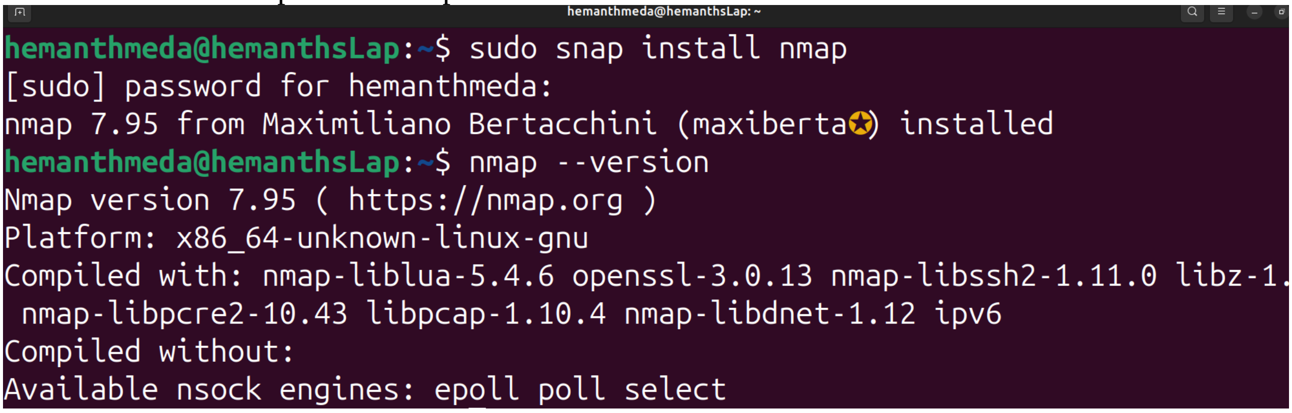
CYBER SECURITY INTERNSHIP (Elevate Labs)

Name : Meda Venkata Naga Hemanth Kumar
Note: I am using Ubuntu as my operating system.

Task – 1: Scan Your Local Network for Open Ports

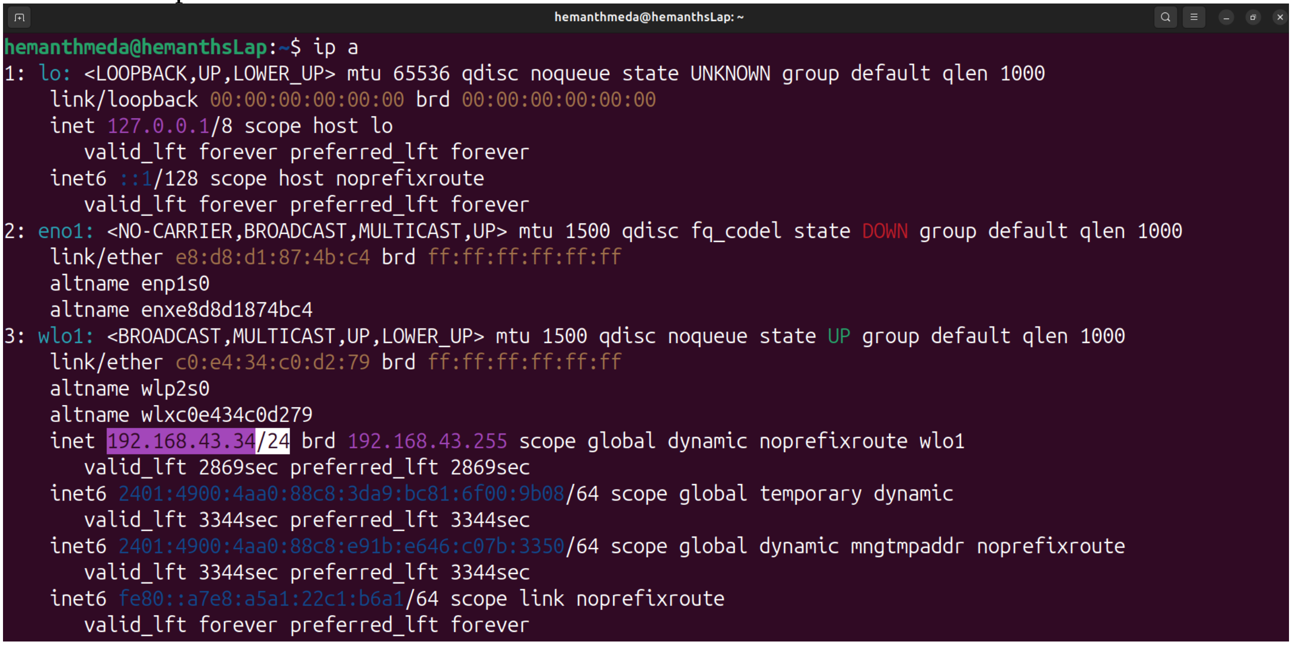
Objective: Learn to discover open ports on devices in your local network to understand network exposure.
Tools: Nmap (free), Wireshark (optional)

