

ATME COLLEGE OF ENGINEERING

13th KM Stone, Bannur Road, Mysore - 560 028



A T M E

College of Engineering

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

- CYBER SECURITY



LECTURE NOTES

COURSE: Hackers Technique, Tools and Incident Handling

COURSE CODE: BCY515C

SEMESTER: V

COURSE COORDINATOR: Ms. Darshini Y

(ACADEMIC YEAR 2026)

INSTITUTIONAL MISSION AND VISION

Objectives

- To provide quality education and groom top-notch professionals, entrepreneurs and leaders for different fields of engineering, technology and management.
- To open a Training-R & D-Design-Consultancy cell in each department, gradually introduce doctoral and postdoctoral programs, encourage basic & applied research in areas of social relevance, and develop the institute as a center of excellence.
- To develop academic, professional and financial alliances with the industry as well as the academia at national and transnational levels.
- To develop academic, professional and financial alliances with the industry as well as the academia at national and transnational levels.
- To cultivate strong community relationships and involve the students and the staff in local community service.
- To constantly enhance the value of the educational inputs with the participation of students, faculty, parents and industry.

Vision

Development of academically excellent, culturally vibrant, socially responsible and globally competent human resources.

Mission

- To keep pace with advancements in knowledge and make the students competitive and capable at the global level.
- To create an environment for the students to acquire the right physical, intellectual, emotional and moral foundations and shine as torch bearers of tomorrow's society.
- To strive to attain ever-higher benchmarks of educational excellence

MODULE-2**Chapter 1: The Information-Gathering Process**

Although this chapter will place emphasis on the foot printing phase of the hacking and information-gathering process, seven steps are actually used. The steps of the information-gathering process include:

1. Gathering information
2. Determining the network range
3. Identifying active machines
4. Finding open ports and access points
5. Detecting operating systems
6. Using fingerprinting services
7. Mapping the network

Of the seven steps, foot printing covers the first two steps in the process. Note that steps 1 and 2 are both passive in nature; they do not require direct interaction with the victim. This is one of the key characteristics of foot printing: to gather information about a victim without directly interacting and potentially providing advance notice of the attack. The following list shows some of the activities an attacker can perform when foot printing an organization:

- Examine the company's Web site
- Identify key employees
- Analyze open positions and job requests
- Assess affiliate, parent, or sister companies
- Find technologies and software used by the organization
- Determine network address and range
- Review network range to determine whether the organization is the owner or if the systems are hosted by someone else
- Look for employee postings, blogs, and other leaked information
- Review collected data

Under the right conditions, a skilled hacker can gather the information mentioned here and use the results to fine-tune what will be scanned or probed on the victim. Remember that the most effective tools that can be employed during this phase are common sense and detective work. You must be able to look for the places where a company may have made information available and seek such information. In fact, footprinting may be the easiest part of the hacking process because most organizations generate massive amounts of information that is made available online. Before a skilled hacker fires up an active tool, such as a port scanner or password cracker, he or she will meticulously carry out the footprinting process to plan and coordinate a more effective attack.

MODULE-2**The Information on a Company Web Site**

When starting the footprinting phase, do not overlook some of the more obvious sources of information, including the company's Web site. As anyone who has used the Internet can attest, Web sites offer various amounts of information about an organization because the Web site has been published to tell customers about the organization. Although Web sites contain much less sensitive data now than was seen in the past, it is still not uncommon to come across Web sites that contain e-mail addresses, employee names, branch office locations, and technologies the organization uses. An example of an average Web site and some information you might find is shown in [Figure 5-1](#).

One problem with Web sites that has only recently been overcome is the amount of sensitive information that can be accessed by the public. Sometimes without even realizing it, a company will publish a piece of information that seems insignificant, but to an attacker that same information may be gold. Consider a practice that used to be quite common: the posting of company directories on the company Web site. Such information may not seem like a problem except that it gives an attacker valuable contact information for employees that may be used to impersonate these individuals. Of course, what is valuable is not just what is visible on a Web site; it can also be the source code or HTML that is used to design the site. It is possible for a particularly astute attacker to browse through the source code and locate comments or other pieces of information that can give insight into an organization.

MODULE-2

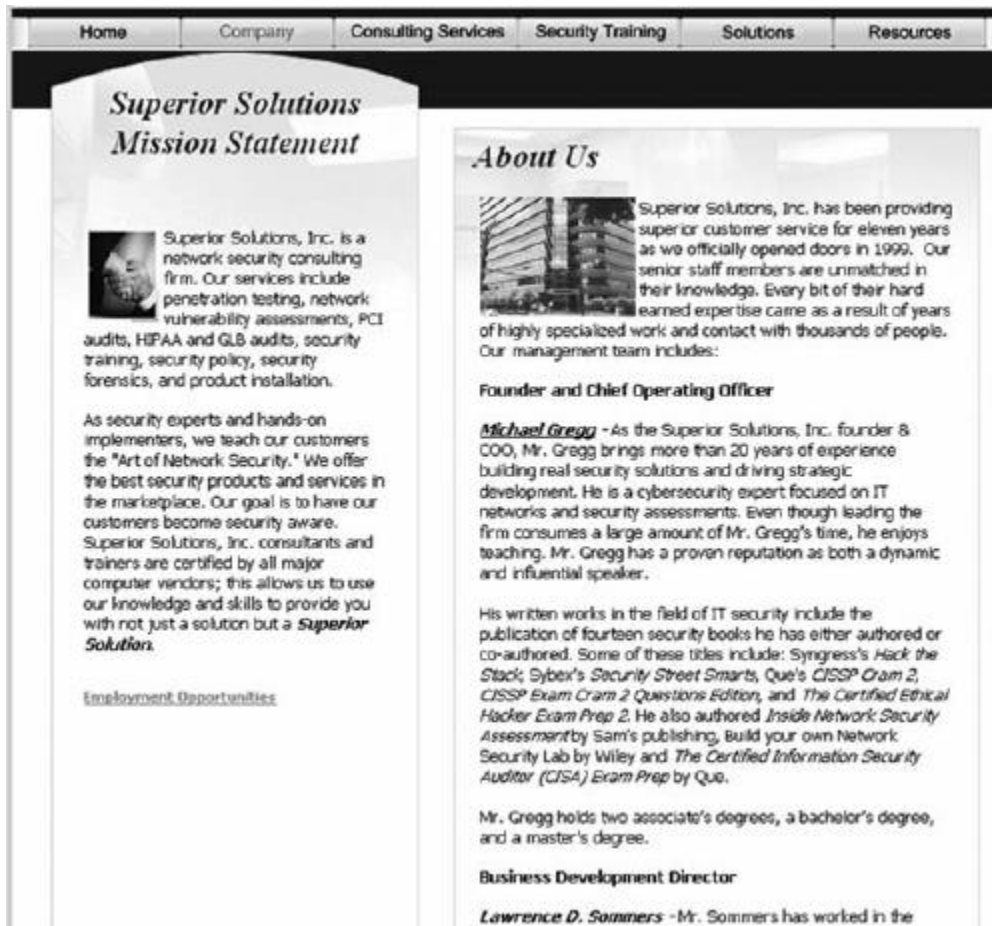


Figure 5-1. Company management.

The following is an example of HTML code with comments

```
<html>  <head>  <title>Company Web page</title>  </head>  <body>  <!-- This Web
page prompts for the password to login to the database server  HAL9000 -->  </body>
</html>
```

The comment included here may seem harmless, but it would tell an attacker the name of the server that is being accessed, assisting in targeting an attack.

NOTE

Site ripping tools such as Blackwidow Pro or Wget can be used to extract a complete copy of the Web site.

Over the last decade, companies have gotten the message that posting some information on the company Web site is not advisable. In some cases, organizations have removed information that could reveal details about internal process, personnel, and other assets.

MODULE-2

On the surface, it would seem that once information is removed from a Web site the problem is eliminated, but this is far from true. In the case of a Web site, the state of a Web site at a particular point in time may still exist somewhere out in cyberspace. One of the tools that a security professional can use to gain information about a past version of a Web site is something known as the Wayback Machine. It is a Web application created by the **Internet Archive** that takes "snapshots" of a Web site at regular intervals and makes them available to anyone who looks. With the Wayback Machine, it is possible to recover information that was posted on a Web site sometime in the past. However, the information may be hopelessly out of date and of limited use. The Wayback Machine is available at <http://www.archive.org/>. An example of this Web site is shown in [Figure 5-2](#).

When a Web site address is entered into the Wayback Machine, the site will return a list of dates representing when a Web site was archived with an asterisk next to any date on which a change was made. Although the Internet Archive does not keep exhaustive results on every Web site, the Web sites it does archive can stretch all the way back to 1996. Currently the Internet Archive has a sizable amount of content cataloged estimated to be in excess of 150 billion Web pages and related content. Of note in the Internet Archive is the fact that every Web site on the Internet is not archived, and those that are may not always go back far enough to reveal any useful information. Another potential drawback is that a site administrator, through use of a file called robots.txt, can block the Internet Archive from making snapshots of the site, denying anyone the use of old information. [Figure 5-3](#) shows an example of how far back Web pages go for a specific company.

NOTE

The Internet Archive is intended to be a historical archive of the Internet for the purposes of research and historical interests. Originally started in 1996, the Internet Archive has grown to include the archived versions of more than 150 billion Web pages; the archive has since been enhanced to include text, video, and images and other content.



Figure 5-2. Wayback Machine query.

MODULE-2

Search Results for Jan 01, 1996 - Aug 05, 2009							
2001	2002	2003	2004	2005	2006	2007	2008
9 pages	15 pages	22 pages	18 pages	11 pages	39 pages	29 pages	5 pages
Mar 13, 2001 *	Jan 05, 2002 *	Feb 05, 2003 *	Jan 03, 2004 *	Jan 20, 2005 *	Jan 03, 2006 *	Jan 30, 2007 *	Jan 21, 2008
Mar 16, 2001	Jan 21, 2002	Feb 15, 2003	Mar 24, 2004 *	Feb 04, 2005	Feb 07, 2006	Jan 30, 2007	Feb 20, 2008
Apr 02, 2001	Apr 14, 2002	Mar 23, 2003 *	Mar 29, 2004 *	Feb 18, 2005 *	Apr 04, 2006	Jan 31, 2007 *	Apr 23, 2008
Apr 06, 2001	May 30, 2002	Apr 03, 2003 *	Apr 01, 2004 *	Feb 07, 2005	May 09, 2006 *	Jan 30, 2007 *	May 24, 2008
Apr 30, 2001 *	Jun 08, 2002	Apr 15, 2003 *	Apr 04, 2004	Feb 10, 2005	Jan 13, 2006 *	Jan 26, 2007 *	Jun 24, 2008
May 17, 2001 *	Jul 20, 2002	Apr 23, 2003	May 16, 2004 *	Mar 07, 2005	Jan 15, 2006	Feb 24, 2007	
Aug 03, 2001	Aug 00, 2002	Apr 25, 2003 *	May 25, 2004 *	Mar 23, 2005	Aug 03, 2006	Mar 09, 2007 *	
Oct 01, 2001 *	Aug 22, 2002	Apr 26, 2003	Jun 13, 2004 *	Mar 24, 2005	Aug 08, 2006	Mar 17, 2007	
Dec 03, 2001	Sept 25, 2002 *	May 27, 2003	Aug 29, 2004 *	Apr 06, 2005 *	Aug 11, 2006	Jan 30, 2007 *	
	Sep 26, 2002 *	Jun 12, 2003 *	Aug 29, 2004 *	Jul 22, 2005 *	Aug 13, 2006	Jul 01, 2007	
	Oct 08, 2002	Jun 23, 2003 *	Aug 20, 2004	Aug 21, 2005	Aug 21, 2006	Jul 16, 2007	
	Nov 23, 2002 *	Jul 18, 2003	Sep 23, 2004 *		Aug 22, 2006	Aug 13, 2007	
	Nov 24, 2002 *	Jul 18, 2003 *	Sep 26, 2004 *		Aug 27, 2006	Aug 17, 2007	
	Nov 29, 2002	Sep 27, 2004	Oct 13, 2004		Aug 29, 2006	Aug 18, 2007	
	Nov 30, 2002 *	Oct 06, 2004 *	Oct 15, 2004		Aug 30, 2006	Aug 24, 2007	
		Oct 11, 2004	Nov 29, 2004		Sep 09, 2006	Sep 25, 2007	
		Oct 23, 2004	Dec 12, 2004 *		Oct 04, 2006	Sep 26, 2007	
		Nov 10, 2004	Dec 13, 2004 *		Nov 11, 2006 *	Sep 30, 2007	
		Dec 01, 2004			Dec 30, 2006 *	Oct 01, 2007	
		Dec 13, 2004				Oct 04, 2007	
		Dec 17, 2004 *				Oct 04, 2007	
		Dec 17, 2004 *				Oct 05, 2007	
						Oct 07, 2007	
						Oct 08, 2007	
						Oct 30, 2007	
						Oct 30, 2007	
						Oct 31, 2007	
						Nov 21, 2007	
						Dec 21, 2007	

Figure 5-3. Wayback Machine results.

