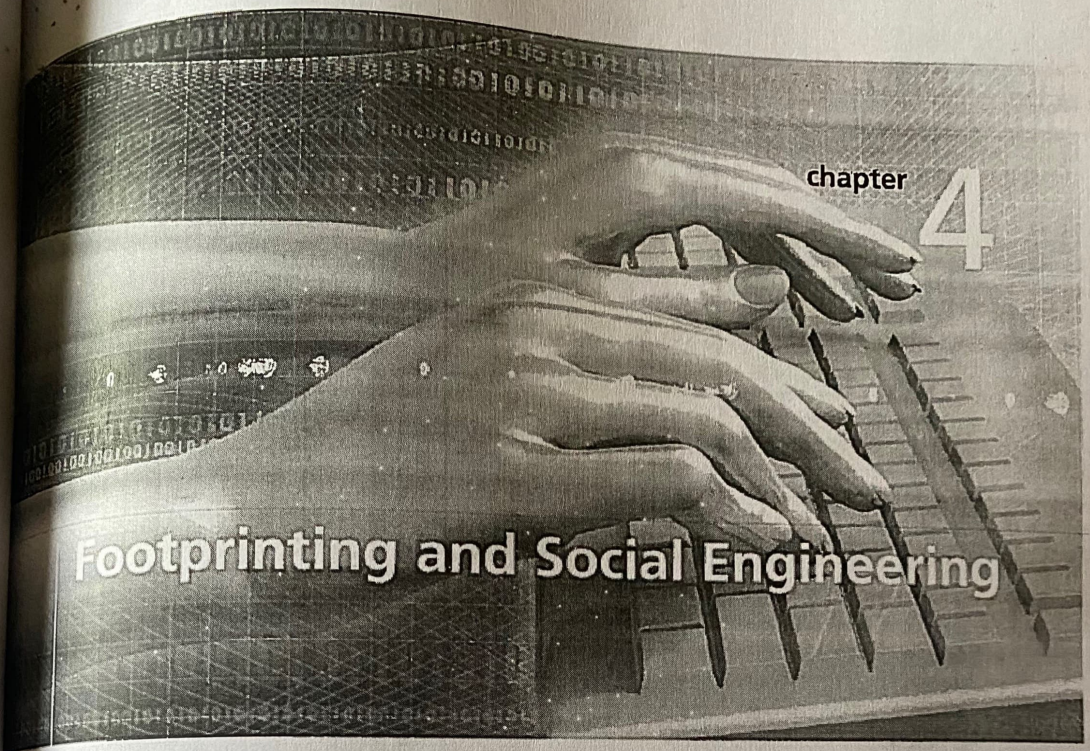


After reading this chapter and completing the exercises, you will be able to:

- Use Web tools for footprinting
- Conduct competitive intelligence
- Describe DNS zone transfers
- Identify the types of social engineering

unit II (1).

In this chapter, you learn how to use tools readily available on the Internet to find out how a company's network is designed. You also learn the skills needed to conduct competitive intelligence and how to use these skills for information gathering. Before you conduct a security test on a network, you need to perform most, if not all, of the footprinting tasks covered in this chapter.

This chapter also explains the tactics of attackers who use social engineering to get information from a company's key employees. In addition, you examine some of the less glamorous methods attackers use—such as looking through garbage cans, wastepaper baskets, and dumpsters for old computer manuals, discarded disks, and other materials—to find information that can enable them to break into a network.

Using Web Tools for Footprinting

In movies, before a thief robs a bank or steals jewelry, he "cases the joint" by taking pictures and getting floor plans. Movie thieves are usually lucky enough to get schematics of alarm systems and air-conditioning/ventilation systems, too. At least, that's how Hollywood portrays thieves. Any FBI agent would tell you that most real-life thieves aren't that lucky. However, the smart ones who don't get caught are meticulous and cautious. Many attackers do case the joint to look over the location, find weaknesses in the security system, and determine what types of locks and alarm systems are being used. They try to gather as much information as possible before committing a crime.

As a security tester, you, too, must find out as much as you can about the organization that hired you to test its network security. That way, you can advise management of any problem areas. In computer jargon, the process of finding information on a company's network is called footprinting. You might also hear the term "reconnaissance" used, and you should be familiar with both terms. An important concept is that footprinting is passive, or nonintrusive; in other words, you aren't accessing information illegally or gathering unauthorized information with false credentials. The security tester (or attacker) tries to discover as much as possible about the organization and its network. Table 4-1 lists some of the many tools available for footprinting.

Table 4-1 Summary of Web tools

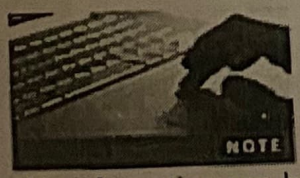
Tool	Function
Google groups (http://groups.google.com)	Search for e mail addresses in technical or nontechnical newsgroup postings
Whois (www.arin.net or www.whois.net)	Gather IP and domain information
SamSpade (www.samspade.org)	Gather IP and domain information; versions available for UNIX and Windows OSs
Web Data Extractor (www.rafasoft.com)	Extract contact data, such as e mail, phone, and fax information, from a selected target
FOCA (www.informatica64.com/FOCA)	Extract metadata from documents on Web sites to reveal the document creator's network logon and e mail address, information on IP addresses of internal devices, and more

Table 4-1 Summary of Web tools (*continued*)

Tool	Function
Necrosoft NScan (*www.nscan.org*)	Windows scanning, DNS lookup, and advanced Dig tools (see Dig command later in this table)
Google search engine (*www.google.com*)	Search for Web sites and company data
Namedroppers (*www.namedroppers.com*)	Run a domain name search; more than 30 million domain names updated daily
White Pages (*www.whitepages.com*)	Conduct reverse phone number lookups and retrieve address information
Metis (*www.severus.org/sacha/metis*)	Gather competitive intelligence from Web sites
Dig (command available on all *nix systems; can be downloaded from *http://members.shaw.ca/nicholas.fong.dig/* for Windows platforms)	Perform DNS zone transfers; replaces the Nslookup command
Netcat (command available on all *nix systems; can be downloaded from *www.securityfocus.com/tools/139* for Windows platforms)	Read and write data to ports over a network
Wget (command available on all *nix systems; can be downloaded from *http://gnu.org/software/wget/wget.html* for Windows platforms)	Retrieve HTTP, HTTPS, and FTP files over the Internet
Paros (*www.parosproxy.org*)	Capture Web server information and possible vulnerabilities in a Web site's pages that could allow exploits such as SQL injection and buffer overflow attacks
Maltego (*www.paterva.com/web4/index.php/maltego*; also on the book's DVD)	Gather competitive intelligence and represent in graphical form previously unknown relationships between personal identities, companies, and Internet networks

Many command-line utilities included for *nix systems aren't part of a Windows environment. For example, the Dig, Netcat, and Wget commands don't work from a Windows XP or Vista command prompt, but you can usually download Windows versions from the Web sites listed in Table 4-1. Security testers should spend time learning to use these command-line tools on a *nix system.

In this chapter, you use the SamSpade Whois utility to get information about a company's Web presence and see how DNS zone transfers can be used to determine computers' IP address ranges and hostnames.



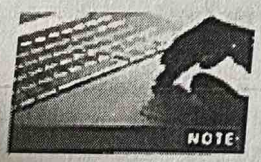
Security Bytes

Each year, Department of Defense (DoD) employees are required to complete security awareness training that emphasizes the dangers of terrorists and spies being able to collect unclassified information. This information can be found in newspapers, Web sites, and TV and radio news programs. By putting small pieces of information together, terrorists can get a fairly detailed picture of the DoD's activities. The DoD wants its employees to realize that discussing seemingly inconsequential information might be more dangerous than imagined. This information, when combined with information from other sources, can be damaging to national security.

For example, a sailor meets a friend in a restaurant and mentions that he'll be gone for six months. At the same restaurant, a civilian working for the DoD mentions over lunch with a friend that she has to work a lot of overtime ordering more supplies. As you can see, terrorists could easily pick up both pieces of information by listening in on conversations. This example might sound farfetched, but it's a major method of gathering intelligence. The point is that you, too, need to pay attention to all information that's available, whether it's on a Web site, in e-mail headers, or in an employee's statement in an interview. Unfortunately, attackers check Web pages and newsgroups, examine IP addresses of companies, and look for postings from IT personnel asking questions about OSs or firewall configurations. Remember that after gathering a piece of information, you shouldn't stop there. Continue to dig to see what else potential attackers could discover.

