01.What is Nmap? Install Nmap from Official Website?

Nmap is a powerful and flexible open-source tool used for scanning and mapping networks. It helps identify hosts, open ports, running services, operating systems, and even vulnerabilities. It's widely used in cybersecurity assessments and ethical hacking.

Here are The some Features and Purpose

- Host Discovery used for the Find online devices
- Port Scanning used for the Check open/closed/filtered ports
- Service Version Detection used for the Find software version (e.g., Apache 2.4.29)
- Operating System used for the Detection Guess OS type (Linux, Windows, etc.)
- NSE Scripting Engine used for the Run custom or built-in scripts to find issues
- Stealth Mode used for the Evade detection by firewalls or IDS (e.g., -sS)

Install Nmap from Official Website

Install Nmap

Windows: Download from https://nmap.org/download.html → Choose the Windows installer.

Linux (e.g., Kali): Run

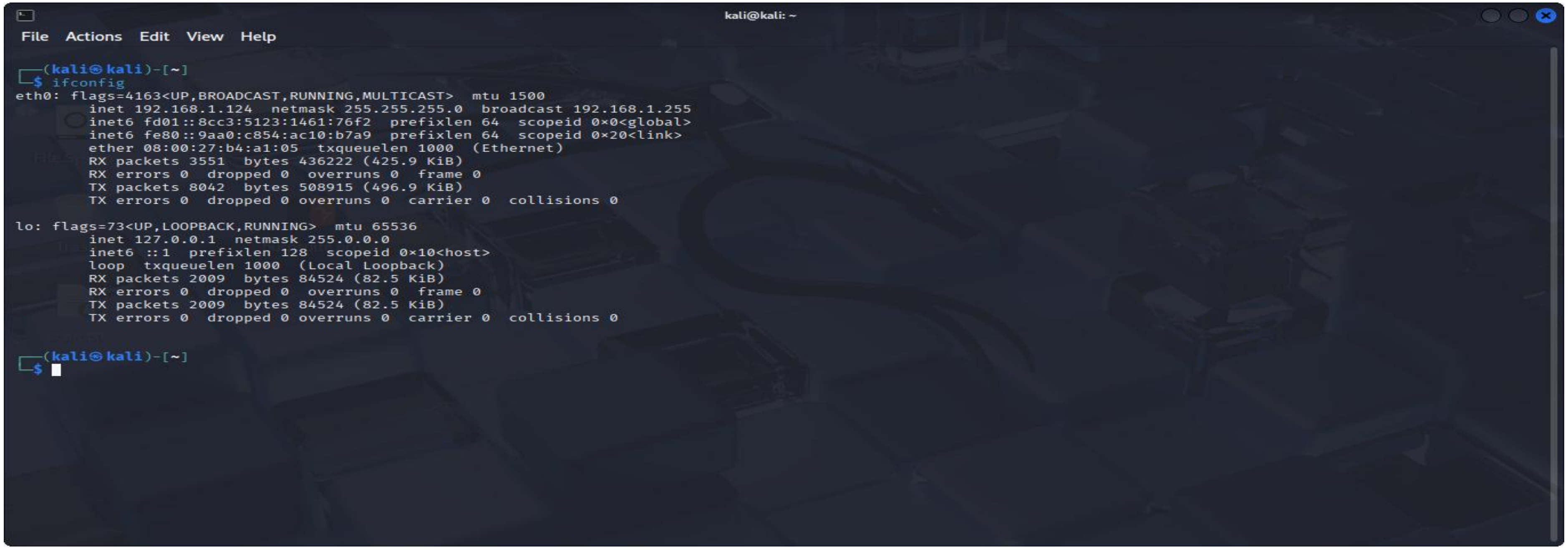
```
sudo apt update && sudo apt install Nmap
```

02.Find your Ip range?

