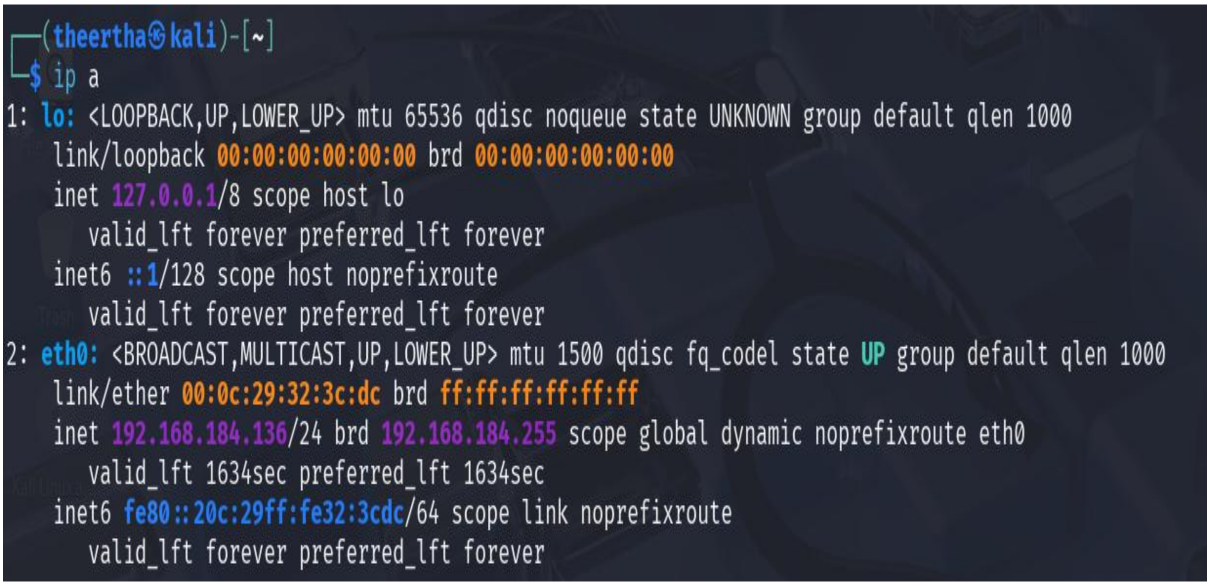
Task 1: Scan Your Local Network for Open Ports

Objective: Learn to discover open ports on devices in your local network to understand network exposure.