Conducting Competitive Intelligence

If you want to open a piano studio to compete against another studio that has been in your neighborhood for many years, getting as much information as possible about your competitor is wise. How could you know the studio was successful without being privy to its bank statements? First, many businesses fail after the first year, so the studio being around for years is a testament to the owner doing something right. Second, you can simply park your car across the street from the studio and count the students entering to get a good idea of the number of clients. You can easily find out the cost of lessons by calling the studio or looking for ads in newspapers, flyers, telephone books, billboards, and so on. Numerous resources are available to help you discover as much as is legally possible about your competition. Business people have been doing this for years. Now this information gathering, called **competitive intelligence**, is done on an even higher level through technology. As a security professional, you should be able to explain to your clients the methods competitors use to gather information. To limit the amount of information a company makes public, you need a good understanding of what a competitor would do to discover confidential information.



Security Bytes

Just because you're able to find information about a company and its employees doesn't mean you should divulge it. For example, you discover that an employee is visiting a dating service Web site or questionable newsgroups. As long as this activity doesn't jeopardize the company in any way, as a security tester, you're not obligated to inform the company. Depending on the laws of your country or state, privacy issues might affect your decision on how to handle this situation. Security professionals and company officials can be sued for releasing confidential information of this nature.

Analyzing a Company's Web Site

Network attacks often begin by gathering information from a company's Web site because Web pages are an easy way for attackers to discover critical information about an organization. Many tools are available for this type of information gathering. For example, Paros is a powerful tool for UNIX and Windows OSs that can be downloaded free (*www.parosproxy.org*).

The screenshots in this section are intended to show one of the many tools that can be used to gather information about a company's Web site and discover any existing vulnerabilities. The specific tool used isn't important. What's important is that you understand the process a security tester uses when beginning a security test.

Paros requires having Java J2SE installed (downloaded from *www.sun.com*). Figure 4-1 shows the main window of Paros.

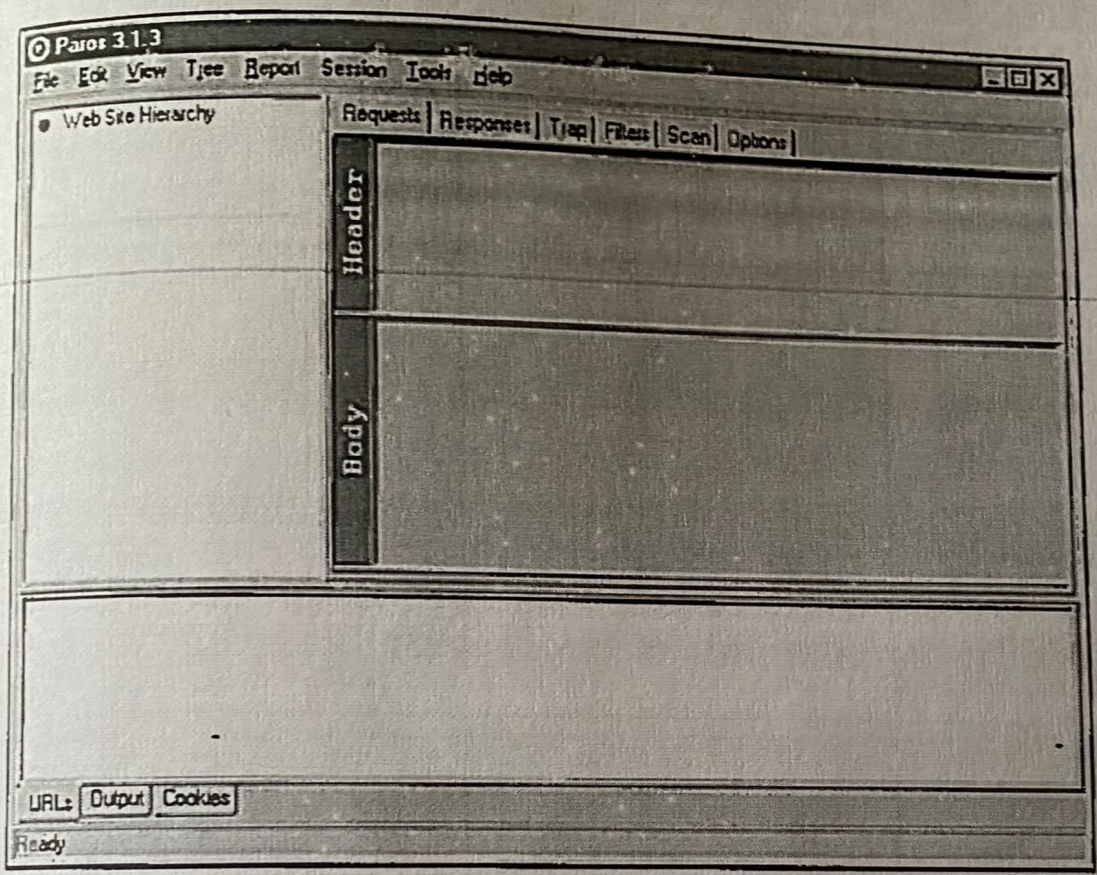


Figure 4-1 The main window of Paros

Courtesy Course Technology/Cengage Learning

Clicking Tools, Spider from the menu prompts you for the Web site's URL, as shown in Figure 4-2.

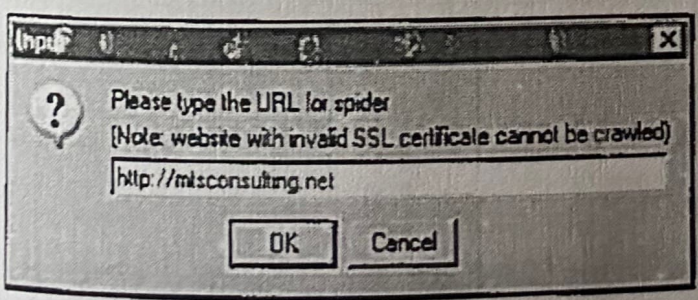


Figure 4-2 Entering a URL in the Input dialog box

Courtesy Course Technology/Cengage Learning

In a matter of seconds, the filenames of every Web page the site contains are displayed (see Figure 4-3).

