1. **What is an open port?**
   An **open port** is a network port on a computer or device that is actively accepting connections or data. It typically means a service or application is listening on that port, ready to communicate over the network (e.g., a web server on port 80).

2. **How does Nmap perform a TCP SYN scan?**
   Nmap's **TCP SYN scan** (also called a "half-open" scan) works by sending a TCP SYN packet (the first step of the TCP handshake) to a target port.

   - If the port responds with a SYN-ACK, it means the port is open.
   - Nmap then sends a RST (reset) packet to avoid completing the handshake, thus remaining stealthy.
   - If the port responds with a RST, the port is closed.
   - If there is no response or an ICMP unreachable message, the port is filtered (blocked by a firewall).

3. **What risks are associated with open ports?**
   Open ports can pose several security risks:

   - They can expose services that might have vulnerabilities, allowing attackers to exploit them.
   - Attackers can use open ports as entry points for unauthorized access or launching attacks like denial of service (DoS).
   - Open ports may reveal information about the system or network, aiding reconnaissance.
   - Malware and worms often scan for open ports to propagate.

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

   - **TCP scanning:** Probes TCP ports by initiating TCP connections or sending TCP control packets. It relies on the TCP handshake or responses (SYN-ACK, RST) to determine port state. TCP scanning is more reliable due to connection-oriented nature.
   - **UDP scanning:** Sends UDP packets to target ports and analyzes responses. If a port sends back an ICMP “port unreachable” message, it is closed. If no response, the port may be open or filtered. UDP scanning is slower and less reliable due to the stateless nature of UDP and less explicit responses.

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

- **Close unnecessary ports** by disabling unused services.
- Use **firewalls** to restrict access to ports based on trusted IPs or networks.
- Apply **patches and updates** regularly to fix vulnerabilities in services.
- Use **intrusion detection/prevention systems** to monitor port activity.
- Employ **strong authentication and encryption** for services accessible via open ports.
- Use **port knocking** or **VPNs** to hide or restrict port access.

6. **What is a firewall's role regarding ports?**

A **firewall** controls and filters network traffic to and from ports based on predefined security rules. It can block or allow traffic on specific ports, effectively controlling which ports are exposed to external or internal networks. Firewalls help prevent unauthorized access through open ports.

7. **What is a port scan and why do attackers perform it?**

A **port scan** is a technique used to discover open ports and services running on a target system by sending packets and analyzing responses.
Attackers perform port scans to identify potential entry points or vulnerabilities to exploit. It's a common reconnaissance step before launching attacks.

8. **How does Wireshark complement port scanning?**

Wireshark is a **network protocol analyzer** that captures and inspects network traffic in detail. It complements port scanning by:

- Allowing analysts to **observe actual packet exchanges** during scans.
- Helping to **detect anomalies or suspicious traffic** related to scanning activity.
- Providing insight into the behavior of services running on open ports.
- Assisting in troubleshooting and verifying firewall and network configurations after scanning.