Interview Questions

1. What is an open port?

An **open port** is a network port on a device that is actively accepting connections or data. It means a service or application is listening for inbound traffic on that port.

🛡️ **Example**: If port 80 is open, the system is likely running a web server (HTTP).

2. How does Nmap perform a TCP SYN scan?

Nmap uses the **TCP SYN scan (`-sS`)** to send a SYN packet to a target port:

- If it receives a **SYN-ACK**, the port is **open**.
- If it gets a **RST**, the port is **closed**.
- If there's **no response** or it's filtered (e.g., by a firewall), it's marked as **filtered**.

💡 It doesn't complete the full TCP handshake, making it **stealthier and faster**.

3. What risks are associated with open ports?

Open ports can expose services that:

- Are **vulnerable** to known exploits (e.g., outdated software).
- Can be **brute-forced** (e.g., SSH with weak credentials).
- May **leak sensitive information** (e.g., NetBIOS).
- Provide **remote access** (e.g., RDP, Telnet) that attackers can exploit.

🚨 **Every open port increases the attack surface.**

4. Explain the difference between TCP and UDP scanning.

Feature	TCP Scan	UDP Scan
Protocol	Connection-oriented	Connectionless

Feature	TCP Scan	UDP Scan
Reliability	More reliable (ACK/RST)	Less reliable (no response = ambiguity)
Scan method	Uses SYN/ACK/RST	Sends empty UDP packets
Common ports	22 (SSH), 80 (HTTP), 443 (HTTPS)	53 (DNS), 161 (SNMP), 123 (NTP)
Detection	Easier to detect	Harder to detect, slower

UDP scanning is **slower and more ambiguous**, but important for identifying non-TCP services.

---

5. How can open ports be secured?

- **Close unused ports** and disable unnecessary services.
- Use **firewalls** to restrict access.
- Implement **access control lists (ACLs)**.
- Use **strong authentication** and encryption (e.g., SSH keys).
- Regularly **patch and update** services.
- Employ **intrusion detection systems (IDS)** to monitor port activity.

---

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

A **firewall** acts as a gatekeeper that **controls traffic to/from ports** based on rules.

- **Blocks or allows** ports based on security policies.
- Can **filter based on IP, port, or protocol**.
- Helps prevent **unauthorized access** and **port scans**.

✅ It's a key defense mechanism for reducing network exposure.

---

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

A **port scan** is a technique to **probe a system for open ports** to discover:

- **Running services**
- **Potential vulnerabilities**
- **System fingerprinting**

🔓 **Why attackers use it**:

- To **map the attack surface** before exploitation.
- To identify **default or misconfigured services**.
- As part of the **reconnaissance phase** in cyberattacks.

---

8. How does Wireshark complement port scanning?

Wireshark is a packet sniffer that captures and analyzes traffic during or after a scan.

✅ It helps:

- **Visualize the scan** (e.g., SYN packets from Nmap).
- Detect **responses** (e.g., SYN-ACK or RST).
- Spot **anomalies or scan attempts** on your network.
- Understand **protocol behavior** in depth.

It's ideal for **real-time traffic analysis** during scans and **incident investigation**.