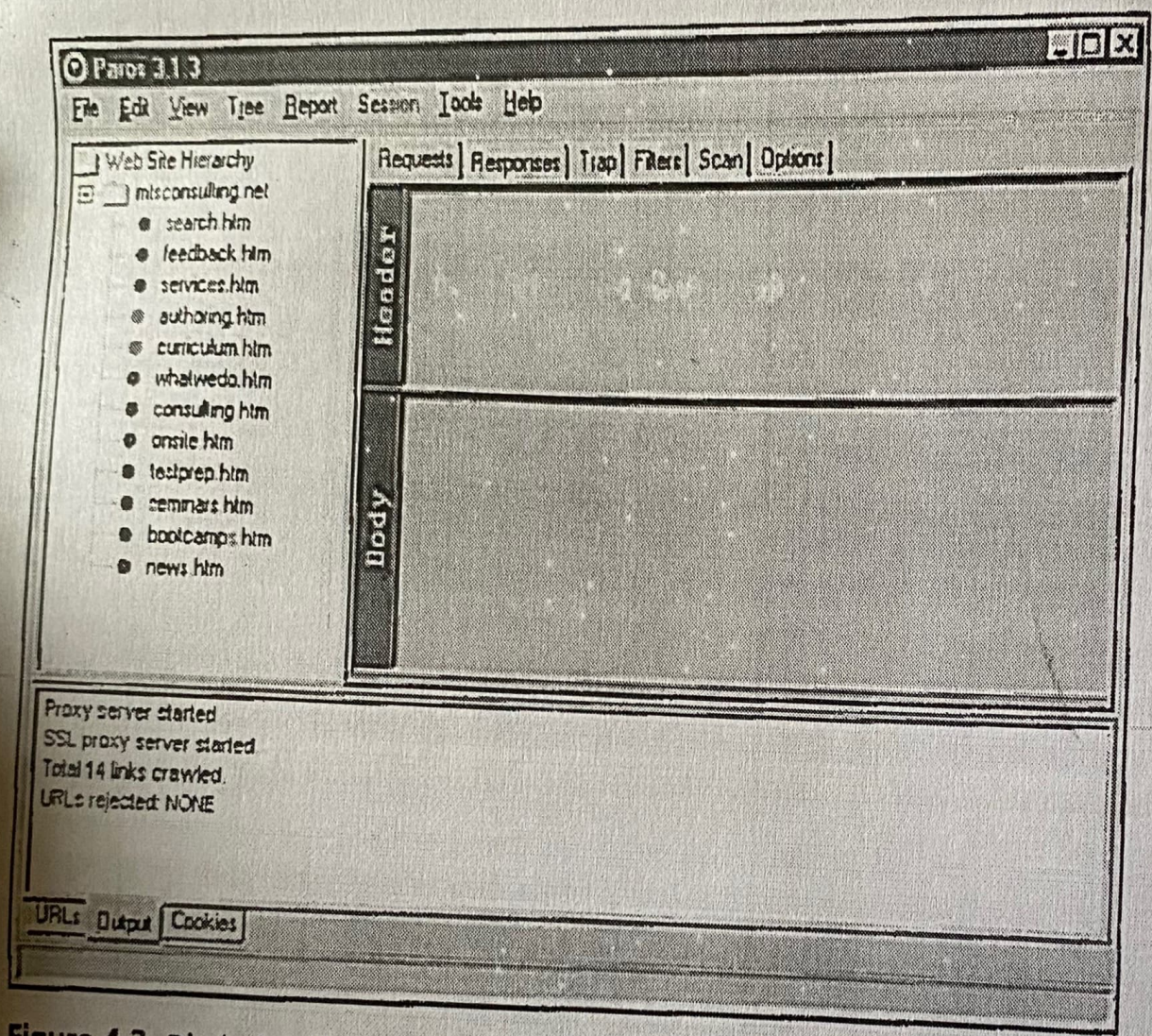


Figure 4-3 Displaying filenames of all Web pages on a site

Courtesy Course Technology/Cengage Learning

After clicking Tree, Scan All from the menu, a report similar to the one in Figure 4-4 is displayed. This report can show an attacker how a Web site is structured and lists Web pages that can be investigated for further information.

As you can see, the scan feature allows testing areas of the site that might have problems. Any vulnerabilities in the Web site are indicated in the Risk Level column as High. In this example, the risk level is flagged as Informational. However, the scan indicates the Internet Information Services (IIS) version used for this Web site, which can be useful information for conducting further investigations or testing. Gathering competitive intelligence through scans of this type

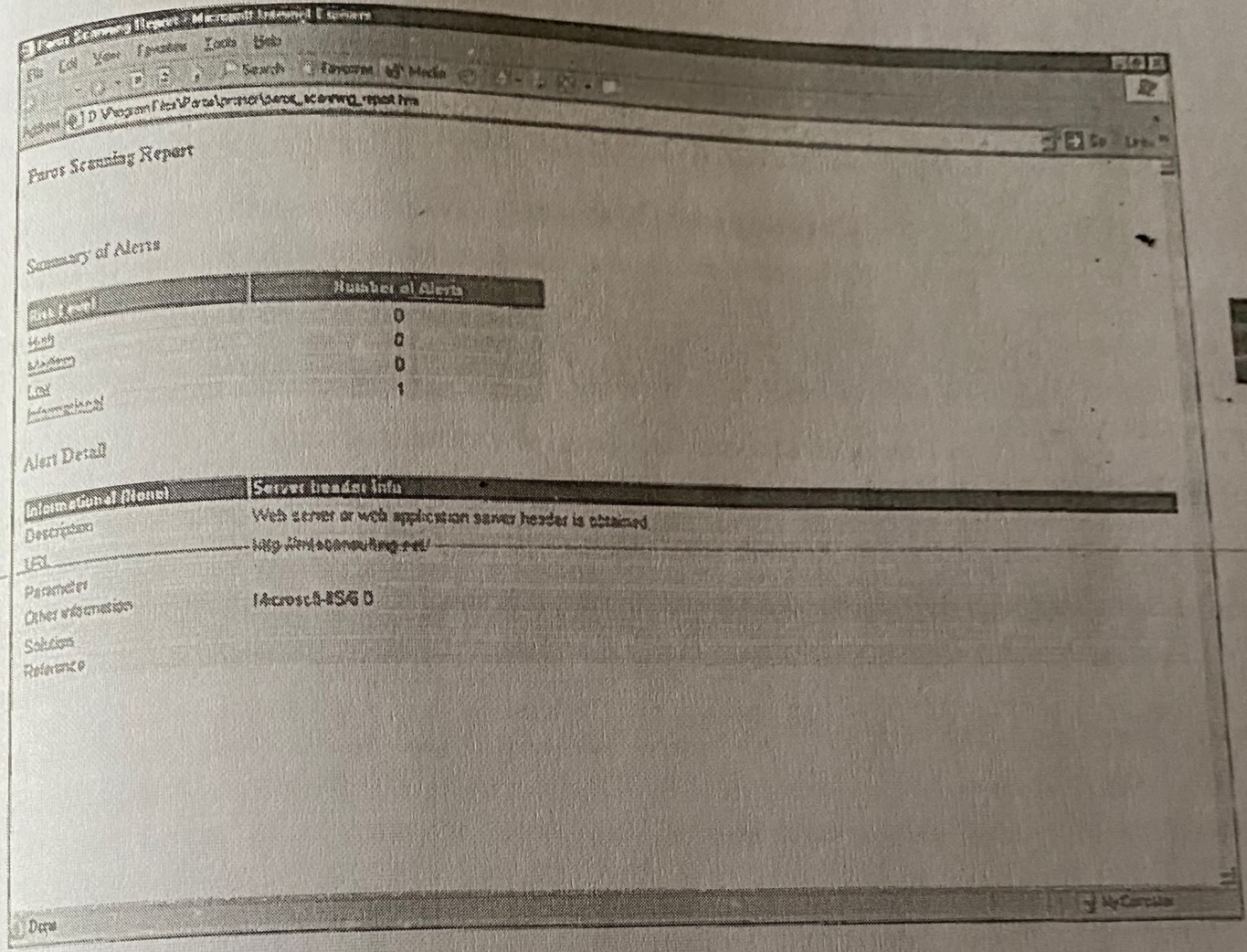


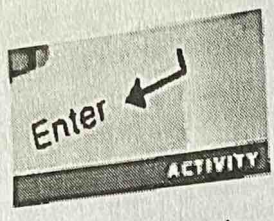
Figure 4-4 The Paros scanning report

Courtesy Course Technology/Cengage Learning

is time consuming, and the more you find out, the deeper you want to dig. Setting a reasonable time frame for this phase of your investigation is important, or you might spend too much time on this activity. On the other hand, you don't want to rush your information gathering because much of what you learn can be used for further testing and investigation. The following section covers additional tools you can use for gathering information.

Using Other Footprinting Tools

The Whois utility is a commonly used Web tool for gathering IP address and domain information. With just a company's Web address, you can discover a tremendous amount of information. Unfortunately, attackers can also make use of this information. Often companies don't realize they're publishing information on the Web that computer criminals can use. The Whois utility gives you information on a company's IP addresses and any other domains the company might be part of. In Activity 4-1, you practice using the SamSpade Whois utility.



Activity 4-1: Using Footprinting Tools

Time Required: 30 minutes

Objective: Learn how to use footprinting tools, such as the SamSpade Whois utility.

Description: Security testers need to know how to use tools for gathering information about networks. With the Whois utility, you can discover which network configuration factors might be used in attacking a network.

1. Start your Web browser, and go to www.samspade.org.
2. Type mit.edu in the Whois text box, click the Whois button, and then scroll down and view the information displayed (see Figure 4-5).

