CHAPTER 3

Footprinting and Scanning

This chapter helps you prepare for the EC-Council Certified Ethical Hacker (CEH) Exam by covering footprinting and scanning. A more detailed list of these items includes the following objectives:

Define the seven-step information gathering process

- The EC-Council divides information gathering into seven basic steps. These include gathering information, determining the network range, identifying active machines, finding open ports and access points, OS fingerprinting, fingerprinting services, and mapping the network.

Define footprinting

- The process of accumulating data regarding a specific network environment, usually for the purpose of finding ways to intrude into the environment.

Locate the network range

- Locating the network range is needed to know what addresses can be targeted and are available for additional scanning and analysis.

Identify active machines

- The identification of active machines is accomplished by means of ping sweeps and port scans. Both aid in an analysis of understanding if the machine is actively connected to the network and reachable.

Understand how to map open ports and identify their underlying applications

- Ports are tied to applications and, as such, can be registered, random, or dynamic.

Describe passive fingerprinting

- Passive fingerprinting is the act of identifying systems without injecting traffic or packets into the network.

State the various ways that active fingerprinting tools work

- Active fingerprinting tools inject strangely crafted packets into the network to measure how systems respond. Specific systems respond in unique ways.

Use tools such as Nmap to perform port scanning and know common Nmap switches

- Understanding Nmap switches is a required test element. Common switches include `-sT`, full connect, and `-sS`, a stealth scan.

Outline

Study Strategies

This chapter addresses information you need to know about footprinting and scanning. To gain a more in-depth understanding of these topics, readers should

- Understand the types of information leakage that organizations can suffer from and list ways to reduce this leakage.
- Review the type of information that a client organization has on its website, and consider how it can be used by a malicious hacker.
- Know the various types of scans such as full, stealth, Null, and Xmas tree. You should also review the various scanning tools, such as Nmap, and understand their operations.
- Be able to identify common ports that are associated with Windows computers.
- Explain why null sessions are a potential risk for the organization and how the risk can be reduced.

Introduction

This chapter introduces you to the two of the most important pre-attack phases: footprinting and scanning. Although these steps don't constitute breaking in, they occur at the point which a hacker will start to get interactive. The goal here is to discover what a hacker or other malicious user can uncover about the organization, its technical infrastructure, locations, employees, policies, security stance, and financial situation. Just as most hardened criminals don't just heist an armored car, elite hackers won't attack a network before they understand what they are up against. Even *script kiddies* can do some amount of pre-attack reconnaissance as they look for a target of opportunity.

This chapter starts off by looking at some general ways that individuals can attempt to gain information about an organization passively and without the organization's knowledge. Next, it gets interactive and reviews scanning techniques. The goal of scanning is to discover open ports and applications.

Determining Assessment Scope

What's the goal of the penetration (pen) test? Before starting any ethical hacking job, it's important that you determine the scope of the assignment. These kinds of details should have been worked out in the written agreement that specifies the scope of the engagement. Is the entire organization, a particular location, or one division to be examined, and will any subsidiaries be assessed? These are some questions that need to be answered up front before you begin any activity. Why is this mentioned here? Because you always want to make sure that you have legal written permission before you begin any footprinting or testing. Once an agreement is in place, there might still be logistical problems. *Scope creep* can be one of the biggest logistical problems you can face. Scope creep is the expansion of the assignment beyond its original specification. The client might want to expand the pen test beyond its original specifications; if so, make sure that the new requirements are added to the contract and that proper *written authorization* has been obtained.

The Seven-Step Information Gathering Process

Objectives:

Define the seven-step information gathering process

Define footprinting

Footprinting is about information gathering and is both passive and active. Reviewing the company's website is an example of passive footprinting, whereas calling the help desk and

attempting to social engineering them out of privileged information is an example of active information gathering. Scanning entails pinging machines, determining network ranges and port scanning individual systems. The EC-Council divides footprinting and scanning into seven basic steps. These include

1. Information gathering
2. Determining the network range
3. Identifying active machines
4. Finding open ports and access points
5. OS fingerprinting
6. Fingerprinting services
7. Mapping the network

Many times, students ask for a step-by-step method of information gathering. Realize that these are just general steps and that ethical hacking is really the process of discovery. Although the material in this book is covered in an ordered approach, real life sometimes varies. When performing these activities, you might find that you are led in a different direction than what you originally envisioned.

Information Gathering

The information gathering steps of footprinting and scanning are of utmost importance. Good information gathering can make the difference between a successful pen test and one that has failed to provide maximum benefit to the client. An amazing amount of information is available about most organizations in business today. This information can be found on the organization's website, trade papers, Usenet, financial databases, or even from disgruntled employees. Some potential sources are discussed, but first, let's review documentation.

Documentation

One important aspect of information gathering is documentation. Most people don't like paperwork, but it's a requirement that can't be ignored. The best way to get off to a good start is to develop a systematic method to profile a target and record the results. Create a matrix with fields to record domain name, IP address, DNS servers, employee information, email addresses, IP address range, open ports, and banner details. Figure 3.1 gives an example of what your *information matrix* might look like when you start the documentation process.

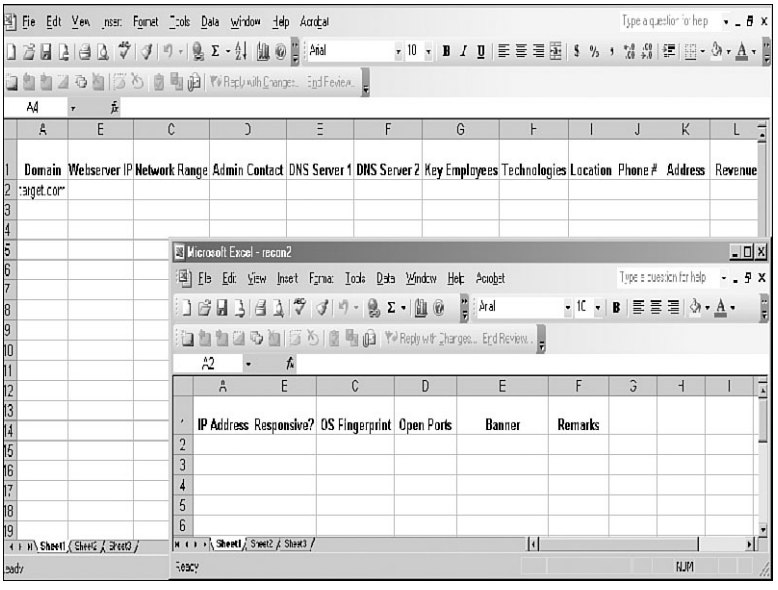

FIGURE 3.1
Documentation finding.

Building this type of information early on will help in mapping the network and planning the best method of attack.

The Organization's Website

With the initial documentation out of the way, it's time to get started. The best place to begin is the organization's website. You want to look for *open source* information, which is information freely provided to clients, customers, or the general public. Let's look at an example of a local web hosting company. A quick review of its site shows it has a news and updates section. Recent news states the following:

"We are proud to have just updated all of our Cobalt servers to Plesk7 Virtual Site Servers. Anyone logging in to these new servers as admin should use the username of the domain, for example, www.xyz.com. The passwords have been transferred from the old servers, so no password reset should be required. We used the existing domain administrator password. Our continued alliance with Enterasys has allowed us to complete our transition from Cisco equipment. These upgrades, along with our addition of a third connection to the Internet, give us a high degree of fault tolerance."

You might consider this good marketing information to provide potential clients. The problem is that this information is available to anyone who browses the website. This information allows attackers to know that the new systems are Linux-based and that the network equipment is all Enterasys. If attackers were planning to launch a denial of service (DoS) attack against the organization, they now know that they must knock out three nodes to the Internet. Even a competitor would benefit from this knowledge as the company is telling the competition everything about its infrastructure.

TIP

The wayback machine located at www.archive.org can be used to browse archived web pages that date back to 1996. It's a useful tool for looking for information that no longer exists on a site.

Another big information leakage point is the company directories. These usually identify key employees or departments. By combining this information with a little social engineering, an attacker can call the help desk, pretend he works for one of these key employees, and demand that a password be reset or changed. He could also use biographical information about a key employee to perform other types of *social engineering* trickery. Kevin Mitnick used just this type of attack to gain access to restricted code that detailed the operation of Motorola cell phones. During a pen test, you will want to record any such findings and make sure to alert the organization as to what information is available and how it might be used in an attack.

NOTE

Gather emails from the target site that can be used for more than just social engineering. One method to gain additional information about the organization's email server is to send an email that will bounce from the site. If the site is www. xyz.com, send a mail to badaddress@xyz.com. It will bounce back to you and give you information in its header, including the email server IP address and email server version. Another great reason for bouncing an email message is to find out if they make use of mail scrubber as well. Whatever you find, you will want to copy the information from the headers and make note of it as you continue to gather information.

Job Boards

If you're lucky, the company has a job posting board. Look this over carefully, as you will be surprised at how much information is given here. If no job listings are posted on the organization's website, get interactive and check out some of the major Internet job boards. Some popular sites are

- Careerbuilder.com
- Monster.com
- Dice.com
- TheITjobboard.com

Once at the job posting site, query for the organization. Here's an example of the type of information typically found:

- Primary responsibilities for this position include management of a Windows 2000 Active Directory environment, including MS Exchange 2000, SQL 2000, and Citrix.

- Interact with the technical support supervisor to resolve issues and evaluate/maintain patch level and security updates.
- Experience necessary in: Active Directory, Microsoft Clustering and Network Load-Balancing, MS Exchange 2000, MS SQL 2000, Citrix MetaFrame XP, EMC CX-400 SAN-related or other enterprise level SAN, Veritas Net Backup, BigBrother, and NetIQ Monitoring SW.
- Maintain, support, and troubleshoot a Windows NT/2000 LAN.

Did these organizations give away any information that might be valuable to an attacker? They actually have told attackers almost everything about their network. Just the knowledge that the organization is still running Windows NT/2000 is extremely valuable.

NOTE

One method to reduce the information leakage from job postings is to reduce the system specific information in the job post or to use a company confidential job posting. Company confidential postings hide the true company's identity and make it harder for attackers to misuse this type of information.

Alternative Websites

If information is leaked on a company website, it cannot always be quickly removed. So, what if sensitive information is on a website that an organization does not control? There's always the chance that disgruntled employees might have leaked this information on purpose. That's why any good information gathering process will include visiting the darker corners of the Internet. Layoffs, reductions in force, and outsourcing are the types of events that don't necessarily put the staff in the best of moods. It could be that the organization's insiders have posted information that could be rather damaging. These unhappy individuals are potential sources of information leakage. This information might be posted on a blog, some type of "sucks" domain, or other site. Shown in Figure 3.2 is the Gap sucks domain. Although the legality of these domains depends on the type of information provided and their status as a non-commercial entity, their existence is something you should be aware of.

Frustrated employees will always find some way to vent their thoughts even if not from a "sucks" domain. One such site that might offer other insider information is internalmemos.com. This site lists information that is usually sensitive and that probably shouldn't be released to the general public. Although some of the content is free, most of the content is considered premium and must be purchased to be viewed. One such document found after a search on the word "security" is shown in Figure 3.3. Don't be surprised at what you find on this site or others like it.

FIGURE 3.2
GAPSucks.org.

