Cyber security internship

TASK:1

Interview questions:

1.What is an open port?

->It is like a door in a computer devices or network devices to get data or leave the network like that.Each port corresponds to a specific service or application.

If the port is open, it means our computer is ready to receive data or connections through that port.

2.How does Nmap perform a TCP SYN scan?

→ **Target:** sends a SYN packet to the target IP by the scanner.

→ **SYN-ACK** → target *is listening* (port is **open**).

Nmap then sends a **RST** to abort the handshake (so the connection is never completed).

RST → target is *not listening* (port is **closed**).

No reply (or ICMP port unreachable / filtered error) → Nmap marks the port **filtered** (firewall or packet filter dropped the probe).

Then nmap records the results whether it is open or closed or filtered.

3.What risks are associated with open ports?

→ Unauthorized Access,Information Leakage,Denial of Service (DoS) Attacks,Malware Communication,Pivoting Inside the Network

4.Explain the difference between TCP and UDP scanning?

→ **TCP scanning** is faster, more reliable, and used for services that need connections.
→ **UDP scanning** is slower and harder to analyze but necessary to find UDP-based services that don't use TCP.

5.How can open ports be secured?

→ Close Unnecessary Ports,Use Firewalls,Use Encryption while transporting the message,Monitor Traffic.

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

→ It is like a security gaurd infront of the house or apartments. Main job regarding to the port is block unwanted access and allows only necessary traffic through it . And also it monitors

the traffic .

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

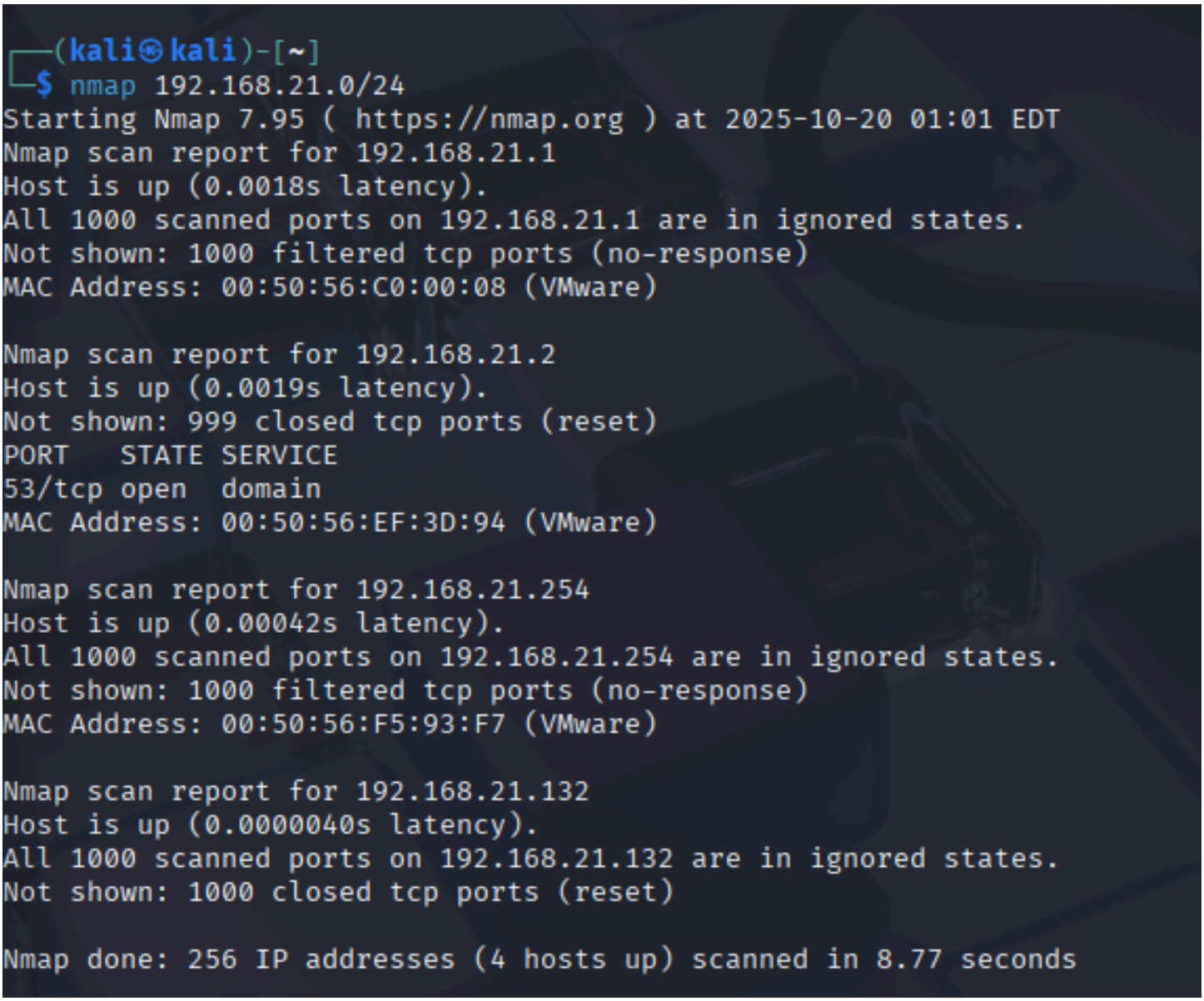
→ It is process where the computer or attacker checks a target system to see which ports are open or closed. Each port respond to a service like ftp,ssh,dns etc.