Of course, the Internet Archive is only one source from which valuable information can be gleaned about an intended target; another valuable source is job postings. Consider that the job postings a company posts on the corporate Web site or on job boards can give valuable clues into what the infrastructure they use looks like. IT should take note of the skills being requested when examining job postings, paying special interest to the skills section. For example, consider the following posting:

Expertise Required:

- Advanced knowledge of Microsoft XP, 7, Server 2003; and products such as Microsoft Access, Microsoft SQL Server, Microsoft IISv6, Visual Basic
- Proficient in Excel, Word, and PowerPoint 2007
- Relevant Experience/Knowledge Cisco PIX; Checkpoint Firewall helpful but not necessary
- Virtual Machine (VMWare), SAP S4P, and other data-gathering systems

Although this is only a snippet of a larger job posting, it still provides insight into what the company happens to be using. Think for a moment how an attacker can make use of the information the company provided. As an example, the attacker could use the information to attempt to fine tune a later attack, doing some research and locating vulnerabilities such as:

- Search for vulnerabilities in the discovered products
- Scan for application specific configuration issues
- Locate product specific defects

If the attacker can successfully use any of these attacks, it is a simple matter to access the target's network and do further harm. On the other hand, if the attacker finds that these vulnerabilities are patched, the posting still provides information on other software in use and insight into the environment.

MODULE-2

NOTE

When a company posts a job on a corporate site or a job posting site such as dice.com or monster.com, care should be taken to sanitize the posting. A company that is thinking ahead may either choose to be less specific on skills or remove information that easily identifies the company in question. Sanitizing seeks to clean up or strip out sensitive information that may be too sensitive or too revealing.

Another gem of information that can be useful in job postings is job location. When browsing a job posting, the location information, when browsed in conjunction with skills, can yield insight into potential activities at a location. When browsing job postings, the appearance of unusual skills at a specific location can be an indicator of activities such as those associated with research and development. An attacker could use the information to target specific locations that are more likely to contain assets of value.

Discovering Financial Information

It is not surprising that an ever-increasing number of attacks are financially motivated in nature. Criminals have discovered that technology can be a new and very effective way of committing old scams on a new medium. For example, consider Albert Gonzales, the hacker convicted of the TJ Maxx hacking attack. According to <http://www.informationweek.com>, Mr. Gonzales did not pick his targets at random. Targets were footprinted prior to being attacked; the footprinting process was specifically used to determine whether a targeted company made enough money to merit an attack. TJ Maxx is only one of the ever-increasing numbers of victims of cybercrime, numbers that are expected to increase as criminals adopt new methods and technologies.

CISCO SYSTEMS INC CIK#: 0000855877 (see all company filings)		
SIC: 3576 - COMPUTER COMMUNICATIONS EQUIPMENT		
State location: CA State of Inc: CA Fiscal Year End: 0728		
(Assistant Director Office No 3)		
Get insider transactions for this issuer.		
Get insider transactions for this reporting owner.		
Filter Results:	Filing Type:	Prior to: (YYYYMMDD)
		Ownership?
		☐ include ☒ exclude ☐ only
Items 1 - 40 RSS Feed		
Filings	Format	Description
SC 13G		Statement of acquisition of beneficial ownership by individuals Acc-no: 0001689394-10-007172 (34 Act) Size: 15 kB
S-8		Securities to be offered to employees in employee benefit plans Acc-no: 0001193125-09-258379 (33 Act) Size: 333 kB
S-8		Securities to be offered to employees in employee benefit plans Acc-no: 0001193125-09-258378 (33 Act) Size: 145 kB
S-8		Securities to be offered to employees in employee benefit plans Acc-no: 0001193125-09-256093 (33 Act) Size: 65 kB
8-K		Current report, Item 8.01 Acc-no: 0001193125-09-242589 (34 Act) Size: 14 kB
DFAN14A		Additional definitive proxy soliciting materials filed by non-management and Rule 14(a)(12) material Acc-no: 0001193125-09-241213 Size: 23 kB
10-Q		Quarterly report [Sections 13 or 15(d)] Acc-no: 0001193125-09-237055 (34 Act) Size: 3 MB
8-K		Current report, Items 1.01, 9.01, and 9.01 Acc-no: 0001193125-09-236335 (34 Act) Size: 416 kB
8-K		Current report, Items 1.01, 2.03, and 9.01 Acc-no: 0001193125-09-234405 (34 Act) Size: 587 kB
8-K/A		[Amend] Current report, Item 5.02 Acc-no: 0001193125-09-234397 (34 Act) Size: 14 kB

MODULE-2

Figure 5-4. Cisco EDGAR 10-Q.

THE VALUE OF FOOTPRINTING

How important is footprinting? According to the Information Security Forum (ISF), profit-driven attacks have largely replaced those of the lone wolf hacker. These new attackers rely on careful footprinting to determine and select suitable targets. Groups of organized criminal hackers have even been known to place bogus employees within organizations to provide inside knowledge that can be used to more effectively carry out an attack.

This new mode of attack is designed to steal valuable and sensitive information or customer data for financial gain and profit. Although not unheard of, such crimes are rarely carried out by one person; these attacks are typically the work of criminal networks that bring together specialist skills and expertise.

It is no surprise that the criminal element is quite often attracted to the prospect of monetary gain, and cybercrime is no exception. When a criminal is choosing a company to attack based on whether that company makes enough money, items such as publicly available financial records can prove vital. In the United States, getting information on the financial health of companies is easy because financial records on publicly traded companies are available for review. These financial records are easily accessible through the Securities and Exchange Commission (SEC) Web site at <http://www.sec.gov>. On the Web site, it is possible to review the Electronic Data Gathering, Analysis, and Retrieval system (EDGAR) database, which contains all sorts of financial information (some updated daily). All foreign and domestic companies that are publicly traded are legally required to file registration statements, periodic reports, and other forms electronically through EDGAR, all of which can be browsed by the public. Of particular interest in the EDGAR database are the items known as the 10-Qs and 10-Ks. These items are quarterly and yearly reports that contain the names, addresses, financial data, and information about acquired or divested industries. For example, a search of the EDGAR database for information about Cisco returns the list of records shown in [Figure 5-4](#).

Closer examination of these records indicates where the company is based, detailed financial information, and the names of the principals, such as the president and members of the board. EDGAR is not the only source of this information, however; other sites provide similar types of information, including the following:

- **Hoovers**—<http://www.hoovers.com/>
- **Dun and Bradstreet**—<http://www.dnb.com/us/>
- **Yahoo Finance**—<http://finance.yahoo.com/>
- **Bloomberg**—<http://www.bloomberg.com/>

FYI

One of the major reasons why Google hacking is so effective is the large amount of information any given company generates. Statistically, the average company tends to double the amount of

MODULE-2

data it possesses every 18 months during normal operations. If a company were to take only a small fraction of that information and make it accessible from the Internet, it would be potentially releasing a large amount of information into the world around it.

Google Hacking

The previous two methods demonstrated simple but powerful tools that can be used to gain information about a target. The methods both showed how they can be used in unintended and new ways to gain information. One more tool that can be used in ways never really intended is Google. Google contains a tremendous amount of information of all types just waiting to be searched and uncovered. In a process known as **Google hacking**, the goal is to locate useful information using techniques already provided by the search engine in new ways. If you can construct the proper queries, Google search results can provide hacker useful data about a targeted company. Google is only one search engine; other search engines, such as Yahoo and Bing, are also vulnerable to being used and abused in this way.

Why is Google hacking effective? Quite simply it is because Google indexes vast amounts of information in untold numbers of formats. Google obviously can index Web pages like any search engine. But Google can also index images, videos, discussion group postings, and all sorts of file types such as .pdf, .ppt and more. All the information that Google, or any search engine, gathers is held in large databases that are designed to be searchable; you only need to know how to look.

There are numerous resources about the process of Google hacking, but one of the best is Johnny Long's Google Hacking Database (GHDB) at <http://www.hackersforcharity.org/ghdb/>. This site offers insight into some of the ways an attacker can easily find exploitable targets and sensitive data by using Google's built-in functionality. An example of what is found at the Web site is seen in [Figure 5-5](#).

The GHDB is merely a database of queries that identifies sensitive data and content that potentially may be of a sensitive nature. Some of the items an attacker can find are available using the following techniques:

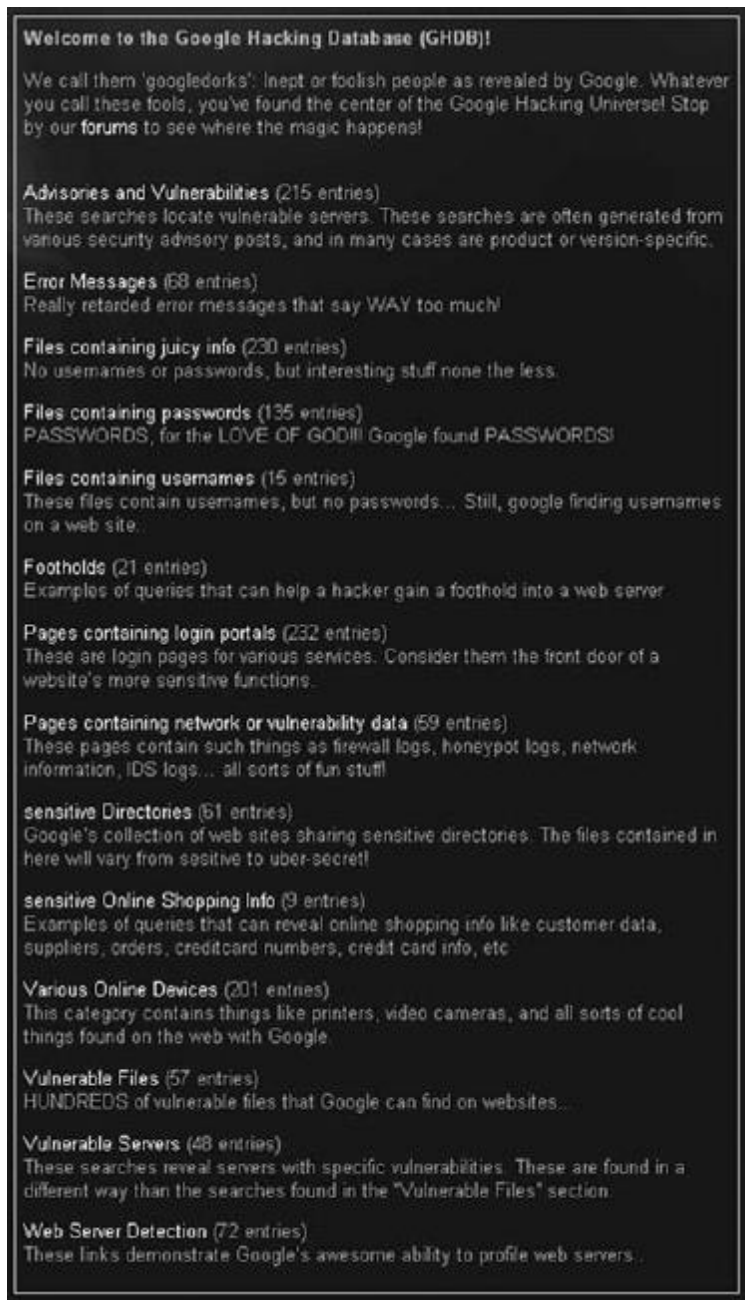
- Advisories and server vulnerabilities
- Error messages that contain too much information
- Files containing passwords
- Sensitive directories
- Pages containing logon portals
- Pages containing network or vulnerability data

What makes this possible is the way in which information is indexed by a search engine. Specific commands such as *intitle* instruct Google to search for a term within the title of a document. Some examples of intitle search strings are shown here:

MODULE-2

- `intitle:"index of" .bash_history`
- `intitle:"index of" etc/shadow`
- `intitle:"index.of" finances.xls`
- `intitle:"index of" httpasswd`
- `intitle:"Index of" inurl:maillog`

The keyword "intitle:" directs Google to search for and return pages which contain the words listed after the intitle: keyword. For example intitle: "index of" finance.xls will return pages that contain files of the name finance.xls.



MODULE-2

Figure 5-5. Google Hacking Database.

Once these results are returned the attacker can browse the results looking for those that contain sensitive or restricted information that may reveal additional details about the organization.

Another popular search parameter is *filetype*. This query allows the search to look for a particular term only within a specific filetype. A few examples of the use of this search string are as follows:

- `filetype:bak inurl:"htaccesspasswd Ishadowlhtusers"`
- `filetype:conf slapd.conf`
- `filetype:ctt "msn"`
- `filetype:mdb inurl:"account|users|admin|administrators|passwd|password"`
- `filetype:xls inurl:"email.xls"`

The keyword "filetype:" instructs Google to return files that have specific extensions. For example, `filetype:doc` or `filetype:xls` will return all the word or excel documents.

To better understand the actual mechanics of this type of attack, a closer examination is necessary. With this type of attack an attacker will need some knowledge ahead of time, such as the information gathered from a job posting regarding applications. The attacker can then determine that a company is hosting a Web server and further details such as the type and version (for example, Microsoft IIS 6.0). An attacker can then use this knowledge to perform a search to uncover whether the company is actually running the Web server version in question. For example, the attacker may have chosen to attack Cisco and as such will need to locate the Web servers that are running IIS 6.0 to move their attack to the next phase. Using Google to find Web servers that are running Microsoft IIS 6.0 servers can be accomplished with a simple Google query such as "intitle:index.of "Microsoft-IIS/6.0 Server at" on the Google search page. The results of this search are shown in [Figure 5-6](#). Notice that more than 2,000 hits were returned.



Figure 5-6. Google Hacking Database search results.

