Chapter 2

True/False
Indicate whether the statement is true or false.

1. Reconnaissance is not by definition illegal, and many reconnaissance techniques are completely legal.
   ANS: T PTS: 1 REF: 18

2. The strongest link in any security scheme is the user.
   ANS: F PTS: 1 REF: 20

3. Most social engineering attacks are opportunistic: the hacker uses whatever technique he or she thinks fits the situation.
   ANS: T PTS: 1 REF: 22

4. Breaking CD-ROMs is sufficient to destroy their data, as data cannot be recovered from broken disks.
   ANS: F PTS: 1 REF: 28

5. Internet footprinting is a technical method of reconnaissance, which interests budding hackers and network security specialists alike.

Multiple Choice
Identify the choice that best completes the statement or answers the question.

1. ____ uses influence and persuasion to deceive people by convincing them that the social engineer is someone he isn't, or by manipulation.
   a. Network enumeration
   b. Network penetration
   c. Social enumeration
   d. Social engineering

   ANS: D PTS: 1 REF: 20

2. ____ is a method of achieving access to information by actually joining the organization as an employee or a consultant.
   a. Deception
   b. Bribery
   c. Impersonation
   d. Conformity

   ANS: A PTS: 1 REF: 22

3. With ____, a user is tricked into giving private information about his or her account with a known large organization.
   a. conformity
   b. phishing
   c. deception
   d. pharming

   ANS: B PTS: 1 REF: 25

4. Newsgroups are part of an online bulletin board system called ____, which contains groups covering a huge variety of subjects.
   a. GROUPS
   b. ARPANET
   c. USENET
   d. NEWSNET

   ANS: C PTS: 1 REF: 30

5. ____ is an Internet tool that aids in retrieving domain name–specific information from the NSI Registrar database.
   a. WHOIS
   b. Locate
   c. DNS
   d. Whereis

   ANS: A PTS: 1 REF: 31

Completion
Complete each statement.

1. _____ is the act of locating targets and developing the methods necessary to attack those targets successfully.
   ANS:Reconnaissance

   PTS: 1 REF: 18

2. _____ is the process of identifying domain names as well as other resources on the target network.
   ANS:Network enumeration

   PTS: 1 REF: 31

3. _____ is a DNS feature that lets a DNS server update its database with the list of domain names in another DNS server.
   ANS:Zone transfer

   PTS: 1 REF: 34

4. There are two ping utilities available for a Linux or Unix machine: ping and _____.
   ANS:ping6

   PTS: 1 REF: 37

5. The Linux command _____ shows you where the files appear in your PATH.
   ANS:whereis

   PTS: 1 REF: 37

Short Answer

1. Describe some legal reconnaissance activities.

   ANS:
   Looking up all of the information about a company available on the Internet, including published phone numbers, office hours, and addresses, is completely legal. Calling with a problem requiring customer service assistance is completely legal (even if it is a made-up problem). Interviewing a member of the staff for a school project is legal. Physical entry of a facility, including attending a tour of the facility, is entirely legal. Making friends with somebody who works there or used to work there is also legal. It would be exceptionally paranoid for company representatives to refuse to answer the phone“just in case it is a hacker performing recon.”All of these methods and many others are completely legal and done for various reasons all the time.

PTS: 1 REF: 19

2. Describe some illegal reconnaissance activities.

ANS:
There are a number of plainly illegal reconnaissance techniques. Developing a “front” company and acting as a representative of that company, specifically for the purpose of robbing or defrauding the target company, is probably illegal. Furthermore, being expensive and time consuming, this is probably reserved for the professional intel agencies. Stealing garbage is illegal in many locales. Entering a home or office to look for information is also illegal, but this often goes undetected as no valuables are being removed. Dropping a keylogger—a tool that records users’ keystrokes—on a vulnerable machine is illegal. Leaving a sniffer, which can intercept and read data packets, on a network is illegal.

PTS: 1 REF: 19

3. Describe conformity as a social engineering technique.

ANS:
This method hinges on the general tendency of people to believe that an *apparent* similarity between themselves and another (unknown) person is an *actual* similarity. The hacker convinces the victim that they have a lot in common and that they share the same values. The hacker becomes the victim’s good friend by appearing honest,trustworthy,and friendly. This is a person in whom one may truly confide. Once the information is garnered, the “good friend” just disengages.

PTS: 1 REF: 22

4. Describe physical intrusion as a social engineering technique.

ANS:
The foremost traditional technique of social engineering is physical intrusion, whereby social engineers physically enter the premises of an organization or the workstations of employees for the sole purpose of collecting information. Any unauthorized entry plan uses the same kinds of research and reconnaissance.

“Casing the joint” before a physical intrusion usually includes:
* Learning the schedules of the organization
* Knowing the floor plan of the building or buildings
* “Baselining” the security procedures

PTS: 1 REF: 23

5. What is the importance of proper discarding of refuse?

ANS:
The security policy must carefully address what is sensitive information and what isn’t, and decide how to treat refuse. Some documents may not be considered sensitive, like employee handbooks and company policy statements. But these can often tell hackers what physical and network security to expect when doing intrusion. The best solution to theft of trash paper is to crosscut-shred it and keep it in locked trash receptacles.

Old hardware cannot be shredded and takes up space; thus, these items are frequently thrown out, or given to employees to take home.Hackers search for outdated hardware, such as tapes, CD-ROMs, and hard disks. There are various tools available to hackers, such as forensics programs, that can restore data from damaged data-storage devices.

PTS: 1 REF: 2