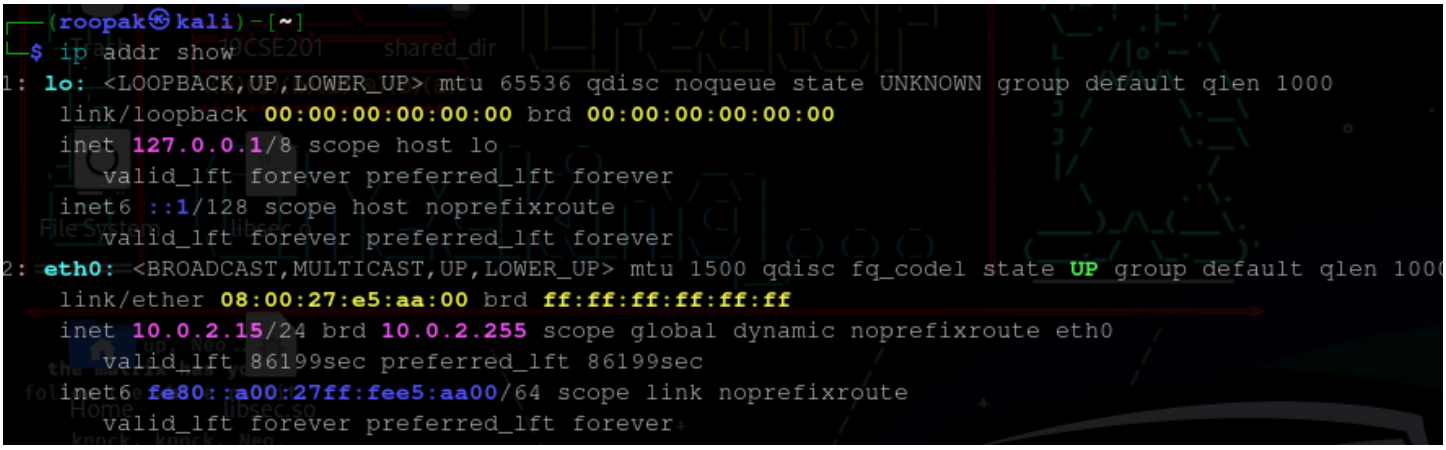
Task-1

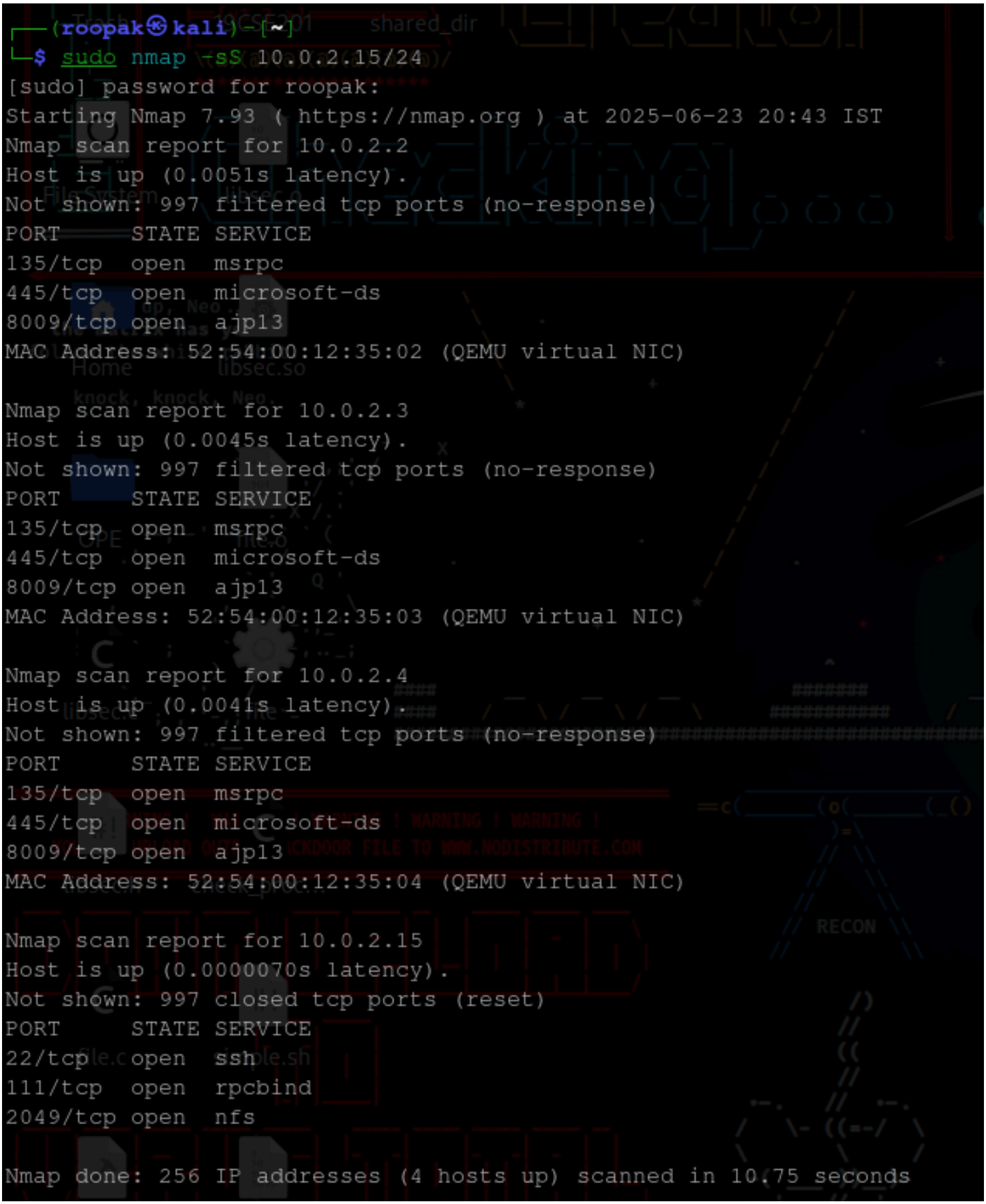
DT:-23/06/2025

checking my IP address using 'ip addr show' command in Linux