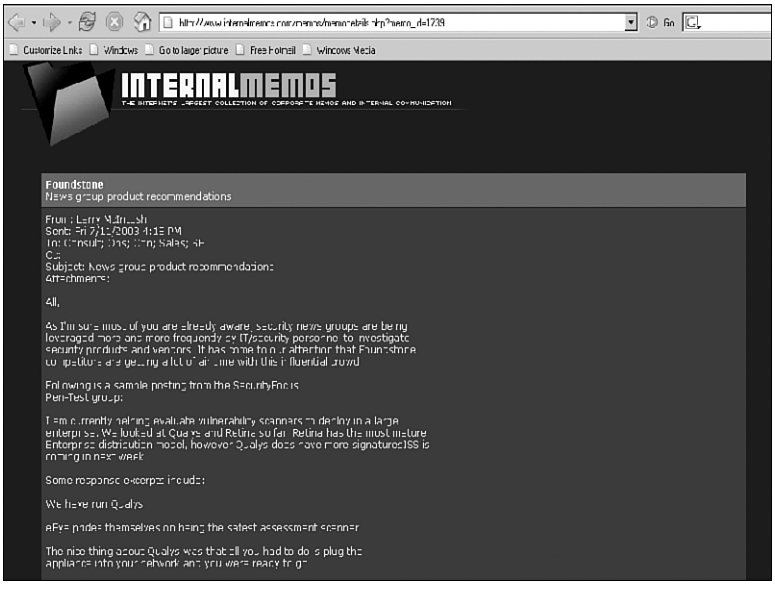

FIGURE 3.3
Internalmemos.com.

Some other sites that can be used to gather information about the target organization and its employees include

- zabasearch.com—Contains names, addresses, phone numbers, date of birth, and other information about individuals.

- anywho.com—Phone book offering forward and reverse lookups.
- maps.yahoo.com—Yahoo! map site.

In combination, these sites allow attackers to locate key individuals, identify their home phone numbers, and even create maps to their houses. Attackers can even see the surroundings of the company or the home they are targeting with great quality satellite pictures.

NOTE

Although some organizations might be relatively secure, gaining the names, addresses, and locations of key employees can allow attackers to war drive their homes and possibly backdoor the organization through an insecure employee's computer.

Free Speech and the Web

As an IT employee of Kmart, I saw firsthand the way internal practice and policies affected the company. That's why after I was fired, I set up one of the very first "sucks" websites. In less time than it takes to announce a blue light special, my site had attracted more than 9,000 visitors. I felt that the site was non-commercial and complied with the law and while Kmart recognized that the content was either true or opinion, the company did threaten me with legal action for the use of the Kmart logo. Therefore, I changed the logo and the name to "The Mart Sucks." I believe that the Internet is successful because of its commitment to open standards, freedom of information, and freedom of speech. Any actions that limit these freedoms and make it less hospitable to the average person shouldn't be tolerated.

This "in the field" segment was contributed by Rodney Fournier, president and lead consultant for Net Working America, Inc. Rodney is an expert in clustering technologies and is a Microsoft MVP.

EDGAR Database

If the organization you are working for is publicly traded, you will want to review the Security and Exchange commision's *EDGAR database*. It's located at www.sec.gov. A ton of information is available at this site. Hackers focus on the 10-Q and 10-K. These two documents contain yearly and quarterly reports. Not only do these documents contain earnings and potential revenue, but also details about any acquisitions and mergers. Anytime there is a merger or one firm acquires another, there is a rush to integrate the two networks. Having the networks integrated is more of an immediate concern than security. Therefore, you will be looking for entity names that are different from the parent organization. These findings might help you discover ways to jump from the subsidiary to the more secure parent company. You will want to record this information and have it ready when you start to research the *IANA* and *ARIN* databases.

Google Hacking

Most of us use Google or another search engine to locate information. What you might not know is that search engines, such as Google, have the capability to perform much more powerful searches than most people ever dream of. Not only can Google translate documents, perform news searches, do image searches, but it can also be used by hackers and attackers to do something that has been termed *Google hacking*. By using basic search techniques combined with advanced operators, Google can become a powerful vulnerability search tool. Some advanced operators include those shown in Table 3.1.

TABLE 3.1 Google Search Terms

Operator	Description
Filetype	This operator directs Google to search only within the test of a particular type of file. Example: filetype:xls
Inurl	This operator directs Google to search only within the specified URL of a document. Example: inurl:search-text
Link	The link operator directs Google to search within hyperlinks for a specific term. Example link:www.domain.com
Intitle	The intitle operator directs Google to search for a term within the title of a document. Example intitle: "Index of…etc"

By using the advanced operators shown in Table 3.1 in combination with key terms, Google can be used to uncover many pieces of sensitive information that shouldn't be revealed. A term even exists for the people who blindly post this information on the Internet; they are called *google dorks*. To see how this works, enter the following phrase into Google:

allinurl:tsweb/default.htm

This query will search in a URL for the tsweb/default.htm string. The search found over 200 sites that had the tsweb/default folder. One of these sites is shown in Figure 3.4.

As you can see, this could represent an easy way for a hacker to log directly in to the organization's servers. Also, notice that there is no warning banner or other notice that unauthorized users should not attempt to connect. Finally, don't forget that finding a vulnerability using Google is not unethical, but using that vulnerability is unless you have written permission from the domain owner. To learn more about Google hacking, take a look at http://johnny.ihackstuff.com. The site's owner, Johnny Long, has also written an excellent book on the subject, *Google Hacking for Penetration Testers*.

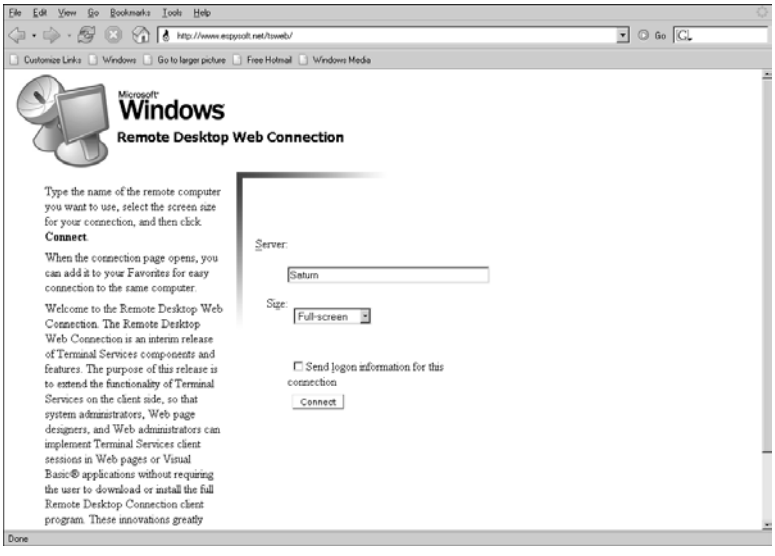

FIGURE 3.4 Google hacking TSWeb.

USENET

USENET is a user's network, which is nothing more than a collection of the thousands of discussion groups that reside on the Internet. Each discussion group contains information and messages centered on a specific topic. Messages are posted and responded to by readers either as public or private emails. Even without direct access to USENET, a convenient way to browse the content is by using *Google Groups*. Google Groups allow any Internet user a way to post and read USENET messages. During a penetration test, you will want to review Google Groups for postings from the target company.

One way to search is to use individual's names you might have uncovered; another is to do a simple search of the company. Searching for @company.com will work. Many times, this will reveal useful information. One company that I performed some work for had listings from the network administrator. He had been asked to set up a new router and was having trouble getting it configured properly. The administrator had not only asked the group for help, but had also posted the router configuration to see if someone could help figure out what was wrong. The problem was that the configuration file had not been sanitized and not only contained IP addresses but also the following information:

enable secret 5 $1$2RKf$OMOAcvzpb7j9uhfw6C5Uj1

enable password 7 583132656321654949

For those of you who might not be Cisco gurus, those are encrypted passwords. Sure, they are encrypted, but given enough time, there's the possibility that they might be cracked. Others of

you who say that it's only router passwords might be right, but let's hope that the administrator doesn't reuse passwords as many people do. As you can see, you can gain additional information about an organization and its technical strengths just by uncovering a few USENET posts.

Insecure Applications

Most applications really aren't bad. Some are more insecure than others, but when deployed with layered controls and properly patched, risk can be minimized. When defense in depth isn't used, problems start to arise. Defense in depth is the layering of one defensive mechanism after another. A case in point is the program Big Brother (www.bb4.com).

Big Brother is a program that can be used to monitor computer equipment. It can monitor and report the status of items, such as the central processing unit (CPU) utilization, disk usage, ssh status, http status, pop3 status, telnet status, and so on. Unlike *Simple Network Monitoring Protocol* (SNMP) in which information is just collected and devices polled, Big Brother can collect this information and forward it to a central web page or location. This makes it a valuable tool to the administrator in that it provides one central location to review network status and indicates status with a simple red/green interface. Problems are indicated in red, whereas operational systems are indicated in green. You might be asking yourself, okay, so what's the problem with all this?

The problem is in how the administrator might have set up or configured Big Brother. Big Brother doesn't need to run as root; therefore, the installation guide recommends that the user create a user named *bb* and configure that user with user privileges. Unless the administrator has changed this, you now know a valid user account on a system. Because the account isn't used by a human, it might have an easy password or one that is not changed often. The makers of Big Brother also recommend that the web page used to store the information Big Brother generates be password protected. After all, this is extremely sensitive information. If this information has not been protected, all someone must do is go to www.google.com and search for "*green:big brother.*" If you scroll through the lists of sites and simply click on one, you'll be taken to a page that displays systems, IP addresses, services, and versions

It's only taken a few minutes for an attacker to gather this type of information, and it's completely legal. These pages are posted so that the entire world can read them. Security professionals should always be concerned about what kind of information is posted on the Web and who can access it.

Registrar Query

Not long ago, searching for domain name information was much easier. There were only a few places to obtain domain names, and the activities of spammers and hackers had yet to cause the Internet Assigned Numbers Authority (IANA) to restrict the release of this information. Today, *The Internet Corporation for Assigned Names and Numbers (ICANN)* is the primary body charged with management of IP address space allocation, protocol parameter assignment, and

domain name system management. Its role is really that of overall management, as domain name registration is handled by a number of competing firms that offer various value added services. These include firms such as networksolutions.com, register.com, godaddy.com, and tucows.com. There is also a series of Regional Internet Registries (RIR) that manage, distribute, and register public IP addresses within their respective regions. There are four primary RIRs with a fifth planned to support Africa. These are shown in Table 3.2.

