Covers all Exam Objectives for CEHv6

Includes Real-World Scenarios, Hands-On Exercises, and Leading-Edge Exam Prep Software Featuring:

- Custom Test Engine
- Hundreds of Sample Questions
- Electronic Flashcards
- Entire Book in PDF

# CEH™

# Certified Ethical Hacker

## STUDY GUIDE

Exam 312-50
Exam EC0-350

Kimberly Graves

SYBEX | SERIOUS SKILLS.

# Table of Contents

Chapter

2

# Gathering Target Information: Reconnaissance, Footprinting, and Social Engineering

## CEH EXAM OBJECTIVES COVERED IN THIS CHAPTER:

- ✓ Define the term footprinting
- ✓ Describe information-gathering methodology
- ✓ Describe competitive intelligence
- ✓ Understand DNS enumeration
- ✓ Understand Whois, ARIN lookup
- ✓ Identify different types of DNS records
- ✓ Understand how traceroute is used in footprinting
- ✓ Understand how email tracking works
- ✓ Understand how web spiders work
- ✓ What is social engineering?
- ✓ What are the common types of attacks?
- ✓ Understand dumpster diving
- ✓ Understand reverse social engineering

- ✓ **Understand insider attacks**
- ✓ **Understand identity theft**
- ✓ **Describe phishing attacks**
- ✓ **Understand online scams**
- ✓ **Understand URL obfuscation**
- ✓ **Social-engineering countermeasures**

The first step of the hacking process is gathering information on a target. Information gathering, also known as *footprinting*, is the process of gathering all available information about an organization. In the age of the Internet, information is available in bits and pieces from many different sources. Seemingly insignificant bits of information can be enlightening when pieced together—which is the purpose of information gathering. Footprinting can be effective in identifying high-value targets, which is what hackers will be looking for to focus their efforts.

A hacker uses information-gathering techniques to determine organizations' high-value targets, where the most valuable information resides. Not only does information gathering help identify where the information is located, but it also helps determine the best way to gain access to the targets. This information can then be used to identify and eventually hack target systems. Many people jump right into running hacking tools, but information gathering is critical in minimizing the chance of detection and assessing where to spend the most time and effort.

Social engineering can also be used to obtain more information about an organization, which can ultimately lead to an attack. Social engineering as an information-gathering tool is highly effective at exploiting the most vulnerable asset in an organization: the people. Human interaction and the willingness to give out information make people an excellent source of information. Good social-engineering techniques can speed up the hacking process and in most cases will yield information much more easily.

In this chapter, we'll look at information gathering as the first step in hacking target systems.

# Reconnaissance

The term *reconnaissance* comes from the military and means to actively seek an enemy's intentions by collecting and gathering information about an enemy's composition and capabilities via direct observation, usually by scouts or military intelligence personnel trained in surveillance. In the world of ethical hacking, reconnaissance applies to the process of information gathering. Reconnaissance is a catchall term for watching the hacking target and gathering information about how, when, and where they do things. By identifying patterns of behavior, of people or systems, an enemy could find and exploit a loophole.

**Real World Scenario**

**Using Reconnaissance to Gain Physical Access**

Every weekday at 3 p.m. the Federal Express driver stops at the loading dock of a building where the offices of Medical Associates, Inc. are located. When the driver backs the truck up to the rear door of the building, he presses the buzzer and lets the security guard know he is at the door. Because the building's security personnel recognize the driver—as he comes to the door every day around the same time for pickup and drop-off—they remotely unlock the door and allow the driver to enter. A hacker is watching this process from a car in the parking lot and takes note of the procedure to gain physical entry into the building.

The next day, the hacker carries a large cardboard box toward the door just as the Federal Express driver has been given entry to the building. The driver naturally holds the door for the hacker because he is carrying what appears to be a heavy, large box. They exchange pleasantries and the hacker heads for the elevator up to Medical Associates' offices. The hacker leaves the box in the hallway of the building as he heads to his target office.

Once he reaches the front desk of the Medical Associates office, he asks to speak with the office manager whose name he previously looked up on the company website. The receptionist leaves her desk to go get the office manager, and the hacker reaches over the desk and plugs a USB drive containing hacking tools into the back of her computer. Because the computer is not locked with a password, he double-clicks on the USB drive icon and it silently installs the hacking software on the receptionist's computer. He removes the USB drive and quickly exits the office suite and building undetected.

This is an example of how reconnaissance and understanding the pattern of people's behavior can enable a hacker to gain physical access to a target—in this case the Medical Associates network via a Trojaned system—and circumvent security checkpoints.

## Understanding Competitive Intelligence

Competitive intelligence means information gathering about competitors' products, marketing, and technologies. Most competitive intelligence is nonintrusive to the company being investigated and is benign in nature—it's used for product comparison or as a sales and marketing tactic to better understand how competitors are positioning their products or services. Several tools exist for the purpose of competitive intelligence gathering and can be used by hackers to gather information about a potential target.

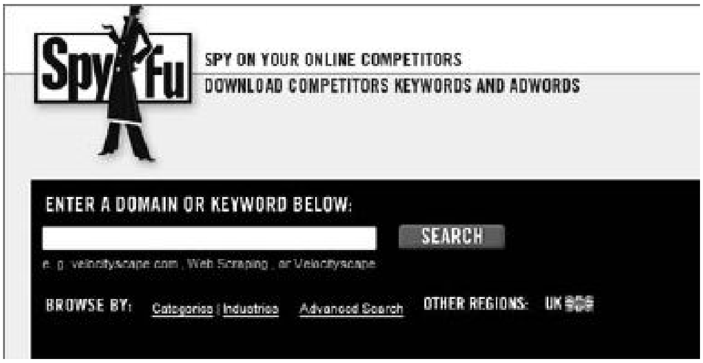
In Exercises 2.1 through 2.3, I will show you how to use the SpyFu and KeywordSpy online tools to gather information about a target website. SpyFu and KeywordSpy will give keywords for websites. This allows you to perform some information gathering regarding a website. I use these two tools because they are easy to use and completely passive, meaning a potential target could not detect the information gathering.

## EXERCISE 2.1

### Using SpyFu

To use the SpyFu online tool to gather competitive intelligence information:

1. Go to the `www.spyfu.com` website and enter the website address of the target in the search field:


SpyFu
SPY ON YOUR ONLINE COMPETITORS
DOWNLOAD COMPETITORS KEYWORDS AND ADWORDS
ENTER A DOMAIN OR KEYWORD BELOW:
SEARCH
e. g. velocityscape.com , Web Scraping , or Velocityscape
BROWSE BY:
Categories | Industries
Advanced Search
OTHER REGIONS:
UK

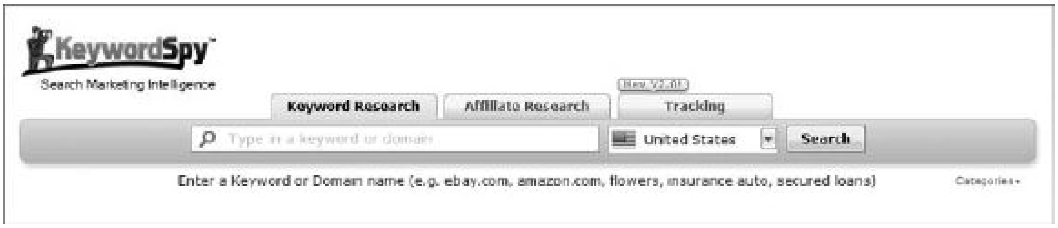
2. Review the report and determine valuable keywords, links, or other information.

