Cyber Security Internship - Interview Questions & Answers

1. What is an open port?

An open port is a network port that is configured to accept incoming connections. It means a service is actively listening for communication. While open ports are necessary for legitimate services (like a web server on port 80), they can also expose a system to potential security threats if left unprotected.

2. How does Nmap perform a TCP SYN scan?

Nmap performs a TCP SYN scan (also known as a half-open scan) by sending a SYN packet to the target port:

- If the port responds with SYN-ACK, it's open.
- If it responds with RST, it's closed.
- If there's no response or it's filtered, the port is likely filtered by a firewall.

This method is stealthy because it doesn't complete the TCP handshake, making it less likely to be logged.

3. What risks are associated with open ports?

Open ports can expose:

- Unpatched services to exploitation.
- Sensitive data to unauthorized access.
- Remote code execution vulnerabilities.
- Brute-force attacks (e.g., on SSH or FTP).

If unused ports are left open, they become attack vectors for hackers.

4. Explain the difference between TCP and UDP scanning.

TCP Scan:

- Uses connection-oriented protocol.
- Responds with SYN/ACK or RST.

- More reliable.

UDP Scan:

- Uses connectionless protocol.

- Usually gives no response or ICMP errors.

- Harder to detect but less reliable.

5. How can open ports be secured?

- Close unused ports using firewall rules.

- Use port knocking to make ports invisible.

- Enable strong authentication for exposed services.

- Apply patches and updates to services.

- Restrict access using IP whitelisting.

- Use intrusion detection systems (IDS) to monitor port activity.

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

A firewall monitors and controls incoming and outgoing network traffic based on predetermined rules. Regarding ports, it can:

- Allow or block traffic to specific ports.

- Detect unauthorized access attempts.

- Log and alert about suspicious port activity.

It's a key component in reducing the attack surface of a network.

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

A port scan is the process of systematically checking a target's ports to find which are open, closed, or filtered. Attackers perform port scans to:

- Identify vulnerable services.

- Map the network environment.

- Discover entry points for attacks.

- Gather intel before launching an exploit.

8. How does Wireshark complement port scanning?

Wireshark is a packet analyzer. It complements port scanning by:

- Showing detailed packet exchanges during a scan.

- Helping identify SYN, SYN-ACK, RST packets.

- Detecting firewall filtering behavior.

- Allowing inspection of protocol-level responses.

It helps verify if a scan was blocked or successful and aids in deep network diagnostics.