TABLE 3.2 RIRs and Their Area of Control

RIR	Region of Control
ARIN	North and South America and SubSaharan Africa
APNIC	Asia and Pacific
RIPE	Europe, Middle East, and parts of Africa
LACNIC	Latin America and the Caribbean
AfriNIC	Planned RIR to support Africa

The primary tool to navigate these databases is Whois. Whois is a utility that interrogates the Internet domain name administration system and returns the domain ownership, address, location, phone number, and other details about a specified domain name. Whois is the primary tool used to query Domain Name Services (DNS). If you're performing this information gathering from a Linux computer, the good news is Whois is built in. From the Linux prompt, users can type in `whois domainname.com` or `whois?` to get a list of various options. Windows users are not as fortunate as Linux users because Windows does not have a built-in Whois client. Windows users will have to use a third-party tool or website to obtain Whois information. One tool that a Windows user can use to perform Whois lookups is Sam Spade. It can be downloaded from www.samspade.org/ssw/download.html. Sam Spade contains a lot more utilities that just Whois, such as ping, finger, and traceroute. There's also a variety of websites that you can use to obtain Whois information. Some of these include

- www.betterwhois.com
- www.allwhois.com
- http://geektools.com
- www.all-nettools.com
- www.tamos.com/products/smartwhois/
- www.dnsstuff.com
- www.samspade.org

Regardless of the tool, the goal is to obtain registrar information. As an example, the following listing shows the results after www.samspade.org is queried for information on www.examcram.com:

```
Registrant:
      Pearson Technology Centre
      Kenneth Simmons
      200 Old Tappan Rd .
      Old Tappan, NJ 07675 USA
      Email: billing@superlibrary.com
 Phone: 001-201-7846187
   Registrar Name....: REGISTER.COM, INC.
   Registrar Whois...: whois.register.com
   Registrar Homepage: www.register.com
DNS Servers:
   usrxdns1.pearsontc.com
   oldtxdns2.pearsontc.com
```

NOTE

A domain proxy is one way that organizations can protect their identity while still complying with laws that require domain ownership to be public information. Domain proxies work by applying anonymous contact information as well an anonymous email address. This information is displayed when someone performs a domain Whois. The proxy then forwards any emails or contact information that might come to those addresses on to you.

This information provides a contact person, address, phone number, and DNS servers. A hacker skilled in the art of social engineering might use this information to call the organization and pretend to be Kenneth, or he might use the phone number to war dial a range of phone numbers looking for modems.

DNS Enumeration

The attacker has also identified the names of the DNS servers. DNS servers might be targeted for zone transfers. A zone transfer is the mechanism used by DNS servers to update each other by transferring the contents of their database. DNS is structured as a hierarchy so that when you request DNS information, your request is passed up the hierarchy until a DNS server is found that can resolve the domain name request. You can get a better idea of how DNS is structured by examining Figure 3.5. There is a total of 13 DNS root servers.

What's left at this step is to try and gather additional information from the organization's DNS servers. The primary tool to query DNS servers is nslookup. Nslookup provides machine name and address information. Both Linux and Windows have nslookup clients. Nslookup is used by typing nslookup from the command line followed by an IP address or a machine name. Doing so will cause nslookup to return the name, all known IP addresses, and all known *CNAMES* for the identified machine. Nslookup queries DNS servers for machine

name and address information. Using nslookup is rather straightforward. Let's look at an example in which nslookup is used to find out the IP addresses of Google's web servers. By entering **`nslookup www.google.com`**, the following response is obtained:

```
C:\>nslookup www.google.com
Server:  dnsr1.sbcglobal.net
Address:  68.94.156.1
Non-authoritative answer:
Name:    www.l.google.com
Addresses:  64.233.187.99, 64.233.187.104
Aliases:  www.google.com
```

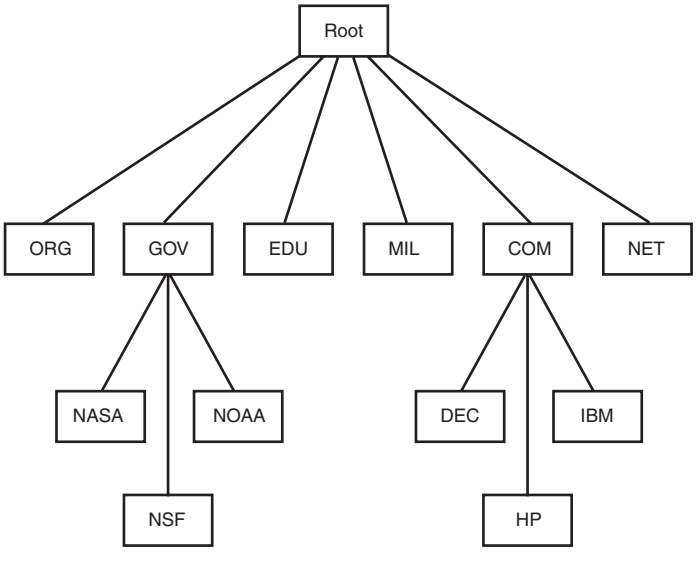

FIGURE 3.5 DNS structure.

The first two lines of output say which DNS servers are being queried. In this case, it's `dnsr1.sbcglobal.net` in Texas. The non-authoritative answer lists two IP addresses for the Google web servers. Responses from non-authoritative servers do not contain copies of any domains. They have a cache file that is constructed from all the DNS lookups it has performed in the past for which it has gotten an authoritative response.

Nslookup can also be used in an interactive mode by just typing **`nslookup`** at the command prompt. In interactive mode, the user will be given a prompt of >; at which point, the user can enter a variety of options, including attempts to perform a zone transfer.

DNS normally moves information from one DNS server to another through the DNS zone transfer process. If a domain contains more than one name server, only one of these servers will be the primary. Any other servers in the domain will be secondary servers. Zone transfers

are much like the DHCP process in that each is a four-step process. DNS zone transfers function as follows:

1. The secondary name server starts the process by requesting the SOA record from the primary name server.
2. The primary then checks the list of authorized servers, and if the secondary server's name is on that list, the SOA record is sent.
3. The secondary must then check the SOA record to see if there is a match against the SOA it already maintains. If the SOA is a match, the process stops here; however, if the SOA has a serial number that is higher, the secondary will need an update. The serial number indicates if changes were made since the last time the secondary server synchronized with the primary server. If an update is required, the secondary name server will send an All Zone Transfer (AXFR) request to the primary server.
4. Upon receipt of the AXFR, the primary server will send the entire zone file to the secondary name server.

Some common DNS resource record names and types are shown in Table 3.3.

TABLE 3.3 DNS Records and Types

Record Name	Record Type	Purpose
Host	A	Maps a domain name to an IP address
Pointer	PTR	Maps an IP address to a domain name
Name Server	NS	Configures settings for zone transfers and record caching
Start of Authority	SOA	Configures settings for zone transfers and record caching
Service Locator	SRV	Used to locate services in the network
Mail	MX	Used to identify SMTP servers

EXAM ALERT

The SOA contains the timeout value, which can be used by a hacker to tell how long any DNS poisoning would last. The TTL value is the last value within the SOA.

A zone transfer is unlike a normal lookup in that the user is attempting to retrieve a copy of the entire zone file for a domain from a DNS server. This can provide a hacker or pen tester with a wealth of information. This is not something that the target organization should be allowing. Unlike lookups that primarily occur on UDP 53, unless the response is greater than 512 bytes, zone transfers use TCP 53. To attempt a zone transfer, you must be connected to

a DNS server that is the authoritative server for that zone. Remember the nslookup information we previously gathered? It's shown here again for your convenience.

```
Registrant:
      Pearson Technology Centre
      Kenneth Simmons
      200 Old Tappan Rd .
      Old Tappan, NJ 07675 USA
      Email: billing@superlibrary.com
 Phone: 001-201-7846187
   Registrar Name....: REGISTER.COM, INC.
   Registrar Whois...: whois.register.com
   Registrar Homepage: www.register.com
DNS Servers:
   usrxdns1.pearsontc.com
   oldtxdns2.pearsontc.com
```

Review the last two entries. Both `usrxdns1.pearsontc.com` and `oldtxdns2.pearsontc.com` are the DNS authoritative servers for ExamCram.com. These are the addresses that an attacker will target to attempt a zone transfer. The steps to try and force a zone transfer are shown here:

1. nslookup—Enter **`nslookup`** from the command line.
2. server <*ipaddress*>—Enter the IP address of the authoritative server for that zone.
3. set type = any—Tells nslookup to query for any record.
4. ls –d <*domain.com*>—Domain.com is the name of the targeted domain of the final step that performs the zone transfer.

One of two things will happen at this point; either you will receive an error message indicating that the transfer was unsuccessful, or you will be returned a wealth of information, as shown in the following:

```
C:\WINNT\system32>nslookup
Default Server:  dnsr1.sbcglobal.net
Address:  128.112.3.12

server 172.6.1.114
set type=any
ls -d example.com

example.com.        SOA hostmaster.sbc.net (950849 21600 3600 1728000 3600)
example.com.        NS     auth100.ns.sbc.net
example.com.        NS     auth110.ns.sbc.net
example.com.        A      10.14.229.23
example.com.        MX     10   dallassmtpr1.example.com
example.com.        MX     20   dallassmtpr2.example.com
```

```
example.com.        MX     30   lasmtpr1.example.com
lasmtpr1            A      192.172.243.240
dallassmtpr1        A      192.172.163.9
dallaslink2         A      192.172.161.4
spamassassin        A      192.172.170.49
dallassmtpr2        A      192.172.163.7
dallasextra         A      192.172.170.17
dallasgate          A      192.172.163.22
lalink              A      172.16.208.249
dallassmtp1         A      192.172.170.49
nygate              A      192.172.3.250
www                 A      10.49.229.203
dallassmtp          MX     10   dallassmtpr1.example.com
dallassmtp          MX     20   dallassmtpr2.example.com
dallassmtp          MX     30   lasmtpr1.example.com
```

NOTE

Dig is another tool that can be used to provide this type of information. It's available for Linux and for Windows. Dig is a powerful tool that can be used to investigate the DNS system.

This type of information should not be made available to just anyone. Hackers can use this to find out what other servers are running on the network, and it can help them map the network and formulate what types of attacks to launch. Notice the first line that has `example.com` listed previously. Observe the final value of `3600` on that line. That is the TTL value discussed previously which would inform a hacker as to how long DNS poisoning would last. 3,600 seconds is 60 minutes. Zone transfers are intended for use by secondary DNS servers to synchronize with their primary DNS server. You should make sure that only specific IP addresses are allowed to request zone transfers. Although most Operating Systems restrict this by default, Windows 2000 did not. So, be aware of this if any 2000 servers are still in your network.

NOTE

All DNS servers should be tested. It is very often the case in which the primary has tight security, but the secondaries will allow zone transfers.

Determining the Network Range

Objective:

Locate the network range

Now that the pen test team has been able to locate name, phone numbers, addresses, some server names, and IP addresses, it's important to find out what range of IP addresses are available

for scanning and further enumeration. If you take the IP address of a web server discovered earlier and enter it into the Whois lookup at www.arin.net, the network's range can be determined. As an example, 192.17.170.17 was entered into the ARIN Whois, and the following information was received:

```
OrgName:    target network
OrgID:      Target-2
Address:    1313 Mockingbird Road
City:       Anytown
StateProv:  Tx
PostalCode: 72341
Country:    US
ReferralServer: rwhois://rwhois.exodus.net:4321/
NetRange:   192.17.12.0 - 192.17.12.255
CIDR:       192.17.0.0/24
NetName:    SAVVIS
NetHandle:  NET-192-17-12-0-1
Parent:     NET-192-0-0-0-0
```

This means that the target network has 254 total addresses. The attacker can now focus his efforts on the range from 192.17.12.1 to 192.17.12.254 /24. If these results don't prove satisfactory, traceroute can be used for additional mapping.

