Interview Questions & Answers – Network Port Scanning

1. What is an open port?

An **open port** is a communication endpoint on a device or server that actively accepts incoming network connections. Each port is tied to a specific service or application (e.g., Port 80 for HTTP, Port 3389 for RDP).

- **Why it matters:** Open ports indicate that a service is available, which can be useful for legitimate network operations but also provides potential entry points for attackers.
- **Example:** A web server on Port 80 is open so users can connect, but it could also be exploited if there's a vulnerability in the web application.

2. How does Nmap perform a TCP SYN scan?

A **TCP SYN scan** (also known as a "half-open scan") works by sending specially crafted TCP packets:

- **Step 1:** Nmap sends a **SYN** packet to the target port (the first step of a TCP handshake).
- **Step 2:** If the port is **open**, the target replies with a **SYN-ACK** (synchronization acknowledgment).
- **Step 3:** Instead of completing the handshake, Nmap sends a **RST** (reset) packet, leaving the connection half-open.
- **Why it's used:**
    - Faster than a full connection scan.
    - Less likely to be logged by intrusion detection systems.
    - Provides quick and stealthy detection of open ports.

3. What risks are associated with open ports?

Open ports expose services that may be **vulnerable or misconfigured**, which attackers can exploit.

Risks include:

- **Unauthorized access:** Attackers can brute-force login credentials (e.g., FTP, RDP).
- **Exploitation of vulnerabilities:** Services running on open ports may have known security flaws.
- **Information disclosure:** Banner grabbing can reveal system information (e.g., software version).
- **DDoS attacks:** Open ports can be abused for amplification or flooding attacks.

Real-world example: The WannaCry ransomware exploited open SMB ports (Port 445) on unpatched systems.

4. Explain the difference between TCP and UDP scanning.

- **TCP Scanning:**
  - Relies on connection-oriented communication.
  - Provides **reliable results** (SYN, ACK responses clearly indicate status).
  - Easier to detect because it involves handshakes.
- **UDP Scanning:**
  - Connectionless protocol — no handshake.
  - Often **slower** and **less reliable** (many services don't respond if ports are closed).
  - Harder for firewalls and IDS to detect, but prone to false negatives.

Use cases:

- TCP is used for precise scanning of critical services.
- UDP is used for discovering less visible services (e.g., DNS on port 53, SNMP on port 161).

5. How can open ports be secured?

Best practices:

1. **Close unused ports** – Disable services you don't need.
2. **Use firewalls** – Allow only trusted IPs and block unauthorized access.
3. **Implement authentication & encryption** – Use SSH instead of Telnet, HTTPS instead of HTTP.
4. **Patch and update regularly** – Fix vulnerabilities in exposed services.
5. **Network segmentation** – Place critical services behind secure internal networks.
6. **Port knocking or VPNs** – Hide sensitive services behind additional authentication layers.

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

A **firewall** monitors and filters network traffic based on rules.

Functions related to ports:

- **Allow/block traffic:** Decide which ports are open to which IPs.
- **Prevent unauthorized access:** Block suspicious or malicious connections.
- **Log activity:** Record attempts to connect to restricted ports.

Example: A firewall may block all RDP (3389) connections except from specific IP addresses.

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

A **port scan** is a technique used to discover open ports and running services on a device or network.

Why attackers do it:

- **Reconnaissance:** Gather information about the network to plan attacks.
- **Vulnerability detection:** Identify outdated or weakly configured services.
- **Mapping the network:** Determine the security posture and available entry points.

Example: An attacker might scan for SSH (port 22) to find systems with weak credentials for brute-forcing.

8. How does Wireshark complement port scanning?

Wireshark is a network protocol analyzer that captures and inspects packets in real time.

How it helps with port scanning:

- **Visualizes Nmap traffic:** See SYN, SYN-ACK, and RST packets in detail.
- **Detects anomalies:** Identify unexpected responses or hidden services.
- **Debugging scans:** Understand why certain ports are filtered or unresponsive.
- **Security analysis:** Examine if scans trigger IDS/IPS responses.

Example: If a SYN scan shows no response, Wireshark can confirm whether the packets were dropped by a firewall.