## EXERCISE 2.2

### Using KeywordSpy

To use the KeywordSpy online tool to gather competitive intelligence information:

1. Go to the `www.keywordspy.com` website and enter the website address of the target in the search field:



Enter a Keyword or Domain name (e.g. ebay.com, amazon.com, flowers, insurance auto, secured loans)

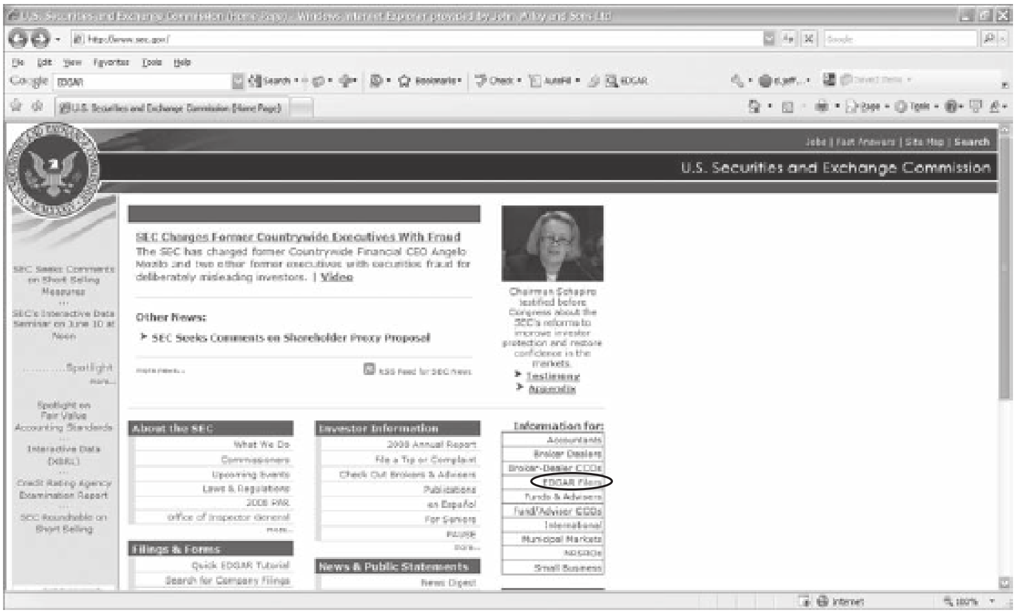
2. Review the report and determine valuable keywords, links, or other information.

Another useful tool to perform competitive intelligence and information gathering is the EDGAR database. This is a database of all the SEC filings for public companies. Information can be gathered by reviewing the SEC filings for contact names and addresses. In Exercise 2.3 I will show you how to use the EDGAR database for gathering information on potential targets.

## EXERCISE 2.3

### Using the EDGAR Database to Gather Information

1. Determine the company's stock symbol using Google.
2. Open a web browser to `www.sec.gov`.
3. On the right side of the page, click the link EDGAR Filers.



SEC Charges Former Countrywide Executives With Fraud
The SEC has charged former Countrywide Financial CEO Angelo Mozilo and two other former executives with securities fraud for deliberately misleading investors. | Video

Other News:
SEC Seeks Comments on Shareholder Proxy Proposal

Chairman Schapiro testified before Congress about the SEC's reforms to improve investor protection and restore confidence in the markets.

4. Click the Search For Filings menu and enter the company name or stock symbol to search the filings for information. You can learn, for example, where the company is registered and who reported the filing.
5. Use the Yahoo! yellow pages (`http://yp.yahoo.com`) to see if an address or phone number is listed for any of the employee names you have located.

**EXERCISE 2.3 *(continued)***

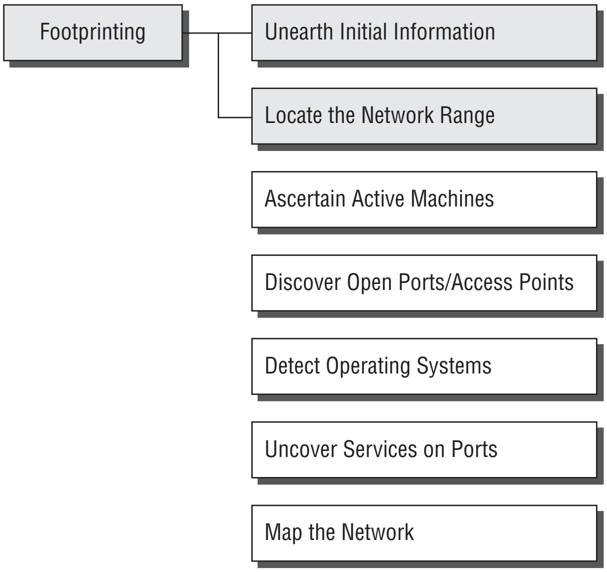
6. Use Google Groups and job-posting websites to search on the names you have found. Are there any IT jobs posted or other information in the newsgroups that would indicate the type of network or systems the organization has?

   The website `www.Netcraft.com` is another good source for passive information gathering. The website will attempt to determine the operating system and web server version running on a web server. This tool will be further discussed in the following chapter.

# Information-Gathering Methodology

Information gathering can be broken into seven logical steps (see Figure 2.1). Footprinting is performed during the first two steps of unearthing initial information and locating the network range.

**FIGURE 2.1** Seven steps of information gathering


Footprinting
Unearth Initial Information
Locate the Network Range
Ascertain Active Machines
Discover Open Ports/Access Points
Detect Operating Systems
Uncover Services on Ports
Map the Network

The other information-gathering steps are covered in Chapter 3, "Gathering Network and Host Information: Scanning and Enumeration."

## Footprinting

*Footprinting* is defined as the process of creating a blueprint or map of an organization's network and systems. Information gathering is also known as footprinting an organization. Footprinting begins by determining the target system, application, or physical location of the target. Once this information is known, specific information about the organization is gathered using nonintrusive methods. For example, the organization's own web page may provide a personnel directory or a list of employee bios, which may prove useful if the hacker needs to use a social-engineering attack to reach the objective.

The information the hacker is looking for during the footprinting phase is anything that gives clues as to the network architecture, server, and application types where valuable data is stored. Before an attack or exploit can be launched, the operating system and version as well as application types must be uncovered so the most effective attack can be launched against the target. Here are some of the pieces of information to be gathered about a target during footprinting:

- Domain name
- Network blocks
- Network services and applications
- System architecture
- Intrusion detection system
- Authentication mechanisms
- Specific IP addresses
- Access control mechanisms
- Phone numbers
- Contact addresses

Once this information is compiled, it can give a hacker better insight into the organization, where valuable information is stored, and how it can be accessed.

### Footprinting Tools

Footprinting can be done using hacking tools, either applications or websites, which allow the hacker to locate information passively. By using these footprinting tools, a hacker can gain some basic information on, or "footprint," the target. By first footprinting the target, a hacker can eliminate tools that will not work against the target systems or network. For example, if a graphics design firm uses all Macintosh computers, then all hacking software that targets Windows systems can be eliminated. Footprinting not only speeds up the hacking process by eliminating certain toolsets but also minimizes the chance of detection as fewer hacking attempts can be made by using the right tool for the job.

