Network scanning clear with more examples

Network scanning is the process of identifying hosts and services on a network to gather information about the network topology, identify potential vulnerabilities or misconfigurations, and gather other useful information for an attacker. Here are some examples of network scanning techniques:

1. Ping scanning: This technique involves sending ICMP echo requests (pings) to a range of IP addresses to identify which hosts are online and responsive. For example, using the ping command in Linux:

```
r
```

Copy code

```
ping -c 4 192.168.1.1-254
```

This will send four ICMP echo requests to each IP address in the range 192.168.1.1 to 192.168.1.254, and report which hosts are responding.

2. Port scanning: This technique involves scanning a range of TCP and/or UDP ports on a target host to identify which services are running and potentially vulnerable to attack. There are several tools that can be used for port scanning, including:

   nmap: a popular open-source tool that can perform a variety of scanning techniques, including TCP and UDP port scanning, version detection, and OS detection.
   netcat (nc): a command-line tool that can be used to open and connect to TCP and UDP ports on a target host.
   Zenmap: a graphical user interface for nmap that makes it easier to perform scans and view the results.

For example, using nmap to scan a host for open TCP ports:

Copy code

```
nmap -sS 192.168.1.1
```

This will perform a TCP SYN scan on host 192.168.1.1 to identify which TCP ports are open and accepting connections.

3. Vulnerability scanning: This technique involves using specialized tools to scan hosts and networks for known vulnerabilities, misconfigurations, or other weaknesses that could be exploited by an attacker. There are several commercial and open-source vulnerability scanning tools available, including:

   Nessus: a popular commercial vulnerability scanner that can scan hosts and networks for thousands of known vulnerabilities and misconfigurations.
   OpenVAS: an open-source vulnerability scanner that is based on the Nessus engine.
   Metasploit: a popular open-source penetration testing framework that includes a variety of scanning and exploitation tools.

For example, using Nessus to scan a network for known vulnerabilities:

cpp Copy code

```
nessuscli scan --hosts 192.168.1.0/24 --template "Basic Network Scan"
```

This will perform a basic network scan on all hosts in the 192.168.1.0/24 network range, and identify any known vulnerabilities or misconfigurations that could be exploited by an attacker.

It's important to note that network scanning can be used for both legitimate and malicious purposes, and some of the techniques mentioned above may be illegal or unethical if used without proper authorization. As with all security-related activities, it's important to obtain proper permission before conducting any kind of network scanning or vulnerability scanning.