**1. What is an open port?**  
An open port is a network port on a computer or device that is actively listening for incoming connections or data. It indicates that a particular service (like HTTP on port 80 or SSH on port 22) is running and accepting communication. Open ports are essential for legitimate network operations but can also expose a system to attacks if not properly secured.

**2. How does Nmap perform a TCP SYN scan?**  
In a TCP SYN scan, Nmap sends a SYN (synchronize) packet to the target port — this is the first step in the TCP three-way handshake.

* If the target port replies with a SYN-ACK, the port is open.
* If it responds with an RST (reset), the port is closed.
* If there is no response or an ICMP unreachable message, the port is filtered (likely blocked by a firewall).  
  Nmap then sends an RST packet instead of completing the handshake, making the scan stealthy since it doesn’t fully open a connection.

**3. What risks are associated with open ports?**  
Open ports can expose systems to several risks, including:

* Unauthorized access: Hackers can exploit vulnerabilities in services running on open ports.
* Information leakage: Banner grabbing can reveal software versions.
* Malware infection: Open ports can be used by worms or backdoors.
* Denial-of-Service (DoS): Attackers can flood open ports to overwhelm the service.

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

* TCP Scanning: Establishes (or partially establishes) a connection using the TCP handshake. It’s reliable, and responses are predictable (e.g., SYN-ACK or RST).
* UDP Scanning: Sends UDP packets to target ports. If the port is closed, an ICMP “Port Unreachable” message is returned; if it’s open, there may be no response, making UDP scanning slower and less reliable but useful for discovering services like DNS or SNMP.

**5. How can open ports be secured?**

* Close unused ports and disable unnecessary services.
* Use firewalls to filter and restrict inbound/outbound traffic.
* Implement intrusion detection systems (IDS) to monitor suspicious activity.
* Regularly scan the network using tools like Nmap to identify new open ports.
* Apply patches and updates to fix known vulnerabilities.

**6. What is a firewall's role regarding ports?**  
A firewall controls network traffic based on predefined security rules. It can allow, block, or filter connections to specific ports:

* Inbound rules manage which external systems can connect.
* Outbound rules control what internal applications can access outside networks.  
  Thus, a firewall helps protect systems by preventing unauthorized access to open ports.

**7. What is a port scan and why do attackers perform it?**A port scan is the process of systematically sending packets to various ports on a host to identify which ones are open, closed, or filtered.  
Attackers perform port scans to:

* Discover open ports and running services.
* Identify potential vulnerabilities for exploitation.
* Map the network and gather intelligence for future attacks.

**8. How does Wireshark complement port scanning?**  
Wireshark is a network protocol analyzer that captures and displays network traffic in real-time. It complements port scanning by:

* Verifying scan results from tools like Nmap.
* Analyzing TCP handshakes and packet responses during scans.
* Detecting anomalies or intrusion attempts.
* Helping security analysts understand packet behavior to fine-tune network defenses.