For the exercises in this chapter, you will perform reconnaissance and information gathering on a target company. I recommend you use your own organization, but because these tools are passive, any organization name can be used.

Some of the common tools used for footprinting and information gathering are as follows:

- Domain name lookup
- Whois
- NSlookup
- Sam Spade

Before we discuss these tools, keep in mind that open source information can also yield a wealth of information about a target, such as phone numbers and addresses. Performing Whois requests, searching domain name system (DNS) tables, and using other lookup web tools are forms of open source footprinting. Most of this information is fairly easy to get and legal to obtain.

### Footprinting a Target

Footprinting is part of the preparatory preattack phase and involves accumulating data regarding a target's environment and architecture, usually for the purpose of finding ways to intrude into that environment. Footprinting can reveal system vulnerabilities and identify the ease with which they can be exploited. This is the easiest way for hackers to gather information about computer systems and the companies they belong to. The purpose of this preparatory phase is to learn as much as you can about a system, its remote access capabilities, its ports and services, and any specific aspects of its security.

## Using Google to Gather Information

A hacker may also do a Google search or a Yahoo! People search to locate information about employees or the organization itself.

The Google search engine can be used in creative ways to perform information gathering. The use of the Google search engine to retrieve information has been termed Google hacking. Go to `http://groups.google.com` to search the Google newsgroups. The following commands can be used to have the Google search engine gather target information:

**`site`** Searches a specific website or domain. Supply the website you want to search after the colon.

**`filetype`** Searches only within the text of a particular type of file. Supply the file type you want to search after the colon. Don't include a period before the file extension.

**`link`** Searches within hyperlinks for a search term and identifies linked pages.

**`cache`** Identifies the version of a web page. Supply the URL of the site after the colon.

**`intitle`** Searches for a term within the title of a document.

**`inurl`** Searches only within the URL (web address) of a document. The search term must follow the colon.

For example, a hacker could use the following command to locate certain types of vulnerable web applications:

```
INURL:["parameter="] with FILETYPE:[ext] and INURL:[scriptname]
```

Or a hacker could use the search string `intitle: "BorderManager information alert"` to look for Novell BorderManager proxy/firewall servers.

NOTE For more syntax on performing Google searches, visit `www.google.com/help/refinesearch.html`.

Blogs, newsgroups, and press releases are also good places to find information about the company or employees. Corporate job postings can provide information as to the type of servers or infrastructure devices a company may be using on its network.

Other information obtained may include identification of the Internet technologies being used, the operating system and hardware being used, active IP addresses, email addresses and phone numbers, and corporate policies and procedures.

NOTE Generally, a hacker spends 90 percent of the time profiling and gathering information on a target and 10 percent of the time launching the attack.

## Understanding DNS Enumeration

*DNS enumeration* is the process of locating all the DNS servers and their corresponding records for an organization. A company may have both internal and external DNS servers that can yield information such as usernames, computer names, and IP addresses of potential target systems.

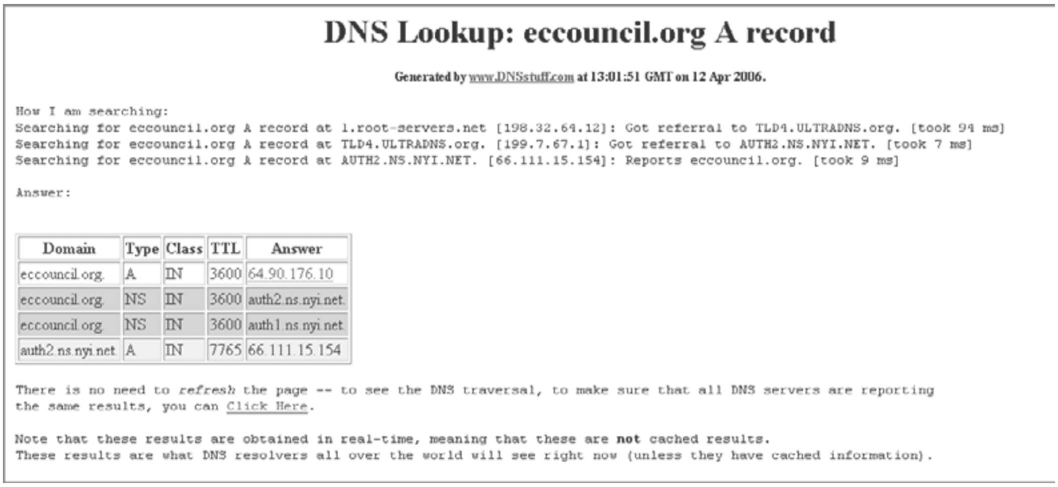
NSlookup, DNSstuff, the American Registry for Internet Numbers (ARIN), and Whois can all be used to gain information that can then be used to perform DNS enumeration.

### NSlookup and DNSstuff

One powerful tool you should be familiar with is NSlookup (see Figure 2.2). This tool queries DNS servers for record information. It's included in Unix, Linux, and Windows operating systems. Hacking tools such as Sam Spade also include NSlookup tools.

Building on the information gathered from Whois, you can use NSlookup to find additional IP addresses for servers and other hosts. Using the authoritative name server information from Whois (`AUTH1.NS.NYI.NET`), you can discover the IP address of the mail server.

**FIGURE 2.2** NSlookup



DNS Lookup: eccouncil.org A record

Generated by www.DNSstuff.com at 13:01:51 GMT on 12 Apr 2006.

```
How I am searching:
Searching for eccouncil.org A record at l.root-servers.net [198.32.64.12]: Got referral to TLD4.ULTRADNS.org. [took 94 ms]
Searching for eccouncil.org A record at TLD4.ULTRADNS.org. [199.7.67.1]: Got referral to AUTH2.NS.NYI.NET. [took 7 ms]
Searching for eccouncil.org A record at AUTH2.NS.NYI.NET. [66.111.15.154]: Reports eccouncil.org. [took 9 ms]

Answer:
```

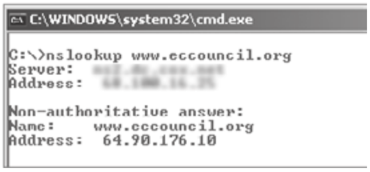
| Domain | Type | Class | TTL | Answer |
|---|---|---|---|---|
| eccouncil.org. | A | IN | 3600 | 64.90.176.10 |
| eccouncil.org. | NS | IN | 3600 | auth2.ns.nyi.net. |
| eccouncil.org. | NS | IN | 3600 | auth1.ns.nyi.net. |
| auth2.ns.nyi.net. | A | IN | 7765 | 66.111.15.154 |

```
There is no need to refresh the page -- to see the DNS traversal, to make sure that all DNS servers are reporting
the same results, you can Click Here.

Note that these results are obtained in real-time, meaning that these are not cached results.
These results are what DNS resolvers all over the world will see right now (unless they have cached information).
```

The explosion of easy-to-use tools has made hacking easy, if you know which tools to use. DNSstuff is another of those tools. Instead of using the command-line NSlookup tool with its cumbersome switches to gather DNS record information, just access the website `www.dnsstuff.com`, and you can do a DNS record search online. Figure 2.3 shows a sample DNS record search on `www.eccouncil.org` using DNSstuff.com.

