10.3 Probing the Network

Perhaps the most critical step in assessing any network is to probe the network for vulnerabilities. This means using various utilities to scan your network for vulnerabilities. Some network administrators skip this step. They audit policies, check the firewall logs, check patches etc. However, the probing tools discussed in this section are those used by hackers.

If you would like to find out how vulnerable your network is, one method is to try the same tools that an intruder would use. In this section, we review the common scanning/probing tools. There are essentially three types of probes that are usually carried out. These are the same types of probes that skilled hackers use to evaluate your network:

- **Port scanning:** This process consists of scanning the well-known ports (there are 1024) or even all the ports (there are 65,535) and seeing which ports are open. Knowing what ports are open tells a lot about a system. If you see that 160 and 161 are open, this tells you that the system is using SNMP. From the perspective of a network administrator, there should be no unnecessary points open.
- **Enumeration:** This is a process whereby the attacker tries to find out what is on the target network. Items such as user accounts, shared folders, printers, and so on are sought after. Any of these might provide a point of attack.
- **Vulnerability assessment:** This tool is used to seek out any known vulnerabilities. The attacker might even try to manually assess the system’s vulnerabilities. There are some outstanding tools that are available for vulnerability assessment.

A number of tools are freely available on the Internet for active scanning. They range from simple to more complex. Anyone involved in preventing or investigating computer crimes should be familiar with a few of these. The most famous vulnerability scanners are Nessus, Qualys, Openvas, Netsparker, Acunetix, Nexpose Community, Retina and Core Impact.