Task Implementation:
1. Installation of Nmap:
Command: sudo snap install nmap



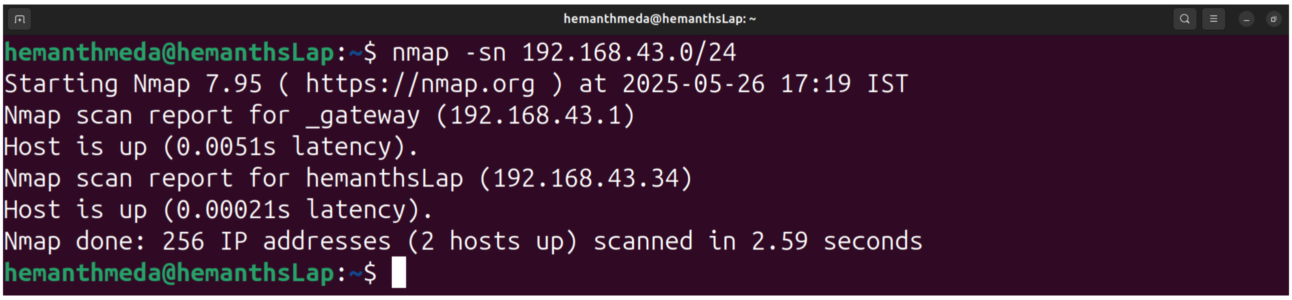
```
hemanthmeda@hemanthsLap:~$ sudo snap install nmap
[sudo] password for hemanthmeda:
nmap 7.95 from Maximiliano Bertacchini (maxiberta✪) installed
hemanthmeda@hemanthsLap:~$ nmap --version
Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-unknown-linux-gnu
Compiled with: nmap-liblua-5.4.6 openssl-3.0.13 nmap-libssh2-1.11.0 libz-1.
 nmap-libpcre2-10.43 libpcap-1.10.4 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

2. Check installation of Nmap:
Command: nmap --version
3. Find local IP range.
Command: ip a



```
hemanthmeda@hemanthsLap:~$ 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: eno1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether e8:d8:d1:87:4b:c4 brd ff:ff:ff:ff:ff:ff
    altname enp1s0
    altname enxe8d8d1874bc4
3: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether c0:e4:34:c0:d2:79 brd ff:ff:ff:ff:ff:ff
    altname wlp2s0
    altname wlxc0e434c0d279
    inet 192.168.43.34/24 brd 192.168.43.255 scope global dynamic noprefixroute wlo1
       valid_lft 2869sec preferred_lft 2869sec
    inet6 2401:4900:4aa0:88c8:3da9:bc81:6f00:9b08/64 scope global temporary dynamic
       valid_lft 3344sec preferred_lft 3344sec
    inet6 2401:4900:4aa0:88c8:e91b:e646:c07b:3350/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 3344sec preferred_lft 3344sec
    inet6 fe80::a7e8:a5a1:22c1:b6a1/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