A final search query that can prove invaluable is the Google keyword *inurl*. The *inurl* string is used to search within a site's uniform resource locator (URL). This is very useful if some knowledge of URL strings or with standard URL strings used by different types of applications and systems is possessed. Some common *inurl* searches include the following:

MODULE-2

- `inurl:admin filetype:db`
- `inurl:admin inurl:backup intitle:index.of`
- `inurl:"auth_user_file.txt"`
- `inurl:"/axs/ax-admin.pl" -script`
- `inurl:"/cricket/grapher.cgi"`

The keyword "inurl:" commands Google to return pages which include specific words or characters in the URL. For example, the search request `inurl:hyrule` will produce such pages that have the word "hyrule" in it.

These search queries and variations are very powerful information-gathering mechanisms that can reveal information that may not be so obvious or accessible normally. Gaining a careful understanding of each search term and keyword can allow a potential attacker to gain information about a target that may otherwise be out of view. The security professional who wants to gain additional insight into how footprinting using Google hacking works should experiment with each term and what it reveals. Knowing how they are used by attackers can help prevent the wrong information ending up in a Web search of your organization through the careful planning and securing of data.

Exploring Domain Information Leakage

A reality of developing security for any public organization is the fact that some information is difficult or impossible to hide. A public company that wants to attract customers must walk a fine line because some information by necessity will have to be made public while other information can be kept secret. An example of information that should be kept secret by any company is domain information, or the information that is associated with the registration of an Internet domain. Currently many tools are available that can be used for obtaining types of basic information, including these:

- Whois
- Nslookup
- Internet Assigned Numbers Authority (IANA) and Regional Internet Registries (RIRs) to find the range of Internet protocol (IP) addresses
- Traceroute to determine the location of the network

Each of these tools can provide valuable information pulled from domain registration information.

Manual Registrar Query

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. Global domain name management is delegated to the **Internet Assigned Numbers Authority (IANA)**. IANA is responsible for the global

MODULE-2

coordination of the Domain Name System (DNS) Root, IP addressing, and other Internet protocol resources.

Root Zone Database

The Root Zone Database represents the delegation details of top-level domains, including gTLDs such as ".COM", and country-code TLDs such as ".UK". As the manager of the DNS root zone, IANA is responsible for coordinating these delegations in accordance with its policies and procedures.

Much of this data is also available via the WHOIS protocol at whois.iana.org.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z ccTLDs gTLDs DNIs		
Domain	Type	Purpose / Sponsoring Organisation
.AC	country-code	Ascension Island Network Information Center (AC Domain Registry) c/o Cable and Wireless (Ascension Island)
.AD	country-code	Andorra Andorra Telecom
.AE	country-code	United Arab Emirates Telecommunication Regulatory Authority (TRA)
.AERO	sponsored	Reserved for members of the air-transport industry Société Internationale de Télécommunications Aéronautiques (SITA INC USA)
.AF	country-code	Afghanistan Ministry of Communications and IT
.AG	country-code	Antigua and Barbuda UNISA School of Medicine

Figure 5-7. Root Zone Database.

Name Servers

Host Name	IP Address(es)
a.gtld-servers.net.	192.5.6.30 2001:503:a83e::0:0:2:30
c.gtld-servers.net.	192.26.92.30
d.gtld-servers.net.	192.31.80.30
e.gtld-servers.net.	192.12.94.30
f.gtld-servers.net.	192.35.51.30
g.gtld-servers.net.	192.42.93.30
i.gtld-servers.net.	192.41.162.30

Subdomain Information

URL for registration services: <http://www.educause.edu/edudomain>

WHOIS Server: whois.educause.edu

Record last updated 2009-12-05. Registration date 1995-01-01.

Figure 5-8. EDU registration services.

When the network range is determined manually, the best resource available to make this happen is the IANA Web site at the Root Zone Database page located

MODULE-2

at <http://www.iana.org/domains/root/db/>. The Root Zone Database represents the delegation details of top level domains (TLDs), including domains such as .com and country-code TLDs such as .us. As the manager of the DNS root zone, IANA is responsible for coordinating these delegations in accordance with its stated policies and procedures. The Web site can be seen in [Figure 5-7](#).

To fully grasp the process of uncovering a domain name and its associated information, it is best to examine the process step by step. In this example, a search for <http://www.smu.edu> will be performed. Of course, the target in this scenario has already been set, but in the real process the target would be the entity to be attacked. After the target has been identified (in this case, <http://www.smu.edu>), move through the list until EDU is located; then click that page. The EDU Web page is shown in [Figure 5-8](#).

At this point, the registration services for the .edu domain are handled by <http://www.educause.edu/edudomain>. Once the registrant for .edu domains has been identified, it is now possible to use the educause Web site at <http://whois.educause.net/> and enter a query for <http://www.smu.edu>. The results of this query are shown in [Figure 5-9](#).

Because organization and planning are essential skills for security professionals, make note of the information uncovered for later use. While the organization method that each individual uses is unique, consider an organization strategy similar to the matrix located in [Table 5-1](#).

Table 5-1. Initial whois findings.

DOMAIN NAME	IP ADDRESS	NETWORK RANGE	DNS SERVER	POINT OF CONTACT
http://www.smu.edu	129.119.64.10		129.119.64.10	Bruce Meikle

MODULE-2

```

Whois Lookup SMU.EDU

Search Results
-----
Domain Name: SMU.EDU

Registrant:
Southern Methodist University
6185 Airline Drive
4th Floor
Dallas, TX 75275-0262
UNITED STATES

Administrative Contact:
Jesse R. Miller
Director of Telecommunications
Southern Methodist University
6185 Airline Dr.
4th Floor
Dallas, TX 75275-0262
UNITED STATES
(214) 768-4225
jrmiller@smu.edu

Technical Contact:
R. Bruce Meikle
Sr. Network Engineer
Southern Methodist University
6185 Airline Dr.
Dallas, TX 75275-0262
UNITED STATES
(214) 768-3471
rbm@smu.edu

Name Servers:
PONY.CIS.SMU.EDU      129.119.64.10
SEAS.SMU.EDU          129.119.3.2
XPONY.SMU.EDU         129.119.64.8
EPONY.SMU.EDU         128.42.182.100

Domain record activated: 31-Aug-1987
Domain record last updated: 05-Feb-2010
Domain expires: 31-Jul-2010

To determine the current accreditation status of SMU.EDU,
search at the US Department of Education Office of Postsecondary Education
accreditation web site.

```

Figure 5-9. SMU query.

Note that in a matter of a few clicks, it was possible to obtain very detailed information about the target such as the IP address of the Web server, DNS server IP address, location, point of contact, and more. In fact, of the information gathered at this point the only thing that is noticeably absent is the actual information about the network range.

To obtain the network range requires the attacker to visit at least one or more of the **Regional Internet Registries (RIRs)**, which are responsible for management, distribution, and registration of public IP addresses within their respective assigned regions. Currently there are five primary RIRs (see [Table 5-2](#)).

MODULE-2

Because RIRs are important to the process of information gathering and hacking, it is important to define the process of using an RIR in the context of <http://www.smu.edu>. When searching for information on the target, it serves some purpose to consider location; earlier research indicated that the host was located in Dallas, Texas. With this piece of information in hand, a query can be run using the ARIN site to obtain still more information about the domain. The <http://www.arin.net> site is shown in [Figure 5-10](#).

Table 5-2. Regional Internet registries.

REGIONAL INTERNET REGISTRY	REGION OF CONTROL
ARIN	North and South America
APNIC	Asia and Pacific
RIPE	Europe, Middle East, and parts of Africa
LACNIC	Latin America and the Caribbean
AfriNIC	Africa



Figure 5-10. ARIN site.

Located in the top-right corner of the Web page is a search box labeled "search whois." In this search box, enter the IP address of <http://www.smu.edu> that was recorded earlier and it is also noted in [Table 5-1](#) for reference. The results of this search are shown in [Figure 5-11](#).

You can see that the network range is 129.119.0.0-129.119.255.255. With this information, the last piece of the network range puzzle is in place, and a clear picture of the address on the network is built. Network range data provides a critical piece of information for an attacker because it confirms that addresses between 129.119.0.0-129.119.255.255 all belong

MODULE-2

to <http://www.smu.edu> (these addresses will be examined in the next step of the process). With this last piece of information included, the table should now resemble what is shown in [Table 5-3](#).

```

OrgName:      Southern Methodist University
OrgID:        SMU-3
Address:      6185 Airline
City:         Dallas
StateProv:    TX
PostalCode:   75275-0000
Country:      US

NetRange:     129.119.0.0 - 129.119.255.255
CIDR:         129.119.0.0/16
OriginAS:     AS1832, AS1875, AS1876
NetName:      SOUTHMETHUNIV
NetHandle:    NET-129-119-0-0-1
Parent:       NET-129-0-0-0-0
NetType:      Direct Assignment
NameServer:   PONY.CIS.SMU.EDU
NameServer:   SEAS.SMU.EDU
NameServer:   XPCONY.SMU.EDU
NameServer:   EPCONY.SMU.EDU
Comment:
RegDate:      1987-11-06
Updated:      2010-02-08

RAbuseHandle: IS04-ARIN
RAbuseName:   Information Security Office
RAbusePhone:  +1-214-768-7321
RAbuseEmail:  abuse@smu.edu

RNOCHandle:   N0C1961-ARIN
RNOCName:     Network Operations Center
RNOCPhone:    +1-214-768-4662
RNOCEmail:    noc@smu.edu

RTechHandle:  RBM17-ARIN
RTechName:    Meikle, R. Bruce
RTechPhone:   +1-214-768-3471
RTechEmail:   rbm@mail.smu.edu

OrgAbuseHandle: IS04-ARIN
OrgAbuseName:   Information Security Office
OrgAbusePhone:  +1-214-768-7321
OrgAbuseEmail:  abuse@smu.edu

OrgNOCHandle:  N0C1961-ARIN
OrgNOCName:     Network Operations Center
OrgNOCPhone:    +1-214-768-4662
OrgNOCEmail:    noc@smu.edu

```

Figure 5-11. ARIN results.

Table 5-3. Final whois findings.

MODULE-2

DOMAIN NAME	IP ADDRESS	NETWORK RANGE	DNS SERVER	POINT OF CONTACT
<i>http://www.smu.edu</i>	129.119.64.10	129.119.0.0–129.119.255.255	129.119.64.10	Bruce Meikle

Automatic Registrar Query

The manual method of obtaining network range information is effective, but it does have the drawback of taking a significant amount of time. You can speed up the process using automated methods to gather this information faster than can be done manually. Several Web sites are dedicated to providing this information in a consolidated view. Numerous Web sites are also dedicated to providing network range information automatically.

```

Domain Name: SMU.EDU

Registrant:
  Southern Methodist University
  6185 Airline Drive
  4th Floor
  Dallas, TX 75275-0262
  UNITED STATES

Administrative Contact:
  Jesse R. Miller
  Director of Telecommunications
  Southern Methodist University
  6185 Airline Dr.
  4th Floor
  Dallas, TX 75275-0262
  UNITED STATES
  (214) 768-4225
  jrmiller@smu.edu

Technical Contact:
  R. Bruce Meikle
  Sr. Network Engineer
  Southern Methodist University
  6185 Airline Dr.
  Dallas, TX 75275-0262
  UNITED STATES
  (214) 768-3471
  rbm@smu.edu

Name Servers:
  PONY.CIS.SMU.EDU      129.119.64.10
  SEAS.SMU.EDU          129.119.3.2
  XPONY.SMU.EDU         129.119.64.8
  EPONY.SMU.EDU         128.42.182.100

Domain record activated: 31-Aug-1987
Domain record last updated: 05-Feb-2010
Domain expires:         31-Jul-2010

```

MODULE-2

Figure 5-12. Domaintools name query.

Some of the more common or popular destinations for searches of this type include the following:

- <http://www.sampade.org>
- <http://www.betterwhois.com>
- <http://www.allwhois.com>
- <http://geektools.com>
- <http://www.all-nettools.com>
- <http://www.smartwhois.com>
- <http://www.dnsstuff.com>
- <http://www.sampade.org>
- <http://whois.domaintools.com>

A point to remember is that no matter what tool the professional prefers, the goal is to obtain registrar information. As an example, [Figure 5-12](#) shows the results of <http://whois.domaintools.com> when <http://www.smu.edu> was queried for information.

Underlying all these tools is a tool known as **whois**, which is software designed to query the databases that hold registration information. Whois is a utility that has been specifically designed to interrogate the Internet domain name administration system and return the domain ownership, address, location, phone number, and other details about a specified domain name. The accessibility of this tool depends on the operating system in use. For Linux users, the tool is just a command prompt away; Windows users have to locate a Windows-compatible version and download it or use a Web site that provides the service.

Whois

The Whois protocol was designed to query databases to look up and identify the registrant of a domain name. Whois information contains the name, address, and phone number of the administrative, billing, and technical contacts of the domain name. It is primarily used to verify whether a domain name is available or whether it has been registered. The following is an example of the whois info for cisco.com

Registrant:

- Cisco Technology, Inc.
- 170 W. Tasman Drive
- San Jose, CA 95134
- US
- Domain Name: CISCO.COM

Administrative Contact:

MODULE-2

- InfoSec
- 170 W. Tasman Drive
- San Jose, CA 95134
- US
- 408-527-3842 fax: 408-526-4575

Technical Contact:

- Network Services
- 170 W. Tasman Drive
- San Jose, CA 95134
- US
- 408-527-9223 fax: 408-526-7373

Record expires on 15-May-2011.

