4.2. Foot printing and Reconnaissance

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.

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.

Passive and Active Reconnaissance

Passive reconnaissance involves gathering information about a potential target without the targeted individual's or company's knowledge. Passive reconnaissance can be as simple as watching a building to identify what time employees enter the building and when they leave. However, most reconnaissance is done sitting in front of a computer.

When hackers are looking for information on a potential target, they commonly run an Internet search on an individual or company to gain information.

Sniffing the network is another means of passive reconnaissance and can yield useful information such as IP address ranges, naming conventions, hidden servers or networks, and other available services on the system or network. Sniffing network traffic is similar to building

monitoring: a hacker watches the flow of data to see what time certain transactions take place and where the traffic is going. Sniffing network traffic is a common hook for many ethical hackers. Once they use some of the hacking tools and are able to see all the data that is transmitted in the clear over the communication networks, they are eager to learn and see more.

Sniffing tools are simple and easy to use and yield a great deal of valuable information. Many times this includes usernames and passwords and other sensitive data. This is usually quite an eye-opening experience for many network administrators and security professionals and leads to serious security concerns.

Active reconnaissance involves probing the network to discover individual hosts, IP addresses, and services on the network. This process involves more risk of detection than passive reconnaissance and is sometimes called rattling the doorknobs. Active reconnaissance can give a hacker an indication of security measures in place, but the process also increases the chance of being caught or at least raising suspicion. Many software tools that perform active reconnaissance can be traced back to the computer that is running the tools, thus increasing the chance of detection for the hacker.

Both passive and active reconnaissance can lead to the discovery of useful information to use in an attack. For example, it's usually easy to find the type of web server and the operating system (OS) version number that a company is using. This information may enable a hacker to find a vulnerability in that OS version and exploit the vulnerability to gain more access.