Traceroute

Objective:

Specify how traceroute works

The *traceroute* utility is used to determine the path to a target computer. Just as with nslookup, traceroute is available on Windows and UNIX platforms. In Windows, it is known as tracert because of 8.3 legacy filename constraints remaining from DOS. Traceroute was originally developed by Van Jacobson to view the path a packet follows from its source to its destination. Traceroute owes its functionality to the IP header *time-to-live* (TTL) field. You might remember from the discussion in Chapter 2, "The Technical Foundations of Hacking," that the TTL field is used to limit IP datagram's. Without a TTL, some IP datagram's might travel the Internet forever as there would be no means of timeout. TTL functions as a decrementing counter. Each hop that a datagram passes through reduces the TTL field by one. If the TTL value reaches 0, the datagram is discarded and a time exceeded in transit Internet Control Message Protocol (ICMP) message is created to inform the source of the failure. Linux traceroute is based on UDP, whereas Windows uses ICMP.

TIP

You will want to be familiar with all the common ICMP types and codes before attempting the CEH exam. They are covered in detail in RFC 792.

To get a better idea of how this works, let's take a look at how Windows would process a traceroute. For this example, say that the target is three hops away. Windows would send out a packet with a TTL of 1. Upon reaching the first router, the packet TTL value would be decremented to 0, which would illicit a time exceeded in transit error message. This message would be sent back to the sender to indicate that the packet did not reach the remote host. Receipt of the message would inform Windows that it had yet to reach its destination, and the IP of the device in which the datagram timed out would be displayed. Next, Windows would increase the TTL to a value of 2. This datagram would make it through the first router, where the TTL value would be decremented to 1. Then it would make it through the second router; at which time, the TTL value would be decremented to 0 and the packet would expire. Therefore, the second router would create a time exceeded in transit error message and forward it to the original source. The IP address of this device would next be displayed on the user's computer. Finally, the TTL would be increased to 3. This datagram would easily make it past the first and second hop and arrive at the third hop. Because the third hop is the last hop before the target, the router would forward the packet to the destination and the target would issue a normal ICMP ping response. The output of this traceroute can be seen here:

```
C:\>tracert 192.168.1.200
Tracing route to 192.168.1.200:
1    10 ms   <10 ms   <10 ms
2    10 ms    10 ms    20 ms
3    20 ms    20 ms    20 ms 192.168.1.200
Trace complete.
```

Linux-based versions of traceroute work much the same way but use UDP. Traceroute sends these UDP packets targeted to high order port numbers that nothing should be listening on. Just as described previously, the TTL is increased until the target device is reached. Because traceroute is using a high order UDP port, typically 33434, the host should ignore the packets after generating port unreachable messages. These ICMP port unreachable messages are used by traceroute to notify the source that the destination has been reached.

It's advisable to check out more than one version of traceroute if you don't get the required results. Some techniques can also be used to try and slip traceroute passed a firewall or filtering device. When UDP and ICMP are not allowed on the remote gateway, TCPTraceroute can be used. Another unique technique was developed by Michael Schiffman, who created a patch called traceroute.diff that allows you to specify the port that traceroute will use. With this handy tool, you could easily direct traceroute to use UDP port 53. Because that port is used for DNS queries, there's a good chance that it could be used to slip past the firewall. If you're looking for a GUI program to perform traceroute with, several are available, which are described here:

- NeoTrace—NeoTrace is a powerful tool for mapping path information. The graphical display shows you the route between you and the remote site, including all intermediate nodes and their registrant information. NeoTrace is probably the most well-known GUI traceroute program. Along with a graphical map, it also displays information on

each node such as IP address, contact information, and location. NeoTrace can be seen in Figure 3.6. That trace shows the results of a traceroute to Microsoft.com. Just remember that NeoTrace builds from provided information that is entered into the routers, and it might not always be accurate.

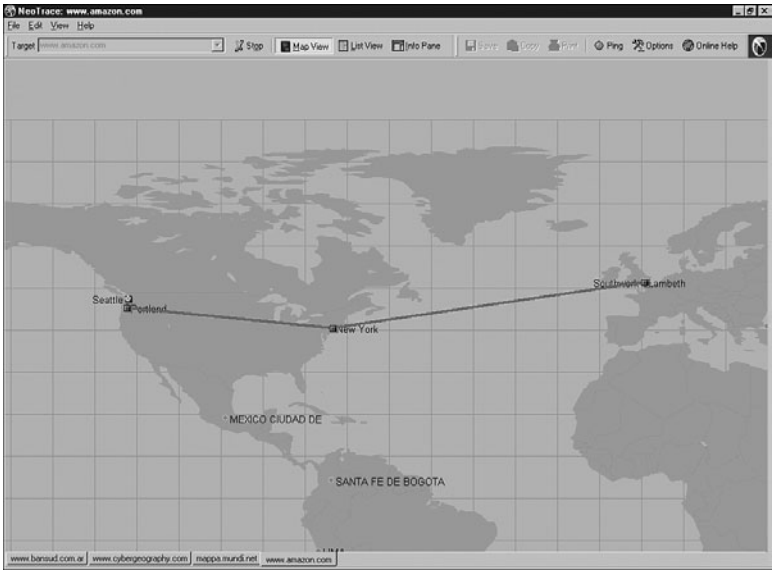

FIGURE 3.6 NeoTrace.

- Trout—Trout is another visual traceroute and Whois program. What's great about this program is its speed. Unlike traditional traceroute programs, trout performs parallel pinging. By sending packets with more than one TTL at a time, it can quickly determine the path to a targeted device.
- VisualRoute—VisualRoute is another graphical traceroute for Windows. VisualRoute not only shows a graphical world map that displays the path packets are taking, but it also lists information for each hop, including IP address, node name, and geographical location.

Traceroute and ping are useful tools for identifying active systems, mapping their location, and learning more about their location. To learn more about these tools, take a few moments to complete the following challenge exercise:

Challenge

1. Open a command prompt on your Windows PC and enter **`ping`**.
2. You will see a list of commands that specify how ping works. Use that information to complete Table 3.4.

TABLE 3.4 Ping Options

Option	Meaning of Specific Option
-t	
-a	
-l	
-f	
-i	

3. Now enter **`tracert`** from the command line and observe the options. Record your findings in Table 3.5.

TABLE 3.5 Tracert Options

Option	Meaning of Option
-d	
-h	

4. Use ping with the –r option to ping www.microsoft.com.
5. Now open a second command prompt and use tracert to trace the route to www.microsoft.com.

Do you see any differences? Each router should respond using the IP address of the interface it transmits the ICMP Timeout messages on, which should be the same as the interface it received the original packets on, whereas ping uses the –r option to record the path of routers the echo request/reply message used. Together, these two tools can be used to map a more accurate diagram of the network.

Identifying Active Machines

Objective:

Identify active machines

Attackers will want to know if machines are alive before they attempt to attack. One of the most basic methods of identifying active machines is to perform a ping sweep. Although ping

is found on just about every system running TCP/IP, it has been restricted by many organizations. Ping uses ICMP and works by sending an *echo request* to a system and waiting for the target to send an *echo reply* back. If the target device is unreachable, a *request time out* is returned. Ping is a useful tool to identify active machines and to measure the speed at which packets are moved from one host to another or to get details like the TTL. Figure 3.7 shows a ping capture from a Windows computer. If you take a moment to examine the ASCII decode in the bottom-left corner, you will notice that the data in the ping packet is composed of the alphabet, which is unlike a Linux ping, which would contain numeric values. That's because the RFC that governs ping doesn't specify what's carried in the packet as payload. Vendors fill in this padding as they see fit. Unfortunately, this can also serve hackers as a *covert channel*. However, hackers can use a variety of programs to place their own information in place of the normal padding. Then what appears to be normal pings are actually a series of messages entering and leaving the network.

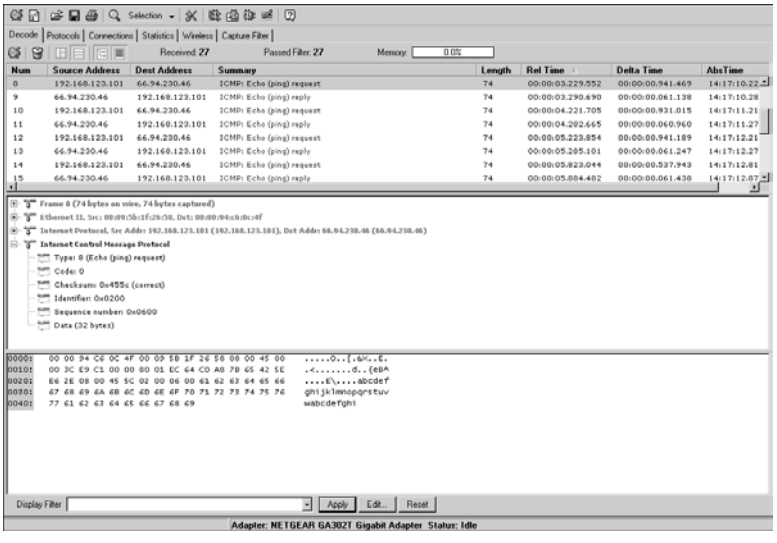

FIGURE 3.7 Ping capture.

Ping does have a couple of drawbacks: First, only one system at a time is pinged and second, not all networks allow ping. To ping a large amount of hosts, a *ping sweep* is usually performed. Programs that perform ping sweeps typically sweep through a range of devices to determine which ones are active. Some of the programs that will perform ping sweeps include

- Angry IP Scanner
- Pinger
- WS_Ping_ProPack
- Network scan tools

- Super Scan
- Nmap

Finding Open Ports and Access Points

Objective:

Understand how to map open ports and identify their underlying applications

With knowledge of the network range and a list of active devices, the next step is to identify open ports and access points. Identifying open ports will go a long way toward potential attack vectors. There is also the possibility of using war dialing programs to find ways around an organization's firewall. If the organization is located close by, the attacker might war drive the area to look for open access points.

Port Scanning

Objective:

Describe the differences between TCP and UDP scanning

Port scanning is the process of connecting to TCP and UDP ports for the purpose of finding what services and applications are running on the target device. After running applications, open ports and services are discovered, the hacker can then determine the best way to attack the system.

As discussed in Chapter 2, there are a total of 65,535 TCP and UDP ports. These port numbers are used to identify a specific process that a message is coming from or going to. Some common port numbers are shown in Table 3.6.

TABLE 3.6 Common Ports and Protocols

Port	Service	Protocol
20/21	FTP	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
69	TFTP	UDP
80	HTTP	TCP
110	POP3	TCP

(continues)

TABLE 3.6 *Continued*

Port	Service	Protocol
135	RPC	TCP
161/162	SNMP	UDP
1433/1434	MSSQL	TCP

As you have probably noticed, some of these applications run on TCP, whereas others run on UDP. Although it is certainly possible to scan for all 65,535 TCP and 65,535 UDP ports, many hackers will not. They will concentrate on the first 1,024 ports. These well-known ports are where we find most of the commonly used applications. A list of well-known ports can be found at www.iana.org/assignments/port-numbers. Now, this is not to say that high order ports should be totally ignored because hackers might break into a system and open a high order port, such as 31337, to use as a backdoor. So, is one protocol easier to scan for than the other? Well, the answer to that question is yes. TCP offers more opportunity for the hacker to manipulate than UDP. Let's take a look at why.

TCP offers robust communication and is considered a connection protocol. TCP establishes a connection by using what is called a 3-way handshake. Those three steps proceed as follows:

1. The client sends the server a TCP packet with the *sequence number flag* (SYN Flag) set and an Initial Sequence Number (ISN).
2. The server replies by sending a packet with the SYN/ACK flag set to the client. The synchronize sequence number flag informs the client that it would like to communicate with it, whereas the acknowledgement flag informs the client that it received its initial packet. The acknowledgement number will be one digit higher than the client's ISN. The server will generate an ISN as well to keep track of every byte sent to the client.
3. When the client receives the server's packet, it creates an ACK packet to acknowledge that the data has been received from the server. At this point, communication can begin.