**FIGURE 2.3** DNS record search of `www.eccouncil.org`



```
C:\>nslookup www.eccouncil.org
Server:  [redacted]
Address:  [redacted]

Non-authoritative answer:
Name:    www.eccouncil.org
Address:  64.90.176.10
```

This search reveals all the alias records for `www.eccouncil.org` and the IP address of the web server. You can even discover all the name servers and associated IP addresses.

The exploits available to you because you have this information are discussed in Chapter 4, "System Hacking: Password Cracking, Escalating Privileges, and Hiding Files."

## Understanding Whois and ARIN Lookups

Whois evolved from the Unix operating system, but it can now be found in many operating systems as well as in hacking toolkits and on the Internet. This tool identifies who has registered domain names used for email or websites. A uniform resource locator (URL), such as `www.Microsoft.com`, contains the domain name (`Microsoft.com`) and a hostname or alias (`www`).

The Internet Corporation for Assigned Names and Numbers (ICANN) requires registration of domain names to ensure that only a single company uses a specific domain name. The Whois tool queries the registration database to retrieve contact information about the individual or organization that holds a domain registration.

### Hacking Tool

SmartWhois is an information-gathering program that allows you to find all available information about an IP address, hostname, or domain, including country, state or province, city, name of the network provider, administrator, and technical support contact information. SmartWhois is a graphical version of the basic Whois program.

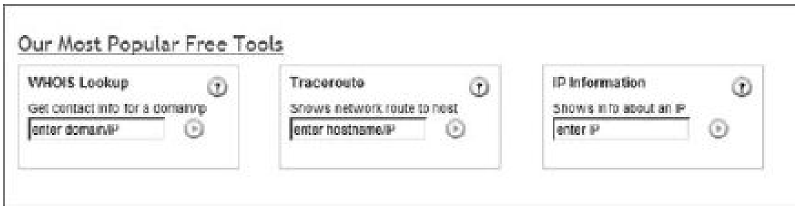
In Exercise 2.4, I will show you how to use a free Whois tool.

**EXERCISE 2.4**

### Using Whois

To use the Whois tool to gather information on the registrar or a domain name:

1. Go to the DNSStuff.com website and scroll down to the free tools at the bottom of the page.



2. Enter your target company URL in the WHOIS Lookup field and click the WHOIS button.
3. Examine the results and determine the following:

   Registered address

   Technical and DNS contacts

   Contact email

**EXERCISE 2.4 *(continued)***

Contact phone number

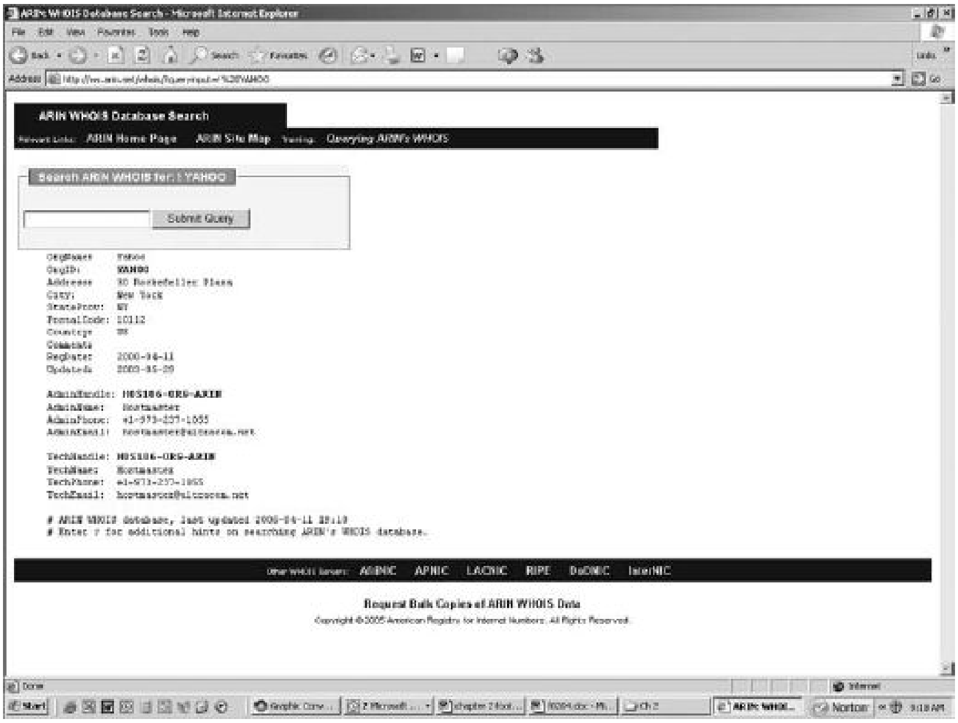
Expiration date

4. Visit the company website and see if the contact information from WHOIS matches up to any contact names, addresses, and email addresses listed on the website.
5. If so, use Google to search on the employee names or email addresses. You can learn the email naming convention used by the organization, and whether there is any information that should not be publicly available.

ARIN is a database that includes such information as the owners of static IP addresses. The ARIN database can be queried using the Whois tool, such as the one located at `www.arin.net`.

Figure 2.4 shows an ARIN Whois search for `www.yahoo.com`. Notice that addresses, emails, and contact information are all contained in this Whois search. This information can be used by an ethical hacker to find out who is responsible for a certain IP address and which organization owns that target system, or it can be used by a malicious hacker to perform a social-engineering attack against the organization. As a security professional, you need to be aware of the information available to the public in searchable databases such as ARIN and ensure that a malicious hacker can't use this information to launch an attack against the network.

**FIGURE 2.4** ARIN output for `www.Yahoo.com`



ARIN WHOIS Database Search - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go
Links
ARIN WHOIS Database Search
Relevant Links: ARIN Home Page ARIN Site Map Training: Querying ARIN's WHOIS
Search ARIN WHOIS for: ! YAHOO
Submit Query

```
OrgName:    Yahoo
OrgID:      YAHOO
Address:    30 Rockefeller Plaza
City:       New York
StateProv:  NY
PostalCode: 10112
Country:    US
Comments:
RegDate:    2000-04-11
Updated:    2003-05-29

AdminHandle: HOS106-ORG-ARIN
AdminName:   Hostmaster
AdminPhone:  +1-973-237-1055
AdminEmail:  hostmaster@altocom.net

TechHandle: HOS106-ORG-ARIN
TechName:   Hostmaster
TechPhone:  +1-973-237-1055
TechEmail:  hostmaster@altocom.net

# ARIN WHOIS database, last updated 2006-04-11 20:10
# Enter ? for additional hints on searching ARIN's WHOIS database.
```

Other WHOIS Servers: AfriNIC APNIC LACNIC RIPE DoDNIC InterNIC
Request Bulk Copies of ARIN WHOIS Data
Copyright © 2005 American Registry for Internet Numbers. All Rights Reserved.
Done
Internet
Start
Graphic Conv...
2 Microsoft ...
chapter 2 fool...
8084.doc - Mi...
Ch 2
ARIN WHOI...
Norton
9:18 AM

NOTE

Be aware that other geographical regions outside North American have their own Internet registries, such as RIPE NCC (Europe, the Middle East, and parts of Central Asia), LACNIC (Latin American and Caribbean Internet Addresses Registry), and APNIC (Asia Pacific Network Information Centre).

## Analyzing Whois Output

A simple way to run Whois is to connect to a website (for instance, `www.networksolutions.com`) and conduct the Whois search. Listing 2.1 is the output of a Whois search of the site `www.eccouncil.org`.