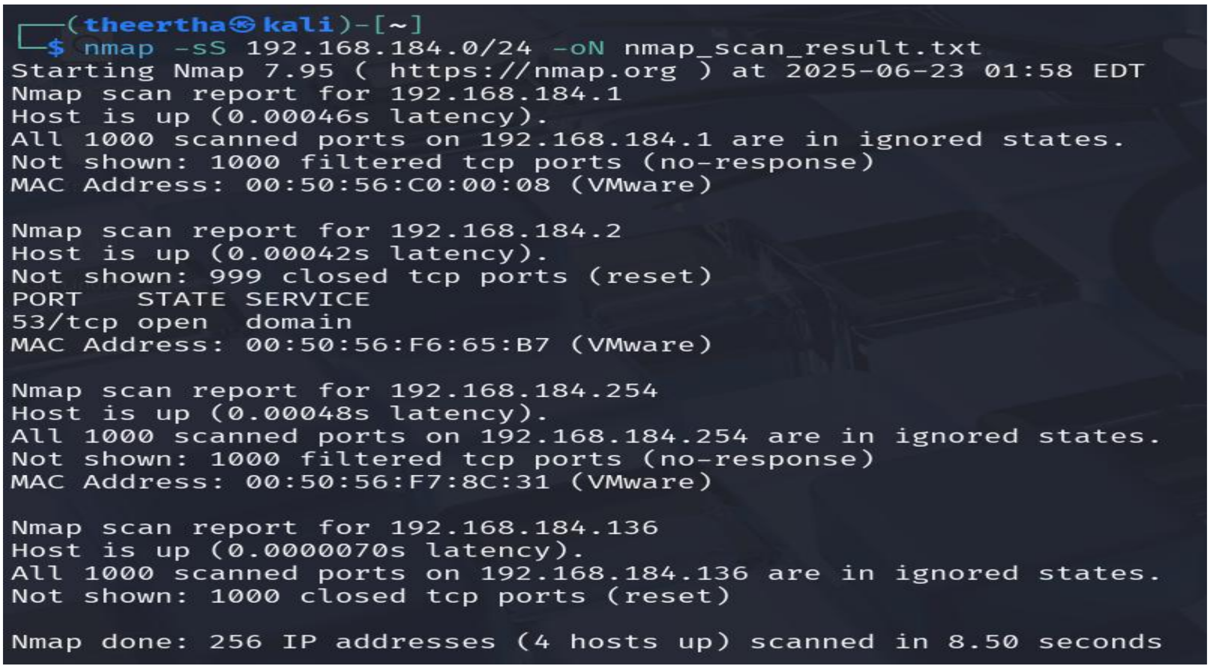
Tools: Nmap ,Wireshark

Firstly I found my IP range as 192.168.184.0/24



```
┌──(theertha㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:32:3c:dc brd ff:ff:ff:ff:ff:ff
    inet 192.168.184.136/24 brd 192.168.184.255 scope global dynamic noprefixroute eth0
       valid_lft 1634sec preferred_lft 1634sec
    inet6 fe80::20c:29ff:fe32:3cdc/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

To identify open ports in my local network, I used the following Nmap command:



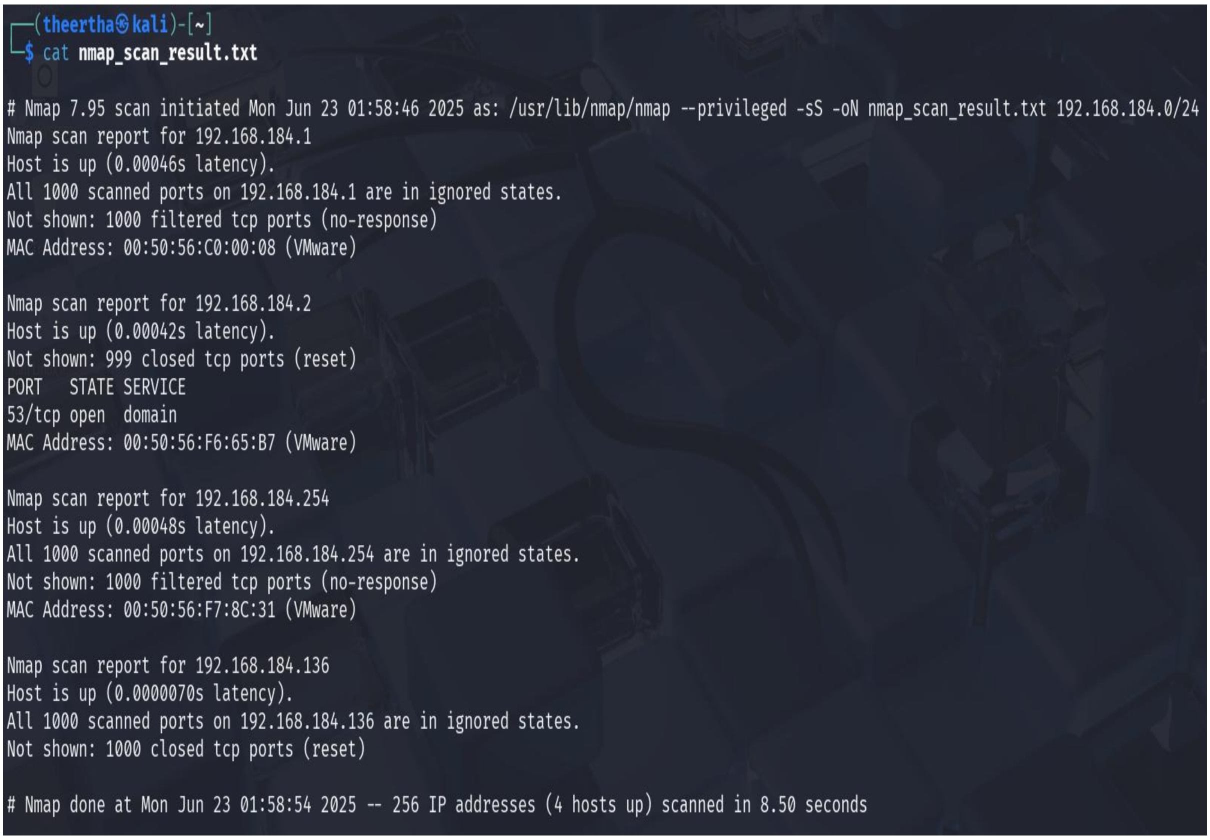
```
┌──(theertha㉿kali)-[~]
└─$ nmap -sS 192.168.184.0/24 -oN nmap_scan_result.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 01:58 EDT
Nmap scan report for 192.168.184.1
Host is up (0.00046s latency).
All 1000 scanned ports on 192.168.184.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.184.2
Host is up (0.00042s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:F6:65:B7 (VMware)