The TCP header contains a one-byte field for the flags. These flags can be seen in Table 3.7.

TABLE 3.7 TCP Flag Types

Flag	Purpose
SYN	Synchronize and Initial Sequence Number (ISN)
ACK	Acknowledgement of packets received
FIN	Final data flag used during the 4-step shutdown of a session
RST	Reset bit used to close an abnormal connection
PSH	Push data bit used to signal that data in the packet should be pushed to the beginning of the queue. Usually indicates an urgent message.
URG	Urgent data bit used to signify that urgent control characters are present in this packet that should have priority.

At the conclusion of communication, TCP terminates the session by using a 4-step shutdown. Those four steps proceed as follows:

1. The client sends the server a packet with the FIN/ACK flags set.
2. The server sends a packet ACK flag set to acknowledge the clients packet.
3. The server then generates another packet with the FIN/ACK flags set to inform the client that it also is ready to conclude the session.
4. The client sends the server a packet with the ACK flag set to conclude the session.

The TCP system of communication makes for robust communication but also allows a hacker many ways to craft packets in an attempt to coax a server to respond or to try and avoid detection of an *intrusion detection system (IDS)*. Many of these methods are built into Nmap and other port scanning tools, but before taking a look at those tools, some of the more popular port scanning techniques are listed here:

- TCP Connect scan—This type of scan is the most reliable, although it is also the most detectable. It is easily logged and detected because a full connection is established. Open ports reply with a SYN/ACK, whereas closed ports respond with an RST/ACK.
- TCP SYN scan—This type of scan is known as half open because a full TCP three-way connection is not established. This type of scan was originally developed to be stealthy and evade IDS systems although most now detect it. Open ports reply with a SYN/ACK, whereas closed ports respond with a RST/ACK.
- TCP FIN scan—Forget trying to set up a connection; this technique jumps straight to the shutdown. This type of scan sends a FIN packet to the target port. Closed ports should send back an RST. This technique is usually effective only on UNIX devices.
- TCP NULL scan—Sure, there should be some type of flag in the packet, but a NULL scan sends a packet with no flags set. If the OS has implemented TCP per RFC 793, closed ports will return an RST.
- TCP ACK scan—This scan attempts to determine access control list (ACL) rule sets or identify if stateless inspection is being used. If an ICMP destination unreachable, communication administrative prohibited message is returned, the port is considered to be filtered.
- TCP XMAS scan—Sorry, there are no Christmas presents here, just a port scan that has toggled on the FIN, URG, and PSH flags. Closed ports should return an RST.

TIP

You will need to know common scan types, such as full and stealth, to successfully pass the exam.

Certain OSes have taken some liberties when applying the TCP/IP RFCs and do things their own way. Because of this, not all scan types will work against all systems. So, results will vary, but Full Connect scans and SYN scans should work against all systems.

These are not the only types of possible scans; however, they are the more popular types. A few others worth briefly noting include

- IDLE scan—Uses an idle host to bounce packets off of and make the scan harder to trace. It is considered the only totally stealth scan.
- FTP Bounce scan—Uses an FTP server to bounce packets off of and make the scan harder to trace.
- RPC scan—Attempts to determine if open ports are RPC ports.
- Window scan—Similar to an ACK scan, but can sometimes determine open ports.

Now let's look at UDP scans. UDP is unlike TCP. Although TCP is built on robust connections, UDP is based on speed. With TCP, the hacker has the ability to manipulate flags in an attempt to generate a TCP response or an error message from ICMP. UDP does not have flags, nor does UDP issue responses. It's a fire and forget protocol! The most you can hope for is a response from ICMP.

If the port is closed, ICMP will attempt to send an ICMP type 3 code 3 port unreachable message to the source of the UDP scan. But, if the network is blocking ICMP, no error message will be returned. Therefore, the response to the scans might simply be no response. If you are planning on doing UDP scans, plan for unreliable results.

Next some of the programs that can be used for port scanning are discussed.

Is Port Scanning Legal?

In 2000, two contractors ended up in a U.S. district court because of a dispute of the legality of port scanning. The plaintiff believed that port scanning is a crime, whereas the defendant believed that only by port scanning was he able to determine what ports were open and closed on the span of network he was responsible for. The U.S. district court judge ruled that port scanning was not illegal, as it does not cause damage. So, although port scanning is not a crime, you should still seek to obtain permission before scanning a network. Also, home users should review their service provider's terms and conditions before port scanning. Most cable companies prohibit port scanning and maintain the right to disconnect customers who perform such acts even when they are performing such activities with permission. Time Warner's policy states the following, "Please be aware that Time Warner Road Runner has received indications of port scanning from a machine connected to the cable modem on your Road Runner Internet connection. This violates the Road Runner AUP (Acceptable Use Policy). Please be aware that further violations of the Acceptable Usage Policy may result in the suspension or termination of your Time Warner Road Runner account."

Nmap

Objective:

Use tools such as Nmap to perform port scanning and know common Nmap switches

Nmap was developed by a hacker named Fyodor Yarochkin. This popular application is available for Windows and Linux as a GUI and command-line program. It is probably the most widely used port scanner ever developed. It can do many types of scans and OS identification. It also allows you to control the speed of the scan from slow to insane. Its popularity can be seen by the fact that it's incorporated into other products and was even used in the movie *The Matrix*. Nmap with the help option is shown here so that you can review some of its many switches.

```
C:\nmap-3.93>nmap -h
Nmap 3.93 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sV Version scan probes open ports determining service and app names/versions
 -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -6 scans via IPv6 rather than IPv4
  -T <Paranoid¦Sneaky¦Polite¦Normal¦Aggressive¦Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
  --win_help Windows-specific features
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
```

TIP

To better understand Nmap and fully prepare for the CEH Exam, it's advisable to download and review Nmap's documentation. It can be found at www.insecure.org/nmap/data/nmap_manpage.html.

As can be seen from the output of the help menu in the previous listing, Nmap can run many types of scans. Nmap is considered a required tool for all ethical hackers. Nmap's output provides the open port's well-known service name, number, and protocol. They can either be open, closed, or filtered. If a port is open, it means that the target device will accept connections on that port. A closed port is not listening for connections, and a filtered port means that a firewall, filter, or other network device is guarding the port and preventing Nmap from fully probing it or determining its status. If a port is reported as unfiltered, it means that the port is closed and no firewall or router appears to be interfering with Nmap's attempts to determine its status. To run Nmap from the command line, type **`Nmap`**, followed by the switch, and then enter a single IP address or a range. For the example shown here, the –sT option was used, which performs a TCP full 3-step connection.

```
C:\nmap-3.93>nmap -sT 192.168.1.108
Starting nmap 3.93 ( http://www.insecure.org/nmap ) at 2005-10-05 23:42 Central
Daylight Time
Interesting ports on Server (192.168.1.108):
(The 1653 ports scanned but not shown below are in state: filtered)
PORT    STATE SERVICE
80/tcp  open  http
139/tcp open  netbios-ssn
515/tcp open  printer
548/tcp open  afpovertcp
Nmap run completed -- 1 IP address (1 host up) scanned in 420.475 seconds
```

Several interesting ports were found on this computer, including 80 and 139. A UDP scan performed with the `-sU` switch returned the following results:

```
C:\nmap-3.93>nmap -sU 192.168.1.108
Starting nmap 3.93 ( http://www.insecure.org/nmap ) at 2005-10-05 23:47 Central
Daylight Time
Interesting ports on Server (192.168.1.108):
(The 1653 ports scanned but not shown below are in state: filtered)
PORT    STATE SERVICE
69/udp  open  tftp
139/udp open  netbios-ssn
Nmap run completed -- 1 IP address (1 host up) scanned in 843.713 seconds
```

Nmap also has a GUI version called NmapFE. Most of the options in NmapFe correspond directly to the command-line version. Some people call NmapFe the Nmap tutor because it displays the command-line syntax at the bottom of the GUI interface. It is no longer updated for Windows but is maintained for the Linux platform. This can be seen in Figure 3.8.

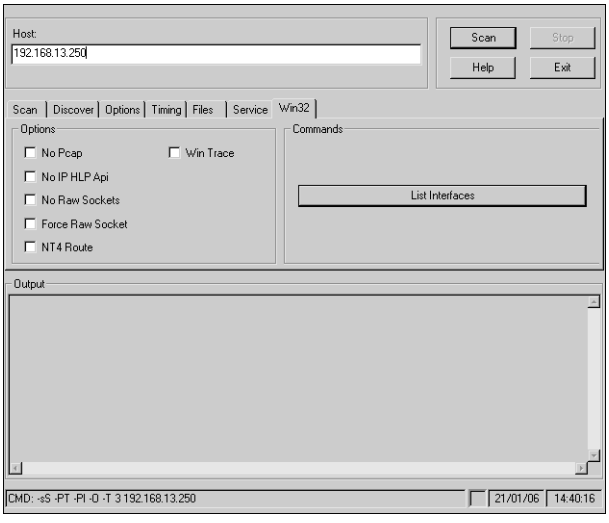

FIGURE 3.8 NmapFE.

SuperScan

Version 4 of SuperScan is written to run on Windows XP and 2000. It's a versatile TCP/UDP port scanner, pinger, and hostname revolver. It can perform ping scans and port scans using a range of IP addresses, or it can scan a single host. It also has the capability to resolve or reverse-lookup IP addresses. It builds an easy-to-use HTML report that contains a complete breakdown of the hosts that were scanned. This includes information on each port and details about any banners that were found. It's free; therefore it is another tool that all ethical hackers should have. To get a better look at the interface, review Figure 3.9.

THC-Amap

THC-Amap is another example of scanning and banner grabbing. One problem that traditional scanning programs have is that not all services are ready and eager to give up the appropriate banner. For example, some services, such as SSL, expect a handshake. Amap handles this by storing a collection of responses that it can fire off at the port to interactively elicit it to respond. Another problem is that scanning programs sometimes make basic assumptions that might be flawed. Many port scanners assume that if a particular port is open, the default application for that port must be present. Amap probes these ports to find out what is really running there. Therefore, this tool excels at allowing a security professional to find services that might have been redirected from their standard ports. One technique is to use this program by taking the greppable format of nmap as an input to scan for those open services. Defeating or blocking Amap is not easy, although one technique would be to use a *port knocking* technique. Port knocking is similar to a secret handshake or combination. Only after inputting a set order of port connections can a connection be made.

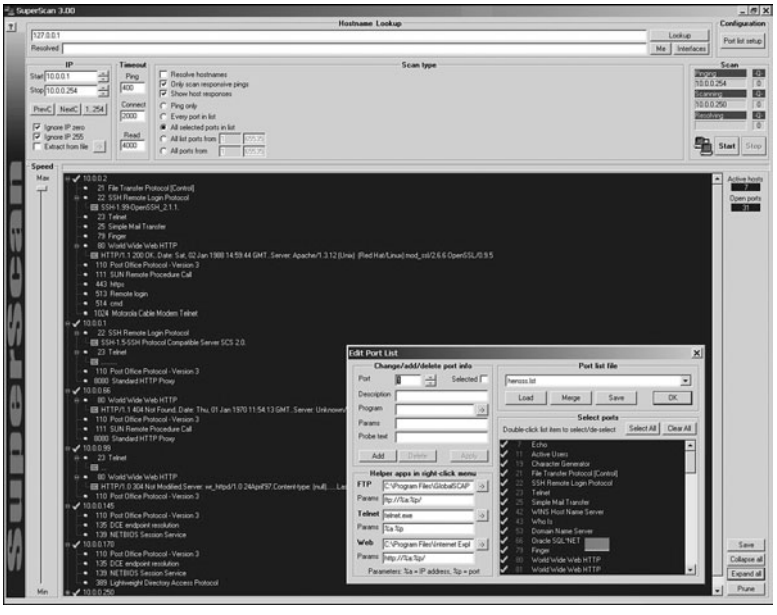

FIGURE 3.9 SuperScan.