Record created on 14-May-1987.

Domain servers in listed order:

- NS1.CISCO.COM 128.107.241.185
- NS2.CISCO.COM 64.102.255.44

NOTE

Whois has also been used by law enforcement to gain information useful in prosecuting criminal activity such as trademark infringement.

By looking at this example it is possible to gain some information about the domain name and the department that is responsible for managing it which, in this case, is the Infosec team. Additionally you will note that we have phone numbers and DNS info for the domain as well, not to mention a physical address that we can look up using Google Earth.

Nslookup

Nslookup is a program to query Internet domain name servers. Both UNIX and Windows come with an Nslookup client. If Nslookup is given an IP address or a fully qualified domain name (FQDN), it will look up and show the corresponding IP address. Nslookup can be used to do the following:

- Find additional IP addresses if authoritative DNS is known from Whois
- List the MX (mail) server for a specific range of IP addresses

Extracting Information with NSLOOKUP:

MODULE-2

- nslookup
- > set type=mx
- > cisco.com
 - Server: x.x.x.x
 - Address: x.x.x.x#53
- Non-authoritative answer:
 - cisco.com mail exchanger = 10 smtp3.cisco.com.
 - cisco.com mail exchanger = 10 smtp4.cisco.com.
 - cisco.com mail exchanger = 10 smtp1.cisco.com.
 - cisco.com mail exchanger = 10 smtp2.cisco.com.
- Authoritative answers can be found from:
 - cisco.com nameserver = ns1.cisco.com.
 - cisco.com nameserver = ns2.cisco.com.
 - cisco.com nameserver = ns3.cisco.com.
 - cisco.com nameserver = ns4.cisco.com.
 - ns1.cisco.com internet address = 216.239.32.10
 - ns2.cisco.com internet address = 216.239.34.10
 - ns3.cisco.com internet address = 216.239.36.10
 - ns4.cisco.com internet address = 216.239.38.10

Looking at these results you can see several pieces of information that would be useful, including the addresses of nameservers and mail exchangers. The nameservers represent the systems used to host DNS while the mail exchangers represent the addresses of servers used to process mail for the domain. The addresses should be recorded for later scanning and vulnerability checking.

Internet Assigned Numbers Authority (IANA)

According to <http://www.iana.org>, "The Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of the DNS root, IP addressing, and other Internet protocol resources." Based on this information, IANA is a good starting point to learn more about domain ownership and to determine registration information. A good place to start is at the Root Zone Database page, which lists all top-level domains, including .com, .edu, .org, and so on. It also shows two-character country codes. Refer to the example shown in [Figure 5-7](#).

DNS 101

Nslookup works with and queries the DNS, which is a hierarchical naming system for servers, computers, and other resources connected to the Internet. This system associates information such as IP address to the name of the resource itself. Once this association is present, it is possible to translate names of systems meaningful to humans into the IP addresses associated with networking equipment for the purpose of locating these devices. DNS can be thought of much in the same way as looking up phone numbers or names in a phonebook. First, a phonebook system is hierarchical with different phonebooks for different regions and within those phonebooks, different area codes. Second, in the phonebook you have names and the

MODULE-2

phone numbers associated with them, along with other information such as physical addresses, much like DNS. When looking up an individual you simply look up their name and see what their phone number is and call them. In DNS this would be called a forward lookup. You also can call Information and give a number and they can do a reverse lookup where they take the phone number and look up the name associated with it.

For example, for a quick look at information on an .edu domain such as Villanova University, you could start at <http://www.iana.org/domains/root/db/edu.html>. The top-level domain for .edu sites is <http://www.educause.edu/edudomain> (and the whois server: whois.educause.edu). The results of this search can be seen in [Figure 5-13](#).

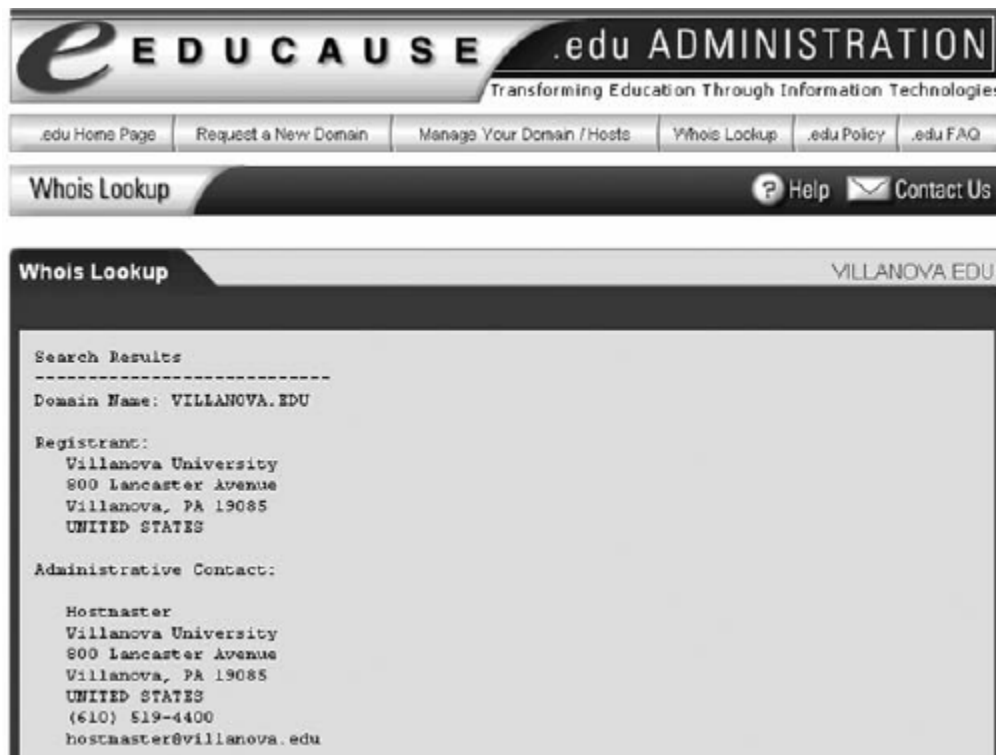


Figure 5-13. EDU whois search result.

The same type of search can be performed against a .com domain such as <http://www.hackthetack.com>. The results of this search are shown here:

- Domain Name: HACKTHESTACK.COM
- Reseller: DomainsRus
- Created on: 27 Jun 2006 11:15:37 EST
- Expires on: 27 Jun 2018 11:15:47 EST
- Record last updated on: 31 May 2009 07:18:10 EST
- Status: ACTIVE
- Owner, Administrative Contact, Technical Contact, Billing Contact:

MODULE-2

- Superior Solutions Inc
- Network Administrator (ID00055881)
- PO Box 1722
- Freeport, TX 77542
- United States
- Phone: +979.8765309
- Email:
- Domain servers in listed order:
- NS1.PLANETDOMAIN.COM
- NS2.PLANETDOMAIN.COM

Notice that these results also include a physical address along with all the other domain information. It would be possible to take the physical address provided and enter it into any of the commonly available mapping tools and gain information on the proximity of this address to the actual company. Now that the domain administrator is known, the next logical step in the process could be to determine a valid network range.

Determining a Network Range

One of the missions of the IANA is to delegate Internet resources to RIRs. The RIRs further delegate resources as needed to customers, who include Internet service providers (ISPs) and end-user organizations. The RIRs are organizations responsible for control of IPv4 and IPv6 addresses within specific regions of the world. The five RIRs are as follows:

- **American registry for Internet Numbers (ARIN)**—North America and parts of the Caribbean
- **Ripe Network Coordination Centre (Ripe NCC)**—Europe, the Middle East, and Central Asia
- **Asia-Pacific Network Information Centre (APNIC)**—Asia and the Pacific region
- **Latin American and Caribbean Internet Addresses Registry (LACNIC)**—Latin America and parts of the Caribbean region
- **African Network Information Centre (AfriNIC)**—Africa

Per standards, each RIR must maintain point-of-contact (POC) information and IP address assignment. As an example, if the IP address 202.131.95.30 corresponding to <http://www.hackthestack.com> is entered, the following response is returned from ARIN:

- OrgName: Asia Pacific Network Information Centre
- OrgID: APNIC
- Address: PO Box 2131
- City: Milton
- StateProv: QLD
- PostalCode: 4064

MODULE-2

- Country: AU
- ReferralServer: whois://whois.apnic.net
- NetRange: 202.0.0.0-203.255.255.255
- CIDR: 202.0.0.0/7
- NetName: APNIC-CIDR-BLK
- NetHandle: NET-202-0-0-0-1

Take note of the range of 202.0.0.0 to 203.255.255.255. This is the range of IP addresses assigned to the network hosting the *http://www.hackthestack.com* Web site.

Many other Web sites can be used to mine this same type of data. Some of them include the following:

- *http://www.all-nettools.com*
- *http://www.Smartwhois.com*
- *http://www.allwhois.com*
- *http://www.Dnsstuff.com*
- *http://www.Samspade.org*

The next section shows how a hacker can help determine the true location of the domain and IP addresses previously discovered.

Traceroute

Traceroute is a software program used to determine the path a data packet traverses to get to a specific IP address. Traceroute, which is one of the easiest ways to identify the path to a targeted Web site, is available on both UNIX and Windows operating systems. In Windows operating systems, the command is known as **tracert**. Regardless of the name the program displays, **tracert** displays the list of routers on a path to a network destination by using Time to Live (TTL) time-outs and Internet control message protocol (ICMP) error messages. This command will not work from a DOS prompt.

```
C:\tracert www.cisco.com
Tracing route to arin.net [202.131.95.30]
 0 1 ms 1 ms 1 ms 192.168.123.254
 1 12 ms 15 ms 11 ms adsl-69-151-223-254.dsl.hstntx.swbell.net
   [69.151.223.254]
 2 12 ms 12 ms 12 ms 151.164.244.193
 3 11 ms 11 ms 11 ms bb1-g14-0.hstntx.sbcglobal.net [151.164.92.204]
 4 48 ms 51 ms 48 ms 151.164.98.61
 5 48 ms 48 ms 48 ms gil--1.wil04.net.reach.com [206.223.123.11]
 6 49 ms 50 ms 48 ms i-0-0-0.wil-core02.bi.reach.com [202.84.251.233]
 7 196 ms 195 ms 196 ms i-15-0.sydp-core02.bx.reach.com [202.84.140.37]
 8 204 ms 202 ms 203 ms unknown.net.reach.com [134.159.131.110]
 9 197 ms 197 ms 200 ms ssg550-1-r1-1.network.netregistry.net
   [202.124.240.66]
10 200 ms 227 ms 197 ms forward.planetdomain.com [202.131.95.30]
```

MODULE-2

Analyzing these results, it is possible to get better look at what traceroute is providing. Traceroute functions by sending out a packet to a destination with the TTL set to 1. When the packet encounters the first router in the path to the destination it decrements the TTL by 1, in this case setting the value to 0, which results in the packet being discarded and a message being sent back to the original sender. This response is recorded and a new packet is sent out with a TTL of 2. This packet will make it through the first router, then will stop at the next router in the path. This second router then sends an error message back to the originating host much like the original router. Traceroute continues to do this over and over until a packet finally reaches the target host, or until a host is determined to be unreachable. In the process, traceroute records the time it took for each packet to travel round trip to each router. It is through this process that a map can be drawn of the path to the final destination.

In the above results you can literally see the IP address, name, and the time it took to reach each host and return a response giving a clear picture of the path to connect to the remote host and the time to do so.

The next-to-last hop before the Web site will often be the organization's edge device, such as a router or firewall. However, you cannot always rely on this information because security-minded organizations tend to limit the ability to perform traceroutes into their networks.

Tracking an Organization's Employees

You can use the Web to find a wealth of information about a particular organization that can be used to plan a later attack. The techniques so far have gathered information on the financial health of a company, its infrastructure, and other similar information that can be used to build a picture of the target. Of all the information gathered so far, there is one area that has yet to be explored: the human element. Gathering information on human beings is something that until recently has not been easy, but now with the ever-increasing amount of information people themselves put online, the task has become easier. The growing usage of social networking such as Facebook, MySpace, and Twitter have all served to provide information that can be searched and tracked back to an individual. According to Harris Interactive for CareerBuilder.com, 45 percent of employers questioned are using social networks to screen job candidates (and so are attackers). Information that can be uncovered online can include the following:

- Posted photographs or information
- Posted content about drinking or drug usage
- Posting derogatory information about previous employers, coworkers, or clients
- Discriminatory comments or fabricated qualifications

The motivation behind providing examples of such information is to give an idea of what the average user of social networking puts on the Internet. An attacker wanting to gain a sense of a company can search social networks and find individuals who work for the target and engage in idle gossip about their work. A single employee of a company talking too liberally about goings on at work can provide another layer of valuable insight that can be used to plan an attack.

