5.1.2 Scanning Process Facts

Scanning is the process of actively connecting to a system to get a response and gather information. Through scanning, you can determine live hosts, open ports, operating systems in use, running services or processes, implemented patches, and firewalls.

This lesson covers the following topics:

- Network scans
- TCP scans
- Port scans
- Operating system fingerprinting

Network Scans

Scan Type	Description
Wardialing	Using a modem, the scan dials a large block of phone numbers and attempts to locate other systems connected to a modem. If the modem gets a response, it can establish a connection. Modems are still often used for fax machines and multi-purpose copiers and as a backup for high-speed internet.
ping	ping works by sending an ICMP message from one system to another. Based on the ICMP reply, you know whether the system is live and how quickly the packets travel from one host to another.
ping sweep	A ping sweep scans a range of IPs to look for live systems. ping sweeps help to build a network inventory. However, they can also alert the security system, potentially resulting in an alarm being triggered or the attempt being blocked.

TCP Flags

TCP is a connection-oriented protocol that uses a three-way handshake to establish a connection with a system port. When examining a TCP packet, you'll notice the flag indicators. Two of these indicators are SYN and ACK. SYN starts a connection between two systems. ACK acknowledges that a packet has been received. There are other flag options as well. Any of these indicators can be turned on or off using a packet crafter.

The three-way handshake occurs when you're trying to use TCP to connect to a port. As indicated by the name, the handshake has three steps:

1. Computer 1 sends a SYN packet to Computer 2.
2. Computer 2 receives the packet and sends a SYN/ACK packet to Computer 1.
3. Computer 1 receives the SYN/ACK packet and replies with an ACK packet, and the connection is complete.

The following table describes TCP flags.

Flag	Description
SYN	Starts a connection between hosts.
ACK	Acknowledges the receipt of a packet.
FIN	Indicates that no additional information will be sent.
RST	Resets a connection.
URG	Flags a packet as urgent.
PSH	Directs the sending system to send buffered data.

Port Scans

After you've found a live system, you'll need to find a way in. To do this, you'll perform a port scan.

Scan	Description	Command
Full open scan	The full open scan completes a full three-way handshake on all ports. Open ports respond with a SYN/ACK, and closed ports respond with an RST flag, ending the attempt. The down side of this type of scan and the reason that it's not frequently used is that somebody now knows you were there.	**nmap –sT** ***IP address***
Half-		

open scan	A half-open scan, also known as a stealth scan, sends an SYN packet to a port. The three-way handshake does not occur because the originating system does not reply with the final ACK. At this point, you have discovered an open port. Because an ACK packet was not sent, a connection was not made, and there is no security log.	**nmap –sS** ***IP address***
Xmas tree scan	An Xmas tree scan gets its name because all of the flags are turned on, and the packet is lit up like a Christmas tree. The recipient has no idea what to do with this packet, so either the packet is ignored or dropped. If you get an RST packet, you know the port is closed. If you don't get a response, the port may be open.	**nmap –sX –v** ***IP address***
FIN scan	The packet is sent with the FIN flag set. This allows the packet to pass through firewalls and onto the intended target without attracting much attention. If a port is open, there will be no response. If the port is closed, an RST response is returned.	**nmap –sF** ***IP address***
NULL scan	The packet is sent with no flags set. If the port is open, there is no response. If the ports are closed, an RST response is returned.	**nmap –sN** ***IP address***
Idle scan	The hacker finds a target machine, but wants to avoid getting caught, so, he finds another system to take the blame. The blamed system is called a zombie machine because it's disposable and creates a good distraction. The scan directs all requests through the zombie machine. If that zombie machine is flagged, the hacker simply creates another zombie machine and continues to scan.	

Operating System Fingerprinting

You may be able to figure out which operating system a target is running by reviewing packet information. Fingerprinting relies on small differences in packets created by various operating systems. You can find differences by examining the TTL values, TCP window size, DHCP requests, ICMP requests, HTTP packets, and open port patterns.