Scanrand

Scanrand is part of a suite of tools known as Paketto Keiretsu developed by Dan Kaminsky. Scanrand is a fast scanning tool, and what makes this tool so fast is that it uses a unique method of scanning TCP ports. Most TCP scanners take the approach of scanning one port at a time. After all, TCP is a stateful protocol, so traditional scanners must probe each port, wait for the response, store the connection in memory, and then move on. Traditional scanning is a serial process.

Scanrand implements *stateless* scanning. This parallel approach to scanning breaks the process into two distinct processes. One process sends out the requests at a high rate of speed, while the other independent process is left to sort out the incoming responses and figure out how it all matches up. The secret to the program's speed is in its use of *inverse SYN cookies*. Basically, Scanrand builds a hashed sequence number placed in the outgoing packet that can be identified upon return. This value contains information that identifies source IP, source port, destination IP, and destination port. If you're tasked with scanning a large number of IP addresses quickly, this is something you'll want to check out, as it is much faster than traditional scanning programs.

Port Knocking

Port knocking is a method of establishing a connection to a host that does not initially indicate that it has any open ports. Port knocking works by having the remote device send a series of connection attempts to a specific series of ports. It is somewhat analogous to a secret handshake. After the proper sequence of port knocking has been detected, the required port is

opened and a connection is established. The advantage of using a port knocking technique is that hackers cannot easily identify open ports. The disadvantages include the fact that the technique does not harden the underlining application. Also, it isn't useful for publicly accessible services. Finally, anyone who has the ability to sniff the network traffic will be in possession of the appropriate knock sequence. www.portknocking.org is a good site to check out to learn more about this defensive technique.

War Dialers

War dialing has been around long before the days of broadband access and was actually popularized in the 1983 movie *War Games*. War dialing is the act of using a modem and software to scan for other systems with modems attached. War dialing is accomplished by dialing a range of phone numbers with the hope of getting one to respond with the appropriate tone. Modems are a tempting target for hackers because they offer them the opportunity to bypass the corporate firewall. A modem can be seen as a backdoor into the network.

Modems are still popular today with network administrators because they can be used for remote access, and they are useful for out-of-band management. After all, they are a low-cost network access alternative if normal network access goes down. The problem is that many of these modems have no authentication or weak authentication at best. If you're planning on war dialing as part of a pen test, you want to make sure and check the laws in your area. Some states have laws that make it illegal to place a call without the intent to communicate. Two of the most well-known war dialing tools include

- ToneLoc—A war dialing program that looks for dial tones by randomly dialing numbers or dialing within a range. It can also look for a carrier frequency of a modem or fax. ToneLoc uses an input file that contains the area codes and number ranges you want to have it dial.
- PhoneSweep—A commercial grade war dialing program that can support multiple lines at once.
- THC-Scan—An older DOS-based program that can use a modem to dial ranges of numbers to search for a carrier frequency from a modem or fax.

Wardriving

Wardriving is named after wardialing as it is the process of looking for open access points. Many pen tests contain some type of war driving activity. The goal is to identify open or rogue access points. Even if the organization has secured it wireless access points, there is always the possibility that employees have installed their own access points without the company's permission. Unsecured wireless access points can be a danger to organizations because much like modems, they offer the hacker a way into the network that might bypass the firewall. A whole host of security tools have been released for Windows and Linux over the last few years that

can be used to probe wireless equipment. Some basic tools that hackers and legitimate pen testers probably have include

- Kismit—802.11 wireless network detector, sniffer, and intrusion detection system.
- Netstumbler—802.11 wireless network detector, also available for Mac and handhelds.
- Airsnort—802.11b wireless cracking tool.
- Airsnare—An intrusion detection system to help you monitor your 802.11 wireless network. It can notify you as soon as a machine connects to your wireless network that is not listed as an approved MAC address.

OS Fingerprinting

Objectives:

Describe passive fingerprinting

State the various ways that active fingerprinting tools work

At this point in the information gathering process, the hacker has made some real headway. IP addresses, active systems, and open ports have been identified. Although the hacker might not yet know the type of systems he is dealing with, he is getting close. There are two ways in which the hacker can attempt to identify the targeted devices. The hacker's first choice is *passive fingerprinting*. The hacker's second choice is to perform *active fingerprinting*, which basically sends malformed packets to the target in hope of eliciting a response that will identify it. Although active fingerprinting is more accurate, it is not as stealthy as passive fingerprinting.

Passive fingerprinting is really sniffing, as the hacker is sniffing packets as they come by. These packets are examined for certain characteristics that can be pointed out to determine the OS. Four commonly examined items that are used to fingerprint the OS include

- The IP TTL value—Different OSes set the TTL to unique values on outbound packets.
- The TCP Window Size—OS vendors use different values for the initial window size.
- The IP DF Option—Not all OS vendors handle fragmentation in the same way.
- The IP Type of Service (TOS) Option—TOS is a three-bit field that controls the priority of specific packets. Again, not all vendors implement this option in the same way.

These are just four of many possibilities that can be used to passively fingerprint an OS. Other items that can be examined include IP Identification Number (IPID), IP options, TCP options, and even ICMP. Ofir Arkin has written an excellent paper on this titled, "ICMP

Usage in Scanning." Probably the most up-to-date passive fingerprinting tool is the Linux-based tool P0f. P0f attempts to passively fingerprint the source of all incoming connections after the tool is up and running. Because it's a truly passive tool, it does so without introducing additional traffic on the network. P0fv2 is available at http://lcamtuf.coredump.cx/p0f.tgz.

Active fingerprinting is more powerful than passive fingerprint scanning because the hacker doesn't have to wait for random packets, but as with every advantage, there is usually a disadvantage. This disadvantage is that active fingerprinting is not as stealthy as passive fingerprinting. The hacker actually injects the packets into the network. Active fingerprinting has a much higher potential for being discovered or noticed. Like passive OS fingerprinting, active fingerprinting examines the subtle differences that exist between different vendor implementations of the TCP/IP stack. Therefore, if hackers probe for these differences, the version of the OS can most likely be determined. One of the individuals who has been a pioneer in this field of research is Fyodor. His site, www.insecure.org/nmap/nmap-fingerprinting-article.html, has an excellent paper on OS fingerprinting. Listed here are some of the basic methods used in active fingerprinting:

- The FIN probe—A FIN packet is sent to an open port, and the response is recorded. Although RFC 793 states that the required behavior is not to respond, many OSes such as Windows will respond with a RESET.
- Bogus flag probe—As you might remember from Table 3.7, there are only six valid flags in the 1 byte TCP header. A bogus flag probe sets one of the used flags along with the SYN flag in an initial packet. Linux will respond by setting the same flag in the subsequent packet.
- Initial Sequence Number (ISN) sampling—This fingerprinting technique works by looking for patterns in the ISN number. Although some systems use truly random numbers, others, such as Windows, increment the number by a small fixed amount.
- IPID sampling—Many systems increment a systemwide IPID value for each packet they send. Others, such as older versions of Windows, do not put the IPID in network byte order, so they increment the number by 256 for each packet.
- TCP initial window—This fingerprint technique works by tracking the window size in packets returned from the target device. Many OSes use exact sizes that can be matched against a database to uniquely identify the OS.
- ACK value—Again, vendors differ in the ways they have implemented the TCP/IP stack. Some OSes send back the previous value +1, whereas others send back more random values.
- Type of service—This fingerprinting type tweaks ICMP port unreachable messages and examines the value in the type of service (TOS) field. Whereas some use 0, others return different values.

- TCP options—Here again, different vendors support TCP options in different ways. By sending packets with different options set, the responses will start to reveal the server's fingerprint.
- Fragmentation handling—This fingerprinting technique takes advantage of the fact that different OS vendors handle fragmented packets differently. RFC 1191 specifies that the MTU is normally set between 68 and 65535 bytes. This technique was originally discovered by Thomas Ptacek and Tim Newsham.

Active Fingerprinting Tools

Objective:

Use tools such as Xprobe2, Winfingerprint, and Amap

One of the first tools to actually be widely used for active fingerprinting back in the late 1990s was Queso. Although no longer updated, it helped move this genre of tools forward. Nmap has supplanted Queso as the tool of choice for active fingerprinting and is one of the most feature-rich free fingerprint tools in existence today. Nmap's database can fingerprint literally hundreds of different OSes. Fingerprinting with Nmap is initiated by running the tool with the –O option. When started with this command, switch nmap probes port 80 and then ports in the 20–23 range. Nmap needs one open and one closed port to make an accurate determination of what OS a particular system is running. An example is shown in the following:

```
C:\nmap-3.93>nmap -O 192.168.123.108
Starting nmap 3.93 ( http://www.insecure.org/nmap ) at 2005-10-07 15:47 Central
Daylight Time
Interesting ports on 192.168.1.108:
(The 1653 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
80/tcp  open  http
139/tcp open  netbios-ssn
515/tcp open  printer
548/tcp open  afpovertcp
Device type: general purpose
Running: Linux 2.4.X¦2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 0.282 days (since Fri Oct 07 09:01:33 2005)
Nmap run completed -- 1 IP address (1 host up) scanned in 4.927 seconds
```

You might also want to try Nmap with the `-v` or `-vv` switch. There are devices such as F5 Load Balancer that will not identify themselves using a normal –O scan but will reveal their ID with

the -vv switch. Just remember that with Nmap or any other active fingerprint tool, you are injecting packets into the network. This type of activity can be tracked and monitored by an IDS. Active fingerprinting tools, such as Nmap, can be countered by tweaking the OS's stack. Anything that tampers with this information can affect the prediction of the target's OS version.

Nmap's dominance of active fingerprinting is being challenged by a new breed of tools. One such tool is Xprobe. Xprobe 2 is a Linux-based active OS fingerprinting tool with a different approach to operating system fingerprinting. Xprobe is unique in that it uses a mixture of TCP, UDP, and *ICMP* to slip past firewalls and avoid *IDS* systems. Xprobe2 relies on fuzzy signature matching. In layman's terms, this means that targets are run through a variety of tests. These results are totaled, and the user is presented with a score that tells the probability of the targeted machine's OS—for example, 75 percent Windows XP and 60 percent Windows 2000.

Because some of you might actually prefer GUI tools, the final fingerprinting tool for discussion is Winfingerprint. This Windows-based tool can harvest a ton of information about Windows servers. It allows scans on a single host or the entire network neighborhood. You can also input a list of IP addresses or specify a custom IP range to be scanned. After a target is found, Winfingerprint can obtain NetBIOS shares, disk information, services, users, groups, detection of Service Pack, and even Hotfixes. A screenshot of Winfingerprint can be seen in Figure 3.10.