MODULE-2

Although disgruntled employees definitely are a security threat, there are other less ominous actions that a human can take that will affect security. A single employee can be a source of information leakage that could result in damaging information leaks or other security threats. Consider the fact that it is not uncommon to find an employee posting information on blogs, Facebook, Twitter, or other locations that can be publicly accessed. Other employees have been known to get upset and set up what is known as a "sucks" domain, in which varying degrees of derogatory information are posted. Some of the sites that hackers have been known to review to obtain more information about a target include the following:

FYI

One of the reasons why social networking is such an effective tool is that the typical user of these services does not think of the information that is being shared. Individuals using social networks have been known to post all sorts of activities, such as dating and clubbing, to information about bathroom and eating habits. Perhaps the best example of how loosely people share information in social networks is Twitter. A cursory look at Twitter quickly reveals a treasure trove of information about most users on the service. Keep in mind that the average user of Twitter does not typically use the features in the application to keep their postings private, either because they don't know about these settings or because they simply want to feel important by broadcasting their thoughts to anyone who might listen.

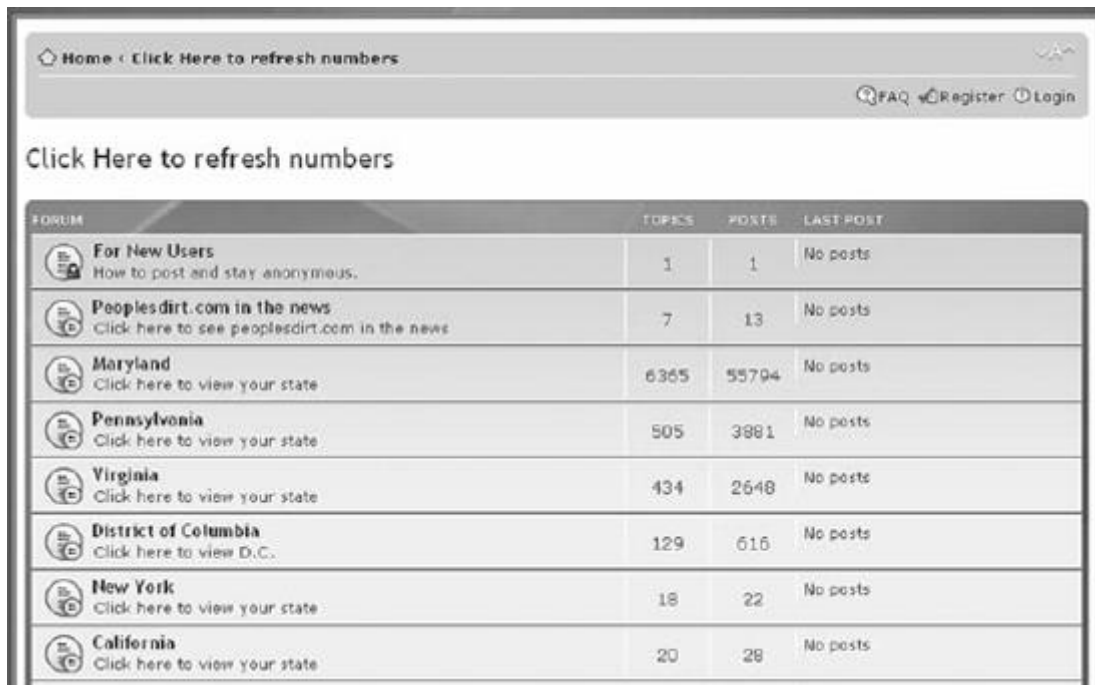
- Blogs
- Personal pages on a **social networking site**: Facebook, MySpace, LinkedIn, Plaxo, Twitter, Sucks domains
- People-tracking sites

Each of these sites can be examined for names, e-mail addresses, addresses, phone numbers, photographs, and so on. As an example, consider the Peoples Dirt site (<http://www.peoplesdirt.com>), which is shown in [Figure 5-14](#).

This site is designed to allow individuals to make anonymous posts about other individuals or organizations. Any disgruntled person can post libelous or hate-filled messages.

Weblogs, or blogs, are a good source for information about a targeted company if one can be located. Anyone can go to one of the many free blogging sites and set up a blog on which to post unfiltered comments and observations. As such, attackers have found them a valuable source of information. However, one of the bigger problems with blogs for the attacker is finding a blog that contains the information that may be useful. Consider the fact that a tremendous amount of blogs exist, and of those only a small amount are ever updated; the rest are simply abandoned by the owners. Wading into the sea of blogs on the Internet is a challenge, but using a site such as <http://www.blogsearchengine.com> will allow for the searches of many blogs quickly. Additional sites such as <http://www.wink.com> and <http://www.spock.com> allow users to search personal pages such as Facebook and MySpace for specific content.

MODULE-2



Home [Click Here to refresh numbers](#)

[FAQ](#) [Register](#) [Login](#)

[Click Here to refresh numbers](#)

FORUM	TOPICS	POSTS	LAST POST
 For New Users How to post and stay anonymous.	1	1	No posts
 Peoplesdirt.com in the news Click here to see peoplesdirt.com in the news	7	13	No posts
 Maryland Click here to view your state	6365	55794	No posts
 Pennsylvania Click here to view your state	505	3881	No posts
 Virginia Click here to view your state	434	2648	No posts
 District of Columbia Click here to view D.C..	129	616	No posts
 New York Click here to view your state	18	22	No posts
 California Click here to view your state	20	28	No posts

Figure 5-14. Peoples Dirt Web site.

MODULE-2

ZABASEARCH**Public Information** Results Summary: 4 L TOOLSIE / 4 TOOLSIE / 213 LENNY**LENNY TOOLSIE - Detailed Background Report**

Comprehensive Report. Criminal Records. Latest Contact Information.

Find LENNY TOOLSIE

Get Current Phone and Address.

Premium Services: [Search by Phone Number](#) [Reverse Phone Search](#) [Run a Background Check](#)**L TOOLSIE - 4 Free Listings**[Check messages for: TOOLSIE - LENNY - LENNY TOOLSIE](#) [Leave a message for LENNY TOOLSIE](#)[E-mail This Page](#) [Know When You're Being Searched on the Internet](#) [Create a Public Record](#)**LENNOX TOOLSIE** Born: Dec 1963 [Get the Dirt](#) [Check for Email Address](#) [Google](#)202 ROCK RD [Neighborhood & Property Report](#) [Record Created: Unknown](#)WICHITA, KS 67206 [Confirm Current Phone & Address](#)[Background Check on LENNOX TOOLSIE](#)**LENNOX TOOLSIE** Born: Dec 1963 [Get the Dirt](#) [Check for Email Address](#) [Google](#)7036 KELLOGG DR [Neighborhood & Property Report](#) [Record Created: 10/2004](#)WICHITA, KS 67207 [Confirm Current Phone & Address](#)[Background Check on LENNOX TOOLSIE](#)**LENNOX TOOLSIE** Born: Dec 1963 [Get the Dirt](#) [Check for Email Address](#) [Google](#)770 SILVER SPRINGS BLVD [Neighborhood & Property Report](#) [Record Created: 04/2009](#)WICHITA, KS 67212 [\(316\) 944-8117](#) [Confirm Current Phone & Address](#)[Background Check on LENNOX TOOLSIE](#)**LENNOX TOOLSIE** Born: Dec 1963 [Get the Dirt](#) [Check for Email Address](#) [Google](#)9007 HARRY ST [Neighborhood & Property Report](#) [Record Created: 03/2009](#)WICHITA, KS 67207 [Confirm Current Phone & Address](#)[Background Check on LENNOX TOOLSIE](#)**Figure 5-15. Zabasearch.**

Sucks domains are domain names that have the word "sucks" in the name (for example, <http://www.walmartsucks.org> and <http://www.paypalsucks.com>). These are sites in which individuals have posted unflattering content about the targeted company due to a perceived slight or wrong. An interesting note about sucks sites is that although such sites may seem wrong or downright illegal, the comments posted on them have been frequently protected under free speech laws. Such sites are usually taken down, however, partly due to the domain name not actually being used or the domain simply being "parked" (although if the site is active and noncommercial, the courts have sometimes ruled such sites legal).

NOTE

Even job search sites such as Monster.com and Careerbuilder.com are prime targets for information. If an organization uses online job sites, pay close attention to what type of information is being given away about the company's technology.

MODULE-2

Finally, another way of gaining information about an individual is to access sites that gather or aggregate information for easy retrieval. One such site is <http://www.zabasearch.com>, of which an example search is shown in [Figure 5-15](#). Another similar site to Zabasearch is <http://www.spokeo.com>, which accumulates data from many sources such as Facebook, public records, photos, and other sources that can be searched to build a picture of an individual.



Figure 5-16. Windows Remote Desktop Web connection.

Exploiting Insecure Applications

Many applications were not built with security in mind. **Insecure applications** such as Telnet, File Transport Protocol (FTP), the "r" commands, Post Office Protocol (POP), Hypertext Transfer Protocol (HTTP), and Simple Network Management Protocol (SNMP) operate without encryption. What adds to the problem is that some organizations even inadvertently put this information on the Web. As an example, a simple search engine query for terminal service Web access TSWEB (another name for Remote Desktop) returns dozens of hits that appear similar to [Figure 5-16](#). This application is designed to allow users to connect to a work or home computer and access files just as if physically sitting in front of the computer. The problem with locating this information online is that an attacker can use the information to get further details about the organization or even break in more quickly in some cases.

Using Basic Countermeasures

Footprinting can be a very powerful tool in the hands of an attacker who has the knowledge and patience to ferret out the information that is available about any entity online. But although footprinting is a powerful tool, there are some countermeasures that can lessen the impact to varying degrees.

NOTE

MODULE-2

Organizations that are more ambitious should consider attempting to footprint themselves to see firsthand what types of information are currently in the public space and whether such information is potentially damaging.

The following shows some of the defenses that can be used to thwart footprinting:

- **Web site**—Any organization should take a long hard look at the information available on the company Web site and determine whether it might be useful to an attacker. Any potentially sensitive or restricted information should be removed as soon as possible, along with any unnecessary information. Special consideration should be given to information such as e-mail addresses, phone numbers, and employee names. Access to such information should be limited to only those who require it. Additionally, the applications, programs, and protocols used by a company should be nondescript to avoid revealing the nature of services or the environment.
- **Google hacking**—This attack can be thwarted to a high degree by sanitizing information that is available publicly wherever possible. Sensitive information should not be posted in any location, either linked or unlinked, that can be accessed by a search engine as the public locations of a Web server tend to be.
- **Job listings**—When possible, use third-party companies for sensitive jobs so the company is unknown to all but approved applicants. If third-party job sites are used, the job listing should be as generic as possible, and care should be taken not to list specific versions of applications or programs. Consider carefully crafting job postings to reveal less about the IT infrastructure.
- **Domain information**—Always ensure that domain registration data is kept as generic as possible, and that specifics such as names, phone numbers, and the like are avoided. If possible, employ any one of the commonly available proxy services to block the access of sensitive domain data. An example of one such service is shown in [Figure 5-17](#).
- **Employee posting**—Be especially vigilant about information leaks generated by well-intentioned employees who may post information in technical forums or discussion groups that may be too detailed. More important, be on the lookout for employees who may be disgruntled and who may release sensitive data or information that can be viewed or accessed publicly. It is not uncommon for information leakage to occur around events such as layoffs or mergers.

MODULE-2



Figure 5-17. Domains by proxy.

- **Insecure applications**—Make it a point to regularly scan search engines to see whether links to private services are available (Terminal Server, Outlook Web App [OWA], virtual private networks [VPNs], and so on). Telnet and FTP have similar security problems because each allows anonymous logon and passwords in cleartext. Consider replacing such applications with a more secure application such as SSH or comparable wherever possible or feasible.

NOTE

A good proactive step is for a company to research the options to block a search engine's bots from indexing a site. One of the best examples of code that tells search engines how a site can be indexed is the robots.txt file. The robots.txt file can be configured to block the areas a search engine looks, but it can also be accessed by a hacker that can open the file in any commonly available text editor.

- **Securing DNS**—Sanitize DNS registration and contact information to be as generic as possible (for example, "Web Services Manager," main company phone number 555-1212, techsupport@hackthestack.com). Have two DNS servers—one internal and one external in the demilitarized zone (DMZ). The external DNS should contain only resource records of the DMZ hosts, not the internal hosts. For additional safety, do not allow zone transfers to any IP address.

MODULE-2

CHAPTER SUMMARY

This chapter covered the process of footprinting, or passively obtaining information about a target. In its most basic form, footprinting is simply information gathering that is performed carefully to avoid detection completely, or for as long as possible, while always trying to maintain a stealthy profile. Ultimately, the goal of footprinting is to gather as much information as possible about the intended victim without giving away intentions or even the presence of the attacker involved.

If done carefully and methodically, footprinting can reveal large amounts of information about a target. The process, when complete, will yield a better picture of the intended victim. In most situations, a large amount of time will be spent performing this process with relatively lesser amounts of time being spent in the actual hacking phase. Patience in the information gathering phase is a valuable skill to learn alongside how to actually gain the information. Ideally, information gathered from a well-planned and executed footprinting process will make the hacking process more effective.

Remember, footprinting includes gathering information from a diverse group of sources and locations. Common sources of information used in the footprinting phase include company Web sites, financial reports, Google searches, social networks, and other similar technologies. Attackers can and will review any source of information that can fill out the picture of the victim more than it would be otherwise.

