Chapter 04 – Footprinting and Social Engineering

Notes

Overview

This chapter describes footprinting, a technique used to find network information. A list of several free web tools that can be used for security testers, or attackers, for footprinting is provided. You will learn about competitive intelligence and why it is important for an organization. Next, you will learn how to gather more information when footprinting a network using DNS. Finally, this chapter presents a discussion on social engineering. Social engineers target the human resources of a network to find its vulnerabilities or perpetrate an attack.

Chapter Objectives

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

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

Tips

Using Web Tools for Footprinting

1. Footprinting is a technique used to find information about a company's network. This information helps security testers get a better idea about the network before starting a security test. Unfortunately, attackers can also use this information for conducting attacks.

2. See Table 4-1 for several Web tools available for footprinting.

Conducting Competitive Intelligence

1. Many companies use competitive intelligence to find out information about their competitors. With the advent of technology, competitive intelligence has been raised to a higher level. Now, companies find information using tools like Web browsers, search engines, and other footprinting tools.

2. You must be able to identify and report all mechanisms used by others to gather information about your organizations.

Analyzing a Company's Web Site

1. Web pages are an easy way to gather information about a company. There are several tools for this purpose, for example Paros.

2. Zed Attack Proxy (ZAP) is a powerful tool for UNIX and Windows OSs and can be downloaded from https://github.com/zaproxy and it requires having Java installed; this can be downloaded from https://*www.java.com*.

3. See Figure 4-1 through Figure 4-4 for the process of analyzing a Web site using ZAP.

Using Other Footprinting Tools

1. The Whois command can be used to gather IP address and domain information. See Figure 4-5

Tip	There are several online Whois tools. Visit http://networking.ringofsaturn.com/Tools/whois.php to find out more. This Web site also allows you to query whois databases.

Using E-mail Addresses

1. E-mail addresses can be used either by security testers or attackers to find more information about a particular company. When analyzing an e-mail address, you can determine the e-mail address format used by the company. Then, using a phone directory, you can find other employees' names. You can combine this data with other employees' e-mail addresses.

2. Activity 4-2 describes how to use *groups.google.com* to determine e-mail addresses for corporate employees.

Using HTTP Basics

1. HTTP is a protocol that operates on port 80. As a security tester, you can use HTTP to find more information about a Web server and its vulnerabilities. Acquire a basic understanding of HTTP error codes and methods.

2. See Table 4-2 for the most important HTTP client error codes.

3. See Table 4-3 for the most important HTTP server error codes.

4. See Table 4-4 for the most important HTTP methods.

5. See Figure 4-6–Figure 4-8 for the use of HTTP methods to find information about a Web server.

Tip	See http://www.softwaregatest.com/qatweb1.html for links to Web site security test tools.

Other Methods of Gathering Information

1. Cookies are text files generated by a Web site and stored on a user's Web browser. Cookies can store personal information and cause privacy problems. For example, if the computer that stores cookies is under attack, the attacker can collect the information stored on those files.

2. Learn how to discover cookies on Web browsers in Activity 4-4.

3. Web bugs are one-pixel by one-pixel image files referenced in <IMG> tags on Web pages. Web bugs usually work with cookies to collect information about a user's browsing habits. The information can later be used, for example, on a customized advertisement. For this reason, Web bugs are considered spyware or adware. Web bugs are commonly developed for third-party companies specialized in data collection.

Using Domain Name Service (DNS) Zone Transfers

1. The DNS service. Words are easier to remember than numbers; this is why people prefer using URLs such as *www.google.com* instead of IP addresses. DNS servers resolve host names to IP addresses. Unfortunately, DNS servers are extremely vulnerable.

2. Zone transfers enable you to see all hosts on a network. It gives you an organization's network diagram! The main tools used when performing zone transfers are the Dig and Host commands. Activity 4-6 shows how to perform a zone transfer. See Figure 4-9.

Introduction to Social Engineering

1. Social engineers target the human component of a network to perpetrate their attacks or to at least to find some information that can help them attack a network. This is why social engineering is the biggest security threat to networks and the most difficult to protect against.