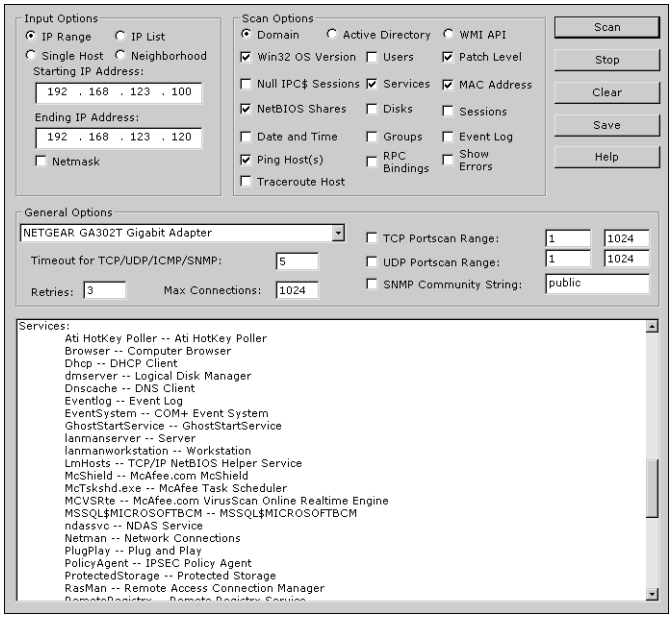

FIGURE 3.10
Winfingerprint.

Fingerprinting Services

Objective:

Be able to perform banner grabbing with tools such as Telnet and netcat

If there is any doubt left as to what a particular system is running, this next step of information gathering should serve to answer those questions. Knowing what services are running on specific ports allows the hacker to formulate and launch application specific attacks. Knowing the common default ports and services and using tools such as Telnet, FTP, and Netcat are two techniques that can be used to ensure success at this pre-attack stage.

Default Ports and Services

A certain amount of default information and behavior can be gleamed from any system. For example, if a hacker discovers a Windows 2003 system with port 80 open, he can assume that the system is running IIS 6.0, just as a Linux system with port 25 open is likely to be running sendmail. Although it's possible that the Windows 2003 machine might be running a version of Apache, that most likely is not a common occurrence.

Just keep in mind that at this point, the attacker is making assumptions. Just because a particular port is active or a known banner is returned, you cannot be certain that information is correct. Ports and banners can be changed and assumptions by themselves can be dangerous. Additional work will need to be done to verify what services are truly being served up by any open ports.

Finding Open Services

The scanning performed earlier in the chapter might have uncovered other ports that were open. Most scanning programs, such as Nmap and SuperScan, will report what common services are associated with those open ports. This easiest way to determine what services are associated with the open ports that were discovered is by banner grabbing.

Banner grabbing takes nothing more than the Telnet and FTP client built in to the Windows and Linux platforms. Banner grabbing provides important information about what type and version of software is running. Many servers can be exploited with just a few simple steps if the web server is not properly patched. Telnet is an easy way to do this banner grabbing for FTP, SMTP, HTTP, and others. The command issued to banner grab with Telnet would contain the following syntax: `Telnet (IP_Address) Port`. Any example of this is shown here. This banner grabbing attempt was targeted against a web server.

```
C:\>telnet 192.168.1.102 80
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Fri, 07 Oct 2005 22:22:04 GMT
Content-Type: text/html
```

```
Content-Length: 87
<html><head><title>Error</title></head><body>The parameter is incorrect. </body>
</html>
Connection to host lost.
```

After the command was entered, telnet 192.168.1.102 80, the Return key was pressed a couple of times to generate a response. As noted in the Telnet response, this banner indicates that the web server is IIS 5.0.

EXAM ALERT

The Microsoft IIS web server's default behavior is to return a banner after two carriage returns. This can be used to pinpoint the existence of an IIS server.

Telnet isn't your only option for grabbing banners; netcat is another option. Netcat is shown here to introduce you to its versatility. Netcat is called the "Swiss army knife of hacking tools" because of its many uses. To banner grab with netcat, you would issue the following command for the command line:

```
nc -v -n IP_Address Port
```

This command will give you the banner of the port you asked to check. Netcat is available for Windows and Linux. If you haven't downloaded netcat, don't feel totally left behind, as FTP is another choice for banner grabbing. Just FTP to the target server and review the returned banner.

NOTE

Although changing banner information is not an adequate defense by itself, it might help to slow a hacker. In the Windows environment, you can install the UrlScan security tool. UrlScan contains the RemoveServerHeader feature, which removes or alters the identity of the server from the "Server" response header in response to the client's request.

Most all port scanners, including those discussed in this chapter, also perform banner grabbing.

Mapping the Network

The hacker would have now gained enough information to map the network. Mapping the network provides the hacker with a blueprint of the organization. There are manual and automated ways to compile this information. Manual and automated tools are discussed in the following sections.

Manual Mapping

If you have been documenting findings, the matrix you began at the start of this chapter should be overflowing with information. This matrix should now contain domain name information, IP addresses, DNS servers, employee info, company location, phone numbers, yearly earnings, recently acquired organizations, email addresses, the publicly available IP address range, open ports, wireless access points, modem lines, and banner details.

Automated Mapping

If you prefer a more automated method of mapping the network, a variety of tools are available. Visual traceroute programs, such as NeoTrace and Visual Route, are one option. Running traceroute to different servers, such as web, email, and FTP, can help you map out the placement of these servers. Automatic mapping can be faster but might generate errors or sometimes provide erroneous results.

When Your Traceroutes Led to the Middle of the Atlantic Ocean

Not quite the middle of the ocean, but the country of Sealand is about six miles off the coast of England. This platform of concrete and steel was originally built during World War II to be used as an anti-aircraft platform but later abandoned. Established as its own country since 1967, the country of Sealand now provides non-traceable network services and has the world's most secure managed servers. Because Sealand is its own country, servers located there are exempt from government subpoenas and search and seizures of equipment or data. Some might see this as ultimate privacy, whereas others might interpret this as a haven for illegal activities.

NLog is one option to help keep track of your scanning and mapping information. NLog allows you to automate and track the results of your nmap scans. It allows you to keep all of your nmap scan logs in a database, making it possible to easily search for specific entries. It's browser based, so you can easily view the scan logs in a highly customizable format. You can add your own extension scripts for different services, so all hosts running a certain service will have a hyperlink to the extension script.

Cheops is another network mapping option. If run from the Internet, the tool will be limited to devices that it can contact. These will most likely be devices within the *demilitarized zone (DMZ)*. Run internally, it will diagram a large portion of the network. In the hands of a hacker, it's a powerful tool, as it uses routines taken from a variety of other tools that permit it to perform OS detection port scans for service detection and network mapping using common traceroute techniques. Linux users can download it from www.marko.net/cheops.

THE SEVEN STEPS OF THE PREATTACK PHASE

Step	Title	Active/Passive	Common Tools
One	Information gathering	Passive	Sam Spade, ARIN, IANA, Whois, Nslookup
Two	Determining network range	Passive	RIPE, APNIC, ARIN
Three	Identify active machines	Active	Ping, traceroute, Superscan, Angry IP scanner
Four	Finding open ports and applications	Active	Nmap, Amap, SuperScan
Five	OS fingerprinting	Active/passive	Nmap, Winfigerprint, P0f, Xprobe2, ettercap
Six	Fingerprinting services	Active	Telnet, FTP, Netcat
Seven	Mapping the network	Active	Cheops, traceroute, NeoTrace

Summary

In this chapter, you learned the seven steps that compose the preattack phase. These include information gathering, determining the network range, identifying active machines, finding open ports and access points, OS fingerprinting, fingerprinting services, and mapping the network.

This chapter is an important step for the ethical hacker because at this point, you are attempting to gather enough information to launch an attack. The more information that is gathered here, the better the chance of success. An important part of ethical hacking is documentation. That's why several ways to collect and document your findings are shown. These notes will be useful when you prepare your report. Finally, make sure that the organization has given you written permission before beginning any work, even the reconnaissance.

Key Terms

- Active fingerprinting
- CNAMES
- Covert channel
- Demilitarized zone (DMZ)
- DoS
- Echo reply
- Echo request
- EDGAR database
- Google dorks
- Google hacking
- Initial Sequence Number
- Internet Assigned Numbers Authority (IANA)
- Information matrix
- Intrusion detection system
- Nslookup
- Open source
- Ping sweep
- Passive fingerprinting
- Port knocking
- Port scanning
- Scope creep
- Script kiddie
- Simple Network Monitoring Protocol (SNMP)
- Social engineering
- Synchronize sequence number
- Time-to-live (TTL)
- Traceroute
- Wardialing
- Wardriving
- Whois
- Written authorization
- Zone transfer

Apply Your Knowledge

You have seen many of the tools used for passive reconnaissance in this chapter. Passive reconnaissance is the act of gathering as much information about a target as passively as you can. Tools such as Whois, Nslookup, Sam Spade, traceroute, ARIN, and IANA are all useful for this task.

In this exercise, you will gather information about several organizations. Your goal is to use the tools discussed in the chapter for passive information gathering. No port scans, no OS fingerprinting, or banner grabbing should be performed. Treat these organizations with the utmost respect.

Exercises

3.1 Performing Passive Reconnaissance

The best way to learn passive information gathering is to use the tools. In this exercise, you will perform reconnaissance on several organizations. Acquire only the information requested.

Estimated Time: 20 minutes.

1. Review Table 3.7 to determine the target of your passive information gathering.

TABLE 3.7 Passive Information Gathering

Domain Name	IP Address	Location	Contact Person	Phone Number	Address
Redriff.com					
Examcram.com					
	72.3.246.59				
Rutgers.edu					

2. Start by resolving the IP address. This can be done by pinging the site.
3. Next, use a tool such as Sam Spade or any of the other tools mentioned throughout the chapter. Some of these include
   - www.betterwhois.com
   - www.allwhois.com
   - http://geektools.com
   - www.all-nettools.com
   - www.dnsstuff.com
   - www.samspade.org

4. To verify the location of the organization, perform a traceroute or a ping with the –r option.
5. Use the ARIN, RIPE, and IANA to fill in any information you have yet to acquire.
6. Compare your results to those found in Table 3.8.

TABLE 3.8 Passive Information Gathering

Domain Name	IP Address	Location	Contact Person	Phone Number	Address
Redriff.com	64.235.246.143	Los Angeles, CA	Admin	213-683-9910	5482 Wilshire Blvd
Examcram.com	63.240.93.157	Old Tappan, NJ	Kenneth Simmons	201-784-6187	123 Old Tappan Rd
Theregister.com	72.3.246.59	Southport Merseyside, UK	Philip Mitchell	+44-798-089-8072	19 Saxon Road
Rutgers.edu	128.6.72.102	Piscataway, NJ	Net Manager	732-445-2293	110 Frelinghuysen Road

3.2 Performing Active Reconnaissance

The best way to learn active information gathering is to use the tools. In this exercise, you will perform reconnaissance on your own internal network. If you are not on a test network make sure you have permission before scanning or it may be seen as the precursor of an attack.

Estimated Time: 15 minutes.