KEY CONCEPTS AND TERMS

- Footprinting
- Google hacking
- Insecure applications
- Internet Archive
- Internet Assigned Numbers Authority (IANA)
- Nslookup
- Regional Internet Registries (RIRs)
- Social networking site
- Traceroute
- Whois

CHAPTER 1 ASSESSMENT

1. What is the best description of footprinting?
 1. Passive information gathering
 2. Active information gathering
 3. Actively mapping an organization's vulnerabilities
 4. Using vulnerability scanners to map an organization

MODULE-2

2. Which of the following is the best example of passive information gathering?
 1. Reviewing job listings posted by the targeted company
 2. Port scanning the targeted company
 3. Calling the company and asking questions about its services
 4. Driving around the targeted company connecting to open wireless connections
3. Which of the following is not typically a Web resource used to footprint a company?
 1. Company Web site
 2. Job search sites
 3. Internet Archive
 4. Phonebooks
4. If you were looking for information about a company's financial history you would want to check the _____ database.
5. Which of the following is the best description of the *intitle* tag?
 1. Instructs Google to look in the URL of a specific site
 2. Instructs Google to ignore words in the title of a specific document
 3. Instructs Google to search for a term within the title of a document
 4. Instructs Google to search a specific URL
6. If you need to find a domain that is located in Canada, the best RIR to check first would be _____.
7. You have been asked to look up a domain that is located in Europe. Which RIR should you examine first?
 1. LACNIC
 2. APNIC
 3. RIPE
 4. ARIN
8. SNMP uses encryption and is therefore a secure program.
 1. True
 2. False
9. You need to determine the path to a specific IP address. Which of the following tools is the best to use?
 1. IANA
 2. Nslookup
 3. Whois
 4. Traceroute
10. During the footprinting process social networking sites can be used to find out about employees and look for technology policies and practices.
 1. True
 2. False

Chapter 2:Determining the Network Range

The first step in port scanning is one of preparation, specifically the gathering of information about the range of Internet protocols (IPs) in use by the target. When identifying the network range, your ultimate goal is to get a picture of what the range of IP addresses in use look like together with the appropriate subnet mask in use. With this information the port scanning process can become much more accurate and effective as only the IP addresses on the intended victim will be scanned. Not having the appropriate network range can result in an inaccurate or ineffective scan that may even inadvertently set off detective measures. When getting information about the network ranges, two options can be used. With a manual registrar query, you simply go directly to the registration sites and query for information manually. With an automatic registrar query, you use Web-based tools. No matter how the range is determined, it is essential that the range be positively identified before you go any further. [Chapter 5](#) provides a more in depth explanation of the tools that can be used: Manual Registrar Query (from the Internet Assigned Numbers Authority, or IANA), Root Zone Database, Whois, and Automatic Registrar Query.

Identifying Active Machines

Once a valid network range has been obtained, the next step is to identify active machines on the network. There are several ways that this task can be accomplished, including the following:

- Wardialing
- Wardriving
- Pinging
- Port scanning

Each of these methods offers different capabilities useful in detecting active systems and as such will need to be explored individually. To use each of these techniques the attacker must clearly understand areas for which they are useful as well as those areas in which they are weak.

Wardialing

An old but still useful technique is wardialing. Wardialing is a technique that has existed for more than 25 years as a footprinting tool, which explains why the process involves the use of modems. Wardialing is very simple: it uses a modem to dial up phone numbers to locate modems. Upon first look, the technique looks sorely out of place in a world of broadband and wireless connection technology, but modems are still widely used due to the low cost of the technology. An attacker who picked a town at random and dialed up a range of phone numbers in that town would likely turn up several computers with modems attached. Wardialing can still be effective even in a world of high-speed connection technologies.

NOTE

The name *wardialing* originated from the 1983 film *WarGames*. In the film, the protagonist programmed his computer to dial phone numbers in a town to locate a computer system with the

CHAPTER 2

game he was looking for. In the aftermath of the popularity of the movie, the name WarGames Dialer was given to programs designed to do the same thing. Over time, the name was shortened to wardialing.

Dialing a range of phone numbers and getting several modems to respond doesn't initially sound significant until what is connected to those modems is considered. While modems are not nearly as popular as they were several years ago, their presence is still felt, as modems can be found connected to devices such as public branch exchanges (PBX), firewalls, routers, fax machines, and a handful of other systems not including actual computers. When you include more sensitive devices such as routers and firewalls, someone dialing up a modem and attaching to a firewall or router remotely takes on new significance. A modem can and should be looked at as a viable backdoor into a network, one that should factor in when planning defensive measures. While there is a long list of wardialing programs that have been created over the years, three well-known wardialing tools include:

- **ToneLoc**—A wardialing 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 it to dial.
- **THC-Scan**—An older DOS-based program that can use a modem to dial ranges of numbers in search for a carrier frequency from a modem or fax.
- **PhoneSweep**—One of the few commercial options available in the wardialing market.

NOTE

Always check local laws before using any security/hacking tools. As an example, some states have laws that make it illegal to place a call without the intent to communicate. In fact, several laws banning the use of automated dialing systems used by companies such as telemarketers were a direct result of wardialing activities.

Why is wardialing still successful? One of the biggest reasons is the relative lack of attention paid to modems by corporations. Modems tend to be thought of as old, low-tech devices unworthy of serious attention by defenders of a network or attackers. As such, it is not uncommon to find modems attached to networks that are still active, but forgotten and unmonitored. In some cases, modems have been discovered active and attached to a company network only after a phone bill was submitted to closer scrutiny, generating questions about what certain phone numbers are used for.

Wardriving

Wardriving is another valuable technique for uncovering access points into a network. Wardriving is the process of locating wireless access points and gaining information about the configuration of each. This "sniffing" can be performed with a notebook, a car, and software designed to record the access points detected. Additionally, a global positioning system (GPS) can be included to go to the next step of mapping the physical location of the access points. Don't get caught up in names, however; wardriving or variations can be performed with the same equipment while walking,

CHAPTER 2

biking, or even flying. If an attacker is able to locate even a single unsecured access point, the dangers can be enormous, as it can give that same attacker quick and easy access to the internal network of a company. An attacker connecting to an unsecured access point is more than likely bypassing protective measures such as the corporate firewall, for example.

BUT IS IT LEGAL?

It has been debated by black hats and white hats whether the act of wardriving is legal or not. Currently there are no laws specifically making wardriving illegal. However, using the information obtained to gain unauthorized access to a network is.

For example, in the United States a case that is generally cited in the debate is the case of *State v. Allen*. In this case, Allen used wardialing techniques in an effort to attach to Southwestern Bell's network in a bid to get free long-distance calling. However, even though Allen connected to Southwestern Bell's system, he did not attempt to bypass any security measure that appeared after the connection was made. In the end, the ruling was that although a connection was made, access was not.

While there are a multitude of tools used to perform wardriving, other tools, including the following, are useful in defending against these attacks:

- **Airsnort**—Wireless cracking tool
- **Airsnare**—An intrusion detection system to help you monitor your wireless networks. It can notify you as soon as an unapproved machine connects to your wireless network.
- **Kismet**—Wireless network detector, sniffer, and intrusion detection system commonly found on Linux
- **Netstumbler**—Wireless network detector; also available for Mac and for handhelds

So why is wardriving successful? One of the most common reasons is that employees install their own access points on the company network without company permission (known as a rogue access points). An individual who installs an access point in such a way will more than likely have no knowledge of, or possibly not care about, good security practices and by extension leave the access point completely unsecured. Another reason is that sometimes when an access point has been installed, those performing the installation have actively decided not to configure any security features. Wardriving generally preys upon situations in which security is not considered or is poorly planned. Steps should be taken to ensure that neither happens.

FYI

By definition wardriving is only the process of locating access points in the surveyed area. In reality, an individual practicing wardriving simply drives through an area, making note of the types and locations of access points, disregarding services that may be offered. If an attacker moves toward investigating further (attempting to determine the services that are available), the attacker is then *piggybacking*.

FYI

CHAPTER 2

Ping is a protocol that is very useful in troubleshooting many network problems and, as such, has a useful purpose. In some situations shutting off or blocking ping may actually affect the network more than the security measure is worth. Astute network administrators are well aware of the potential danger of leaving ping available, but in many instances they leave it enabled anyway to make network management easier.

Pinging

A technique that is useful at determining whether a system is present and active is a **ping sweep** of an IP address range. By default, a computer will respond to a ping request with a ping reply or echo. A ping is actually an **Internet Control Message Protocol (ICMP)** message. With the use of a ping, it is possible to identify active machines and measure the speed at which packets are moved from one host to another as well as obtain details such as the Time to Live (TTL).

NOTE

If you want to learn more about ping and how ICMP works, take a moment to review RFC 792. It can be found at <http://www.faqs.org/rfcs/rfc792.html>.

A key advantage of ICMP scanning is that it can be performed rapidly because it runs scanning and analysis processes in parallel. In other words, it means more than one system can be scanned simultaneously; thus it is possible to scan an entire network rapidly. There are several tools available that can perform ping scans, but three of the better known ones include Pinger, Friendly Pinger, and WS Ping Pro.

Of course, for every pro there is a con, and pinging in this manner is not without issue. First, it is not uncommon for network administrators to specifically block ping at the firewall or even turn off ping completely on host devices. Second, it is a safe bet that any intrusion detection system (IDS) or intrusion prevention system (IPS) that is in place will detect and alert network managers in the event a ping sweep occurs. Finally, ping sweeps have no capability to detect systems that are plugged into the network but powered down.

NOTE

Remember, just because a ping sweep doesn't return any results, it does not mean that no systems are available. Ping could be blocked and/or the systems pinged may be off.

Port Scanning

The next step to take after discovering active systems is to find out what is available on the systems; in this case, a technique known as port scanning is used. Port scanning is designed to probe each port on a system in an effort to determine which ports are open. It is effective for gaining information about a host because the probes sent toward a system have the ability to reveal more information than a ping sweep can. A successful port scan will return results that will give a clear picture of what is running on a system. This is because ports are bound to applications.

CHAPTER 2

A discussion of port scanning can't proceed without a clear understanding of some of the fundamentals of ports. In all, there are 65,535 TCP and 65,535 UDP ports on any given system. Each of these port numbers identifies a specific process that is either sending or receiving information at any time. At first glance, it might seem that a security professional would have to memorize all 65,000 plus ports in order to be adequately prepared, but this is not the case. In reality, only a few ports should ever be committed to memory, and if a port scan returns any ports that are not immediately recognizable, those port numbers should be further scrutinized. Some common port numbers are shown in [Table 6-1](#).

Table 6-1. Common port numbers.

PORT	SERVICE	PROTOCOL
20/21	FTP	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
80	HTTP	TCP
110	POP3	TCP
135	RPC	TCP
161/162	SNMP	UDP
1433/1434	MSSQL	TCP

Contained in the list of common port numbers in [Table 6-1](#) is an important detail located in the last column. In this column, the protocol in use is listed as either TCP or UDP (the same protocols discussed earlier when reviewing the TCP/IP suite of protocols). In practice, applications that access the network can do so using either TCP or UDP, based on how the service is designed. An effective port scan will be designed to take into account both TCP and UDP as part of the scanning

CHAPTER 2

process; these protocols work in different ways. TCP acknowledges each connection attempt; UDP does not, so it tends to produce less reliable results.

FYI

A complete list of all ports and their assigned services is available at <http://www.iana.org/assignment/port-numbers>. Memorizing all the ports available is not necessary and a pointless exercise; instead, it is worth knowing several of the common ports and looking up those that are suspicious or unusual. A good practice is to be able to access the list of ports at a site such as <http://www.iana.org> in case an unfamiliar port appears on a scan.

Table 6-2. TCP flag types.

FLAG	PURPOSE
SYN	Synchronize sequence number
ACK	Acknowledgement of sequence number
FIN	Final data flag used during the four-step shutdown
RST	Reset bit used to close an abnormal connection
PSH	Push data bit used to signal that data in this packet should be pushed to the beginning of the queue
URG	Urgent data bit used to signify that there are urgent control characters in this packet that should have priority

A Closer Look at TCP Port Scanning Techniques

TCP is a protocol that was designed to enable reliable communication, fault tolerance, and reliable delivery. Each of these attributes allows for a better communication mechanism, but at the same time these features allow an attacker to craft TCP packets designed to gain information about running applications or services.

To better understand these attacks, a quick overview of flags is needed. Flags are bits that are set in the header of a packet, each describing a specific behavior as shown in [Table 6-2](#). A penetration tester or attacker with a good knowledge of these flags can use this knowledge to craft packets and tune scans to get the best results every time.

CHAPTER 2

TCP offers a tremendous capability and flexibility due to flags that can be set as needed. However, UDP does not offer the same capabilities, largely because of the mechanics of the protocol itself. UDP can be thought of as a fire-and-forget or best-effort protocol and, as such, uses none of the flags and offers none of the feedback that is provided with TCP. UDP is harder to scan with successfully; as data is transmitted, there are no mechanisms designed to deliver feedback to the sender. A failed delivery of a packet from a client to a server offers only an ICMP message as an indicator of events that have transpired.

One of the mechanisms that port scanning relies on is the use of a feature known as flags. Flags are used in the TCP protocol to describe the status of a packet and the communication that goes with it. For example a packet flagged with the FIN flag signals the end or clearing of a connection. The ACK flag is a signal used to indicate that a connection has been acknowledged. An XMAS scan is a packet that has all its flags active at once, in effect "lit up" like a XMAS tree.