Find Your Local IP Range
Open terminal and run:

```
ip a   # (Linux/Kali)
ipconfig  # (Windows CMD)
```

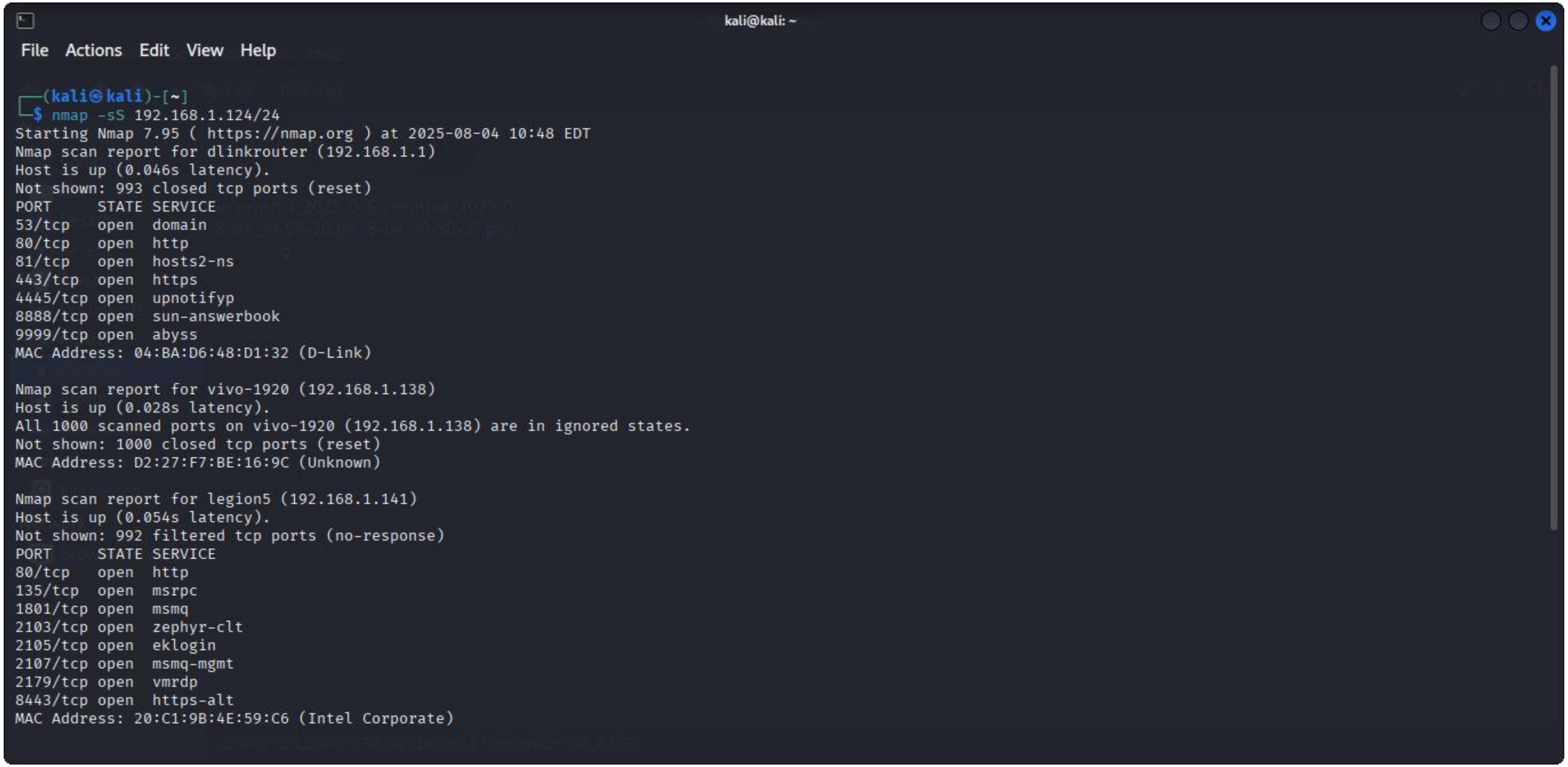
Look for your IP, e.g., 192.168.1.12
Your network range will typically be 192.168.1.0/24, where:
192.168.1.0 is the network address