Found out my IP address is 10.0.2.15/24

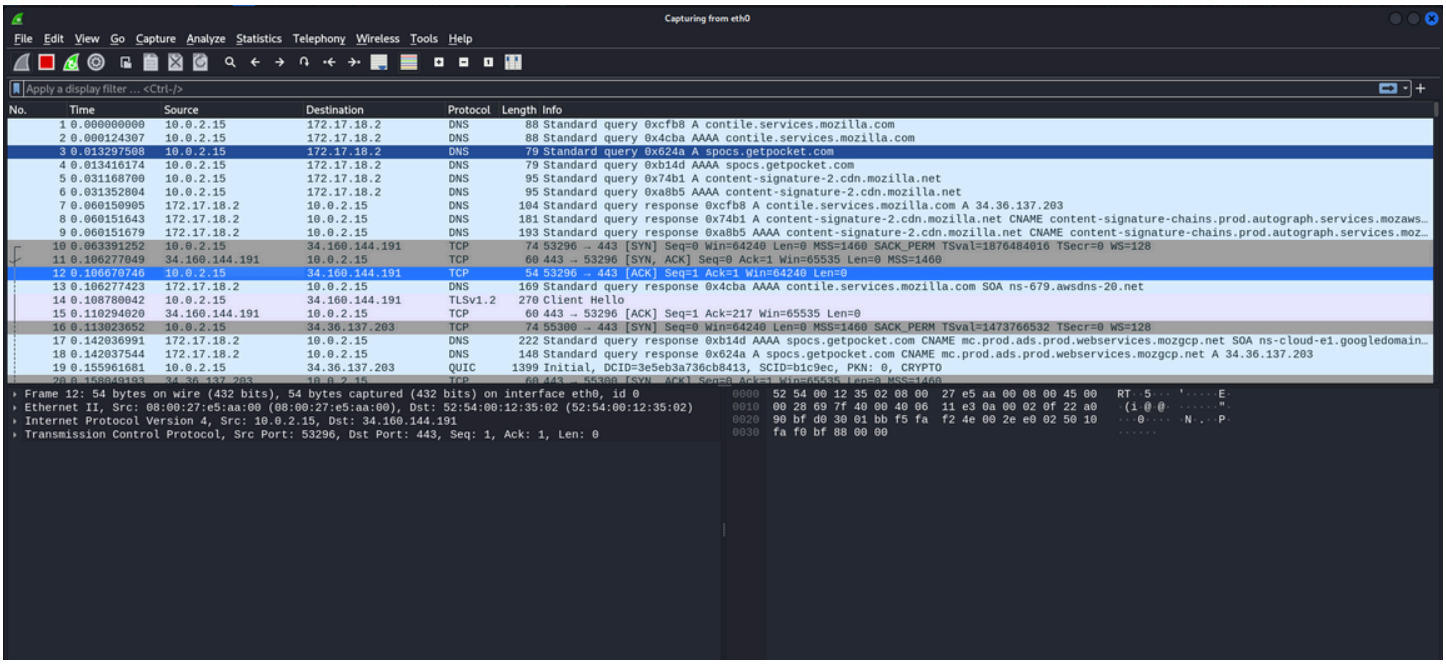
now using this i did port scan using the nmap tool and the command used is sudo nmap -sS 10.0.2.15/24

