5.1.3 Reconnaissance Facts

Reconnaissance is the process of gathering information about an organization. It is a pre-attack phase. There are two types of reconnaissance:

Type	Description

Organizational	*Organizational reconnaissance* is researching a company in order to find critical details. This information could include facts such as business relationships; the function, size and profitability of the company; contact information; and system infrastructure. From this, a profile of the organization can be created.
	
	Performing organizational reconnaissance could include:
	
	▪ Gathering information by utilizing internet-based resources such as:
	  ▪ The organization's website
	  ▪ Google searches
	  ▪ WHOIS utility
	  ▪ Dun & Bradstreet
	  ▪ Monster.com
	  ▪ Archive.org
	▪ Making organizational queries by contacting the company to gather information, such as names, phone numbers, email addresses, and points of contact (a person in an organization who coordinates an activity or program within the organization).

Technical	*Technical reconnaissance* is using electronic means to scan systems to collect configuration and security data. Two types of scans are common during technical reconnaissance: ▪ A *horizontal scan* is a scan of an entire network. ▪ A *vertical scan* is a scan of an individual machine, such as a port scan to identify the open ports. Technical reconnaissance uses information gathered during organizational reconnaissance to target computer systems. Examples of technical reconnaissance include: ▪ A registrar query checks with DNS registrars to determine the status of the domain name. ▪ A DNS query uses a tool, such as **nslookup,** to submit name resolution requests to identify DNS name servers and IP addresses for hosts. ▪ Network enumeration is used to identify the devices on a network. **Nmap** is an open source security scanner that is used to create a map of configuration details of a network. ▪ ARP scans identify and associate MAC and IP addresses with live devices on a subnet. ▪ Ping sweeps send ICMP ECHO requests to multiple hosts to determine the IP addresses of computers that are accessible. ▪ Port scanning sends a message to host ports to identify open (available) ports on a network. ▪ Operating system identification, also called footprinting or fingerprinting, can be determined by sending uniquely fashioned packets to a recipient, and then analyzing the response to requests to determine the operating system of the recipient. For example, you can identify the operating system used by examining the format of the response to specific probes or messages. ▪ Tracing the devices in the path between two hosts, using tools such as **traceroute** or **neotrace**. ▪ Tracing email sources. Samspade is freeware used to identify the source of spam emails.

The following table outlines the basic stages of reconnaissance:

Stage	Description
Passive reconnaissance	*Passive reconnaissance* is characterized by gathering data. Passive reconnaissance does not directly affect the target. Examples of this stage include: ▪ Putting a sniffer on the wire. ▪ Eavesdropping on employee conversations. ▪ Dumpster diving. ▪ Browsing the organization's website.
Active scanning	*Active scanning* is coming into contact with the system. Active scanning can include: ▪ Social engineering. ▪ War driving (scanning for wireless access points within the organization). ▪ War dialing (trying to access phone lines that will answer a calling modem). ▪ Banner grabbing (capturing information transmitted by the remote host, including the application type, application version, and even operating system type and version). ▪ Probing the corporate network with scanning tools, often using the same tools used by hackers, such as SATAN and Nessus.

There are various types of scanning:

- A FIN scan sends TCP packets to a device without first going through the normal TCP handshaking, thus preventing non-active TCP sessions from being formally closed.
- A stealth scan sends a single frame to a TCP port without any TCP handshaking or additional packet transfers, with the expectation of receiving a single response.
- A Christmas tree scan sends a TCP frame to a remote device with the URG, PSH, and FIN flags set.
- A null scan turns off all flags in a TCP header, creating a lack of TCP flags that should never occur in the real world.

Scanners can also probe common ports to look for open firewall ports and to identify services running on a target system.

The best countermeasures for preventing reconnaissance on your system are to:

- Install antivirus applications.
- Make sure your system has all of the latest patches and drivers.
- Upgrade your applications as often as possible; the older an application is, the more vulnerabilities it will have.
- Limit the amount of information that could be made available to an attacker.