NOTE

The contact names and server names in this book have been changed.

**Listing 2.1**

### WHOIS OUTPUT FOR WWW.ECCOUNCIL.ORG

```
Domain ID:D81180127-LROR
Domain Name:ECCOUNCIL.ORG
Created On:14-Dec-2001 10:13:06 UTC
Last Updated On:19-Aug-2004 03:49:53 UTC
Expiration Date:14-Dec-2006 10:13:06 UTC
Sponsoring Registrar:Tucows Inc. (R11-LROR)
Status:OK
Registrant ID:tuTv2ItRZBMNd4lA
Registrant Name: John Smith
Registrant Organization:International Council of E-Commerce Consultants
Registrant Street1:67 Wall Street, 22nd Floor
Registrant Street2:
Registrant Street3:
Registrant City:New York
Registrant State/Province:NY
Registrant Postal Code:10005-3198
Registrant Country:US
Registrant Phone:+1.2127098253
Registrant Phone Ext.:
Registrant FAX:+1.2129432300
 Registrant FAX Ext.:
 Registrant Email:forum@eccouncil.org
 Admin ID:tus9DYvpp5mrbLNd
 Admin Name: Susan Johnson
 Admin Organization:International Council of E-Commerce Consultants
 Admin Street1:67 Wall Street, 22nd Floor
 Admin Street2:
 Admin Street3:
 Admin City:New York
 Admin State/Province:NY
 Admin Postal Code:10005-3198
 Admin Country:US
 Admin Phone:+1.2127098253
 Admin Phone Ext.:
 Admin FAX:+1.2129432300
 Admin FAX Ext.:
 Admin Email:ethan@eccouncil.org
 Tech ID:tuE1cgAfi1VnFkpu
 Tech Name:Jacob Eckel
 Tech Organization:International Council of E-Commerce Consultants
 Tech Street1:67 Wall Street, 22nd Floor
 Tech Street2:
 Tech Street3:
 Tech City:New York
 Tech State/Province:NY
 Tech Postal Code:10005-3198
 Tech Country:US
 Tech Phone:+1.2127098253
 Tech Phone Ext.:
 Tech FAX:+1.2129432300
 Tech FAX Ext.:
 Tech Email:forum@eccouncil.org
 Name Server: ns1.xyz.net
 Name Server: ns2.xyz.net
```

Notice the four highlighted lines. The first shows the target company or person (as well as their physical address, email address, phone number, and so on). The next shows the administration or technical contact (and their contact information). The last two highlighted lines show the names of domain name servers.

## Finding the Address Range of the Network

Every ethical hacker needs to understand how to find the network range and subnet mask of the target system. IP addresses are used to locate, scan, and connect to target systems. You can find IP addresses in Internet registries such as ARIN or the Internet Assigned Numbers Authority (IANA).

An ethical hacker may also need to find the geographic location of the target system or network. This task can be accomplished by tracing the route a message takes as it's sent to the destination IP address. You can use tools like traceroute, VisualRoute, and NeoTrace to identify the route to the target.

Additionally, as you trace your target network, other useful information becomes available. For example, you can obtain internal IP addresses of host machines; even the Internet IP gateway of the organization may be listed. These addresses can then be used later in an attack or further scanning processes.

# Identifying Types of DNS Records

The following list describes the common DNS record types and their use:

**A (Address)** Maps a hostname to an IP address

**SOA (Start of Authority)** Identifies the DNS server responsible for the domain information

**CNAME (Canonical Name)** Provides additional names or aliases for the address record

**MX (Mail Exchange)** Identifies the mail server for the domain

**SRV (Service)** Identifies services such as directory services

**PTR (Pointer)** Maps IP addresses to hostnames

**NS (Name Server)** Identifies other name servers for the domain

# Using Traceroute in Footprinting

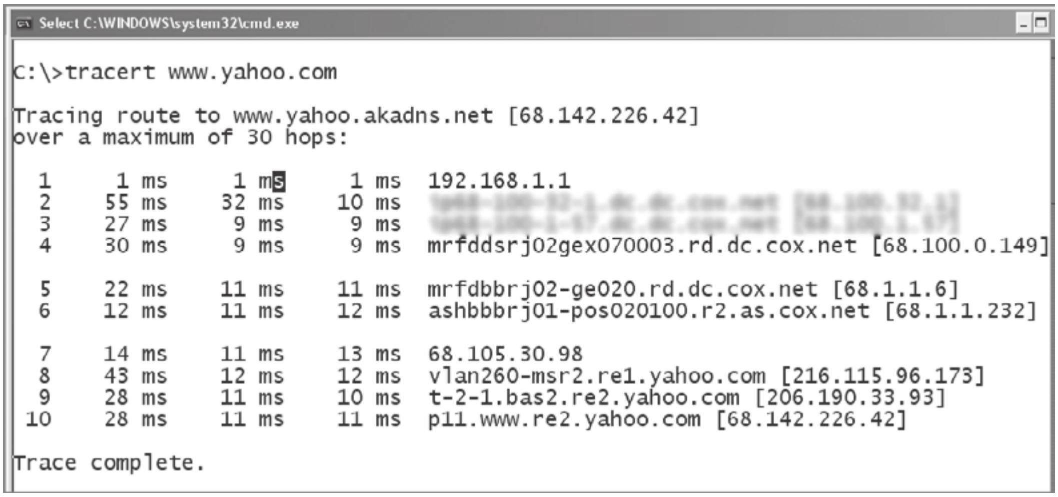
Traceroute is a packet-tracking tool that is available for most operating systems. It operates by sending an Internet Control Message Protocol (ICMP) echo to each hop (router or gateway) along the path, until the destination address is reached. When ICMP messages are sent back from the router, the time to live (TTL) is decremented by one for each router along the path. This allows a hacker to determine how many hops a router is from the sender.

One problem with using the traceroute tool is that it times out (indicated by an asterisk) when it encounters a firewall or a packet-filtering router. Although a firewall stops the traceroute tool from discovering internal hosts on the network, it can alert an ethical hacker to the presence of a firewall; then, techniques for bypassing the firewall can be used.

NOTE These techniques are part of system hacking, which is discussed in Chapter 4.

Sam Spade and many other hacking tools include a version of traceroute. The Windows operating systems use the syntax `tracert` *`hostname`* to perform a traceroute. Figure 2.5 is an example of traceroute output for a trace of `www.yahoo.com`.

**FIGURE 2.5** Traceroute output for `www.yahoo.com`



```
C:\>tracert www.yahoo.com

Tracing route to www.yahoo.akadns.net [68.142.226.42]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.1.1
  2    55 ms    32 ms    10 ms  [redacted]
  3    27 ms     9 ms     9 ms  [redacted]
  4    30 ms     9 ms     9 ms  mrfddsrj02gex070003.rd.dc.cox.net [68.100.0.149]

  5    22 ms    11 ms    11 ms  mrfdbbrj02-ge020.rd.dc.cox.net [68.1.1.6]
  6    12 ms    11 ms    12 ms  ashbbbrj01-pos020100.r2.as.cox.net [68.1.1.232]

  7    14 ms    11 ms    13 ms  68.105.30.98
  8    43 ms    12 ms    12 ms  vlan260-msr2.re1.yahoo.com [216.115.96.173]
  9    28 ms    11 ms    10 ms  t-2-1.bas2.re2.yahoo.com [206.190.33.93]
 10    28 ms    11 ms    11 ms  p11.www.re2.yahoo.com [68.142.226.42]

Trace complete.
```

Notice in Figure 2.5 that the message first encounters the outbound ISP to reach the Yahoo! web server, and that the server's IP address is revealed as 68.142.226.42. Knowing this IP address enables the ethical hacker to perform additional scanning on that host during the scanning phase of the attack.