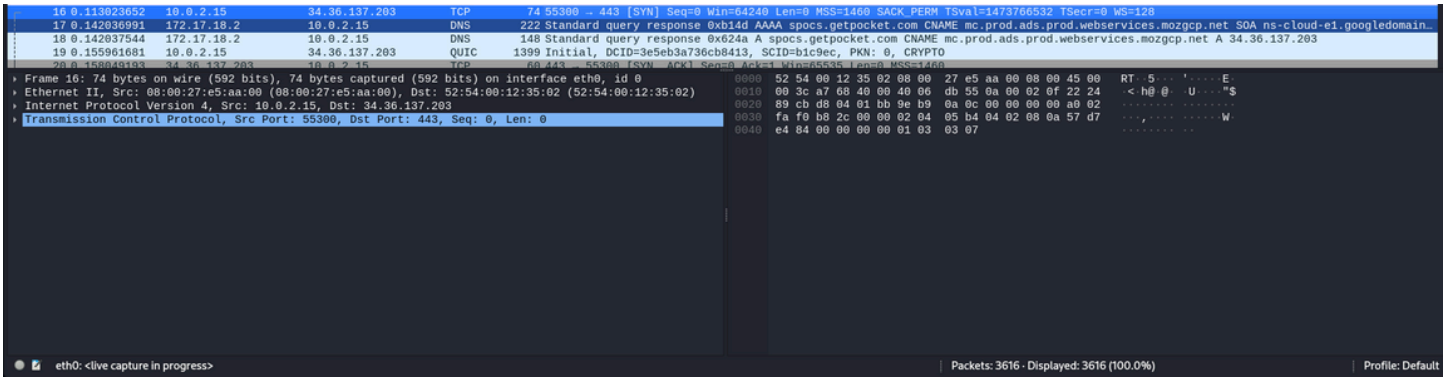


the above command shows the open ports available in the subnet from 10.0.2.0 - 10.0.2.255

the IPs 10.0.2.2,10.0.2.3,10.0.2.4,10.0.2.15

5)Capturing packets using wireshark





In above image packet details such as source port destination port protocol used can be seen even the IPs of source and destination also can be seen

Total of 3615 packets have been captured until i stopped

6)

Ports and the services

For **10.0.2.2**, **10.0.2.3**, **10.0.2.4**

Port	Service	Description
135/tcp	msrpc	Used for Microsoft Remote Procedure Call. Common on Windows systems for allowing services and applications to communicate over the network. Often targeted in Windows-based exploits.
445/tcp	microsoft-ds	Used for SMB protocol. Helps in file sharing, printer sharing, etc., mostly on Windows machines. Vulnerable to attacks like EternalBlue.
8009/tcp	ajp13	Apache JServ Protocol. Helps connect web servers to application servers like Tomcat. Exposing this can lead to remote code execution, like in Ghostcat attack.

For **10.0.2.15**

Port	Service	Description
22/tcp	ssh	Secure Shell. Used for remote login and command execution. Common on Linux. Needs strong authentication to stay secure.
111/tcp	rpcbind	Maps RPC services to their respective ports. Required by services like NFS. Can be misused if exposed to untrusted networks.
2049/tcp	nfs	Network File System. Lets users access files over the network like they're local. Should only be available in trusted environments.

7)

Ports 135 and 445 (Windows RPC and SMB) are high-risk, often targeted for remote code execution (e.g., EternalBlue). Port 8009 (AJP13) can lead to remote access if misconfigured (e.g., Ghostcat). Port 22 (SSH) risks brute-force if not secured. Ports 111 and 2049 (rpcbind, NFS) can expose file systems if left open.