Using E-mail Addresses

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

Activity 4-2: Identifying Company E-mail Accounts

Time Required: 30 minutes

Objective: Determine e-mail addresses for company employees.

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

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

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

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

6. Did you find any information that could be useful to a security tester? How old are many of the returned links?
7. To view more recent postings, modify your query to include **"2015"** and **"2016."** (Include the quotation marks around search terms to make sure you don't get phone numbers or addresses containing these numbers in your search results.)

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

Using HTTP Basics

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

Error	Description
400 Bad Request	Request not understood by server
401 Unauthorized	Request requires authentication
402 Payment Required	Reserved for future use
403 Forbidden	Server understands the request but refuses to comply
404 Not Found	Unable to match request
405 Method Not Allowed (*Note*: Methods are covered later in this chapter.)	Request not allowed for the resource
406 Not Acceptable	Resource doesn't accept the request
407 Proxy Authentication Required	Client must authenticate with proxy
408 Request Timeout	Request not made by client in allotted time
409 Conflict	Request couldn't be completed because of an inconsistency
410 Gone	Resource is no longer available
411 Length Required	Content length not defined
412 Precondition Failed	Request header fields evaluated as false
413 Request Entity Too Large	Request is larger than server is able to process
414 Request-URI (uniform resource identifier) Too Long	Request-URI is longer than the server is willing to accept

Table 4-2 HTTP client errors