1. What is an open port?

An **open port** is a network port that is actively listening for incoming connections. It indicates that a service or application is running and reachable on that port. Open ports can be accessed over a network and may allow data transfer or communication, depending on the service.

2. How does Nmap perform a TCP SYN scan?

In a **TCP SYN scan** (nmap -sS), Nmap sends a **SYN packet** to the target port. Based on the response:

- **SYN-ACK** → The port is **open**.
- **RST** → The port is **closed**.
- **No response or filtered** → The port is **filtered or blocked**.

Nmap then sends a **RST** to tear down the connection, so the full TCP handshake is never completed—this makes it a **stealthy** scan.

A **TCP SYN scan** (also called a **"half-open" scan**) only does **part** of the handshake:

1. Nmap sends a **SYN** packet.
2. If the port is **open**, the target replies with a **SYN-ACK**.
3. **Instead of completing the handshake**, Nmap immediately sends a **RST (Reset)** packet.

✅ This **RST cancels the connection** before it's fully established

Why This Is Called a "Stealth" Scan

- It **doesn't complete** the full handshake (no ACK sent).
- That makes it **less likely to be logged or noticed** by the server or its logging systems.
- It's **faster and less intrusive**, which is great for recon

3. What risks are associated with open ports?

- **Exposure to vulnerabilities**: Services listening on open ports may have known exploits.
- **Brute-force attacks**: Open ports on services like SSH or RDP can be targeted.
- **Information leakage**: Misconfigured services may reveal sensitive information.
- **Backdoors**: Malware can use open ports for remote access.

4. Explain the difference between TCP and UDP scanning.

- **TCP Scanning**:
  - Relies on the 3-way handshake.
  - More reliable and easier to detect.
  - Can confirm if ports are open/closed.
- **UDP Scanning**:
  - Connectionless; sends a UDP packet.

  - If no response: the port might be open or filtered.
  - If ICMP Port Unreachable is received: the port is closed.
  - Less reliable, slower, and harder to detect accurately

- **First, Compare to TCP (Connection-Oriented):**
- With **TCP**, before any data is exchanged, a **connection must be established** using the 3-way handshake (SYN, SYN-ACK, ACK). This is called **connection-oriented** communication.
- ✅ TCP checks if the other side is ready and ensures the data arrives correctly and in order.

UDP Is Different — It's "Connectionless":

- When you use **UDP** (User Datagram Protocol):
- It just **sends the data** — no handshake, no setup.
- The sender **doesn't check if the receiver is ready**.
- The receiver may or may not respond.
- No guarantee the packet will arrive or arrive in order.
- ✅ This makes UDP **faster**, but **less reliable** than TCP.

5. How can open ports be secured?

- **Close unused ports**.
- **Use firewalls** to restrict access by IP or protocol.
- **Implement intrusion detection/prevention systems (IDS/IPS)**.
- **Regularly update and patch services**.
- **Use port-knocking or VPNs** to hide services.
- **Apply least privilege principles** to limit exposure.

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

A **firewall** controls network traffic by **allowing or blocking** connections based on rules. It:

- Blocks **unwanted or unauthorized ports**.
- Limits access to **specific IPs or applications**.
- Can detect and prevent **port scanning** attempts.
- Acts as a first layer of defense to protect open ports.

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

A **port scan** is a method to find **which ports are open**, closed, or filtered.

Attackers use port scans to:

- Identify **potential entry points**.
- Map the **network and services**.
- Prepare for **targeted attacks or exploits**.
- Test for **vulnerabilities** in exposed services.

8. How does Wireshark complement port scanning?

Wireshark captures and analyzes network traffic, helping you:

- See **packets generated by Nmap** scans.
- Verify **responses** from scanned ports.
- Detect if scans are being **blocked or dropped**.
- Understand **network behavior** during scanning.

It’s a great tool for **learning how scans work** and **validating scan results** at the packet level.