Computer Security and Penetration Testing

Chapter 2
Reconnaissance
Objectives

- Identify various techniques for performing reconnaissance
- Distinguish and discuss the methods used in social engineering
- Discuss the importance of dumpster diving in reconnaissance
- Identify a variety of phases of Internet footprinting
Reconnaissance

- Act of locating targets and developing the methods necessary to attack those targets successfully
- May be extremely flexible and creative
- Reconnaissance is not by definition illegal
  - Many reconnaissance techniques are completely legal
Figure 2-1  Abridged organization chart
Some Legal Reconnaissance

- Legal activities
  - Looking up all of the information about a company available on the Internet
  - Calling with a problem requiring customer service assistance
  - Interviewing a member of the staff for a school project
  - Physical entry of a facility, including attending a tour of the facility
  - Making friends with somebody who works there or used to work there
Some Questionable Reconnaissance

- Questionable activities
  - Performing a passive port scan
  - Reading the names on the mail sitting on a mail cart
  - Scanning the document lying loose on a desk
  - Picking up trash in the parking lot
  - Picking up a copy of the employee newsletter
  - Asking for a phone list, business card or product specs
  - Looking through a garbage can
  - War driving
Some Illegal Reconnaissance

- Illegal activities
  - Developing a “front” company for the purpose of robbing or defrauding
  - Stealing garbage
  - Entering a home or office to look for information
  - Dropping a keylogger
  - Leaving a sniffer
Social Engineering

- **Social engineering** works, for the most part, because people are trusting and helpful
- The weakest link in any security scheme is the user
- The success or failure of social engineering
  - Depends on the ability of hackers to manipulate human psychology, contacts, and physical workstations
Social Engineering Techniques

- **Impersonation**
  - Could be at an instance level (impersonating someone)
  - Could be on a role or function level (dressing like a service person)

- **Bribery**
  - Hacker can pit a person’s greed and ignorance against his loyalty to the organization
  - Blackmail is a common tactic to keep a target employee fruitful
Social Engineering Techniques (continued)

- Deception
  - Achieve access to information by joining the company
    - As an employee or a consultant
- Conformity
  - Hacker convinces the victim that they have a lot in common and that they share the same values
  - Hacker becomes the victim’s good friend
- Reverse social engineering
  - Hacker projects herself as an authority vested with the power to solve peoples’ problems
Physical Intrusion

- Foremost traditional technique of social engineering
- Requires
  - Learning the schedules of the organization
  - Knowing the floor plan of the building or buildings
  - “Baselining” the security procedures
- Hacker can develop fake identification cards
- Last step is to acquire useful or valuable information
Physical Intrusion (continued)

- Avoiding suspicion
  - Never collect all the required information from a single user or source
  - Never hold a position after the value of the position has ended
- The more valuable the information is, the more likely hackers are working with a team
- When physical intrusion is not a possibility, hackers use communication media
Communication Media

- Postal Mail
  - Powerful tool for social engineers
  - Typical attack
    - Victim receives a letter announcing that he or she has won a prize
    - Mailer asks for tax information, phone numbers, e-mail addresses, and other information
    - Greed leads the victim to happily surrender all sorts of information

- E-mail
  - Used in a variety of scams and false offerings
Communication Media (continued)

- **E-mail**
  - **Attacks**
    - Hacker sends an e-mail purported to be from a legitimate IT e-mail account
      - Asks for user’s password to help solve a problem
    - Hacker sends e-mail message invitations to join online competitions for receiving prizes
      - Joining requires sending sensitive information
  - **Phishing**
    - User is tricked into giving private information about his or her account with a known large organization
Figure 2-2  An obvious phishing form
Communication Media (continued)

- **Instant Messaging**
  - Social engineer attempts to befriend the victim
    - To gather information or send the victim to a Web link she might be likely to visit

- **Telephone Communication**
  - Social engineers may manipulate background sounds and their own voice to produce a required effect
  - Help desk personnel are vulnerable targets
  - Social engineers often impersonate technicians
Countering Social Engineering

- Steps to counter social engineering attempts:
  - Do not provide any information to unknown people.
  - Do not disclose any confidential information to anyone over the telephone.
  - Do not type passwords or other confidential information in front of unknown people.
  - Do not submit information to any insecure Web site.
  - Do not use same username/password for all accounts.
  - Verify credentials of persons asking for passwords.
Countering Social Engineering (continued)

- Steps to counter social engineering attempts:
  - Keep confidential documents locked
  - Lock or shut down computers when away from the workstation
  - Instruct help desk employees to provide information only after they have gained proper authentication
Dumpster Diving

- Dumpster diving
  - Often the mother lode of sensitive information as well as actual hardware and software
- Hackers look specifically for sales receipts and paperwork
  - That contain personal data or credit card information
- Shredded documents can lead to data leaks
- Drafts of letters are routinely left whole in the trash
- Company directory sheets, catalog lists, unused or misprinted labels, and policy manuals
Importance of Proper Discarding of Refuse

- Security policy must carefully address what is sensitive information
  - And decide how to treat refuse
- Best solution to theft of trash paper
  - Crosscut-shred it and keep it in locked trash receptacles
- Hackers search for outdated hardware
  - There are tools that can restore data from damaged data-storage devices
Prevention of Dumpster Diving