Some of the more popular scans designed for TCP port scanning include:

- **TCP connect scan**—This type of scan is the most reliable but also the easiest to detect. This attack can be easily logged and detected because a full connection is established. Open ports reply with a SYN/ACK while closed ports respond with a RST/ACK.
- **TCP SYN scan**—This type of scan is commonly referred to as half open because a full TCP connection is not established. This type of scan was originally developed to be stealthy and evade IDS systems, although most modern systems have adapted to detect it. Open ports reply with a SYN/ACK while closed ports respond with a RST/ACK.
- **TCP FIN scan**—This scan attempts to detect a port by sending a request to close a nonexistent connection. This type of attack is enacted by sending a FIN packet to a target port; if the port responds with a RST, it signals a closed port. This technique is usually effective only on UNIX devices.
- **TCP NULL scan**—This attack is designed to send packets with no flags set. The goal is to elicit a response from a system to see how it responds and then use the results to determine the ports that are open and closed.
- **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 is unreachable, the port is considered to be filtered.
- **TCP XMAS tree scan**—This scan functions by sending packets to a target port with flags set in combinations that are illegal or illogical. The results are then monitored to see how a system responds. Closed ports should return an RST.

DETECTING HALF-OPEN CONNECTIONS

Half-open connections can still be detected, but less easily than full-open scans. One way to detect half-open connections on Windows is to run the following command followed by the results:

```
netstat -n -p TCP
```

CHAPTER 2

PROTOCOL	LOCAL ADDRESS	FOREIGN ADDRESS	STATE
TCP	10.150.0.200:21	237.177.154.8:25882	Established
TCP	10.150.0.200:21	236.15.133.204:2577	Established
TCP	10.150.0.200:21	127.160.6.129:51748	Established
TCP	10.150.0.200:21	230.220.13.25:47393	Established
TCP	10.150.0.200:21	227.200.204.182:60427	Established
TCP	10.150.0.200:21	232.115.18.38:278	Established
TCP	10.150.0.200:21	229.116.95.96:5122	Established
TCP	10.150.0.200:21	236.219.139.207:49162	Established
TCP	10.150.0.200:21	238.100.72.228:37899	Established

The connections have specifically been labeled with the text SYN_RECV, which indicates a half-open connection. Running this command in practice would be impractical, but the example does show that it is possible to detect half-open connections.

Port Scanning Countermeasures

Port scanning is a very effective tool for an ethical hacker or attacker, and proper countermeasures should be deployed. These countermeasures include the range of techniques utilized by an organization's IT security group to detect and prevent successful port scanning from occurring. As there are a number of techniques that can be used to thwart port scanning, it would be impossible to cover them all, but listed here are some countermeasures that prevent an attacker from acquiring information via a port scan:

- **Deny all**—Designed to block all traffic to all ports unless such traffic has been explicitly approved
- **Proper design**—A careful and well-planned network that includes security measures such as IDSs and firewalls
- **Firewall testing**—Scanning a firewall is used to verify its capability to detect and block undesirable traffic.

CHAPTER 2

- **Port scanning**—Utilizes the same tools that an attacker will use to attack a system with the goal of gaining a better understanding of the methods involved
- **Security awareness training**—An organization should strive to provide a level of security awareness within the organization. With proper security awareness in place, personnel will know how to look for certain behaviors and maintain security. Security awareness will also be used to verify security policies and practices are being followed and to determine whether adjustments need to be made.

Mapping Open Ports

With scanning completed and information obtained, the next step of mapping the network can be performed. An attack in this stage has moved into a more interactive and aggressive format. There are many tools available that can be used to map open ports and identify services on a network. Because every tool cannot be covered, it is necessary to limit the discussion to those tools that are widely used and well known. No matter which tools are to be used, however, the activity here can be boiled down to determining whether a target is live and then port scanning the target.

Nmap

Nmap is one of the most widely used security tools and a firm understanding of Nmap is considered a requirement for security professionals. At its core, Nmap is a port scanner that has the ability to perform a number of different scan types. The scanner is freely available for several operating systems, including Windows, Linux, MacOS, and others. By design, the software runs as a command line application, but to make usage easier, a graphical user interface (GUI) is available through which the scan can be configured. The strength of Nmap is that it has numerous command line switches to tailor the scan to return the desired information. The most common command switches are listed in [Table 6-3](#).

Table 6-3. Nmap options.

NMAP COMMAND	SCAN PERFORMED
-sT	TCP connect scan
-sS	SYN scan
-sF	FIN scan
-sX	XMAS tree scan
-sN	NULL scan

CHAPTER 2

NMAP COMMAND	SCAN PERFORMED
-sP	Ping scan
-sU	UDP scan
-sO	Protocol scan
-sA	ACK scan
-sW	Windows scan
-sR	RPC scan
-sL	List/DNS scan
-sI	Idle scan
-Po	Don't ping
-PT	TCP ping
-PS	SYN ping
-PI	ICMP ping
-PB	TCP and ICMP ping
-PB	ICMP timestamp
-PM	ICMP netmask
-oN	Normal output
-oX	XML output

CHAPTER 2

NMAP COMMAND	SCAN PERFORMED
-oG	Greppable output
-oA	All output
-T Paranoid	Serial scan; 300 sec between scans
-T Sneaky	Serial scan; 15 sec between scans
-T Polite	Serial scan; .4 sec between scans
-T Normal	Parallel scan
-T Aggressive	Parallel scan
-T Insane	Parallel scan

To perform an Nmap scan, at the Windows command prompt, type Nmap IP address, followed by the switches that are needed to perform the scan desired. For example, to scan the host with the IP address 192.168.123.254 using a full TCP connecting scan type, enter the following at the command line:

```
Nmap -sT 92.168.123.254
```

The response will be similar to this:

```
Starting Nmap 4.62 (http://nmap.org) at 2010-03-21 10:37 Central
Daylight Time
Interesting ports on 192.168.123.254:
Not shown: 1711 filtered ports
PORT STATE SERVICE
21/tcp open ftp
80/tcp open http
2601/tcp open zebra
2602/tcp open ripd
MAC Address: 00:16:01:D1:3D:5C (Linksys)
Nmap done: 1 IP address (1 host up) scanned in 113.750 seconds
```

CHAPTER 2

These results are providing information about the victim system, specifically the ports that are open and ready to accept connections. Additionally, since the scan was performed against a system on the local network, it also displays the media access control (MAC) address of the system being scanned. The port information can be used later to obtain more information as will be explored later.

Nmap's results can display the status of the port in one of three states:

- **Open**—The target device is accepting connections on the port.
- **Closed**—A closed port is not listening or accepting connections.
- **Filtered**—A firewall, filter, or other network device is monitoring the port and preventing full probing to determining its status.

FYI

One of the more common types of scan is a full TCP connection scan (-sT) because it completes all three steps of the TCP handshake. While a full connect scan is the most common, a stealth scan is seen as more covert because only two steps of the three-step handshake are performed. One of the techniques to perform a somewhat stealthy scan is a SYN scan which only performs the first two steps. This type of scan is also known as "half open" scanning as it does not complete the connection.

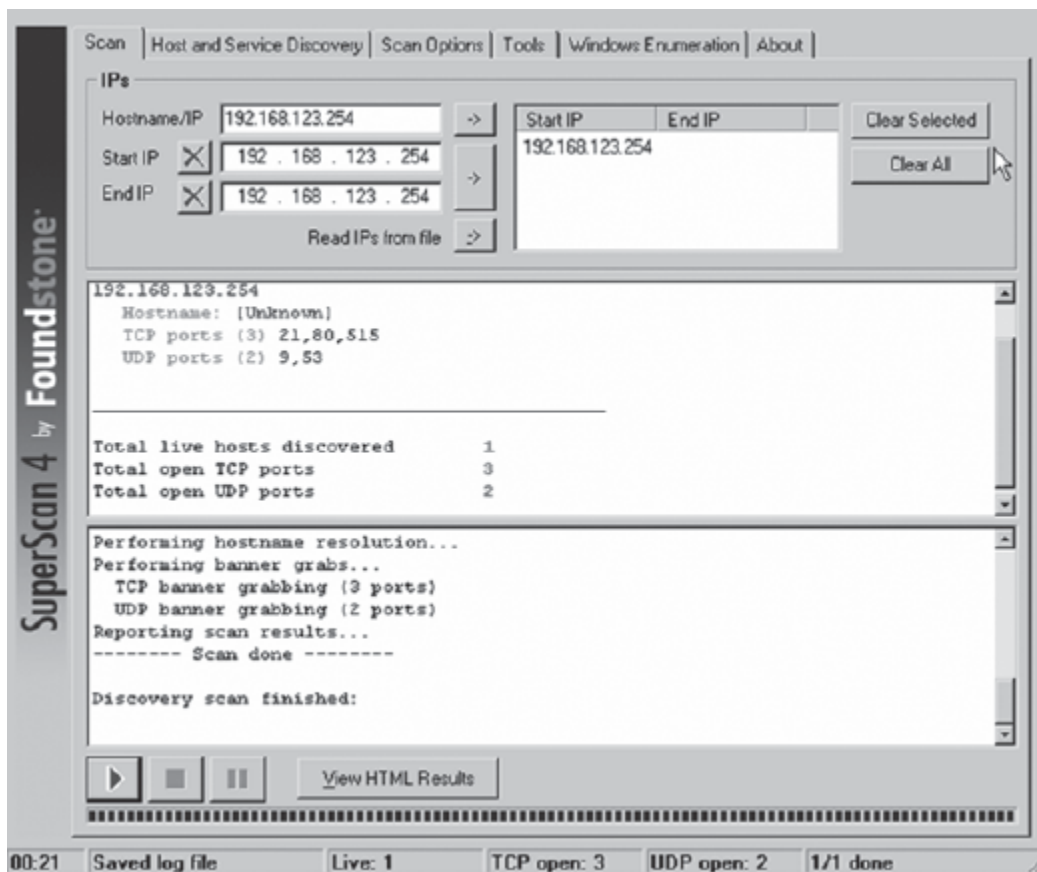


Figure 6-1. Superscan.**Superscan**

Superscan is a Windows-based port scanner developed by Foundstone. This port scanner is designed to scan TCP and UDP ports, perform ping scans, run Whois queries, and use tracert. Superscan is a GUI-based tool that has a preconfigured list of ports to scan or can be customized to scan a specific range. It's shown in [Figure 6-1](#).

Scanrand

Scanrand is a scanning tool that is designed to scan a single host up to large-scale networks quickly and then return results about the network. Scanrand is unique among network scanners because although most scan a port at a time, Scanrand scans ports in parallel using what is known as stateless scanning. By using stateless scanning, Scanrand can perform scans much faster than other network scanners.

NOTE

Scanrand is available for both the Linux and UNIX platforms; there is no Windows equivalent.

Stateless scanning is an approach to scanning that splits scanning into two distinct processes. The two processes work together to complete the scanning process with one process transmitted and the other listening for results. Specifically, the first process transmits connection requests at a high rate, and the second process is responsible for sorting out the results. The power of this program is a process known as inverse SYN cookies.

Scanrand builds a hashed sequence number that is 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. Scanrand is useful to a security professional when a large number of IP addresses need to be scanned quickly.

THC-Amap

THC-Amap (Another Mapper) is a scanner that offers a different approach to scanning. When using traditional scanning programs, problems arise when services that use encryption are scanned, because these services might not return a **banner**, due to the fact that certain services such as the Secure Sockets Layer (SSL) expect a handshake. Amap handles this by storing a collection of normal responses that can be provided to ports to elicit a response. The tool also excels at allowing the security professional to find services that have been redirected from standard ports.

NOTE

CHAPTER 2

THC-Amap is similar to Nmap in that it can identify a service that is listening on a given port. Amap does not include the extensive identification abilities possessed by Nmap, but it can be used to confirm results of Nmap or to fill in any gaps.

OS Fingerprinting

Open ports that have been uncovered during the port scanning phase need to be further investigated because the mere existence of an open port does not mean vulnerability exists; this must still be determined. The open ports that are discovered provide clues to what operating system is in use on the target. Determining the operating system that is in use on a specific target is the purpose of what is known as OS fingerprinting. Once an operating system is identified, it is possible to better focus the attacks that come later. To identify an OS, there are two different methods that can be utilized: **active fingerprinting** or **passive fingerprinting**.

OS fingerprinting relies on the unique characteristics that each OS possesses to function. Each operating system responds to communication attempts in different ways that, once analyzed, can allow for a well-educated guess to be made about the system in place. To seek out these unique characteristics, active and passive fingerprinting can probe a system to generate a response or listen to a system's communications for details about the OS.

FYI

There are literally untold numbers of techniques available to use in an attack. In some cases, these techniques are specific to an operating system due to the vulnerability involved such as a design flaw in the OS or a software defect. When an attack is meant to be used against a specific OS, it would be pointless to unleash it against a target that is not vulnerable, which would both waste time and risk detection.

EVERYTHING HAS A PRICE

Active OS fingerprinting has advantages that make it an attractive option, at least on the surface. The process generally does not take as long to identify a target because the attacker requests information instead of waiting for it, as in passive fingerprinting. While performance is a benefit, the downside is that the process of active fingerprinting has a much higher chance of revealing the attack. It is more than likely that the process of active fingerprinting will trigger defensive countermeasures such as IDS and firewalls, which will respond by alerting the network owners about the attack and shutting it down.

Does this mean active fingerprinting is a bad idea? Not necessarily—there is a time and place for it, and knowing when to use active methods and how aggressively to use them is important. Active fingerprinting, for example, is an ideal mechanism to scan a large amount of hosts quickly, but the danger of being detected and stopped still exists.