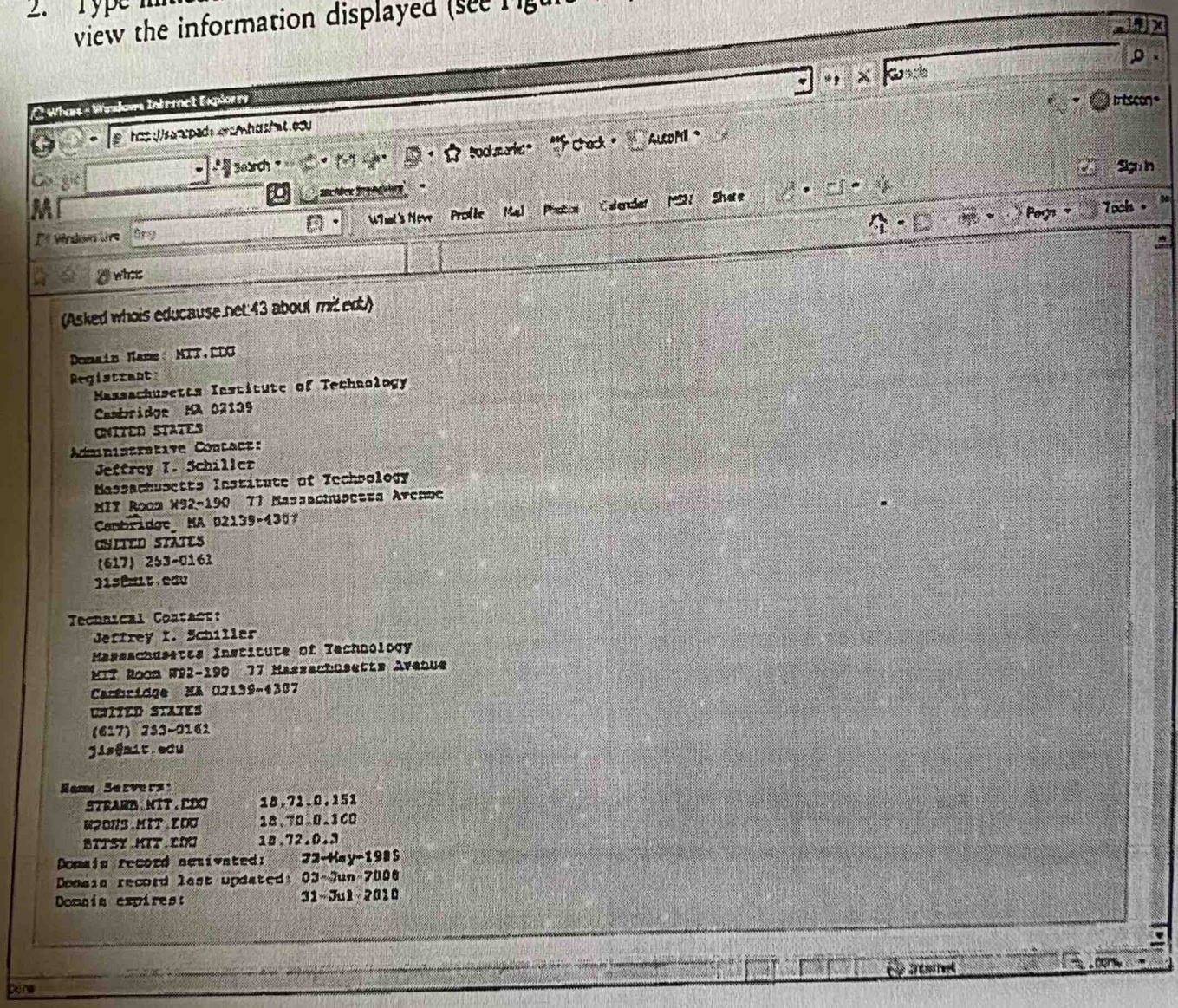


Figure 4-5 Viewing information with the SamSpade Whois utility

Courtesy Course Technology/Cengage Learning

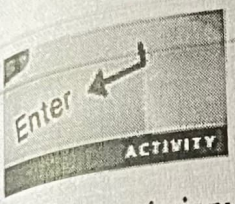
3. Note the name of the person listed in the Administrative Contact section. This information is important when you do Activity 4-2 later in the chapter. Also, note the IP addresses and name servers listed. Chapter 5 covers port scanning and explains how these IP addresses can be used to gather more information about name servers.
4. Try entering several other organizations in the Whois text box and repeat Steps 2 and 3. Note that some organizations are more discreet about what's listed in their output

screens. For example, when describing an administrative contact, giving just a job title is better than listing an actual name, as you'll soon discover.

5. Leave your Web browser open for the next activity.

Using E-mail Addresses

After seeing the information you can gather with the commands covered in this chapter, you might wonder what else you can do. Knowing a user's e-mail address can help you dig even further. Based on an e-mail account listed in DNS output, you might discover that the company's e-mail address format is first name initial, followed by last name and the *@companyname.com* sequence. You can guess other employees' e-mail accounts by getting a company phone directory or searching the Internet for any *@companyname.com* references. *Groups.google.com* is the perfect tool for this job. In Activity 4-2, you use it to find corporate e-mail addresses.



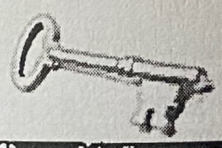
Activity 4-2: Identifying Corporate E-mail Accounts

Time Required: 30 minutes

Objective: Determine e-mail addresses for corporate employees.

Description: Knowing the e-mail addresses of employees can help you discover security vulnerabilities and gather competitive intelligence data. For example, you might discover that an employee has joined a newsgroup using his or her corporate e-mail account and shared proprietary information about the company. IT employees, when posting technical questions to a newsgroup, might reveal detailed information about the company's firewall or IDS, or a marketing director might mention a new ad campaign strategy the company is considering.

1. Start your Web browser, if necessary, and go to **http://groups.google.com**.
2. On the search page, type **@microsoft.com** and press Enter. This method is a fast and easy way to find e-mail accounts of people posting questions to the Microsoft domain.
3. Scroll down the list of items and try to find postings from employees who work at different companies. (*Hint*: Choose entries containing Re: in the listing. They're usually responses to questions sent by employees.) The list will vary, but it should give you an idea of the danger in using a company's e-mail address when posting questions to forums or newsgroups.

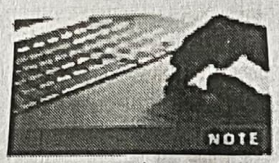


TIP

Remember that messages posted to newsgroups aren't private, and people can look them up for many years. You can test this by entering any e-mail address you've used in the past 10 years to post newsgroup messages. You might be surprised to find your messages still available for anyone to see. As a security tester, you should recommend that employees use a Web-based e-mail account (such as Hotmail or Gmail) rather than corporate e-mail accounts for posting messages to newsgroups.

4. In a new query, type **@sourcefire.com** and press Enter. Now you can find out who's posting questions to the security company SourceFire. Most likely, the postings are from users of SourceFire's products. Can you see how an attacker could use this information?
5. Scroll through the list and look for questions from employees of the security company and customers wanting advice. Could attackers use this information for negative purposes?

6. In a new query, enter the first and last name of the administrative contact you discovered in Activity 4-1. (*Tip*: Place quotation marks around the name to reduce the number of search results.)
7. Did you find any information that could be useful to a security tester? How old are many of the returned links?
8. To view more recent postings, modify your query to include "2008" and "2009". (Include the quotation marks around search terms to make sure you don't get phone numbers or addresses containing these numbers in your search results.)
9. Did the administrative contact use a different e-mail address in some postings? If yes, what could a security tester do with this information?
10. When you're finished, exit your Web browser.



The name used in the activity was obtained from the Whois utility. However, if you know a user's e-mail address, you can enter it in the *groups.google.com* search page. In Case Project 4-1, you get a chance to search on a specific e-mail address. If you were conducting a security test in the real world, you would search for e-mail accounts of IT staff and other key personnel.

Using HTTP Basics

As you learned in Chapter 3, HTTP operates on port 80. A security tester can pull information from a Web server by using HTTP commands. You've probably seen HTTP client error codes before, such as 404 Not Found. A basic understanding of HTTP can be beneficial to security testers, and you don't have to learn too many codes to get data from a Web server. If you know the return codes a Web server generates, you can determine what OS is used on the computer where you're conducting a security test. Table 4-2 lists common HTTP client errors, and Table 4-3 lists HTTP server errors that might occur.

Table 4-2 HTTP client errors

Error	Description
400 Bad Request	Request not understood by server
401 Unauthorized	Request requires authentication
402 Payment Required	Reserved for future use
403 Forbidden	Server understands the request but refuses to comply
404 Not Found	Unable to match request
405 Method Not Allowed (methods are covered later in this section)	Request not allowed for the resource
406 Not Acceptable	Resource doesn't accept the request
407 Proxy Authentication Required	Client must authenticate with proxy
408 Request Timeout	Request not made by client in allotted time
409 Conflict	Request couldn't be completed because of an inconsistency
410 Gone	Resource is no longer available

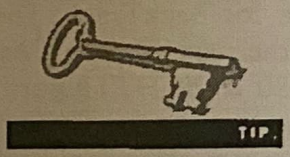
Table 4-2 HTTP client errors (*continued*)

Error	Description
411 Length Required	Content length not defined
412 Precondition Failed	Request header fields evaluated as false
413 Request Entity Too Large	Request is larger than server is able to process
414 Request URI (uniform resource identifier) Too Long	Request URI is longer than the server is willing to accept

Table 4-3 HTTP server errors

Error	Description
500 Internal Server Error	Request couldn't be fulfilled by the server
501 Not Implemented	Server doesn't support the request
502 Bad Gateway	Server received invalid response from the upstream server
503 Service Unavailable	Server is unavailable because of maintenance or overload
504 Gateway Timeout	Server didn't receive a timely response
505 HTTP Version Not Supported	HTTP version not supported by the server

In addition, you need to understand some of the available HTTP methods, shown in Table 4-4. You don't have to be fluent in using HTTP methods, but you need to be well versed enough to use the most basic HTTP method: `GET / HTTP/1.1`.

