13.1 Hacking Preparation

Skilled hackers rarely start an attack for no reason. They first want to gather information about the target before attacking. This is similar to a skilled bank robber first casing the bank to learn all he can before actually trying to rob it. A skilled hacker wants to understand everything he can about the target organisation and its system. This preparation phase is important. It is also a reason why a security-conscious organisation should be very careful about what information is allowed in public.

13.1.1 Passive Information Gathering

The first step in any computer attack is a passive search. This is any attempt to gather information that does not actually involve connecting to the target system. If the target system has firewall logs, an intrusion detection system (IDS), or similar capabilities, then an active scan might alert the company. The first step is to simply search the web for the organisation in question.

You might discover that it has an announcement stating a move to a new router model, or that it uses IIS 7.0 for its web server. Any information about the target system enables the attacker to narrow his search for vulnerabilities. In the second example, the hacker can now simply search for “security flaws in IIS 7.0” or in another similar search term.

The possibility that the attacker will learn about people in the organisation also exists. Knowing actual names, phone numbers, office locations and other information can aid in a social engineering attack. The more information one has on a target organisation, the easier the attack will be.

Several websites can help with this. Websites such as www.netcraft.com, www.shodan.io and www.censys.io can provide information about a target web server or what ports are open on the public IP address of the organisation in question.

13.1.2 Active Scanning

Although passive scanning can yield a lot of useful information, at some point the attacker needs to complete an active scan, which

involves some level of actual connection to the target system. It is the most likely to be detected, but also the most likely to yield actionable information. Several types of active scanning exist:

- **Port scanning:** This is a process of scanning the 1024 well-known ports or even all the ports (there are 65,535) to see which ports are open. This can tell an attacker a great deal of information. For example, port 161 indicates the target is using Simple Network Management Protocol, which might provide a vulnerability that can be exploited. Port 88 tells an attacker that the target system uses Kerberos authentication.
- **Enumeration:** This is a process whereby the attacker tries to find out what is on the target network. Items such as shared folders, user accounts, and similar items are sought after. Any of these can provide a point of attack.
- **Vulnerability assessment:** This is the use of a tool which seeks out known vulnerabilities. The attacker might also try to manually assess vulnerabilities. The latter can be done in many ways.

A number of tools are freely available on the Internet for active scanning. They range from the very simple to the complex. Anyone involved in preventing computer crimes or investigating computer crimes should be familiar with a few of these.

When you are doing a port scan, you have a number of options. The most common types of scans and their limitations are as follow:

- **Ping scan:** This scan sends a ping packet to the target IP address. This is to see if a given port is open. The problem with ping scanning is that many firewalls block ICMP packets. Internet Control Message Protocol (ICMP) is the protocol used by ping and tracert (traceroute for Unix/Linux users).
- **Connect scan:** This type of scan actually tries to make a full connection to the target IP address at a given port. This is the most reliable type of scan. It will not yield false positives or false negatives. However, it is the scan that is most likely to be detected by the target network.
- **SYN scan:** This scan is based on knowledge of how network connectivity works. Any time you connect to any server an exchange of packets negotiates the connection. Your machine sends a packet with a SYN flag, which means synchronize.

Basically, you are asking permission to connect. The server responds with a packet that has a SYN-ACK flag, a synchronize-acknowledgment.

That is the server saying “ok, you can connect.” Your computer then sends a packet with an ACK flag, acknowledging the new connection. A SYN scan simply sends a connection request to each port. This is to check to see whether the port is open. As servers and firewalls routinely get SYN packets, this is unlikely to trigger any alarms on the target system.

- **FIN scan:** This scan has the FIN flag, or the connection finished flag, set. This also will not usually usually not going to attract unwanted attention at the target network because connections are being closed routinely, so packets with the FIN flag set are not unusual.

Other scans include the Null scan, with no flags set, and the XMAS scan, with several flags set. Whatever the specific scan used, most will leave some trace of the attack in the server or firewall logs.