Interview Questions (task1)

1. **What is an open port?**
   An open port is a network port that is actively accepting connections. It indicates that a service is running and reachable, making it a potential entry point for communication—or attack.

2. **How does Nmap perform a TCP SYN scan?**
   Nmap sends a SYN packet to a target port and waits for a response. If it receives a SYN-ACK, the port is open; it then sends a RST to avoid a full connection—this is why it's called a "half-open" scan.

3. **What risks are associated with open ports?**
   Open ports can expose services that may be vulnerable or misconfigured. Attackers can exploit these to gain unauthorized access or gather sensitive information.

4. **Explain the difference between TCP and UDP scanning.**
   TCP scanning involves establishing or simulating a connection, while UDP scanning sends datagrams and relies on the lack of response or ICMP errors to infer port status. TCP is more reliable; UDP is stealthier.

5. **How can open ports be secured?**
   By closing unused ports, using firewalls to restrict access, and regularly scanning and auditing network services. Service hardening also helps reduce exposure.

6. **What is a firewall's role regarding ports?**
   A firewall monitors and controls incoming and outgoing traffic based on rules. It can block or allow access to specific ports, preventing unauthorized connections.

7. **What is a port scan and why do attackers perform it?**
   A port scan probes a host to find open ports and active services. Attackers use it during reconnaissance to identify vulnerabilities and plan further exploitation.

8. **How does Wireshark complement port scanning?**
   Wireshark captures and analyzes packets on the network. It helps validate scan results, detect scanning behavior, and understand how services respond to probes.