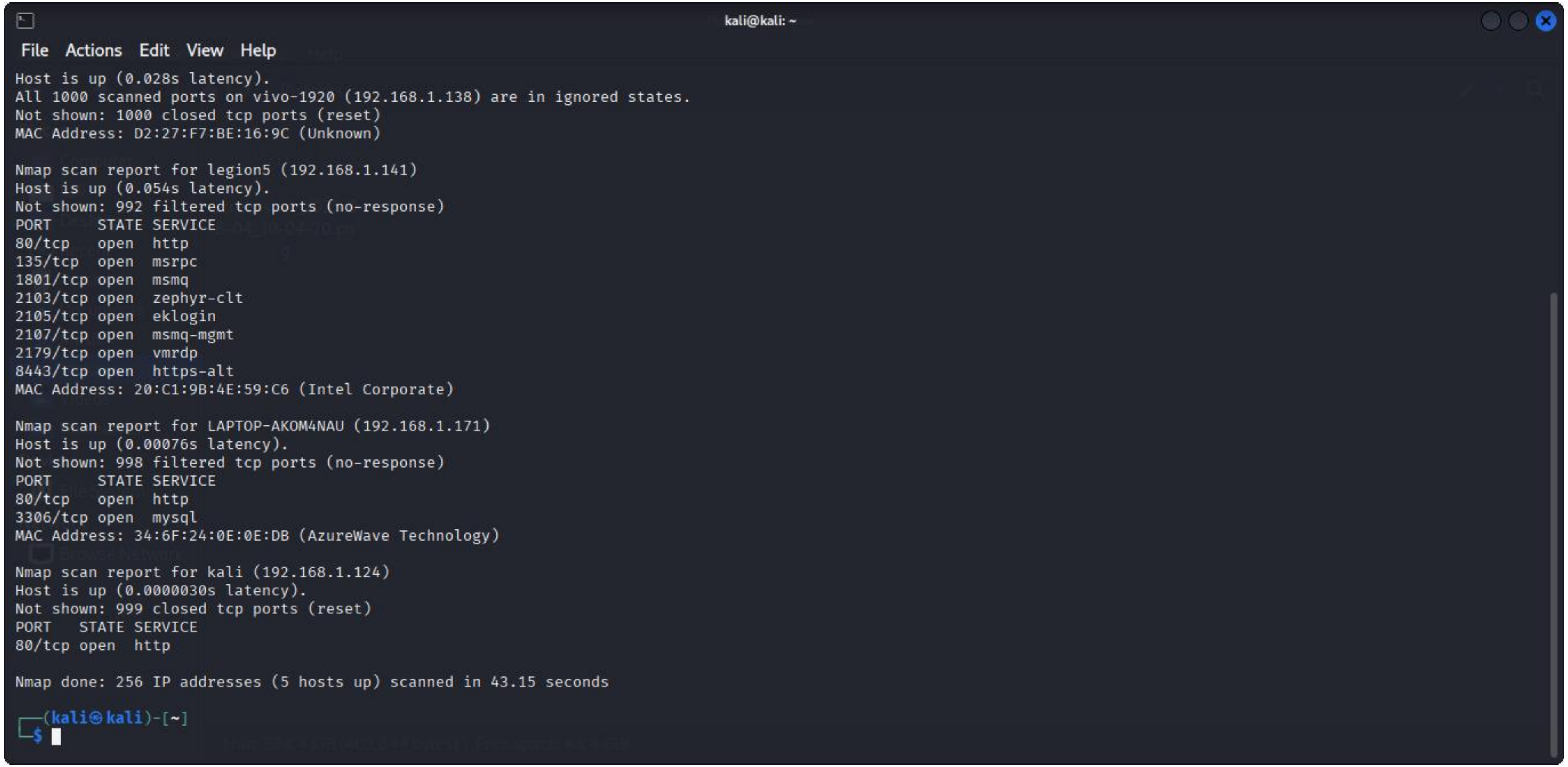
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.124  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fd01::8cc3:5123:1461:76f2  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::9aa0:c854:ac10:b7a9  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b4:a1:05  txqueuelen 1000  (Ethernet)
        RX packets 3551  bytes 436222 (425.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8042  bytes 508915 (496.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2009  bytes 84524 (82.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2009  bytes 84524 (82.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ 
```

03.RUN Nmap -sS IP address To perform TCP SYN Scan?

Command:- nmap -sS 192.168.1.124/24
sS = SYN scan (stealthy, faster)
This shows live devices and their open TCP ports



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.1.124/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 10:48 EDT
Nmap scan report for dlinkrouter (192.168.1.1)
Host is up (0.046s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
81/tcp   open  hosts2-ns
443/tcp  open  https
4445/tcp open  upnotifyp
8888/tcp open  sun-answerbook
9999/tcp open  abyss
MAC Address: 04:BA:D6:48:D1:32 (D-Link)

Nmap scan report for vivo-1920 (192.168.1.138)
Host is up (0.028s latency).
All 1000 scanned ports on vivo-1920 (192.168.1.138) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: D2:27:F7:BE:16:9C (Unknown)

Nmap scan report for legion5 (192.168.1.141)
Host is up (0.054s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
2179/tcp open  vmrdp
8443/tcp open  https-alt
MAC Address: 20:C1:9B:4E:59:C6 (Intel Corporate)
```

