1• **What is an open port?**
An open port is a network port that is configured to accept incoming connections. It typically means a service or application is actively listening on that port.

2• **How does Nmap perform a TCP SYN scan?**
Nmap sends a TCP SYN packet to the target port. If the port is open, the target replies with a SYN-ACK. Nmap then sends an RST (reset) instead of completing the handshake, making the scan stealthy and fast.

3• **What risks are associated with open ports?**
Open ports can expose services that may have vulnerabilities. Attackers can exploit these to gain unauthorized access, install malware, or disrupt services.

4• **Explain the difference between TCP and UDP scanning.**

- **TCP Scanning**: Uses connection-oriented protocols and checks for open ports using handshake processes (e.g., SYN scan).
- **UDP Scanning**: Sends UDP packets to ports. If no response or an ICMP "port unreachable" is returned, the scanner deduces port status. It's slower and less reliable due to lack of acknowledgment.

5• **How can open ports be secured?**

- Close unused ports
- Use firewalls to filter access
- Enable intrusion detection systems (IDS)
- Regularly scan for open ports and vulnerabilities
- Apply patches and secure configurations to services

6• **What is a firewall's role regarding ports?**
A firewall controls traffic by allowing or blocking data to specific ports based on rules, thus protecting systems from unauthorized access or attacks.

7• **What is a port scan and why do attackers perform it?**
A port scan is the process of probing a system for open ports. Attackers use it to identify active services, find vulnerabilities, and plan further exploitation.

8• **How does Wireshark complement port scanning?**
Wireshark captures and analyzes network traffic. It helps observe port scanning activity in real-time, verify responses, and detect suspicious scanning patterns or attempts.