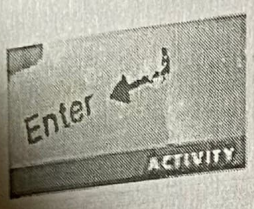


For a more detailed definition of HTTP methods, see RFC-2616.

Table 4-4 HTTP methods

Method	Description
GET	Retrieves data by URI
HEAD	Same as the GET method but retrieves only the header information of an HTML document, not the document body
OPTIONS	Requests information on available options
TRACE	Starts a remote Application layer loopback of the request message
CONNECT	Used with a proxy that can dynamically switch to a tunnel connection, such as Secure Sockets Layer (SSL)
DELETE	Requests that the origin server delete the identified resource
PUT	Requests that the entity be stored under the Request URI
POST	Allows data to be posted (that is, sent to a Web server)

If you know HTTP methods, you can send a request to a Web server and, from the generated output, determine what OS the Web server is using. You can also find other information that could be used in an attack, such as known vulnerabilities of operating systems and other software, as you learned in Chapter 3. After you determine which OS version a company is running, you can search for any exploits that might be used against that network's systems.

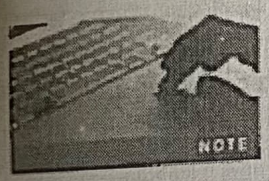


Activity 4-3: Using HTTP Methods

Time Required: 30 minutes

Objective: Determine Web server information by using HTTP methods.

Description: Armed with the information gathered from a company Web server by using basic HTTP methods, a security tester can discover system vulnerabilities and use this information for further testing. For example, querying a Web server might reveal that the server is running the Linux OS and using Apache software. In this activity, you use the Netcat command to connect to port 80 and then use HTTP methods.



If you can't get results in this activity by using mit.edu, the Web site has probably changed its security and won't allow using the HEAD or OPTIONS methods. If so, try using isecom.org instead of mit.edu.

1. Boot your computer into Linux with the BackTrack DVD. At the shell prompt, type startx and press Enter to open the KDE desktop manager for BackTrack. Then open a command shell by clicking the Konsole terminal icon on the panel taskbar. At the command prompt, type nc mit.edu 80 and press Enter. (Port 80 is the HTTP port.)
2. On the next line, type OPTIONS / HTTP/1.1 and press Enter. (Note the spaces around the slash character between the words OPTIONS and HTTP.)
3. On the next line, type HOST: 127.0.0.1 and press Enter twice. After several seconds, you see the screen shown in Figure 4-6.

```
root@5[root]# nc mit.edu 80
OPTIONS / HTTP/1.1
HOST: 127.0.0.1

HTTP/1.1 200 OK
Date: Mon, 22 Nov      21:43:55 GMT
Server: MIT Web Server Apache/1.3.26 Mark/1.4 (Unix) mod_ssl/2.8.8 OpenSSL/0.9.6g
Content-Length: 0
Allow: GET, HEAD, OPTIONS, TRACE

root@5[root]#
```

Figure 4-6 Using the OPTIONS HTTP method

Courtesy Course Technology/Cengage Learning

4. What information generated from the Netcat command might be useful to a security tester? What other options are available when accessing this Web server? (*Note*: Use Figure 4-6 to answer the question if the command doesn't work at this time.)

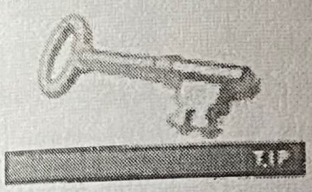
5. Type nc mit.edu 80 and press Enter.
6. On the next line, type HEAD / HTTP/1.0 and press Enter twice to retrieve header information. Your screen should look similar to Figure 4-7. Note the additional information the HEAD method produced, such as indicating that the connection has been closed and specifying the content length (16554 bytes).

```
root@3[root]# nc mit.edu 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 22 Nov      22:11:02 GMT
Server: MIT Web Server Apache/1.3.26 Mark/1.4 (Unix) mod_ssl/2.8.9 OpenSSL/0.9.
Last-Modified: Mon, 22 Nov      04:55:22 GMT
ETag: "71d07c0-40aa-41a1722a"
Accept-Ranges: bytes
Content-Length: 16554
Connection: close
Content-Type: text/html

root@3[root]#
```

Figure 4-7 Using the HEAD HTTP method

Courtesy Course Technology/Cengage Learning

7. Close the Konsole shell and log off Linux for the next activity.



To see additional parameters that can be used with the Netcat command, you can type nc -h at the command prompt (see Figure 4-8).

```
root@3[root]# nc -h
[v1.10]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
options:
        -e prog                 program to exec after connect [dangerous!!]
        -b                      allow broadcasts
        -g gateway              source-routing hop point[s], up to 8
        -G num                  source-routing pointer: 4, 8, 12, ...
        -h                      this cruft
        -i secs                 delay interval for lines sent, ports scanned
        -l                      listen mode, for inbound connects
        -n                      numeric-only IP addresses, no DNS
        -o file                 hex dump of traffic
        -p port                 local port number
        -r                      randomize local and remote ports
        -q secs                 quit after EOF on stdin and delay of secs
        -s addr                 local source address
        -t                      answer TELNET negotiation
        -u                      UDP mode
        -v                      verbose [use twice to be more verbose]
        -w secs                 timeout for connects and final net reads
        -z                      zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive]
root@3[root]#
```

Figure 4-8 Netcat parameters

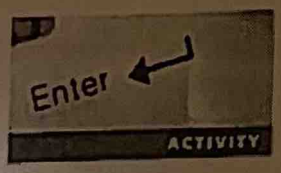
Courtesy Course Technology/Cengage Learning

Other Methods of Gathering Information

So far, you have learned several methods for gathering information from company Web sites and e-mail addresses. With just a URL, you can determine which Web server and OS a company is using and learn the names of IT personnel, for example. You need to be aware of other methods attackers use to gather information about a company. Some of these methods, such as using cookies and Web bugs, are unscrupulous.

Detecting Cookies and Web Bugs A cookie is a text file generated by a Web server and stored on a user's browser. The information in this file is sent back to the Web server when the user returns to the Web site. For example, a returning customer can be shown a customized Web page when he or she revisits an online store's Web site. Some cookies can cause security issues because unscrupulous people might store personal information in cookies that can be used to attack a computer or server.

A Web bug is a 1-pixel × 1-pixel image file referenced in an `<IMG>` tag, and it usually works with a cookie. Its purpose is similar to that of spyware and adware: to get information about the person visiting the Web site, such as an IP address, the time the Web bug was viewed, and the type of browser used to view the page. All this information can be useful to hackers. Web bugs are not from the same Web site as the Web page creator. They come from third-party companies specializing in data collection. Because Web bugs are just another image file, usually a GIF, they can't be blocked by a browser or rejected by a user. Also, Web bugs usually match the color of the Web page's background, which renders them invisible. If you don't have a tool for detecting Web bugs, usually the only way to find them is examining the Web page's source code to find a file in an `<IMG>` tag loading from a different Web server than other image files on the page. Security professionals need to be aware of cookies and Web bugs to keep these information-gathering tools off company computers.



Activity 4-4: Discovering Cookies in Web Pages

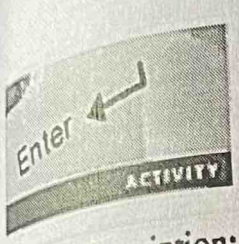
Time Required: 30 minutes

Objective: Determine whether cookies are present in Web pages.

Description: Many companies include cookies in their Web pages to gather information about visitors to their Web sites. This information might be used for competitive intelligence or, for example, to determine visitors' buying habits. Security testers should know how to verify whether a Web page contains cookies.