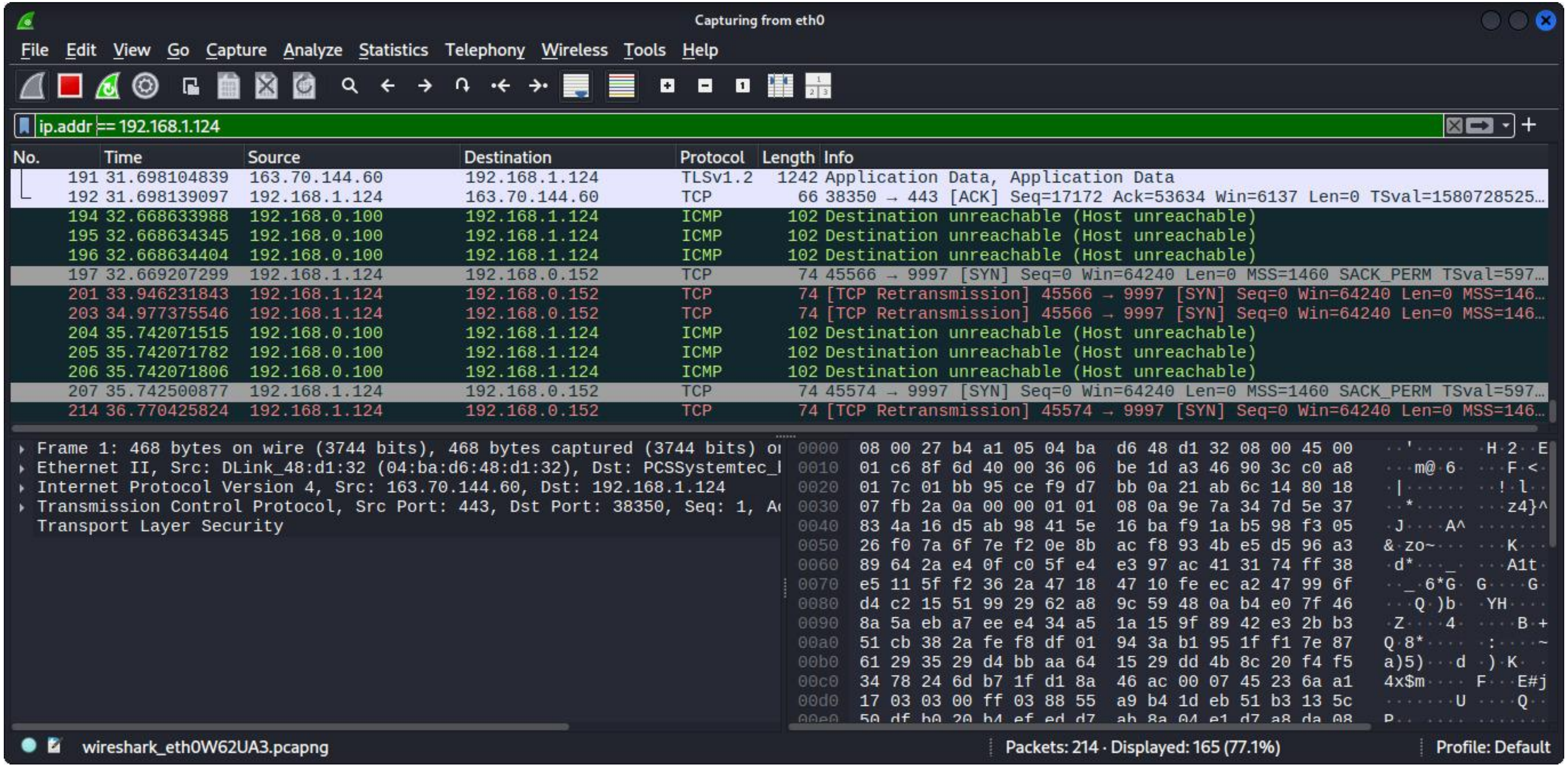


```
Host is up (0.028s latency).
All 1000 scanned ports on vivo-1920 (192.168.1.138) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: D2:27:F7:BE:16:9C (Unknown)

Nmap scan report for legion5 (192.168.1.141)
Host is up (0.054s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
2179/tcp open  vmrdp
8443/tcp open  https-alt
MAC Address: 20:C1:9B:4E:59:C6 (Intel Corporate)

Nmap scan report for LAPTOP-AKOM4NAU (192.168.1.171)
Host is up (0.00076s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 34:6F:24:0E:0E:DB (AzureWave Technology)

Nmap scan report for kali (192.168.1.124)
Host is up (0.0000030s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 256 IP addresses (5 hosts up) scanned in 43.15 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

04.Optionally analyze packet capture with Wireshark?

Wireshark is a network protocol analyzer — a powerful tool used to capture, inspect, and analyze network traffic in real time.It lets you see everything happening on a network — like who is communicating with whom, what data is being sent, and which protocols are being used.

Open Wireshark and select your active network adapter.
ip.addr == 192.168.1.X


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.1.124

No.	Time	Source	Destination	Protocol	Length	Info