The `tracert` command identifies routers located en route to the destination's network. Because routers are generally named according to their physical location, `tracert` results help you locate these devices.

### Hacking Tools

NeoTrace, VisualRoute, and VisualLookout are all packet-tracking tools with a GUI or visual interface. They plot the path the packets travel on a map and can visually identify the locations of routers and other internetworking devices. These tools operate similarly to traceroute and perform the same information gathering; however, they provide a visual representation of the results.

## Understanding Email Tracking

Email-tracking programs allow the sender of an email to know whether the recipient reads, forwards, modifies, or deletes an email. Most email-tracking programs work by appending a domain name to the email address, such as `readnotify.com`. A single-pixel graphic file that isn't noticeable to the recipient is attached to the email. Then, when an action is performed on the email, this graphic file connects back to the server and notifies the sender of the action.

**Hacking Tool**

Visualware's eMailTrackerPro (`www.emailtrackerpro.com/`) and MailTracking (`http://mailtracking.com/`) are tools that allow an ethical hacker to track email messages. When you use these tools to send an email, forward an email, reply to an email, or modify an email, the resulting actions and tracks of the original email are logged. The sender is notified of all actions performed on the tracked email by an automatically generated email.

## Understanding Web Spiders

Spammers and anyone else interested in collecting email addresses from the Internet can use *web spiders*. A web spider combs websites collecting certain information such as email addresses. The web spider uses syntax such as the @ symbol to locate email addresses and then copies them into a list. These addresses are then added to a database and may be used later to send unsolicited emails.

Web spiders can be used to locate all kinds of information on the Internet. A hacker can use a web spider to automate the information-gathering process. A method to prevent web spidering of your website is to put the `robots.txt` file in the root of your website with a listing of directories that you want to protect from crawling.

# Social Engineering

*Social engineering* is a nontechnical method of breaking into a system or network. It's the process of deceiving users of a system and convincing them to perform acts useful to the hacker, such as giving out information that can be used to defeat or bypass security mechanisms. Social engineering is important to understand because hackers can use it to attack the human element of a system and circumvent technical security measures. This method can be used to gather information before or during an attack.

A social engineer commonly uses the telephone or Internet to trick people into revealing sensitive information or to get them to do something that is against the security policies of the organization. By this method, social engineers exploit the natural tendency of a person to trust their word, rather than exploiting computer security holes. It's generally agreed that users are the weak link in security; this principle is what makes social engineering possible.

The following is an example of social engineering recounted by Kapil Raina, currently a security expert at VeriSign, based on an actual workplace experience with a previous employer:

> One morning a few years back, a group of strangers walked into a large shipping firm and walked out with access to the firm's entire corporate network. How did they do it? By obtaining small amounts of access, bit by bit, from a number of different employees in that firm. First, they did research about the company for two days before even attempting to set foot on the premises. For example, they learned key employees' names by calling HR. Next, they pretended to lose their key to the front door, and a man let them in. Then they "lost" their identity badges when entering the third floor secured area, smiled, and a friendly employee opened the door for them.
>
> The strangers knew the CFO was out of town, so they were able to enter his office and obtain financial data off his unlocked computer. They dug through the corporate trash, finding all kinds of useful documents. They asked a janitor for a garbage pail in which to place their contents and carried all of this data out of the building in their hands. The strangers had studied the CFO's voice, so they were able to phone, pretending to be the CFO, in a rush, desperately in need of his network password. From there, they used regular technical hacking tools to gain super-user access into the system.
>
> In this case, the strangers were network consultants performing a security audit for the CFO without any other employees' knowledge. They were never given any privileged information from the CFO but were able to obtain all the access they wanted through social engineering.

The most dangerous part of social engineering is that companies with authentication processes, firewalls, virtual private networks, and network-monitoring software are still wide open to attacks, because social engineering doesn't assault the security measures directly. Instead, a social-engineering attack bypasses the security measures and goes after the human element in an organization.

# The Art of Manipulation

Social engineering includes the acquisition of sensitive information or inappropriate access privileges by an outsider, based on the building of inappropriate trust relationships. The goal of a social engineer is to trick someone into providing valuable information or access to that information. Social engineering preys on qualities of human nature, such as the desire to be helpful, the tendency to trust people, and the fear of getting in trouble. Hackers who are able to blend in and appear to be a part of the organization are the most successful at social-engineering attacks. This ability to blend in is commonly referred to as the *art of manipulation*.

People are usually the weakest link in the security chain. A successful defense depends on having good policies in place and teaching employees to follow the policies. Social engineering is the hardest form of attack to defend against because a company can't protect itself with hardware or software alone.

# Types of Social Engineering-Attacks

Social engineering can be broken into two common types:

**Human-Based** Human-based social engineering refers to person-to-person interaction to retrieve the desired information. An example is calling the help desk and trying to find out a password.

**Computer-Based** Computer-based social engineering refers to having computer software that attempts to retrieve the desired information. An example is sending a user an email and asking them to reenter a password in a web page to confirm it. This social-engineering attack is also known as *phishing*.

We'll look at each of these more closely in the following sections.

## Human-Based Social Engineering

Human-based social engineering techniques can be broadly categorized as follows:

**Impersonating an Employee or Valid User** In this type of social-engineering attack, the hacker pretends to be an employee or valid user on the system. A hacker can gain physical access by pretending to be a janitor, employee, or contractor. Once inside the facility, the hacker gathers information from trashcans, desktops, or computer systems.

**Posing as an Important User** In this type of attack, the hacker pretends to be an important user such as an executive or high-level manager who needs immediate assistance to gain access to a computer system or files. The hacker uses intimidation so that a lower-level employee such as a help desk worker will assist them in gaining access to the system. Most low-level employees won't question someone who appears to be in a position of authority.

**Using a Third Person** Using the third-person approach, a hacker pretends to have permission from an authorized source to use a system. This attack is especially effective if the supposed authorized source is on vacation or can't be contacted for verification.

**Calling Technical Support** Calling tech support for assistance is a classic social-engineering technique. Help desk and technical support personnel are trained to help users, which makes them good prey for social-engineering attacks.

**Shoulder Surfing** Shoulder surfing is a technique of gathering passwords by watching over a person's shoulder while they log in to the system. A hacker can watch a valid user log in and then use that password to gain access to the system.

**Dumpster Diving** Dumpster diving involves looking in the trash for information written on pieces of paper or computer printouts. The hacker can often find passwords, filenames, or other pieces of confidential information.

A more advanced method of gaining illicit information is known as *reverse social engineering*. Using this technique, a hacker creates a persona that appears to be in a position of authority so that employees ask the hacker for information, rather than the other way around. For example, a hacker can impersonate a help desk employee and get the user to give them information such as a password.