→ If the attacker want to perfrom this he/she wants to find which ports are open to plan a attack on their system or their assets. Main aim of those attckers are steal the information .

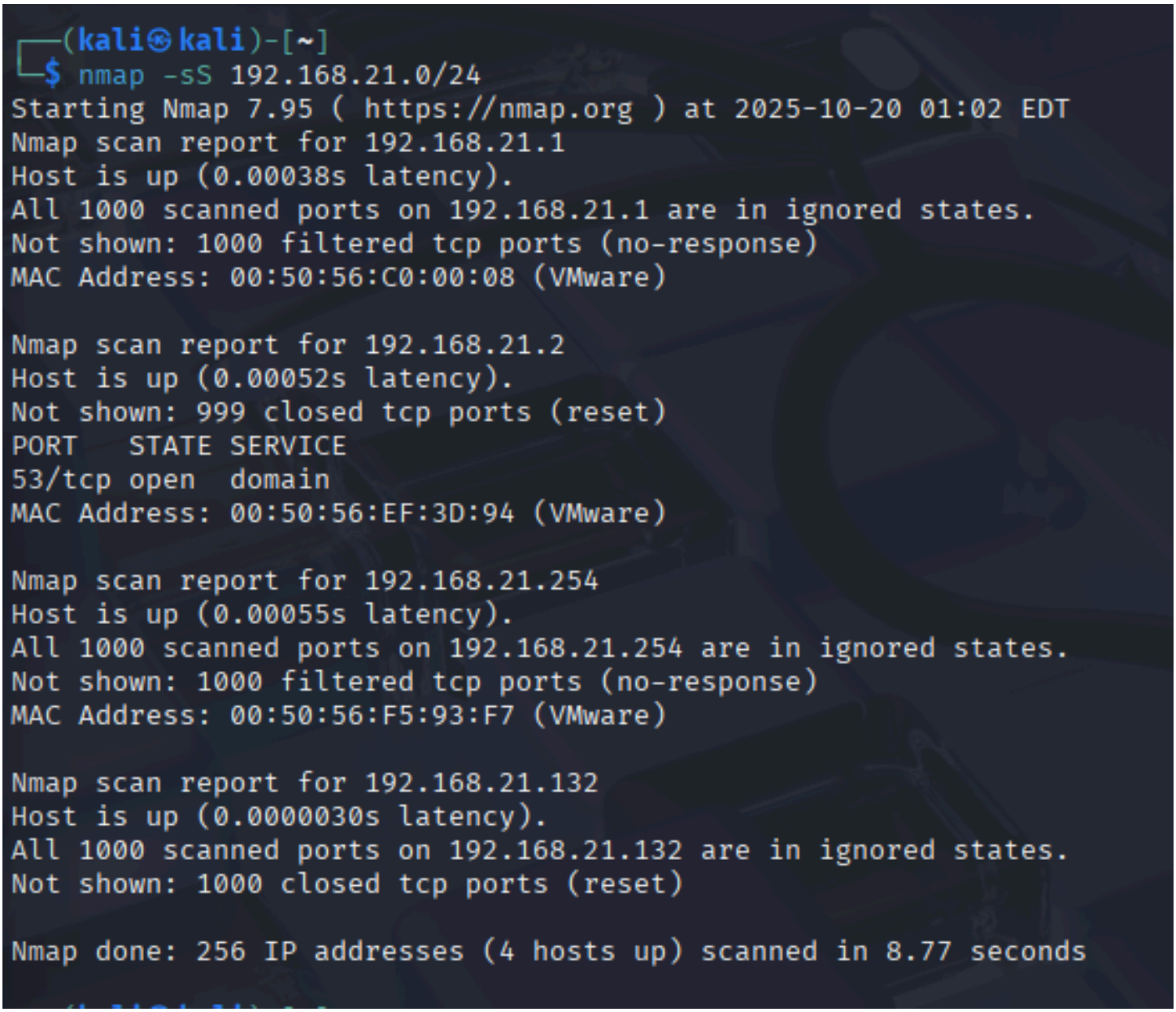
8.How does Wireshark complement port scanning?

→ Wireshark complements port scanning by letting us see the actual network packets sent and received during a scan.
While tools like Nmap show which ports are open or closed, Wireshark helps us verify and understand how those results happen by capturing SYN, ACK, or ICMP packets.
→ It helps in analyzing, troubleshooting, and confirming the behavior of ports and network traffic during scanning.

2.Find your local IP range (e.g., 192.168.1.0/24)



.Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan.



Note down IP addresses and open ports found.

open port 192.168.21.2 → 53/tcp