Nmap scan report for 192.168.184.254
Host is up (0.00048s latency).
All 1000 scanned ports on 192.168.184.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F7:8C:31 (VMware)

Nmap scan report for 192.168.184.136
Host is up (0.0000070s latency).
All 1000 scanned ports on 192.168.184.136 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 8.50 seconds
```

- This command performs a TCP SYN scan on the full subnet `192.168.184.0/24`.
- The -sS` flag sends half-open TCP probes to check for open ports without completing full handshakes.
- The scan discovered 4 active hosts.
- Only one open port was found:

  192.168.184.2 , Port 53/tcp (Service: domain, used for DNS)

All other devices had no open ports or were filtered by firewalls.

I saved the scan output as a text file



```
┌──(theertha㉿kali)-[~]
└─$ cat nmap_scan_result.txt

# Nmap 7.95 scan initiated Mon Jun 23 01:58:46 2025 as: /usr/lib/nmap/nmap --privileged -sS -oN nmap_scan_result.txt 192.168.184.0/24
Nmap scan report for 192.168.184.1
Host is up (0.00046s latency).
All 1000 scanned ports on 192.168.184.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.184.2
Host is up (0.00042s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:F6:65:B7 (VMware)

Nmap scan report for 192.168.184.254
Host is up (0.00048s latency).
All 1000 scanned ports on 192.168.184.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F7:8C:31 (VMware)

Nmap scan report for 192.168.184.136
Host is up (0.0000070s latency).
All 1000 scanned ports on 192.168.184.136 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

# Nmap done at Mon Jun 23 01:58:54 2025 -- 256 IP addresses (4 hosts up) scanned in 8.50 seconds
```

The open port identified in the scan was:

192.168.184.2 , Port 53/tcp (DNS service)

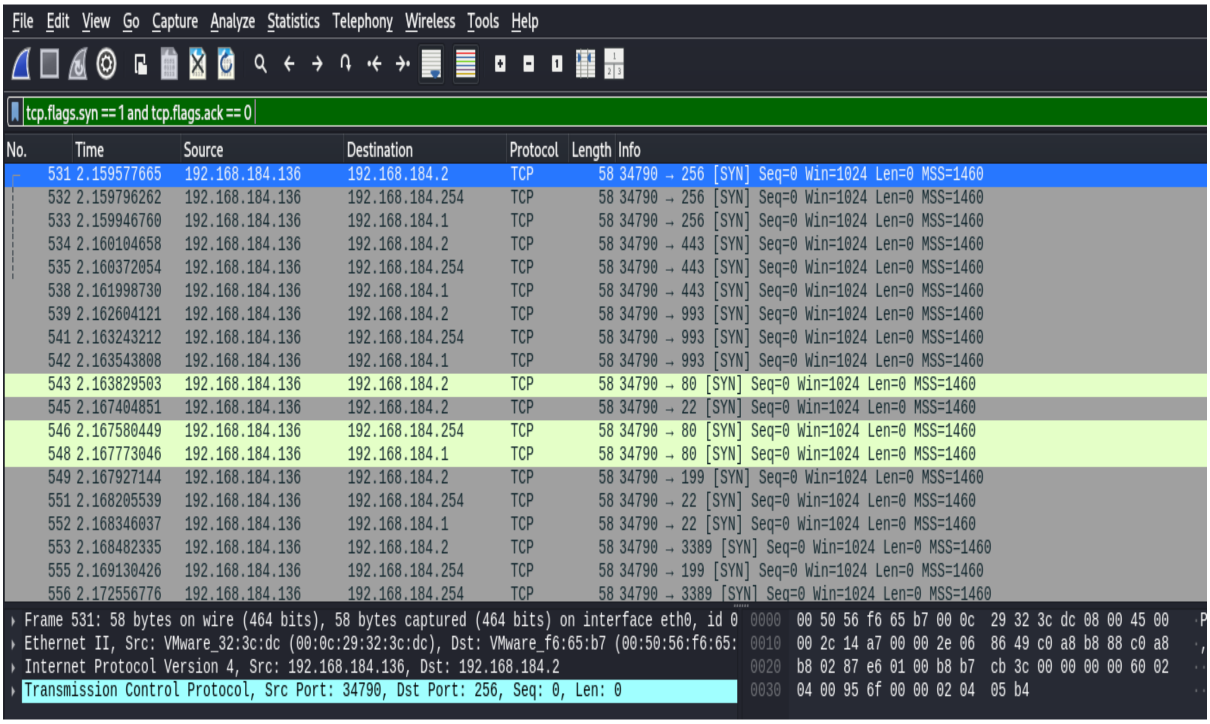
This indicates a DNS service is exposed on the local network.

<u>Potential Threats:</u>

- **DNS Tunneling**: Attackers can use DNS to hide data transfers or backdoor communication.
- **Cache Poisoning**: If unpatched, the DNS server may redirect users to malicious sites.
- **DDoS Amplification**: Misconfigured DNS can be abused in amplification-based attacks.
- **Information Leakage**: Publicly answering internal queries can reveal sensitive network info.

To verify network activity during the scan, I used **Wireshark** to capture traffic on my interface. I applied the filter:

tcp.flags.syn == 1 and tcp.flags.ack == 0



