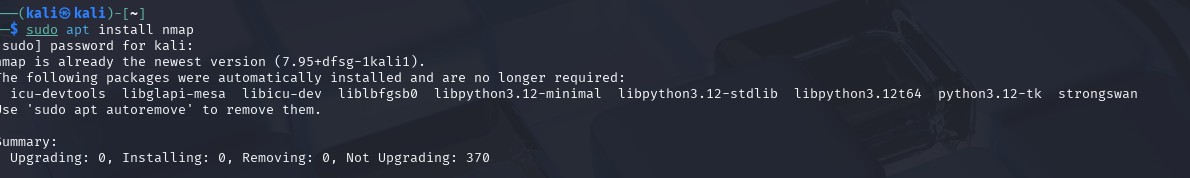
**TASK 1:-**

1.INSTALL NMAP FROM OFFICIAL WEBSITE

Command used is

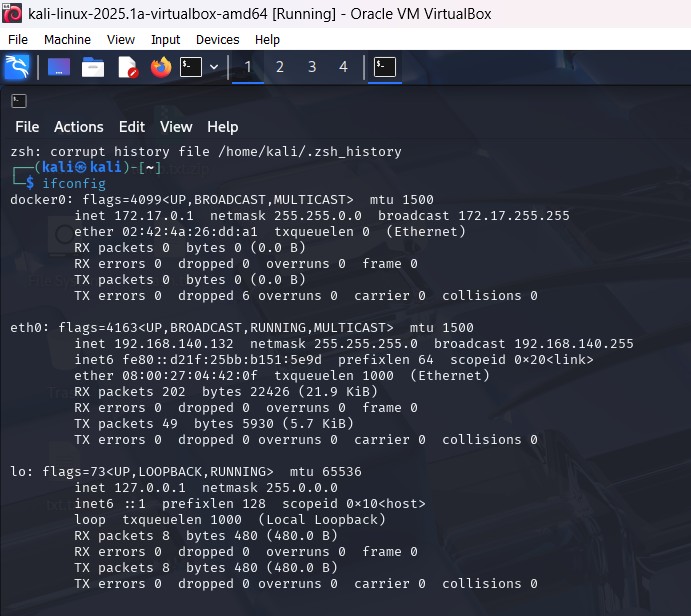
sudo apt install nmap



2.FIND YOUR LOCAL IP RANGE

Command used is

ifconfig

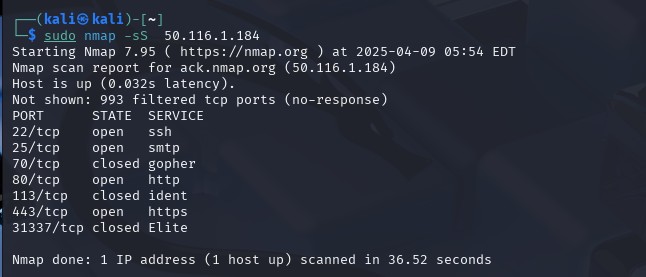


The local ip range is 192.168.140.132 or 192.168.140.0/24

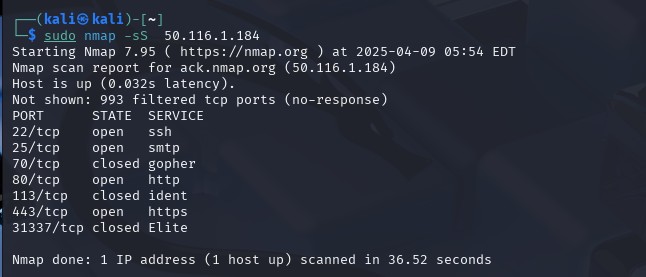
3.PERFORM TCP SYN SCAN

Command used is

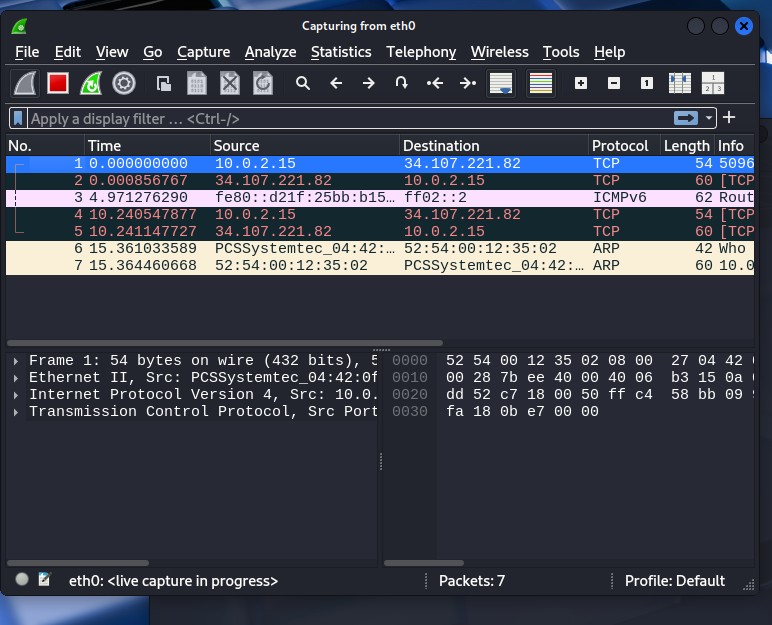
Sudo nmap -sS <ip>

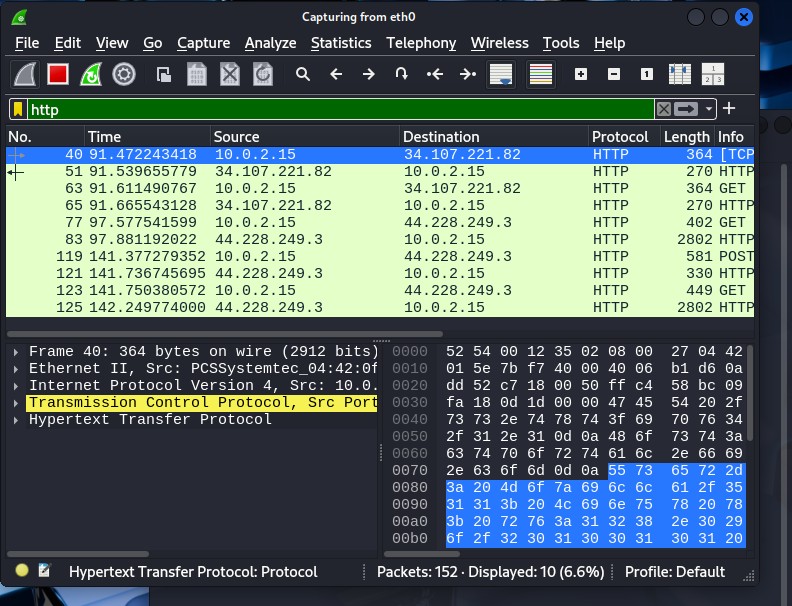


4.NOTE DOWN ALL IP ADDRESSES AND OPEN PORTS

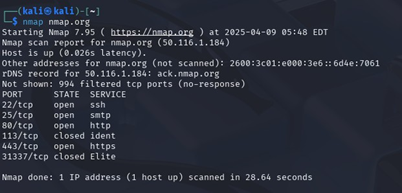


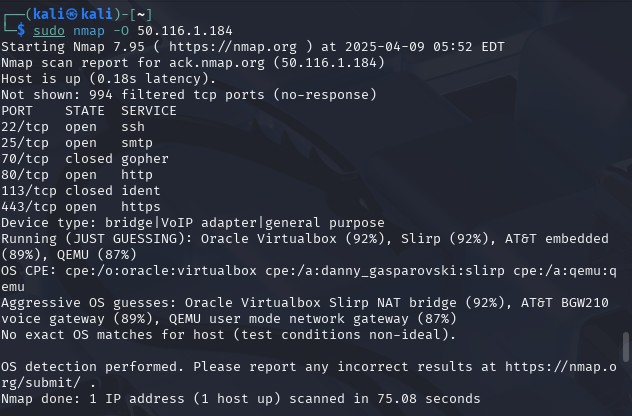
5.OPTIONALLY ANALYZE PACKET CAPTURE WITH WIRESHARK

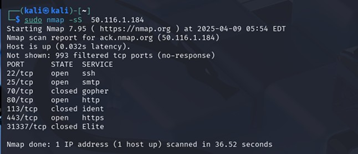


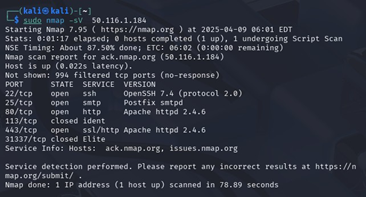


6.RESEARCH COMMON SERVICES RUNNING ON THOSE PORTS









7.IDENTIFY POTENTIAL SECURITY RISKS FROM OPEN PORTS

Potential Security Risks from Open Ports:

1. Unauthorized access: Open ports can be exploited to gain access to services.

2. Exposed services: Services like FTP, SSH, or databases may have vulnerabilities.

3. Information leakage: Banner grabbing can reveal software versions.

4. Backdoors/Trojans: Attackers may use open ports to install backdoors.

5. DDoS attacks: Some ports can be exploited for amplification attacks.

How to Find Open Ports in Kali Linux: Use Nmap (pre-installed in Kali):

nmap -sS -Pn <target-ip>

For a more detailed scan:

nmap -sV -T4 -O <target-ip>

-sS: SYN scan (stealth)

-Pn: Skip ping (treat host as up)

-sV: Detect service version

-O: OS detection