**Real World Scenario**

### Social-Engineering Demonstration

The facilitator of a live Computer Security Institute demonstration showed the vulnerability of help desks when he dialed up a phone company, got transferred around, and reached the help desk. "Who's the supervisor on duty tonight?" "Oh, it's Betty." "Let me talk to Betty." [He's transferred.] "Hi Betty, having a bad day?" "No, why?" "Your systems are down." Betty said, "My systems aren't down, we're running fine." He said, "You better sign off." She signed off. He said, "Now sign on again." She signed on again. He said, "We didn't even show a blip, we show no change." He said, "Sign off again." She did. "Betty, I'm going to have to sign on as you here to figure out what's happening with your ID. Let me have your user ID and password."

So this senior supervisor at the help desk tells him her user ID and password. In a few minutes a hacker is able to get information that might have taken him days to get by capturing traffic and cracking the password. It is much easier to gain information by social engineering than by technical methods.

## Computer-Based Social Engineering

Computer-based social-engineering attacks can include the following:

- Email attachments
- Fake websites
- Pop-up windows

## Insider Attacks

If a hacker can't find any other way to hack an organization, the next best option is to infiltrate the organization by getting hired as an employee or finding a disgruntled employee to assist in the attack. Insider attacks can be powerful because employees have physical access and are able to move freely about the organization. An example might be someone posing as a delivery person by wearing a uniform and gaining access to a delivery room or loading dock. Another possibility is someone posing as a member of the cleaning crew who has access to the inside of the building and is usually able to move about the offices. As a last resort, a hacker might bribe or otherwise coerce an employee to participate in the attack by providing information such as passwords.

## Identity Theft

A hacker can pose as an employee or steal the employee's identity to perpetrate an attack. Information gathered in dumpster diving or shoulder surfing in combination with creating fake ID badges can gain the hacker entry into an organization. Creating a persona that can enter the building unchallenged is the goal of identity theft.

## Phishing Attacks

Phishing involves sending an email, usually posing as a bank, credit card company, or other financial organization. The email requests that the recipient confirm banking information or reset passwords or PINs. The user clicks the link in the email and is redirected to a fake website. The hacker is then able to capture this information and use it for financial gain or to perpetrate other attacks. Emails that claim the senders have a great amount of money but need your help getting it out of the country are examples of phishing attacks. These attacks prey on the common person and are aimed at getting them to provide bank account access codes or other confidential information to the hacker.

## Online Scams

Some websites that make free offers or other special deals can lure a victim to enter a username and password that may be the same as those they use to access their work system. The hacker can use this valid username and password once the user enters the information in the website form.

Mail attachments can be used to send malicious code to a victim's system, which could automatically execute something like a software keylogger to capture passwords. Viruses, Trojans, and worms can be included in cleverly crafted emails to entice a victim to open the attachment. Mail attachments are considered a computer-based social-engineering attack.

Here is an example of an email that which tries to convince the receiver to open an unsafe attachment:

```
Mail server report.


Our firewall determined the e-mails containing worm copies are being sent from
your computer.
```

```
Nowadays it happens from many computers, because this is a new virus type (Network
Worms).

Using the new bug in the Windows, these viruses infect the computer unnoticeably.
After the penetrating into the computer the virus harvests all the e-mail
addresses and sends the copies of itself to these e-mail addresses

Please install updates for worm elimination and your computer restoring.

Best regards,
Customer support service
```

Pop-up windows can also be used in computer-based engineering attacks, in a similar manner to email attachments. Pop-up windows with special offers or free stuff can encourage a user to unintentionally install malicious software.

## URL Obfuscation

The URL (uniform resource locator) is commonly used in the address bar of a web browser to access a particular website. In lay terms, it is the website address. URL obfuscation consists of hiding a fake URL in what appear to be a legitimate website address. For example, a website of 204.13.144.2/Citibank may appear to be a legitimate web address for Citibank but in fact is not. URL obfuscation is used in phishing attacks and some online scams to make the scam seem more legitimate. A website address may be seen as an actual financial institution name or logo, but the link leads to a fake website or IP address. When users click the link, they're redirected to the hacker's site.

Addresses can be obfuscated in malicious links by the use of hexadecimal or decimal notations. For example, the address 192.168.10.5 looks like 3232238085 as a decimal. The same address looks like C0A80A05 in IP hex. This conversion requires that you divide 3232238085 by 16 multiple times. Each time the remainder reveals the address, starting from the least significant value.

Here's the explanation:

3232238085/16 = 202014880.3125 (.3125 × 16 = 5)

202014880/16 = 12625930.0 (.0 × 16 = 0)

12625930/16 = 789120.625 (.625 × 16 = 10 = A)

789120/16 = 49320.0 (.0 × 16 = 0)

49320.0/16 = 3082.5 (.5 × 16 = 8)

3082/16 = 192.625 (.625 × 16 = 10 = A)

192/16 = 12 = C

## Social-Engineering Countermeasures

Knowing how to combat social engineering is critical for any certified ethical hacker. There are a number of ways to do this.

Documented and enforced security policies and security awareness programs are the most critical component in any information security program. Good policies and procedures aren't effective if they aren't taught and reinforced to employees. The policies need to be communicated to employees to emphasize their importance and then enforced by management. After receiving security awareness training, employees will be committed to supporting the security policies of the organization.

The corporate security policy should address how and when accounts are set up and terminated, how often passwords are changed, who can access what information, and how policy violations are to be handled. Also, the policy should spell out help desk procedures for the previous tasks as well as a process for identifying employees—for example, using an employee number or other information to validate a password change. The destruction of paper documents and physical access restrictions are additional areas the security policy should address. Lastly, the policy should address technical areas, such as use of modems and virus control.

One of the advantages of a strong security policy is that it removes the responsibility of employees to make judgment calls regarding a hacker's request. If the requested action is prohibited by the policy, the employee has guidelines for denying it.

The most important countermeasure for social engineering is employee education. All employees should be trained on how to keep confidential data safe. Management teams are involved in the creation and implementation of the security policy so that they fully understand it and support it throughout the organization. The company security awareness policy should require all new employees to go through a security orientation. Annual classes should be required to provide refreshers and updated information for employees.

Another way to increase involvement is through a monthly newsletter with security awareness articles.

# Summary

In this chapter, you learned how to take the first steps toward ethical hacking. Information gathering, in the form of reconnaissance, footprinting, and social engineering, is necessary to learn as much about the target as possible. By following the information-gathering methodology, ethical hackers can ensure they are not missing any steps and valuable information. Time spent in the information-gathering phase is well worth it to speed up and produce successful hacking exploits.

# Exam Essentials

**Know how to search for a company's news, press releases, blogs, and newsgroup postings.** Search job postings from the target company or organization to determine system versions and other vital pieces of information such as firewall or IDS types and server types. Google hacking can be used to gather information from these locations, making it easy for a hacker to quickly locate information about a target.

Use all available public resources to locate information about a target company and gather data about its network and system security.

Use Yahoo! People search or other Internet search engines to find employees of the target company.

**Know how to query DNS for specific record information.** Know how to use DNSstuff, NSlookup, or Sam Spade to query a DNS server for record information, such as hosts and IP addresses.

**Understand how to perform Whois lookups for personal or company information.** Know how to use the ARIN, LACNIC, RIPE NCC, APNIC, and Whois databases to locate registrar and company contact information.

**Know how to find the name of a target company's external and internal domain names.** You should be able to use the Whois and Sam Spade tools to locate the domain information for a given company. Knowledge of the ARIN database is also necessary for the exam.