Active OS Fingerprinting

CHAPTER 2

The process of active OS fingerprinting is accomplished by sending specially crafted packets to the targeted system. In practice, several probes or triggers are sent from the scanning system to the target. When the responses are received from a targeted system, based on the responses an educated guess can be made as to the OS that is present. Though it may appear otherwise, **OS identification** is an accurate method of determining the system in place because the tools have become much more accurate than in the past.

Xprobe2

Xprobe2, a commonly used active fingerprinting tool, relies on a unique method to identify an operating system known as fuzzy signature matching. This method consists of performing a series of tests against a certain target and collecting the results. The results are then analyzed to a probability that a system is running a specific OS. Xprobe2 cannot say definitively which operating system is running, but instead uses the results to infer what system is running. As an example, running Xprobe2 against a targeted system yields the following results:

```
75% Windows 7
20% Windows XP
5% Windows 98
```

The results that Xprobe2 is presenting here are the probability that the system is running a given OS. Xprobe2 comes with several predefined profiles for different OSs, and the results are compared against these profiles to generate the results seen here. The results show that there are three OSs that match profiles to different degrees: The results for Windows 7 are at 75 percent and the others are quite low, so it can be assumed with some confidence that Windows 7 is in place. This score is intended to determine which operating system the target computer is running.

WHICH METHOD IS BETTER?

Nmap can be used with or without a GUI, and it is up to the individual users to determine which is best for their own particular style. For those who are not comfortable with the command line, the GUI is a great way to learn and get acquainted with what the command line switches look like for specific operations. The Zenmap GUI is a front end for Nmap that makes the product easier to use while allowing the operator to see what the command line looks like. Consider using Zenmap to start; then use the command line once a comfort level is achieved with the commands.

Nmap

Valuable in OS fingerprinting as well as port scanning, Nmap can provide reliable data on which operating system is present. Nmap is effective at identifying the OSs of networked devices and generally can provide results that are highly accurate. Several Nmap options that can be used to fine-tune the scan include:

- -sV Application version detection
- -O OS fingerprinting

CHAPTER 2

- -A Both of the previous options

An example of an Nmap scan with the -O option is shown here:

```
Nmap -O 192.168.123.254
Starting Nmap 4.62 (http://nmap.org) at 2010-03-21 12:09 Central
Daylight Time
Interesting ports on 192.168.123.22:
Not shown: 1712 closed ports
PORT STATE SERVICE
80/tcp open http
2601/tcp open zebra
2602/tcp open ripd
MAC Address: 00:16:01:D1:3D:5C (Netgear)
Device type: general purpose
Running: Linux 2.4.X
OS details: Linux 2.4.18-2.4.32 (likely RedHat)
Uptime: 77.422 days (since Sun Jan 03 01:01:46 2010)
Network Distance: 1 hop
```

Nmap has identified this system as Linux along with version and uptime information. An attacker gaining this information can now target an attack to make it more effective because it would be possible to focus on only those exploits that are appropriate—for example, no Windows attacks. Nmap is capable of identifying commonly encountered network devices and is a tool that should not be overlooked.

Passive OS Fingerprinting

The alternative to active fingerprinting is passive fingerprinting, which approaches the process differently. Passive fingerprinting, by design, does not interact with the target system itself. It is a passive tool that monitors or captures network traffic. The traffic monitored is analyzed for patterns that would suggest which operating systems are in use. Passive OS fingerprinting tools simply sniff network traffic and then match that traffic to specific OS signatures. The database of known patterns can be updated from time to time as new operating systems are released and updated. As an example, a tool may have a fingerprint for Windows Vista but will need to be updated to include Windows 7.

A passive identification requires larger amounts of traffic, but offers a level of stealth, as it is much harder to detect these tools, since they do not perform any action that would reveal their presence. These tools are similar in that they examine specific types of information found in IP and TCP headers. While you do not need to understand the inner workings of TCP/IP to use these tools, you should have a basic understanding as to what areas of these headers these tools examine. These include:

- TTL Value
- Don't Fragment Bit (DF)

CHAPTER 2

- Type of Service (TOS)
- Window Size

The p0f Tool

A tool for performing passive OS fingerprinting is a tool named p0f, which can identify an OS using passive techniques. That means p0f can identify the target without placing any additional traffic on the network that can lead to detection. The tool makes attempts to fingerprint the system based on the incoming connections that are attempted.

PATIENCE IS A VIRTUE

While passive OS fingerprinting generally does not yield results as quickly as active OS fingerprinting, there are still benefits. Passive OS fingerprinting allows an attacker to obtain information about a target without triggering network defensive measures such as IDS or firewalls. While the process may take longer than active fingerprinting, the benefit is that the victim has less chance of detecting and reacting to the impending attack.

Remember: Active fingerprinting contacts the host; passive fingerprinting does not.

ARE WE THERE YET?

The results of the scanning process shown here can be misleading because it is possible that p0f will not be able to identify a system for a number of different reasons. In such events, p0f will return results that will state "unknown" for the operating system instead of an actual OS. In these cases, it may be necessary to try another passive tool or switch to active methods to determine the OS.

The following results have been generated using p0f:

```
C:\>p0f -i2
p0f-passive os fingerprinting utility, version 3.0.4
(C) M. Zalewski <lcamtuf@disone.cc>, W. Stearns <wstearns@pobox.com>
WIN32 port (C) M. Davis <mike@datanerds.net>, K. Kuehl <kkuehl@cisco.com>
p0f: listening (SYN) on '\Device\NPF_{AA134627-43B7-4FE5-AF9B-18CD840ADW7E}', 11
2 sigs (12 generic), rule: 'all'.
192.168.123.254:1045-Linux RedHat
```

Once p0f is running, it will attempt to identify the system that is being connected to, based on the traffic that it observes. The previous example shows that p0f has identified the system in question as being a distribution of Linux known as RedHat.

Mapping the Network

CHAPTER 2

The next step in the process is to generate a picture of the network that is being targeted. When the information has been collected and organized, a network diagram can be produced that will show vulnerable or potentially vulnerable devices on the target network. A number of network management tools can produce an accurate map of the network built of information that has been gathered previously in addition to new information. Some tools that can help in the process include SolarWinds Toolset, Cheops, Queso, and Harris Stat.

NOTE

The tools in this category were designed to help those who create networks manage them. However, as with most tools, the possibility for abuse exists. As is true in most cases, the tool isn't evil or bad; it's the intention of the user that actually determines whether honorable or less-than-honorable actions will be the result.

Even without these tools, you should be able to manually map your findings. This information can be recorded in a notebook or a simple spreadsheet. This spreadsheet should contain domain name information, IP addresses, domain name system (DNS) servers, open ports, OS version, publicly available IP address ranges, wireless access points, modem lines, and application banner details you may have discovered.

Cheops

Cheops is an open source network management tool that can assist in viewing the network layout and the devices therein. Cheops can assist an attacker in the same way it would assist a network admin—it performs tasks such as identifying hosts on a network and the services each offers. Even more useful is the ability to display the whole network in a graphic format showing the paths of data between systems on the target network.

Solarwinds

Solarwinds is another network management tool that can be used to render a diagram of a network and the services within. Solarwinds has the ability to detect, diagram, and reflect changes in the network architecture with a few button clicks. It is even possible for Solarwinds to generate network maps that can be viewed in products such as Microsoft's diagramming product Visio.

Analyzing the Results

With a wealth of data on hand, the attacker now must undertake the process of analyzing that data to learn more about the target. Understanding the vulnerabilities of the victim and identifying potential points of entry require careful analysis and organization. At this point, the attacker starts to plan the attack. When analyzing data, for example, items such as an open wireless access point can lead a hacker to consider additional wardriving or wireless attack activities in an attempt to connect to the network. Another example is an unpatched Web server that would present the hacker an opportunity to run an attack against the server itself. Generally, these steps would be the following:

CHAPTER 2

- Analyze the services that have been revealed.
- Explore vulnerabilities for each service or system.
- Research and locate any potential exploits that can be used to attack the system.

Once each of these items has been completed, the attacker can now use a search engine to gather information about potential attacks by searching the OS and exploits. Plenty of information is available for an attacker to learn how to position an attack. One example, <http://www.securityfocus.com>, was searched for vulnerabilities for Windows Web server IIS version 5. The results are shown in [Figure 6-2](#). Notice that there are more than three pages of results.

The screenshot shows a search results page from securityfocus.com. At the top, there's a header 'Vulnerabilities' and a pagination link '(Page 1 of 3) 1 2 3 Next >'. Below this is a search filter section with dropdown menus for 'Vendor' (set to Microsoft), 'Title' (set to IIS), and 'Version' (set to 5.0). There's also a 'Search by CVE' section with a text input field and a 'Submit' button. The main content area lists several vulnerabilities:

- RETIREDD: Microsoft IIS Malformed Local Filename Security Bypass Vulnerability**
2009-12-29
<http://www.securityfocus.com/bid/37460>
- Microsoft IIS FTPd NLST Remote Buffer Overflow Vulnerability**
2009-11-18
<http://www.securityfocus.com/bid/36189>
- Microsoft IIS FTPd Globbing Functionality Remote Denial of Service Vulnerability**
2009-10-13
<http://www.securityfocus.com/bid/36273>
- RETIREDD: Microsoft IIS FTPd Globbing Functionality Remote Denial of Service Vulnerability**
2009-09-04
<http://www.securityfocus.com/bid/36276>
- Microsoft Collaboration Data Objects Remote Buffer Overflow Vulnerability**
2009-07-12
<http://www.securityfocus.com/bid/15067>
- Microsoft XML Parser Remote Denial of Service Vulnerability**
2009-07-12
<http://www.securityfocus.com/bid/11384>

Figure 6-2. Microsoft IIS vulnerabilities.

It is at this point that the reasons for patiently and thoroughly collecting information about a target become clear. With the results of previous scans, maps, and other data gathered, a target can be more accurately pinpointed resulting in a more effective and potentially devastating attack.

CHAPTER SUMMARY

This chapter introduced the concept of port scanning. Port scanning is a technique that is used to identify services present on a system or range of systems. The purpose of port scanning is to get a better idea of what is present and running on a target prior to carrying out an actual attack against a system. In order to learn more about the services that are available on a system, several techniques can be used, including wardriving, wardialing, and ping sweeps. Once services have been identified and confirmed, the next step is to learn about the operating system to better target the attack itself.

CHAPTER 2

To get the best results from an attack, the operating system needs to be known. There are two ways to determine the OS: active and passive fingerprinting. Active fingerprinting identifies a system or range of systems by sending specially crafted packets designed to reveal unique characteristics about the target. The downside of this type of fingerprinting is that the process can be easily detected. Active fingerprinting tools include Nmap and Xprobe2. The alternative to active fingerprinting is passive fingerprinting, which is stealthier, but is not as accurate. One of the best passive fingerprinting tools is p0f.

The attacker will then move on to mapping the network to determine the nature and relationship of the hosts on the network. Network mapping reveals the nature and relationship of the network in a graphical format, allowing for a better view of the network. Network mapping is one of the last steps before choosing an attack.

Once applications have been mapped and operating systems identified, the attack moves to the final steps, which include mapping the network and analyzing the results. An attacker that has obtained information about services is very close to being able to launch an attack. As a security professional, your goal is to find these problems and fix them before the hacker can exploit these findings.

KEY CONCEPTS AND TERMS

- Active fingerprinting
- Banner
- Internet Control Message Protocol (ICMP)
- OS identification
- Passive fingerprinting
- Ping sweep

CHAPTER 2 ASSESSMENT

1. _____ is a popular though easily detectable scanning technique.
 1. Full connect
 2. Half open scanning
 3. NULL scan
 4. Xmas tree scan
2. Which of the following is the Nmap command line switch for a full connect port scan?
 1. -sS
 2. -sU
 3. -sT
 4. -O
3. Which of the following is an example of a passive fingerprinting tool?
 1. Superscan
 2. Xprobe2
 3. Nmap
 4. p0f

CHAPTER 2

4. TCP and UDP both use flags.
 1. True
 2. False
5. Which of the following statements is most correct?
 1. Active fingerprinting tools inject packets into the network.
 2. Passive fingerprinting tools inject traffic into the network.
 3. Nmap can be used for passive fingerprinting.
 4. Passive fingerprinting tools do not require network traffic to fingerprint an operating system.
6. Which of the following is not a network mapping tool?
 1. Solarwinds
 2. Netstat
 3. Cheops
 4. Harris
7. _____ is the point at which an attacker starts to plan his or her attack.
 1. Active OS fingerprinting
 2. Passive OS fingerprinting
 3. Port scanning
 4. Analyzing the results
8. A XMAS tree scan sets all of the following flags except _____.
 1. SYN
 2. URG
 3. PSH
 4. FIN
9. Of the two protocols discussed, which is more difficult to scan for?
10. You have been asked to perform a port scan for POP3. Which port will you scan for?
 1. 22
 2. 25
 3. 69
 4. 110
11. Ping scanning does not identify open ports.
 1. True
 2. False
12. The process of determining the underlying version of the system program being used is best described as _____.
 1. OS fingerprinting
 2. Port scanning
 3. Wardialing
 4. Wardriving
13. Which of the following switches is used for an ACK scan?
 1. -sI
 2. -sS
 3. -sA
 4. -sT

CHAPTER 2