Interview Questions & Answers - Task 1 (Nmap Port Scanning)

1. What is an open port?

An open port is a network port that is configured to accept incoming connections. It indicates a service or application is actively listening and can be accessed remotely.

2. How does Nmap perform a TCP SYN scan?

Nmap sends a SYN (synchronize) packet to the target port. If it receives a SYN-ACK response, the port is open. If it gets an RST (reset), the port is closed. It doesn't complete the full TCP handshake, making it fast and stealthy.

3. What risks are associated with open ports?

Open ports may expose vulnerable services to attackers. If not properly secured, they can be exploited to gain unauthorized access, run exploits, or gather sensitive information.

4. Explain the difference between TCP and UDP scanning.

TCP Scan: Uses connection-based protocol; more reliable; responses indicate port status.

UDP Scan: Connectionless; harder to detect responses; more stealthy but slower and less accurate.

5. How can open ports be secured?

Use firewalls to block unused ports

Disable unnecessary services

Use strong authentication

Apply regular updates and patches

Monitor network traffic

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

A firewall filters incoming and outgoing traffic based on rules. It can block or allow traffic on specific ports, helping to prevent unauthorized access and protect the system.

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

A port scan is the process of sending packets to ports on a host to find which ones are open. Attackers use it to discover services that may be vulnerable and exploitable.

8. How does Wireshark complement port scanning?

Wireshark captures and analyzes network packets in real time. It helps observe how devices respond during scans, making it useful for understanding traffic patterns and detecting suspicious behavior.