1. Boot your computer into Windows, and start the Mozilla Firefox Web browser. If you have been using this browser in Windows, cookies are probably loaded on your computer already, so you need to clear them and then visit a new site.
2. First, to clear any cookies from your computer, click **Tools**, **Options** from the browser menu. In the Options dialog box, click the **Privacy** icon at the top. In the Cookies section, click the **Show Cookies** button.
3. In the Cookies dialog box, click the **Remove All Cookies** button. Click **Close**, and then click **OK** to close the Options dialog box.

4. Next, go to www.amazon.com. Return to the Options dialog box and click Show Cookies again. If any cookies are listed, simply click one to view information about it. Do any of the cookies have personal information stored?
5. If time permits, visit some sites that require signing in with an account logon and password. See whether these sites create any cookies with personal information.
6. Click the Cancel button twice to return to the Amazon Web page, and leave your Web browser open for the next activity.



Activity 4-5: Examining Web Bugs and Privacy

Time Required: 30 minutes

Objective: Gain an understanding of data collection with Web bugs.

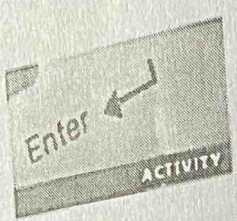
Description: Web bugs are considered more invasive than cookies. As a security professional, you should understand how companies use them to gather information on users who visit Web sites.

1. Start your Web browser in Windows, if necessary, and go to www.knowprivacy.org.
2. Click the Web Bugs tab on the home page, and read all sections.
3. Which Web sites have the most Web bugs? (List the top five.)
4. The article explains that Google creates incentives for site operators to share data by offering premium services only to Web sites willing to share data they gather from Web bugs. Break up into teams of three or four students, and be prepared to argue for Google or the Know Privacy organization.
5. After reading the article, exit your Web browser.

Using Domain Name System Zone Transfers

Another way to gather information when footprinting a network is through Domain Name System (DNS). As you know from learning basic networking concepts, DNS is the network component responsible for resolving hostnames to IP addresses and vice versa. People would much rather memorize a URL than an IP address. Unfortunately, using URLs comes at a high price. DNS is a major area of potential vulnerability for network attacks.

Without going into too much detail, DNS uses name servers to resolve names. After you determine what name server a company is using, you can attempt to transfer all the records for which the DNS server is responsible. This process, called a zone transfer, can be done with the Dig command. (For those familiar with the Nslookup command, Dig is now the recommended command.) To determine a company's primary DNS server, you can look for a DNS server containing a Start of Authority (SOA) record. An SOA record shows for which zones or IP addresses the DNS server is responsible. After you determine the primary DNS server, you can perform another zone transfer to see all host computers on the company network. In other words, the zone transfer give you an organization's network diagram. You can use this information to attack other servers or computers that are part of the network infrastructure.



Activity 4-6: Identifying IP Addresses by Using Zone Transfers (Optional)

Time Required: 30 minutes

Objective: Perform a zone transfer on a DNS server.

Description: When footprinting a network, finding the IP addresses and hostnames of all servers, computers, and other nodes connected to the network is important. With commands such as Dig, you can perform zone transfers of DNS records. You can then use this information to create network diagrams and establish a good picture of how the network is organized. For example, you can see how many hosts are on the network and how many subnets have been created.

In this example, mit.edu is used to demonstrate conducting a zone transfer so that you can see what kind of information can be gathered from a zone transfer. At the time of this writing, the zone transfer with mit.edu worked. However, many universities are tightening security and no longer allow zone transfers, but you should still know the steps for performing one.

1. Boot your computer into Linux with the BackTrack DVD, and open a Konsole shell. At the command prompt, type dig soa mit.edu and press Enter. You should see a screen similar to Figure 4-9. Three name servers, indicated by "NS," are listed: STRAWB.mit.edu, BITSY.mit.edu, and W2ONS.mit.edu. (This information might change by the time you read this book. If so, ask your instructor for guidelines.) Most likely, you'll have to use a different university. These commands shouldn't work if a DNS administrator has configured DNS correctly. As you'll learn, however, sometimes administrators don't do what they should, which leaves systems vulnerable to attacks.

```
; <O> DiG 9.2.3 <O> soa mit.edu
root@1[root]# dig soa mit.edu

; <O> DiG 9.2.3 <O> soa mit.edu
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47643
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;mit.edu.                       IN      SOA

;; ANSWER SECTION:
mit.edu.                21600   IN      SOA     BITSY.mit.edu. NETWORK-REQUEST.mit
.edu. 3566 3600 900 3600000 21600

;; AUTHORITY SECTION:
mit.edu.                18348   IN      NS      STRAWB.mit.edu.
mit.edu.                18348   IN      NS      BITSY.mit.edu.
mit.edu.                18348   IN      NS      W2ONS.mit.edu.

;; ADDITIONAL SECTION:
BITSY.mit.edu.          6846    IN      A       18.72.0.3
W2ONS.mit.edu.          18348   IN      A       18.70.0.160
STRAWB.mit.edu.         18348   IN      A       18.71.0.151

;; Query time: 158 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Tue Nov 23 13:43:18
;; MSG SIZE  rcvd: 185

root@1[root]#
```

Figure 4-9 Using the Dig command

2. To perform a zone transfer on the BITSY.mit.edu DNS server, type dig @BITSY.mit.edu mit.edu axfr and press Enter. BITSY.mit.edu is the server on which you're attempting the zone transfer, and the second mit.edu statement is the domain where the server is located.
3. After a short wait, your screen should fill with thousands of records. Press Ctrl+C to stop the transfer. (*Tip*: If you want to find out how many records the DNS server is responsible for, you can let the transfer finish and check the summary page at the end.)
4. Do the transfer again, but this time use the |less parameter by typing dig @BITSY.mit.edu mit.edu axfr |less and pressing Enter.
5. Press Enter or the spacebar to view additional records, and then press q to quit. Close the Konsole shell, and log off Linux.

The tools you've just learned about aren't the only way to get information. Sometimes information about a company is gathered by using nontechnical skills. In fact, the best hackers aren't necessarily the most technically adept people. Instead, they possess a more insidious—and often underestimated—skill called social engineering, discussed in the following section.

Introduction to Social Engineering

The art of social engineering has been around much longer than computers. Social engineering means using knowledge of human nature to get information from people. In computer attacks, the information is usually a password to a network or other information an attacker could use to compromise a network. A salesperson, for example, can get personal information about customers, such as income, hobbies, social life, drinking habits, music preferences, and the like, just by asking the customer the right questions. A salesperson uses charm and sometimes guile to relax customers and even attempts to bond with customers by pretending to be empathetic with them. After leaving the store, customers might regret some of the information they gave freely, but if the salesperson was personable, they might not think twice about it. Social engineers might also use persuasion tactics, intimidation, coercion, extortion, and even blackmail to gather the information they need. They are probably the biggest security threat to networks and the most difficult to protect against.

You have probably heard the saying "Why try to crack a password when you can simply ask for it?" Many attackers do just that: They ask for it. Unfortunately, many users give attackers everything they need to break into a network. Anyone who has worked at a help desk or in network support knows this to be true. Even if a company policy states that passwords must not be given to anyone, users often think this policy doesn't apply to IT personnel. How many times have users said their passwords out loud when an IT technician is seated in front of their computers? IT personnel don't want to know a user's password. They especially don't want a user to say it aloud or on the telephone or type it in e-mails. Yet users often don't consider their company passwords private, so they don't guard passwords as they might PINs for their ATM cards. They might not think that what they have on their company's computers is important or would be of interest to an attacker. Social engineers know how to put these types of users at ease. The following is an example of a typical social-engineering tactic.

First, the social engineer poses as "Mike," a name he found after performing a zone transfer and examining the company's DNS server. Mike might not be the current IT point of contact (POC), but it doesn't matter. Depending on the company's size, users often don't know

everyone on the IT staff. The social engineer then places a call for Sue, an employee name he found from the zone transfer information and several company Web pages that showed the format of e-mail addresses. To get the phone number, he simply calls the company's main switchboard and asks for Sue. Then he says he wants to leave a message for Sue and asks to be directed to her voicemail. "Sue's in the office now," replies the friendly receptionist. "Would you like me to connect you to her?" The social engineer says "Darn, my other line is ringing. I misplaced her extension. Can you please give it to me, and I'll call her back in a few minutes? I really have to get that call."

In this exchange, his tactic is to create a sense of urgency yet remain cordial. It usually works because most receptionists don't see a problem with connecting a caller to an employee or giving an employee's direct number or extension. After all, the caller knows Sue's name and seems to know her. "Extension 4100," the receptionist says. "Thanks! Gotta go," the social engineer replies.