Guidelines that help preventing dumpster diving

- Develop a written recycling and trash-handling policy
- Use the policy to develop a consistent, systematic method for handling trash
- The trash-handling policy should state that all papers be shredded
- Erase all data from tapes, floppies, and hard disks
- Simply breaking CD-ROMs is not sufficient, place them in a microwave and heat them
Internet Footprinting

- A technical method of **reconnaissance**
- Hackers like this method because it is clean, legal, and safe
- Four methods used in Internet footprinting
  - Web searching
  - Network enumeration
  - Domain Name System (DNS)-based reconnaissance
  - Network-based reconnaissance
Web Searching

- Search Engines
  - Can be used to collect information about any subject or organization
  - Companies’ basic information are available through search engines
  - Any company or organization is vulnerable to innocent searches
- HTML Source Code
  - You can view the source code of any Web page
  - Area of interest in an HTML source code is its comment entries and the hints of the organization of the site
Web Searching (continued)

- **HTML Source Code (continued)**
  - Knowing the format of usernames or passwords can be useful
  - You should have a default or an index page in every subdirectory

- **Newsgroups**
  - Text-based online groups in which users discuss subjects that interest them
  - Part of an online bulletin board system called USENET
  - Hackers read postings in newsgroups to discover information and documents relating to targeted systems
Web Searching (continued)

- Security-Related Web Sites
  - Hackers study these Web sites to learn about new developments in information security
    - Especially about new exploits
- Newsletters
  - Provide cutting-edge developments to hackers
  - Most of the time are available free of charge
  - Automatically e-mailed to individuals
Network Enumeration

- Process of identifying domain names as well as other resources on the target network
- WHOIS Search
  - WHOIS
    - Internet tool that aids in retrieving domain name-specific information from the NSI Registrar database
    - Allows the InterNIC database to be queried
      - Displays the information about the searched item
  - Hackers use the WHOIS tool first to extract critical data about their target system
    - And then to conduct hacking activities
Figure 2-3  WHOIS interface on www.dnsstuff.com
Network Enumeration (continued)

- `whois` CLI Command
  - WHOIS Web application is also available at the command-line interface (CLI)
    - Of POSIX systems like UNIX, Solaris, and Linux
Figure 2-4  CLI view of the whois command (on Ubuntu Linux)
Domain Name System (DNS)–Based Reconnaissance

- **DNS Lookup**
  - Tools help Internet users discover the DNS names of target computers
  - Web sites that provide DNS lookup tools
    - www.dnsstuff.com
    - www.network-tools.com
    - www.networksolutions.com

- **DNS Zone Transfer**
  - Every DNS server has a name space, known as a zone
  - A zone stores data about domain names
Domain Name System (DNS)–Based Reconnaissance (continued)

- DNS Zone Transfer (continued)
  - Zone transfer is a DNS feature that lets a DNS server update its database
    - With the list of domain names in another DNS server
  - An incorrectly configured DNS server may allow any Internet user to perform a zone transfer
  - Commands to perform a DNS zone transfer
    - `nslookup`
      - Allows anyone to query a DNS server for information
    - `host`
      - Program that permits you to perform DNS lookup
Domain Name System (DNS)–Based Reconnaissance (continued)

Figure 2-5  \textit{nslookup} for NetworkSolutions.com’s NS1 nameserver
Figure 2-6  host lookup for NetworkSolutions.com
Figure 2-7  Attempted DNS zone transfer
Domain Name System (DNS)–Based Reconnaissance (continued)

- DNS Zone Transfer (continued)
  - Commands to perform a DNS zone transfer
    - `dig`
      - Domain information groper (`dig`)
      - Used to collect DNS-related data
Network-Based Reconnaissance

- **ping**
  - Part of the Internet Control Message Protocol (ICMP)
  - Helps to verify whether a host is active
  - Command is available for all platforms
  - There are two ping utilities available for a Linux or Unix machine: ping and ping6

- **traceroute**
  - A request for a Web page that resides on a remote server must pass through several servers on its way
  - Command can track all of the intermediate servers
Figure 2-8  Option sets for ping and ping6
Figure 2-9  The *whereis* and *which* commands
Network-Based Reconnaissance (continued)

- **traceroute**
  - In UNIX-based operating systems use **traceroute** command
  - In Windows operating systems use **tracert** command
Figure 2-10 Options and sample output of *traceroute* command
Network-Based Reconnaissance (continued)

- *netstat*
  - Allows all the transmission Control Protocol (TCP), User Datagram Protocol (UDP), and IP connections on a computer to be viewed
  - Also helps to locate
    - IP address of computers
    - IP addresses of the hosts connected to the computers
    - Port of the host to which a computer is connected
Figure 2-11  Output of the netstat -h command
Summary

- Reconnaissance is the act of locating targets and developing the methods necessary to attack those targets successfully.
- Social engineering works because people are, for the most part, trusting and helpful.
- To counter social engineering, organizations must establish known security policies and conduct mandatory security training.
- Dumpster diving can provide hackers with sensitive information, as well as hardware and software.
Summary (continued)

- Four methods of Internet footprinting: Web searching, network enumeration, Domain Name System (DNS)-based reconnaissance, and network-based reconnaissance
- During Web searching, hackers collect information about a target organization by reading Web pages produced by that organization
- Network enumeration is the process of identifying domain names and other resources on the target network
Summary (continued)

- DNS-based reconnaissance uses information available from DNS servers about the IP addresses of target network domain names.
- Network-based reconnaissance is the process of identifying active computers and services on a target network via tools such as ping, traceroute, and netstat.