anonymizer to hide the source address to make the system surfing the Web appear anonymous. HTTP tunneling and IP spoofing are two methods of hiding the physical address or protocols that a hacker may be using. They're useful in evading firewalls and obfuscating the hacker's identity or whereabouts.

Understand how to enumerate user accounts. Enumeration involves making active connections to systems through either SMB/CIFS or NetBIOS vulnerabilities and querying the system for information.

Be aware of the type of information that can be enumerated on a system and enumeration countermeasures. The type of information enumerated by hackers includes network resources and shares, users and groups, and applications and banners. Use a firewall to block ports 135 and 139, or patch the Registry to prevent null sessions. Turn off the SNMP services, or change the default read and read/write community names.

Understand null sessions. Connecting to a system using a blank password is known as a null session. Null sessions are often used by hackers to connect to target systems and then run enumeration tools against the system.

Know the types of enumeration tools and how to identify vulnerable accounts. NetBIOS and SNMP enumerations can be performed using tools such as SNMPUtil and Enum. Tools such as User2SID, SID2User, and UserInfo can be used to identify vulnerable user accounts.

Know how to perform a DNS zone transfer on Windows 2000 computers. NSlookup can be used to perform a DNS zone transfer.

Review Questions

1. What port number does FTP use?
 - A. 21
 - B. 25
 - C. 23
 - D. 80
2. What port number does HTTPS use?
 - A. 443
 - B. 80
 - C. 53
 - D. 21
3. What is war dialing used for?
 - A. Testing firewall security
 - B. Testing remote access system security
 - C. Configuring a proxy filtering gateway
 - D. Configuring a firewall
4. Banner grabbing is an example of what?
 - A. Passive operating system fingerprinting
 - B. Active operating system fingerprinting
 - C. Footprinting
 - D. Application analysis
5. What are the three types of scanning?
 - A. Port, network, and vulnerability
 - B. Port, network, and services
 - C. Grey, black, and white hat
 - D. Server, client, and network
6. What is the main problem with using only ICMP queries for scanning?
 - A. The port is not always available.
 - B. The protocol is unreliable.
 - C. Systems may not respond because of a firewall.
 - D. Systems may not have the service running.

7. What does the TCP RST command do?
 - A. Starts a TCP connection
 - B. Restores the connection to a previous state
 - C. Finishes a TCP connection
 - D. Resets the TCP connection
8. What is the proper sequence of a TCP connection?
 - A. SYN-SYN-ACK-ACK
 - B. SYN-ACK-FIN
 - C. SYN-SYNACK-ACK
 - D. SYN-PSH-ACK
9. A packet with all flags set is which type of scan?
 - A. Full Open
 - B. Syn scan
 - C. XMAS
 - D. TCP connect
10. What is the proper command to perform an nmap SYN scan every 5 minutes?
 - A. `nmap -ss - paranoid`
 - B. `nmap -sS -paranoid`
 - C. `nmap -sS -fast`
 - D. `namp -sS -sneaky`
11. To prevent a hacker from using SMB session hijacking, which TCP and UDP ports would you block at the firewall?
 - A. 167 and 137
 - B. 80 and 23
 - C. 139 and 445
 - D. 1277 and 1270
12. Why would an attacker want to perform a scan on port 137?
 - A. To locate the FTP service on the target host
 - B. To check for file and print sharing on Windows systems
 - C. To discover proxy servers on a network
 - D. To discover a target system with the NetBIOS null session vulnerability

- 13.** SNMP is a protocol used to manage network infrastructure devices. What is the SNMP read/write community name used for?
- A.** Viewing the configuration information
 - B.** Changing the configuration information
 - C.** Monitoring the device for errors
 - D.** Controlling the SNMP management station
- 14.** Why would the network security team be concerned about ports 135–139 being open on a system?
- A.** SMB is enabled, and the system is susceptible to null sessions.
 - B.** SMB is not enabled, and the system is susceptible to null sessions.
 - C.** Windows RPC is enabled, and the system is susceptible to Windows DCOM remote sessions.
 - D.** Windows RPC is not enabled, and the system is susceptible to Windows DCOM remote sessions.
- 15.** Which step comes after enumerating users in the CEH hacking cycle?
- A.** Crack password
 - B.** Escalate privileges
 - C.** Scan
 - D.** Cover tracks
- 16.** What is enumeration?
- A.** Identifying active systems on the network
 - B.** Cracking passwords
 - C.** Identifying users and machine names
 - D.** Identifying routers and firewalls
- 17.** What is a command-line tool used to look up a username from a SID?
- A.** UsertoSID
 - B.** Userenum
 - C.** SID2User
 - D.** GetAcct
- 18.** Which tool can be used to perform a DNS zone transfer on Windows?
- A.** NSlookup
 - B.** DNSlookup
 - C.** Whois
 - D.** IPconfig

- 19.** What is a null session?
- A.** Connecting to a system with the administrator username and password
 - B.** Connecting to a system with the admin username and password
 - C.** Connecting to a system with a random username and password
 - D.** Connecting to a system with no username and password
- 20.** What is a countermeasure for SNMP enumeration?
- A.** Remove the SNMP agent from the device.
 - B.** Shut down ports 135 and 139 at the firewall.
 - C.** Shut down ports 80 and 443 at the firewall.
 - D.** Enable SNMP read-only security on the agent device.

Answers to Review Questions

1. A. FTP uses TCP port 21. This is a well-known port number and can be found in the Windows Services file.
2. A. HTTPS uses TCP port 443. This is a well-known port number and can be found in the Windows Services file.
3. B. War dialing involves placing calls to a series of numbers in hopes that a modem will answer the call. It can be used to test the security of a remote-access system.
4. A. Banner grabbing is not detectable; therefore it is considered passive OS fingerprinting.
5. A. Port, network, and vulnerability are the three types of scanning.
6. C. Systems may not respond to ICMP because they have firewall software installed that blocks the responses.
7. D. The TCP RST command resets the TCP connection.
8. A. A SYN packet is followed by a SYN-ACK packet. Then, an ACK finishes a successful TCP connection.
9. C. An XMAS scan has all flags set.
10. B. The command `nmap -sS -paranoid` performs a SYN scan every 300 seconds, or 5 minutes.
11. C. Block the ports used by NetBIOS null sessions. These are 139 and 445.
12. D. Port 137 is used for NetBIOS null sessions.
13. B. The SNMP read/write community name is the password used to make changes to the device configuration.
14. A. Ports in the 135 to 139 range indicate the system has SMB services running and is susceptible to null sessions.
15. A. Password cracking is the next step in the CEH hacking cycle after enumerating users.
16. C. Enumeration is the process of finding usernames, machine names, network shares, and services on the network.
17. C. SID2User is a command-line tool that is used to find a username from a SID.
18. A. NSlookup is a Windows tool that can be used to initiate a DNS zone transfer that sends all the DNS records to a hacker's system.
19. D. A null session involves connecting to a system with no username and password.
20. A. The best countermeasure to SNMP enumeration is to remove the SNMP agent from the device. Doing so prevents it from responding to SNMP requests.

