Port scanning techniques clear with more examples

Port scanning is the process of systematically scanning a network to identify open ports on devices. Port scanners are tools that enable the detection of open ports on a network. There are several techniques used by port scanners to scan networks, including:

1. TCP Connect Scan: This technique is the most basic port scanning technique. It involves trying to connect to each port using a TCP handshake. If the port is open, the handshake will be completed, and the scanner will know that the port is open.

Example command: **`nmap -sT <IP address>`**

2. SYN Scan: This technique involves sending a SYN packet to the target device. If the device responds with a SYN-ACK packet, the scanner knows that the port is open. If the device responds with a RST packet, the scanner knows that the port is closed.

Example command: **`nmap -sS <IP address>`**

3. UDP Scan: This technique involves sending a UDP packet to each port. If the device responds with an ICMP Port Unreachable packet, the scanner knows that the port is closed. If the device does not respond, the scanner assumes that the port is open.

Example command: **`nmap -sU <IP address>`**

4. ACK Scan: This technique involves sending an ACK packet to each port. If the device responds with a RST packet, the scanner knows that the port is closed. If the device does not respond, the scanner assumes that the port is filtered.

Example command: **`nmap -sA <IP address>`**

5. XMAS Scan: This technique involves sending a packet with the FIN, PSH, and URG flags set to each port. If the device responds with a RST packet, the scanner knows that the port is closed. If the device does not respond, the scanner assumes that the port is open or filtered.

Example command: **`nmap -sX <IP address>`**

6. Null Scan: This technique involves sending a packet with no flags set to each port. If the device responds with a RST packet, the scanner knows that the port is closed. If the device does not respond, the scanner assumes that the port is open or filtered.

Example command: `nmap -sN <IP address>`

It is important to note that port scanning can be used for legitimate purposes, such as network troubleshooting or vulnerability assessment, but it can also be used by attackers to identify potential attack vectors on a network. Therefore, it is important to use port scanning tools responsibly and ethically.