191	31.698104839	163.70.144.60	192.168.1.124	TLSv1.2	1242	Application Data, Application Data
192	31.698139097	192.168.1.124	163.70.144.60	TCP	66	38350 → 443 [ACK] Seq=17172 Ack=53634 Win=6137 Len=0 TSval=1580728525…
194	32.668633988	192.168.0.100	192.168.1.124	ICMP	102	Destination unreachable (Host unreachable)
195	32.668634345	192.168.0.100	192.168.1.124	ICMP	102	Destination unreachable (Host unreachable)
196	32.668634404	192.168.0.100	192.168.1.124	ICMP	102	Destination unreachable (Host unreachable)
197	32.669207299	192.168.1.124	192.168.0.152	TCP	74	45566 → 9997 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=597…
201	33.946231843	192.168.1.124	192.168.0.152	TCP	74	[TCP Retransmission] 45566 → 9997 [SYN] Seq=0 Win=64240 Len=0 MSS=146…
203	34.977375546	192.168.1.124	192.168.0.152	TCP	74	[TCP Retransmission] 45566 → 9997 [SYN] Seq=0 Win=64240 Len=0 MSS=146…
204	35.742071515	192.168.0.100	192.168.1.124	ICMP	102	Destination unreachable (Host unreachable)
205	35.742071782	192.168.0.100	192.168.1.124	ICMP	102	Destination unreachable (Host unreachable)
206	35.742071806	192.168.0.100	192.168.1.124	ICMP	102	Destination unreachable (Host unreachable)
207	35.742500877	192.168.1.124	192.168.0.152	TCP	74	45574 → 9997 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=597…
214	36.770425824	192.168.1.124	192.168.0.152	TCP	74	[TCP Retransmission] 45574 → 9997 [SYN] Seq=0 Win=64240 Len=0 MSS=146…