2. The main tactics used by social engineers when profiling a person include:
   A. Persuasion
   B. Intimidation
   C. Coercion
   D. Extortion
   E. Blackmailing

3. Social engineers study human behavior. They try to recognize personality traits such as shyness or insecurity. They also know how to read body language.

4. The main techniques used by social engineers include:
   A. Urgency
   B. Quid pro quo
   C. Status quo
   D. Kindness
   E. Position

5. The best defense against social engineers is education. Security professionals should train their users not to reveal company's information to outsiders and to always verify the identity of a caller.
   A. Ask questions
   B. Get the phone number and call back

The Art of Shoulder Surfing

1. An attacker can gain confidential information by shoulder surfing. The attacker observes what you type from a nearby location. They might be very close to the victim and look over the victim's shoulder, or they might use binocular or high-powered telescopes to spy from a safe distance. Shoulder surfers try to obtain the following information:
   a. Logon names
   b. Passwords
   c. PINs
   d. Credit card numbers

2. You can use to protect yourself from shoulder surfing by:
    a. Avoid typing when someone is nearby
    b. Avoid typing when someone nearby is talking on a cell phone
    c. Computer monitors should face away from the door or cubicle entryway
    d. Immediately change your password if you suspect someone has been observing you

Tip	Security lens are recommended when traveling to prevent shoulder surfing.

The Art of Dumpster Diving

1. An attacker can gain information by dumpster diving. Many companies do not pay attention to what they dispose as trash; an eager social engineer can use this information getting a better picture about the company. This seemingly innocuous information can be used by social engineers on more elaborate attacks. For example, discarded phone directories can give attacker a list of all employees' full names. Examples of what dumpster divers look for:
    a. Financial reports
    b. Interoffice memos
    c. Discarded computer programs
    d. Company organizational charts showing managers' names
    e. Resumes of employees
    f. Company policies or systems and procedures manuals
    g. Professional journals or magazines
    h. Utility bills
    i. Solicitation notices from outside vendors
    j. Regional manager reports
    k. Quality assurance reports
    l. Risk management reports
    m. Minutes of meetings
    n. Federal, state, or city reports
    o. Employee charge card receipts

2. To protect yourself from dumpster diving:
    a. Educate your users about dumpster diving
    b. Use proper trash disposal
    c. Format disks before disposing them
    d. Format disks with software that writes binary zeros
    e. Format disks at least seven times
    f. Discard computer manuals offsite
    g. Shred documents before disposal

The Art of Piggybacking

1. Piggybacking is a technique used by attackers to gain access to restricted areas without alerting security personnel. The piggybacker observes the secured area entryway and waits for an authorized person to enter; he or she then quickly joins that person. Attackers may have both hands full and seem to be struggling to remove an access card from a purse or pants pocket. They can even wear fake badges or pretend to have problems passing security cards on the card reader.

2. As a security professional, you should educate your users about piggybacking and show them effective techniques to prevent it from happening. These techniques include:
   a. Use turnstiles
   b. Train personnel to notify security of the presence of strangers
   c. Do not hold secured doors for anyone, even for people you know
   d. All employees must use their secure cards

Phishing

1. A phishing e-mail message is usually framed as an urgent request to visit a Web site to make sure you are not locked out of an account, such as banking services. The Web site is a fake and tries to trick victims into giving out personal information.

2. Spear phishing attacks are directed to specific people. The e-mail message may appear to come from someone the receiver knows and mention a topic of mutual interest. The goal is to entice victims into opening an attachment or clicking a link; this action installs "spear phished" malware, which can have devastating effects.

Additional Resources

1. Dig command man pages:
   http://www.kloth.net/services/dig-man.php

2. Wget command man pages:
   http://linux.maruhn.com/sec/wget-man-gz.html

3. DNS stuff:
   http://www.dnsstuff.com

4. How Domain Name Servers Work:
   http://computer.howstuffworks.com/dns.htm

5. Social Engineering at SecurityFocus:
   http://www.securityfocus.com/infocus/1527

Key Terms

- **competitive intelligence**
- **cookie**
- **dumpster diving**
- **footprinting**
- **phishing**
- **piggybacking**
- **shoulder surfing**
- **social engineering**
- **spidering (or crawling)**
- **spear phishing**
- **Web bug**
- **zone transfer**