**1. What is an open port?**An open port is a network endpoint on a device that’s listening for incoming connections or packets — like a door left partly open. It represents a running service (HTTP, SSH, etc.) that other machines can connect to.

**2. How does Nmap perform a TCP SYN scan?**Nmap’s SYN scan sends a SYN packet (the first step of TCP’s handshake) to a target port and watches the reply: SYN+ACK means open, RST means closed. Because it usually doesn’t finish the handshake, it’s faster and a bit stealthier than a full connect scan.

**3. What risks are associated with open ports?**Open ports expose services that might have unpatched bugs, weak configurations, or default credentials, giving attackers possible entry points. The more ports exposed, the larger your attack surface.

**4. Explain the difference between TCP and UDP scanning.**TCP scanning checks ports by attempting TCP handshakes or probes and relies on clear responses (SYN/ACK, RST). UDP scanning sends datagrams and infers state from replies or silence, which tends to be slower and less reliable because UDP is connectionless.

**5. How can open ports be secured?**Close or disable unnecessary services, keep software patched, enforce strong authentication and access controls, and restrict access with firewall rules or network segmentation. Running services on non-default ports is only a minor obscurity — not real security.

**6. What is a firewall's role regarding ports?**A firewall controls which ports and protocols are allowed in and out of a host or network, acting as a gatekeeper. It blocks unwanted traffic, enforces access policies, and reduces the number of services exposed to untrusted networks.

**7. What is a port scan and why do attackers perform it?**A port scan is an automated probe of a host’s ports to discover which services are running and reachable. Attackers use scans to map a target’s attack surface and find vulnerable services to exploit.

**8. How does Wireshark complement port scanning?**Wireshark captures and inspects actual packet-level traffic so you can see how services communicate, diagnose unexpected responses, and verify what a scanner (or attacker) is doing. It’s excellent for troubleshooting and confirming whether a port is truly open, filtered, or misconfigured.