```
▸ Frame 1: 468 bytes on wire (3744 bits), 468 bytes captured (3744 bits) oı
▸ Ethernet II, Src: DLink_48:d1:32 (04:ba:d6:48:d1:32), Dst: PCSSystemtec_I
▸ Internet Protocol Version 4, Src: 163.70.144.60, Dst: 192.168.1.124
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 38350, Seq: 1, Ac
  Transport Layer Security
```

```
0000  08 00 27 b4 a1 05 04 ba  d6 48 d1 32 08 00 45 00   ··'·····H·2··E·
0010  01 c6 8f 6d 40 00 36 06  be 1d a3 46 90 3c c0 a8   ···m@·6····F·<··
0020  01 7c 01 bb 95 ce f9 d7  bb 0a 21 ab 6c 14 80 18   ·|········!·l···
0030  07 fb 2a 0a 00 00 01 01  08 0a 9e 7a 34 7d 5e 37   ··*········z4}^7
0040  83 4a 16 d5 ab 98 41 5e  16 ba f9 1a b5 98 f3 05   ·J····A^········
0050  26 f0 7a 6f 7e f2 0e 8b  ac f8 93 4b e5 d5 96 a3   &·zo~······K····
0060  89 64 2a e4 0f c0 5f e4  e3 97 ac 41 31 74 ff 38   ·d*···_····A1t·8
0070  e5 11 5f f2 36 2a 47 18  47 10 fe ec a2 47 99 6f   ··_·6*G·G····G·o
0080  d4 c2 15 51 99 29 62 a8  9c 59 48 0a b4 e0 7f 46   ···Q·)b··YH····F
0090  8a 5a eb a7 ee e4 34 a5  1a 15 9f 89 42 e3 2b b3   ·Z····4·····B·+·
00a0  51 cb 38 2a fe f8 df 01  94 3a b1 95 1f f1 7e 87   Q·8*·····:····~·
00b0  61 29 35 29 d4 bb aa 64  15 29 dd 4b 8c 20 f4 f5   a)5)···d·)·K····
00c0  34 78 24 6d b7 1f d1 8a  46 ac 00 07 45 23 6a a1   4x$m····F···E#j·
00d0  17 03 03 00 ff 03 88 55  a9 b4 1d eb 51 b3 13 5c   ·······U····Q··\
00e0  50 df b0 20 b4 ef ed d7  ab 8a 04 e1 d7 a8 da 08   P···············
```

wireshark_eth0W62UA3.pcapng   Packets: 214 · Displayed: 165 (77.1%)   Profile: Default

You can see the live packets while Nmap is scanning.

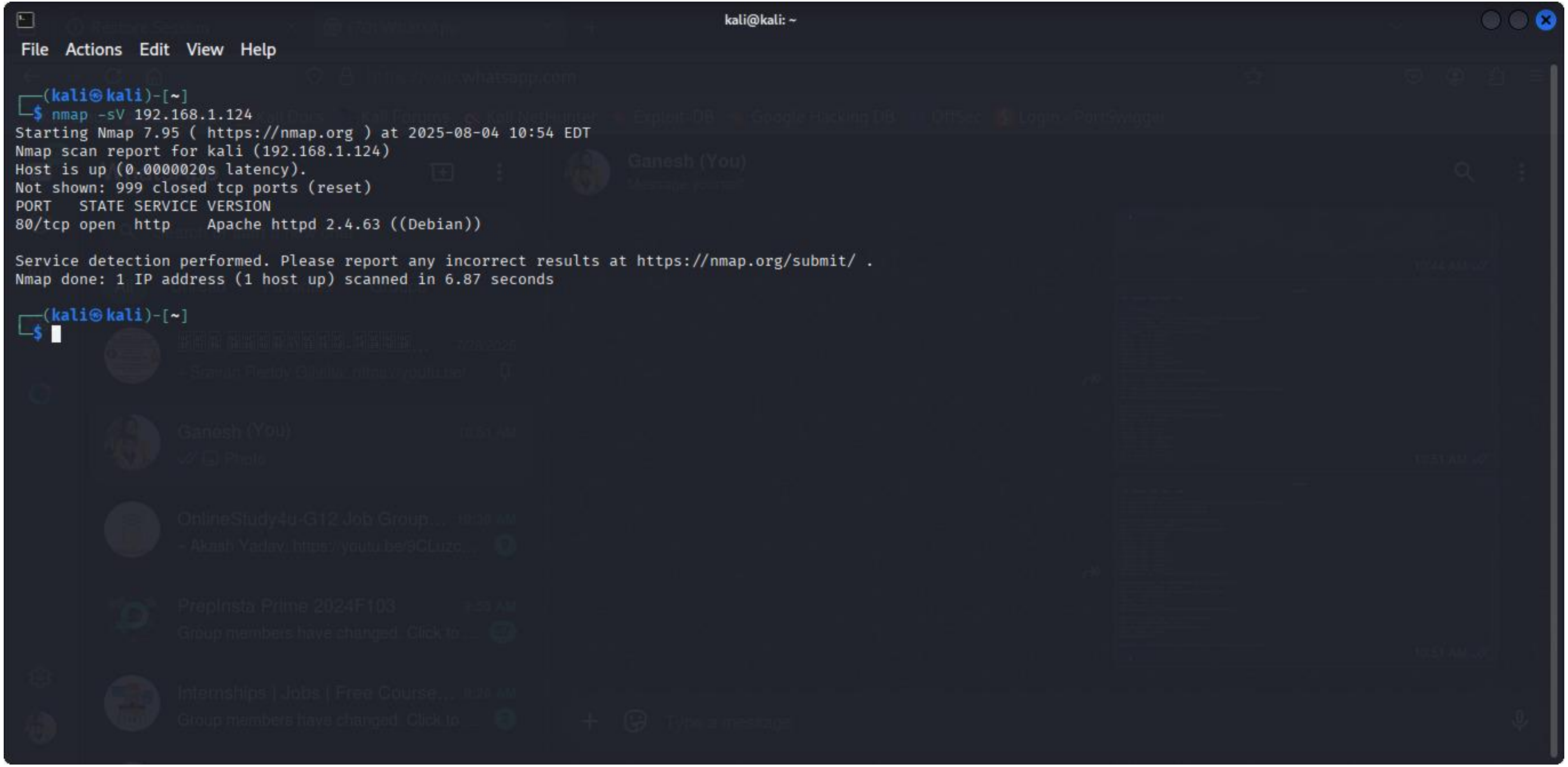
06. 6.Research common services running on those ports.

Look up ports and services:

- **Port 22 → SSH**

- **Port 80 → HTTP (Web)**
- **Port 443 → HTTPS**