1. Download the most current version of Nmap from www.insecure.org/nmap/download.html. For Windows systems, the most current version is 3.95.
2. Open a command prompt and go to the directory that you have installed Nmap in.
3. Run Nmap –h from the command line to see the various options.
4. You'll notice that Nmap has many different options. Review and find the option for a full connect scan. Enter your result here: _____
5. Review and find the option for a stealth scan. Enter your result here: ____
6. Review and find the option for a UDP scan. Enter your result here: ____
7. Review and find the option for a fingerprint scan. Enter your result here: ____
8. Perform a full connect scan on one of the local devices you have identified on your network. The syntax is `Nmap -sT IP_Address`.
9. Perform a stealth scan on one of the local devices you have identified on your network. The syntax is `Nmap -sS IP_Address`.
10. Perform a UDP scan on one of the local devices you have identified on your network. The syntax is `Nmap -sU IP_Address`.

11. Perform a fingerprint scan on one of the local devices you have identified on your network. The syntax is `Nmap -O IP_Address`.

12. Observe the results of each scan. Was Nmap capable of successfully identifying the system? Were the ports it identified correct?

Exam Questions

1. Your client has asked you to run an Nmap scan against the servers they have located in their DMZ. They would like you to identify the OS. Which of the following switches would be your best option?

   - ❍ **A.** Nmap –P0
   - ❍ **B.** Nmap -sO
   - ❍ **C.** Nmap -sS
   - ❍ **D.** Nmap -O

2. Which of the following should be performed first in any penetration test?

   - ❍ **A.** Social engineering
   - ❍ **B.** Nmap port scanning
   - ❍ **C.** Passive information gathering
   - ❍ **D.** OS fingerprinting

3. ICMP is a valuable tool for troubleshooting and reconnaissance. What is the correct type for a ping request and a ping response?

   - ❍ **A.** Ping request type 5, ping reply type 3
   - ❍ **B.** Ping request type 8, ping reply type 0
   - ❍ **C.** Ping request type 3, ping reply type 5
   - ❍ **D.** Ping request type 0, ping reply type 8

4. You have become interested in fragmentation scans and how they manipulate the MTU value. What is the minimum value specified for IP's MTU?

   - ❍ **A.** 1500 bytes
   - ❍ **B.** 576 bytes
   - ❍ **C.** 68 bytes
   - ❍ **D.** 1518 bytes

5. Which of the following does Nmap require for an OS identification?

   - ❍ **A.** One open and one closed port
   - ❍ **B.** Two open ports and one filtered port
   - ❍ **C.** One closed port
   - ❍ **D.** One open port

6. Which of the following netcat commands could be used to perform a UDP scan of the lower 1024 ports.

   - ❍ **A.** Nc -sS -O target 1-1024
   - ❍ **B.** Nc –hU <host(s)>
   - ❍ **C.** Nc –sU –p 1-1024 <host(s)>
   - ❍ **D.** Nc –u –v –w2 <host> 1-1024

7. Which of the following terms is used to refer to a network that is connected as a buffer between a secure internal network and an insecure external network such as the Internet?

   - ❍ **A.** A proxy
   - ❍ **B.** DMZ
   - ❍ **C.** IDS
   - ❍ **D.** Bastion host

8. What is a null scan?

   - ❍ **A.** A scan in which the FIN, URG, and PSH flags are set
   - ❍ **B.** A scan in which all flags are off
   - ❍ **C.** A scan in which the SYN flag is on
   - ❍ **D.** A scan in which the window size is altered

9. You have captured some packets from a system you would like to passively fingerprint. You noticed that the IP header length is 20 bytes and there is a datagram length of 84 bytes. What do you believe the system to be?

   - ❍ **A.** Windows 98
   - ❍ **B.** Linux
   - ❍ **C.** Windows 2000
   - ❍ **D.** Windows NT

10. Which of the following tools is used for passive OS guessing?

- ❍ **A.** Nmap
- ❍ **B.** P0f
- ❍ **C.** Queso
- ❍ **D.** Xprobe 2

11. This type of scan is harder to perform because of the lack of response from open services and because packets could be lost due to congestion or from firewall blocked ports.

- ❍ **A.** Stealth scanning
- ❍ **B.** ACK scanning
- ❍ **C.** UDP scanning
- ❍ **D.** FIN Scan

12. A connect or SYN scan of an open port produces which of the following responses from a target?

- ❍ **A.** SYN/ACK
- ❍ **B.** ACK
- ❍ **C.** RST
- ❍ **D.** RST/ACK

13. You have just performed an ACK scan and have been monitoring a sniffer while the scan was performed. The sniffer captured the result of the scan as an ICMP type 3 code 13. What does this result mean?

- ❍ **A.** The port is filtered at the router.
- ❍ **B.** The port is open.
- ❍ **C.** The target is using a port knocking technique.
- ❍ **D.** The port is closed.

14. One of the members of your security assessment team is trying to find out more information about a client's website. The Brazilian-based site has a .com extension. She has decided to use some online whois tools and look in one of the regional Internet registries. Which of the following represents the logical starting point?

- ❍ **A.** AfriNIC
- ❍ **B.** ARIN
- ❍ **C.** APNIC
- ❍ **D.** RIPE

15. While footprinting a network, what port/service should you look for to attempt a zone transfer?

    - ❍ **A.** 53 UDP
    - ❍ **B.** 53 TCP
    - ❍ **C.** 161 UDP
    - ❍ **D.** 22 TCP

Answers to Exam Questions

1. **D**. Running Nmap –O would execute OS guessing. Answer A is incorrect, as Nmap –P0 means do not ping before scanning. Answer B is incorrect because Nmap –sO would perform a IP Protocol scan. Answer C is incorrect, as Nmap –sS would execute a TCP stealth scan.

2. **C**. Passive information gathering should be the first step performed in the penetration test. EC-Council defines seven steps in the pre-attack phase, which include passive information gathering, determining the network range, identifying active machines, finding open ports and access points, OS fingerprinting, fingerprinting services, and mapping the network. Answer A is incorrect because social engineering is not the first step in the process. Answer B is incorrect, as Nmap port scanning would not occur until after passive information gathering. Answer D is incorrect because OS fingerprinting is one of the final steps, not the first.

3. **B**. Ping is the most common ICMP type. A ping request is a type 8, and a ping reply is a type 0. All other answers are incorrect because a request is always a type 8 and a reply is always a type 0. An ICMP type 5 is redirect, and a type 3 is destination unreachable. For a complete listing of ICMP types and codes, reference RFC 792.

4. **C**. RFC 1191 specifies that when one IP host has a large amount of data to send to another host, the data is transmitted as a series of IP datagrams. IP is designed so that these datagrams be of the largest size that does not require fragmentation anywhere along the path from the source to the destination. The specified range is from 68 to 65535 bytes. Answer A is incorrect, as 1500 bytes is the MTU for Ethernet. Answer B is incorrect, as 576 bytes is the default MTU for IP. Answer D is incorrect because that value is the frame size for Ethernet.

5. **A**. Nmap requires one open and one closed port to perform OS identification. Answers B, C, and D are incorrect because none of these answers list one open and one closed port, which is the minimum required for OS identification.

6. **D**. The proper syntax for a UDP scan using Netcat is Netcat –u –v –w2 <host> 1-1024. Netcat is considered the Swiss army knife of hacking tools because it is so versatile. Answers A, B, and C are incorrect because they do not correctly specify the syntax used for UDP scanning with netcat.

7. **B**. A DMZ is a separate network used to divide the secure inner network from the unsecure outer network. Services such as HTTP, FTP, and email may be placed there. Answer A is incorrect, as a proxy is simply a system that stands in place of and does not specifically define a DMZ. Answer C is incorrect because an IDS is used to detect intrusions or abnormal traffic. Answer D is incorrect,

as a bastion host is a computer that is fully on the public side of the demilitarized zone and is unprotected by a firewall or filtering router.

8. **B**. A null scan is a TCP-based scan in which all flags are turned off. Answer A is incorrect because it describes a XMAS scan. Answer C is incorrect because this could describe a TCP full connect of a stealth scan. Answer D is incorrect, as it describes a TCP WIN scan.

9. **B**. Active fingerprinting works by examining the unique characteristics of each OS. One difference between competing platforms is the datagram length. On a Linux computer, this value is typically 84, whereas Microsoft computers default to 60. Therefore, answers A, C, and D are incorrect, as they are all Windows OSes.

10. **B**. P0f is a passive OS fingerprinting tool. Answers A, C, and D are incorrect, as Queso was the first active fingerprinting tool, Nmap is probably the most well-known, and Xprobe 2 is the next generation of OS fingerprinting tools. These active tools have the capability to look at peculiarities in the way that each vendor implements the RFCs. These differences are compared with its database of known OS fingerprints. Then a best guess of the OS is provided to the user.

11. **C**. UDP scanning is harder to perform because of the lack of response from open services and because packets could be lost due to congestion or a firewall blocking ports. Answer A is incorrect, as a stealth scan is a TCP-based scan and is much more responsive than UDP scans. Answer B is incorrect because an ACK scan is again performed against TCP targets to determine firewall settings. Answer D is incorrect, as FIN scans also target TCP and seek to elicit a RST from a Windows-based system.

12. **A**. A full connect or SYN scan of a host will respond with a SYN/ACK if the port is open. Answer B is incorrect, as an ACK is not the normal response to the first step of a three step startup. Answer C is incorrect because an RST is used to terminate an abnormal session. Answer D is incorrect because an RST/ACK is not a normal response to a SYN packet.

13. **A**. An ICMP type 3 code 13 is administrative filtered. This type response is returned from a router when the protocol has been filtered by an ACL. Answer B is incorrect, as the ACK scan only provides a filtered or unfiltered response; it never connects to an application to confirm an open state. Answer C is incorrect, as port knock requires you to connect to a certain number of ports in a specific order. Answer D is incorrect, as again, an ACK scan is not designed to report a closed port; its purpose it to determine the router or firewall's rule set. Although this might appear limiting, the ACK scan can characterize the capability of a packet to traverse firewalls or packet filtered links.

14. **B**. Regional registries maintain records from the areas from which they govern. ARIN is responsible for domains served within North and South America; therefore, would be the logical starting point for that .com domain. Answer A is incorrect because AfriNIC is the RIR proposed for Africa. Answer C is incorrect because APNIC is the RIR for Asia and Pacific Rim countries. Answer D is incorrect because RIPE is the RIR for European-based domains.

15. **B**. TCP port 53 is used for zone transfers; therefore, if TCP 53 is open on the firewall, there is an opportunity to attempt a zone transfer. Answer A is incorrect, as UDP 53 is typically used for DNS lookups. Answer C is incorrect because UDP 161 is used for SNMP. Answer D is incorrect, as TCP 22 is used for SSH.

Suggested Reading and Resources

www.infosecwriters. com/text_resources/doc/Demystifying_Google_Hacks.doc—Demystifying Google hacks

www.professionalsecuritytesters.org/modules.php?name=Downloads&d_op=getit&lid=13—Reconnaissance and footprinting cheat sheet

http://www.windowsnetworking.com/kbase/WindowsTips/WindowsXP/AdminTips/Network/nslookupandDNSZoneTransfers.html—DNS zone transfers

http://www.auditmypc.com/freescan/readingroom/port_scanning.asp—Port scanning techniques

http://johnny.ihackstuff.com/security/premium/The_Google_Hackers_Guide_v1.0.pdf—The Google Hackers Guide

http://www.securityfocus.com/infocus/1224—Passive fingerprinting

www.microsoft.com/technet/archive/winntas/maintain/tcpip.mspx—TCP/IP from a security viewpoint

www.sys-security.com/archive/papers/ICMP_Scanning_v2.5.pdf—ICMP usage in scanning