```
tcp.flags.syn == 1 and tcp.flags.ack == 0

No.     Time         Source           Destination      Protocol Length Info
    531 2.159577665  192.168.184.136  192.168.184.2    TCP      58 34790 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    532 2.159796262  192.168.184.136  192.168.184.254  TCP      58 34790 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    533 2.159946760  192.168.184.136  192.168.184.1    TCP      58 34790 → 256 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    534 2.160104658  192.168.184.136  192.168.184.2    TCP      58 34790 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    535 2.160372054  192.168.184.136  192.168.184.254  TCP      58 34790 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    538 2.161998730  192.168.184.136  192.168.184.1    TCP      58 34790 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    539 2.162604121  192.168.184.136  192.168.184.2    TCP      58 34790 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    541 2.163243212  192.168.184.136  192.168.184.254  TCP      58 34790 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    542 2.163543808  192.168.184.136  192.168.184.1    TCP      58 34790 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    543 2.163829503  192.168.184.136  192.168.184.2    TCP      58 34790 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    545 2.167404851  192.168.184.136  192.168.184.2    TCP      58 34790 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    546 2.167580449  192.168.184.136  192.168.184.254  TCP      58 34790 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    548 2.167773046  192.168.184.136  192.168.184.1    TCP      58 34790 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    549 2.167927144  192.168.184.136  192.168.184.2    TCP      58 34790 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    551 2.168205539  192.168.184.136  192.168.184.254  TCP      58 34790 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    552 2.168346037  192.168.184.136  192.168.184.1    TCP      58 34790 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    553 2.168482335  192.168.184.136  192.168.184.2    TCP      58 34790 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    555 2.169130426  192.168.184.136  192.168.184.254  TCP      58 34790 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
    556 2.172556776  192.168.184.136  192.168.184.254  TCP      58 34790 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

▸ Frame 531: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0   0000  00 50 56 f6 65 b7 00 0c  29 32 3c dc 08 00 45 00
▸ Ethernet II, Src: VMware_32:3c:dc (00:0c:29:32:3c:dc), Dst: VMware_f6:65:b7 (00:50:56:f6:65:  0010  00 2c 14 a7 00 00 2e 06  86 49 c0 a8 b8 88 c0 a8
▸ Internet Protocol Version 4, Src: 192.168.184.136, Dst: 192.168.184.2                         0020  b8 02 87 e6 01 00 b8 b7  cb 3c 00 00 00 00 60 02
▸ Transmission Control Protocol, Src Port: 34790, Dst Port: 256, Seq: 0, Len: 0                 0030  04 00 95 6f 00 00 02 04  05 b4
```

This shows the SYN packets Nmap sends to identify open ports. From the capture:

- I confirmed that Nmap sent TCP SYN packets to all 256 hosts
- Only one host responded with an open port (53), matching the Nmap result

The capture file was saved as nmap_scan_capture.pcapng.