- **Port 445 → SMB (Windows File Sharing)**
- **Port 3306 → MySQL**

Command:- nmap -sV 192.168.1.124

- 

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.124
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 10:54 EDT
Nmap scan report for kali (192.168.1.124)
Host is up (0.0000020s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.63 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.87 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

07.Identifying potential security risks from open ports?

When you scan a system with tools like *Nmap, open ports can reveal **vulnerable services* or *entry points* for attackers.

Port	Port	Potential Risk
21	FTP	Unencrypted login; susceptible to brute-force or anonymous access
22	SSH	Brute-force attack, weak passwords, outdated SSH version
23	Telnet	Unencrypted communication; attacker can sniff login credentials
25	SMTP	Open relays used to send spam; vulnerable to spoofing
53	DNS	Can be used for DNS poisoning or amplification DDoS attacks
80	HTTP	If web server has vulnerabilities (e.g., outdated WordPress, Apache)
443	HTTPS	Misconfigured SSL/TLS can expose to MITM attacks
110	POP3	Credentials sent in plain text if not secured
139/445	SMB	Used in WannaCry ransomware attack; vulnerable to remote code execution
3306	MySQL	Can expose databases if misconfigured or default passwords used
3389	RDP	Targeted in brute-force and remote desktop attacks

How Open Ports Become a Risk:
Outdated Software– Unpatched services listening on open ports.
Default Credentials – Especially common in routers, FTP, or DB services.
No Access Control – Services like MySQL or MongoDB exposed to the internet.
Port Forwarding Misuse – From NAT/router misconfigurations.
No Firewall or IDS/IPS – System is directly exposed.