Elevate Labs Cybersecurity Internship

Task 1: Scan your Local Network for Open Ports

Interview Questions:

1.What is an open port?
Ans: An open port is a logical connection point on a device that is configured to accept incoming network traffic. Its a channel for communication that allows a computer to receive data from other devices on a network or the internet.

2.How does Nmap perform a TCP SYN scan?
Ans: Nmap performs a TCP SYN scan by sending a SYN(synchronise) packet to the target port. If the port is open, the target will respond with a SYN/ACK(synchronise/acknowledge) packet. If the port is closed, the target will respond with RST(reset) packet. The type of scan is also known as a "half-open" scan because a full TCP connection is never established, which makes it faster and stealthier than a full TCP connection scan.

3.What risks are associated with open ports?
Ans: The risks associated with open ports include potential security vulnerabilities. An open port can be exploited by attackers to gain unauthorised access to a system, exfiltrate data, or disrupt services. For example, a web server with an open port might have a vulnerability that an attacker can exploit to inject malicious code.

4.Explain the difference between TCP and UDP scanning.
Ans: TCP scanning: This scan attempts to complete the full TCP three-way handshake is complete, the port is open. It's less stealthy than a SYN scan because it creates a full connection.

UDP scanning: This scan sends a UDP packet to the target port. UDP is a connectionless protocol, so it doesn't send a response if the port is open. If the port is closed, the target system usually sends an ICMP "port unreachable" error message. The absence of a response typically means the port is opened or filtered

5.How can open ports be secured?
Ans: Open ports can be secured by implementing firewall rules to restrict access, using strong authentication, and regularly patching and updating the software that uses those ports to fix vulnerabilities. You should only keep ports open for services that are absolutely necessary.

6.What is a firewall's role regarding ports?
Ans: firewall acts as a network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules. Its role regarding ports is to protect a network from unauthorized access by blocking or filtering specific ports. A firewall can be configured to allow only trusted traffic and block traffic from suspicious sources

7.What is a port scan and why do attackers perform it?
Ans: port scan is a method of probing a server or host for open ports. Attackers perform port scans as a reconnaissance technique to identify active hosts and discover which services are running on a target network. This information is used to find potential entry points and vulnerabilities to exploit.

8.How does Wireshark complement port scanning?
Ans: Wireshark is a packet analyzer that captures and displays network traffic. It complements port scanning by allowing a user to analyze the raw packets exchanged during a scan. This helps to understand how the scan is being performed and can be used to troubleshoot network issues or detect unauthorized scan activity