Scanning Networks clear with more examples

Scanning networks is an important part of information gathering in cybersecurity. It involves identifying hosts and devices on a network and determining their characteristics and vulnerabilities. Here are some additional examples of network scanning techniques:

1. Ping Sweep: Ping Sweep is a network scanning technique used to identify active hosts on a network. It works by sending ICMP echo requests to a range of IP addresses to determine which ones respond. For example, in Linux:

Copy code

```
nmap -sn 192.168.1.0/24
```

This will send ICMP echo requests to all IP addresses in the range 192.168.1.0/24 and identify which ones respond.

2. Port Scanning: Port scanning is a technique used to determine which TCP and UDP ports are open on a target system or network. It can be used to identify potential vulnerabilities and services running on the target system. For example, in Linux:

css Copy code

```
nmap -p 1-65535 192.168.1.1
```

This will scan all TCP and UDP ports on the target system at IP address 192.168.1.1 and identify which ones are open and which services are running.

3. OS Fingerprinting: OS fingerprinting is a technique used to identify the operating system running on a target system or network. It can be used to identify potential vulnerabilities specific to the target operating system. For example, in Linux:

Copy code

```
nmap -O 192.168.1.1
```

This will scan the target system at IP address 192.168.1.1 and attempt to identify the operating system running on it.

4. Banner Grabbing: Banner grabbing is a technique used to identify the specific software and version running on a target system or network. It can be used to identify potential vulnerabilities specific to the software running on the target system. For example, in Linux:

Copy code

```
nmap -sV 192.168.1.1
```

This will scan the target system at IP address 192.168.1.1 and attempt to identify the software and version running on each open port.

5. Network Mapping: Network mapping is a technique used to create a map of the network and identify the relationships between different hosts and devices. It can be used to identify potential vulnerabilities and misconfigurations in the network architecture. For example, using the Linux tool Netcat:

Copy code

```
nc -z -v -n 192.168.1.0/24 1-1000
```

This will scan all IP addresses in the range 192.168.1.0/24 and identify which ports are open on each system.

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.