After 30 minutes or so, the social engineer calls the company again. "Hello. Extension 4101, please," he asks. The receptionist connects him, and a man answers "Bob Smith, Accounting." "Sorry, Bob. Mike here. I was calling Sue, but I guess I got your extension by mistake. Sue was having a problem connecting to the Internet, so we're checking IP address information. We just fixed her system. Are you also having a problem?" Bob says, "It looks like only the accounting department is having a problem with the VLAN config." Mike then asks, "Still running Windows XP?" Bob answers no but tells Mike which operating system he's using. Bob probably feels as though he knows Mike, even though he doesn't.

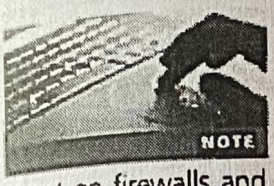
Another way to find out how the IT staff operates is for Mike to pose as Bob and call with a question or problem he's having. Mike would then learn how the help desk person handles the call. Does the help desk issue a help ticket? Does Bob have to give any information to the caller other than his name and phone number? Many help desk offices require assigning a unique number to the help call until the problem is solved.

The social engineer used Sue's name to give his call more credibility. Also, because he had gathered information about the operating system through other means, he took advantage of that knowledge, as shown by his Windows XP question. Mike might try to go for the kill now, or he might decide to attempt the final attack with Sue. If he calls her, he can talk about Bob as though they're old friends. What he wants is Bob or Sue's password. He might try the following ploy: "Bob, there's a good chance we'll have to shut down accounting's network connectivity for an hour or so. I could reduce this time for your system to five minutes if I could work on the problem from here. Only problem is I need your password. I already have your logon account as bsmith@gmail-info. Is that correct?" Chances are good that Bob will give his password to Mike over the telephone.

Not all social engineering takes place on the telephone, but it's probably the most common method because it's anonymous and allows a social engineer to carry out multiple attacks in the same organization. This method can be more difficult if one or two employees hear different stories from the same person. However, a well-dressed person carrying a clipboard can also be successful in gathering information from employees. This approach requires more courage because the social engineer has to face the people from whom he's attempting to gather information.

Social engineers study human behavior. They can recognize personality traits, such as shyness or insecurity, and understand how to read body language: slouched shoulders,

avoidance of eye contact, nervous fidgeting, and so on. If the ploy is conducted over the telephone, the person's tone of voice can give the social engineer clues. Many profess to practice on people they date or try to get useless information from unsuspecting victims just to hone their skills. Like a tiger seeking out the weakest gazelle in the herd, social engineers can identify the most vulnerable person in an organization. They know who to approach and who to avoid.

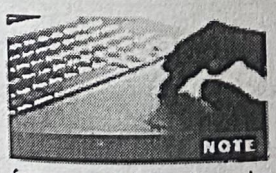


Security Bytes

A security professional's most difficult job is preventing social engineers from getting crucial information from company employees. No matter how thorough a security policy is or how much money is spent on firewalls and intrusion detection systems (IDSs), employees are still the weakest link in an organization. Attackers know this fact and use it. Employees must be trained and tested periodically on security practices. Just as fire drills help prepare people to evacuate during a fire, random security drills can improve a company's security practices. For example, randomly selecting and testing employees each month to see whether they give their passwords to someone within or outside the organization is a good way to find out whether your security memos are being read and followed.

Social engineers use many different techniques in their attempts to gain information from unsuspecting people:

- *Urgency*—"I need the information now or the world will come to an end!" For example, a social engineer might tell a user he needs the information quickly or the network will be down for a long time, thus creating a false sense of urgency.
- *Quid pro quo*—"I can make your life better if you give me the information I need." The social engineer might promise the user faster Internet access, for example, if he or she helps by supplying information.
- *Status quo*—"Everyone else is doing it, so you should, too." By using the names of other employees, a social engineer can easily convince others to reveal their passwords.
- *Kindness*—This tactic is probably the most dangerous weapon social engineers wield. People want to help those who are kind to them. The saying "It's easier to catch flies with honey than with vinegar" also applies to social engineering.
- *Position*—Convincing an employee that you're in a position of authority in the company can be a powerful means of gaining information. This is especially true in the military, where rank has its privileges. Social engineers can claim that a high-ranking officer is asking for the information, so it's imperative to give it as quickly as possible.



Security Bytes

As a security tester, you should never use social-engineering tactics unless the person who hired you gives you permission in writing. You should also confirm on which employees you're allowed to perform social-engineering tests and document the tests you conduct. Your documentation should include the responses you received, and all test results should, of course, be confidential. Figures 4-10 and 4-11 show social-engineering templates included in the OSSTMM. You can print them from your copy of the OSSTMM on the book's DVD.

OSSTMM Social Engineering Template

Company	
Company Name	
Company Address	
Company Telephone	
Company Fax	
Company Web Page	
Products and Services	
Primary Contacts	
Departments and Responsibilities	
Company Facilities Location	
Company History	
Partners	
Resellers	
Company Regulations	
Company Info Security Policy	
Company Traditions	
Company Job Postings	
Temporary Employment Availability	
Typical IT Threats	
People	
Employee Information	
Employee Names and Positions	
Employee Place in Hierarchy	
Employee Personal Pages	
Employee Best Contact Methods	
Employee Hobbies	
Employee Internet Traces (SENET, Forums)	
Employee Opinions Expressed	
Employee Friends and Relatives	
Employee History (Including Work History)	
Employee Character Traits	
Employee Values and Priorities	
Employee Social Habits	
Employee Speech and Speaking Patterns	
Employee Gestures and Manners	

Figure 4-10 The OSSTMM social engineering template

Courtesy Course Technology/Cengage Learning

OSSTMM Social Engineering Telephone Attack Template

Attack Scenario	
Telephone #	
Person	
Description	
Results	

Figure 4-11 The OSSTMM telephone attack template

Courtesy Course Technology/Cengage Learning

Training users not to give outsiders any information about OSs is important. Employees should also be taught to confirm that the person asking questions is indeed the person he or she claims to be. Employees shouldn't be embarrassed to ask the person for a company telephone number to call back instead of trusting the person on the other end of the phone line. Simply making employees aware that most hacking is done through social engineering, not programming skills, can make them more aware of how attackers operate.

The Art of Shoulder Surfing

Another method social engineers use to gain access to information is shoulder surfing. A shoulder surfer is skilled at reading what users enter on their keyboards, especially logon names and passwords. This skill certainly takes practice, but with enough time, it can be mastered easily. Shoulder surfers also use this skill to read PINs entered at ATMs or to detect long-distance authorization codes that callers dial. ATM theft is much easier than computer shoulder surfing because a keypad has fewer characters to memorize than a computer keyboard. If the person throws away the receipt in a trash can near the ATM, the shoulder surfer can match the PIN with an account number and then create a fake ATM card. Often shoulder surfers use binoculars or high-powered telescopes to observe PINs being entered, making it difficult to protect against this attack.

Security Bytes

A common tactic of shoulder surfers is using cell phone cameras to take photos of unaware shoppers' credit cards in supermarkets and stores. With this technique, they can get the credit card number and expiration date. Combining this technique with observing the shopper entering his or her PIN increases the risk of identity theft.

Many keyboard users don't follow the traditional fingering technique taught in typing classes. Instead, they hunt and peck with two or three fingers. However, shoulder surfers train themselves to memorize key positions on a standard keyboard. Armed with this

knowledge, they can determine which keys are pressed by noticing the location on the keyboard, not which finger the typist is using.

Shoulder surfers also know the popular letter substitutions most people use when creating passwords: $ for s, @ for a, 1 for i, 0 for o, and so forth. Many users think p@$$w0rd is difficult to guess, but it's not for a skilled shoulder surfer. In addition, many users are required to use passwords containing special characters, and often they type these passwords more slowly to make sure they enter the correct characters. Slower typing makes a shoulder surfer's job easier.

Security Bytes

With so many people taking their laptops to the airport, commercial airlines warn customers to be aware of shoulder surfers. In the tight confines of an airplane, someone could easily observe the keys pressed and read the data on a laptop monitor. Products that prevent off-axis viewing of screens, such as screen overlays or a security lens, are recommended for travelers. Many employees conduct business on airplanes, and shoulder surfers can use the information gathered there to compromise computer systems at the company.

To help prevent shoulder-surfing attacks, you must educate users not to type logon names and passwords when someone is standing directly behind them—or even standing nearby. You should also caution users about typing passwords when someone nearby is talking on a cell phone because of the wide availability of camera phones. To further reduce the risk of shoulder surfing, make sure all computer monitors face away from the door or the cubicle entryway. Warn your users to change their passwords immediately if they suspect someone might have observed them entering their passwords.