**Know how to physically locate a target company's web server and other network infrastructure devices.** Use NeoTrace, VisualRoute, or VisualLookout to get a graphical view of the route to a target company's network. These tools enable you to physically locate the servers.

**Know how to track email to or from a company.** You should be able to use email tracking programs to track an email to a target organization and gain additional information to be used in an attack.

**Understand the difference between human-based and computer-based social-engineering attacks.** Human-based social engineering uses nontechnical methods to initiate an attack, whereas computer-based social engineering employs a computer.

Impersonation, posing as important user, the third-person approach, posing as technical support, shoulder surfing, and dumpster diving are types of human-based social engineering.

Email attachments, fake websites, pop-up windows, and reverse social engineering are all computer-based social-engineering methods.

**Understand the importance of employee education.** Educating employees on the signs of social engineering and the company's security policy is key to preventing social-engineering attacks.

# Review Questions

1. Which are the four regional Internet registries?
   - **A.** APNIC, PICNIC, NANIC, RIPE NCC
   - **B.** APNIC, MOSTNIC, ARIN, RIPE NCC
   - **C.** APNIC, PICNIC, NANIC, ARIN
   - **D.** APNIC, LACNIC, ARIN, RIPE NCC

2. Which of the following is a tool for performing footprinting undetected?
   - **A.** Whois search
   - **B.** Traceroute
   - **C.** Ping sweep
   - **D.** Host scanning

3. Which of the following tools are used for footprinting? (Choose 3.)
   - **A.** Whois
   - **B.** Sam Spade
   - **C.** NMAP
   - **D.** SuperScan
   - **E.** NSlookup

4. What is the next immediate step to be performed after footprinting?
   - **A.** Scanning
   - **B.** Enumeration
   - **C.** System hacking
   - **D.** Bypassing an IDS

5. Which are good sources of information about a company or its employees? (Choose all that apply.)
   - **A.** Newsgroups
   - **B.** Job postings
   - **C.** Company website
   - **D.** Press releases

**6.** How does traceroute work?

**A.** It uses an ICMP destination-unreachable message to elicit the name of a router.

**B.** It sends a specially crafted IP packet to a router to locate the number of hops from the sender to the destination network.

**C.** It uses a protocol that will be rejected by the gateway to determine the location.

**D.** It uses the TTL value in an ICMP message to determine the number of hops from the sender to the router.

**7.** What is footprinting?

**A.** Measuring the shoe size of an ethical hacker

**B.** Accumulation of data by gathering information on a target

**C.** Scanning a target network to detect operating system types

**D.** Mapping the physical layout of a target's network

**8.** NSlookup can be used to gather information regarding which of the following?

**A.** Hostnames and IP addresses

**B.** Whois information

**C.** DNS server locations

**D.** Name server types and operating systems

**9.** Which of the following is a type of social engineering?

**A.** Shoulder surfing

**B.** User identification

**C.** System monitoring

**D.** Face-to-face communication

**10.** Which is an example of social engineering?

**A.** A user who holds open the front door of an office for a potential hacker

**B.** Calling a help desk and convincing them to reset a password for a user account

**C.** Installing a hardware keylogger on a victim's system to capture passwords

**D.** Accessing a database with a cracked password

**11.** What is the best way to prevent a social-engineering attack?

**A.** Installing a firewall to prevent port scans

**B.** Configuring an IDS to detect intrusion attempts

**C.** Increasing the number of help desk personnel

**D.** Employee training and education

**12.** Which of the following is the best example of reverse social engineering?

- **A.** A hacker pretends to be a person of authority in order to get a user to give them information.
- **B.** A help desk employee pretends to be a person of authority.
- **C.** A hacker tries to get a user to change their password.
- **D.** A user changes their password.

**13.** Using pop-up windows to get a user to give out information is which type of social-engineering attack?

- **A.** Human-based
- **B.** Computer-based
- **C.** Nontechnical
- **D.** Coercive

**14.** What is it called when a hacker pretends to be a valid user on the system?

- **A.** Impersonation
- **B.** Third-person authorization
- **C.** Help desk
- **D.** Valid user

**15.** What is the best reason to implement a security policy?

- **A.** It increases security.
- **B.** It makes security harder to enforce.
- **C.** It removes the employee's responsibility to make judgments.
- **D.** It decreases security.

**16.** Faking a website for the purpose of getting a user's password and username is which type of social-engineering attack?

- **A.** Human-based
- **B.** Computer-based
- **C.** Web-based
- **D.** User-based

**17.** Dumpster diving can be considered which type of social-engineering attack?

- **A.** Human-based
- **B.** Computer-based
- **C.** Physical access
- **D.** Paper-based

18. What information-gathering tool will give you information regarding the operating system of a web server?

    A. NSlookup

    B. DNSlookup

    C. `tracert`

    D. Netcraft

19. What tool is a good source of information for employee's names and addresses?

    A. NSlookup

    B. Netcraft

    C. Whois

    D. `tracert`

20. Which tool will only work on publicly traded companies?

    A. EDGAR

    B. NSlookup

    C. Netcraft

    D. Whois

# Answers to Review Questions

1. D. The four Internet registries are ARIN (American Registry of Internet Numbers), RIPE NCC (Europe, the Middle East, and parts of Central Asia), LACNIC (Latin American and Caribbean Internet Addresses Registry), and APNIC (Asia Pacific Network Information Centre).

2. A. Whois is the only tool listed that won't trigger an IDS alert or otherwise be detected by an organization.

3. A, B, E. Whois, Sam Spade, and NSlookup are all used to passively gather information about a target. NMAP and SuperScan are host and network scanning tools.

4. A. According to CEH methodology, scanning occurs after footprinting. Enumeration and system hacking are performed after footprinting. Bypassing an IDS would occur later in the hacking cycle.

5. A, B, C, D. Newsgroups, job postings, company websites, and press releases are all good sources for information gathering.

6. D. Traceroute uses the TTL values to determine how many hops the router is from the sender. Each router decrements the TTL by one under normal conditions.

7. B. Footprinting is gathering information about a target organization. Footprinting is not scanning a target network or mapping the physical layout of a target network.

8. A. NSlookup queries a DNS server for DNS records such as hostnames and IP addresses.

9. A. Of the choices listed here, shoulder surfing is considered a type of social engineering.

10. B. Calling a help desk and convincing them to reset a password for a user account is an example of social engineering. Holding open a door and installing a keylogger are examples of physical access intrusions. Accessing a database with a cracked password is system hacking.

11. D. Employee training and education is the best way to prevent a social-engineering attack.

12. A. When a hacker pretends to be a person of authority in order to get a user to ask them for information, it's an example of reverse social engineering.

13. B. Pop-up windows are a method of getting information from a user utilizing a computer. The other options do not require access to a computer.

14. A. Impersonation involves a hacker pretending to be a valid user on the system.

15. C. Security policies remove the employee's responsibility to make judgments regarding a potential social-engineering attack.

16. B. Website faking is a form of computer-based social-engineering attack because it requires a computer to perpetuate the attack.

17. A. Dumpster diving is a human-based social-engineering attack because it is performed by a human being.

18. D. The Netcraft website will attempt to determine the operating system and web server type of a target.

19. C. Whois will list a contact name address and phone number for a given website.

20. A. EDGAR is the SEC database of filings and will only work on publicly traded firms.