Security Bytes

When you're entering your long-distance access code at a pay phone, a shoulder surfer holding a calculator while pretending to talk on the phone next to you can simply enter each number you dial into his or her calculator. With this method, he or she doesn't have to memorize a long sequence of numbers. The calculator entry contains the access code for placing a long-distance call charged to your phone card.

The Art of Dumpster Diving

Another method social engineers use to gain access to information is **dumpster diving**. Although it's certainly not a glamorous form of gathering information, you'd be surprised at what you can find by examining someone's trash. For example, discarded computer manuals can indicate what OS is being used. If the discarded manual is for Windows NT 4.0, there's a good chance the new system is a more recent Windows OS, such as Windows Server 2003. Sometimes network administrators write notes in manuals or even jot down passwords, and social engineers can make use of this information.

Company phone directories are another source of information. A dumpster diver who finds a directory listing company employees can use this information to pose as an employee for the purpose of gathering information. Company calendars with meeting schedules, employee vacation schedules, and so on can be used to gain access to offices that won't be occupied

for a specified time period. Trash can be worth its weight in gold for the dumpster diver who knows what to do with it. Here are some other items that can be useful to dumpster divers:

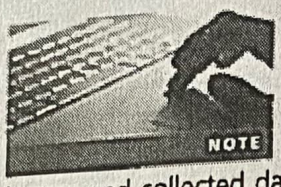
- Financial reports
- Interoffice memos
- Discarded computer programs
- Company organizational charts showing managers' names
- Resumes of employees
- Company policies or systems and procedures manuals
- Professional journals or magazines
- Utility bills
- Solicitation notices from outside vendors
- Regional manager reports
- Quality assurance reports
- Risk management reports
- Minutes of meetings
- Federal, state, or city reports

Dumpster diving can produce a tremendous amount of information, so educating your users on the importance of proper trash disposal is important. Disks or hard drives containing company information should be formatted with "disk-cleaning" software that writes binary 0s on all portions of the disks. This formatting should be done at least seven times to ensure that all previous data is unreadable. Old computer manuals should be discarded offsite so that dumpster divers can't associate the manuals with the company. Before disposal, all these items should be placed in a locked room with adequate physical, administrative, and technical safeguards. All documents should be shredded, even if the information seems innocuous. Social engineers know how to pull together information from many different sources. Putting a puzzle together from many small pieces makes it possible for attackers to break into a network.

The Art of Piggybacking

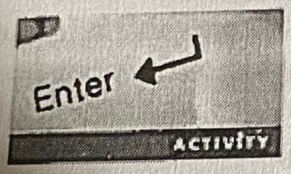
Sometimes security testers need to enter part of a building that's restricted to authorized personnel. In this case, a tester or an attacker uses a technique called piggybacking. Piggybacking is trailing closely behind an employee who has access to an area without the person realizing you didn't use a PIN or a security badge to enter the area. Those skilled in piggybacking watch authorized personnel enter secure areas and wait for the opportune time to join them quickly at the security entrance. They count on human nature and the desire of others to be polite and hold open a secured door. This ploy usually works, especially if the piggybacker has both hands full and seems to be struggling to remove an access card from a purse or pants pocket. Some piggybackers wear a fake badge around their necks or pretend to scan a security card across a card reader. If they're detected, they might say their card has been giving them problems and use their social-engineering skills to convince the security guard to let them through.

A good preventive measure against piggybacking is using turnstiles at areas where piggybacking can occur. However, the best preventive measure is to train personnel to notify security when they notice a stranger in a restricted area. Employees must feel a vested interest in area security and should not rely on security personnel. Employees should be taught not to hold secured doors open for anyone, even people they know. Educate your users to get in the habit of making sure all employees use their access cards to gain entry into a restricted area and to report any suspicious or unknown people to security.



Security Bytes

A well-dressed security tester walked into a hospital with a wireless laptop and sat down in the waiting area adjacent to the nurses' station. He was able to access passwords and logon information on his laptop and collected data for more than a week without being questioned by security or hospital personnel. In fact, the security tester felt as though he was invisible. Doctors, nurses, administrators, and other hospital personnel never questioned the presence of the stranger in their midst, even though he had covered most of the waiting room table with legal pads and his laptop. After the security test was completed, it was determined that everyone thought the stranger was working for someone else in the area. No one felt responsible for finding out who the stranger was and why he was there.



Activity 4-7: Learning Piggybacking Skills

Time Required: 30 minutes

Objective: Learn how piggybacking can be used to gain access to restricted areas.

Description: In this activity, you learn the piggybacking skills used to gain access to areas restricted to authorized personnel. Assume you're conducting a security test and need access to a company's server room. To enter the room, you must scan an access card over a card reader, and then push open a door within several seconds, during which time a bell rings softly. If the door isn't opened in the allotted time, the card must be swiped again. Form teams of two and demonstrate to the class how you would use piggybacking to get into the classroom if it was secured. One student should pretend to be an authorized user while the other student uses piggybacking techniques to gain entry. Have a class discussion about these attempts, and note which one was the most successful.

Phishing

Almost everyone with an e-mail address has received a phishing e-mail at some point. "Update your account details" is a typical subject line. The message is usually framed as an urgent request to visit a Web site to make sure you're not locked out of an account, such as your online banking service. The Web site is a fake, but if you're tricked into giving out your personal account data, the money you lose is real. Figure 4-12 shows an actual phishing e-mail purportedly from PayPal. One clue that the e-mail isn't legitimate is that the recipient is addressed by the generic "Dear PayPal Member" instead of his or her name.

Please Restore Your Account Access RX1065

Reply Reply all Forward Add to calendar Delete Junk Print Previous Next

service@paypal.com [service@paypal.com] Add contact

To: lenz@lentbachman.com

Please Restore Your Account Access RX1065

Dear PayPal Member,

As part of our security measures, we regularly screen activity in the PayPal system. We recently contacted you after noticing an issue on your account.

We requested information from you for the following reason:

A recent review of your account determined that we require some additional information from you in order to provide you with secure service.

Case ID Number: PP-657-579-435

This is a third and final reminder to log in to PayPal as soon as possible.

Be sure to log in securely by clicking on the link below. Once you log in, you will be provided with steps to restore your account access. We appreciate your understanding as we work to ensure account safety.

https://secure.paypal.com/us/cgi-bin/webscr?cmd=_login-submit

In accordance with PayPal's User Agreement, your account access will remain limited until the issue has been resolved.

Unfortunately, if access to your account remains limited for an extended period of time, it may result in further limitations or eventual account closure.

We encourage you to log in to your PayPal account as soon as possible to help avoid this.

To review your account and some or all of the information that PayPal used to make its decision to limit your account access,

please visit the Resolution Center. If, after reviewing your account information, you seek further clarification regarding your account access,

please contact PayPal by visiting the Help Center or click the link below

https://secure.paypal.com/helpscr?cmd=_help&locale=en_US&countrycode=PE&_dynamicframe=1&IE-8&1=solutionTab&ms=solutionPanel&solutionId=13136

https://secure.purple-pay.com/mb/%20/secure.paypal.com/us/cgi-bin/webscr?_cmd=login-SESSION=1ex5bkqzhm7W1jOSn0m1QsTbV3OmAU71/

Figure 4-12 A phishing e mail

Courtesy Course Technology/Cengage Learning

What's potentially more dangerous to companies is spear phishing, another attack carried out by e-mail that combines social engineering with exploiting vulnerabilities. Attackers have used spear phishing to steal millions of dollars. Unlike phishing, this attack is directed at specific people in an organization and uses social engineering based on previous reconnaissance data to hook victims. A spear phishing e-mail might appear to come from a sender the recipient knows and mention topics of mutual interest. The goal is to entice victims into opening an attachment or clicking a link; this action installs the "spear phished" malware, which can have devastating effects on an organization's network. Some security consulting companies incorporate spear phishing attacks as part of their testing, using tools that can inject shell code into Adobe PDF files. One example of these tools is Metasploit (included on the Back-Track DVD and discussed in Chapter 7). These tools make the technical engineering of a spear phishing attack so easy a caveman could do it. E-mail authentication technologies—such as Sender Policy Framework, DomainKeys Identified Mail, S/MIME, and PGP—as well as security awareness training for users and constant vigilance help reduce the threat of phishing and spear phishing.