here my local IP range is 192.168.43.34/24
4. Scan the network for live hosts
Command: nmap -sn 192.168.43.0/24



```
hemanthmeda@hemanthsLap:~$ nmap -sn 192.168.43.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 17:19 IST
Nmap scan report for _gateway (192.168.43.1)
Host is up (0.0051s latency).
Nmap scan report for hemanthsLap (192.168.43.34)
Host is up (0.00021s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.59 seconds
hemanthmeda@hemanthsLap:~$
```

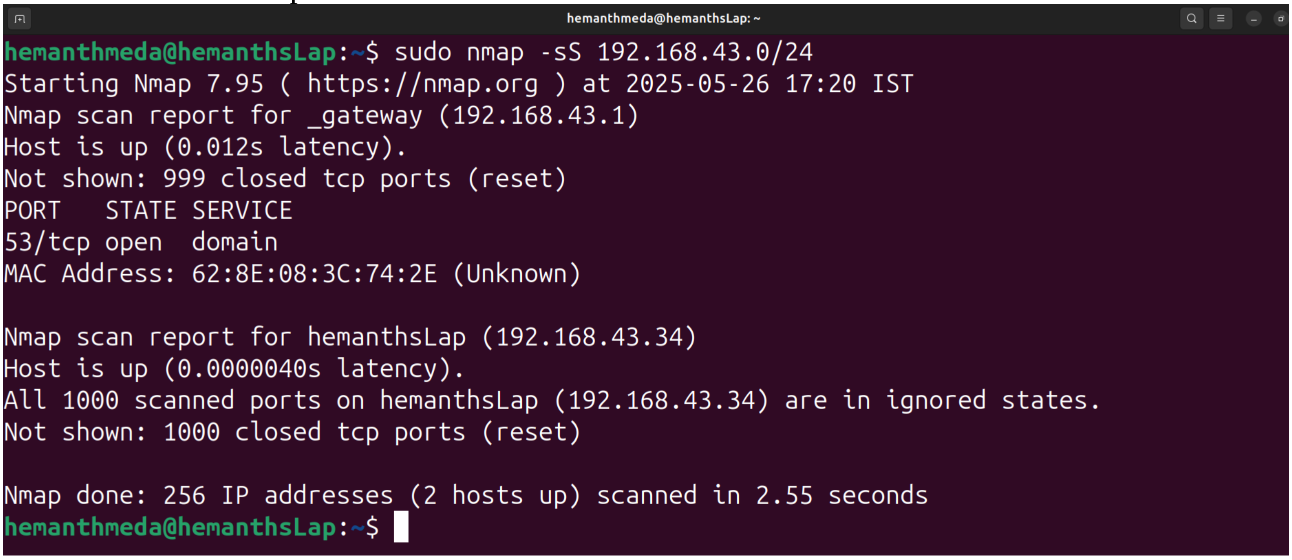
only two active hosts on my network found:

one is Wi-Fi router gateway: 192.168.43.1

other is my laptop: 192.168.43.34

5. Scan for open ports using a TCP SYN Scan

Command: sudo nmap -sS 192.168.43.0/24



```
hemanthmeda@hemanthsLap:~$ sudo nmap -sS 192.168.43.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 17:20 IST
Nmap scan report for _gateway (192.168.43.1)
Host is up (0.012s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 62:8E:08:3C:74:2E (Unknown)

Nmap scan report for hemanthsLap (192.168.43.34)
Host is up (0.0000040s latency).
All 1000 scanned ports on hemanthsLap (192.168.43.34) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (2 hosts up) scanned in 2.55 seconds
hemanthmeda@hemanthsLap:~$
```

open ports found : port – 53/tcp
state – open
service – domain(DNS)

Indicates router is running a DNS server.

6.For analyzing packet capture on Wireshark

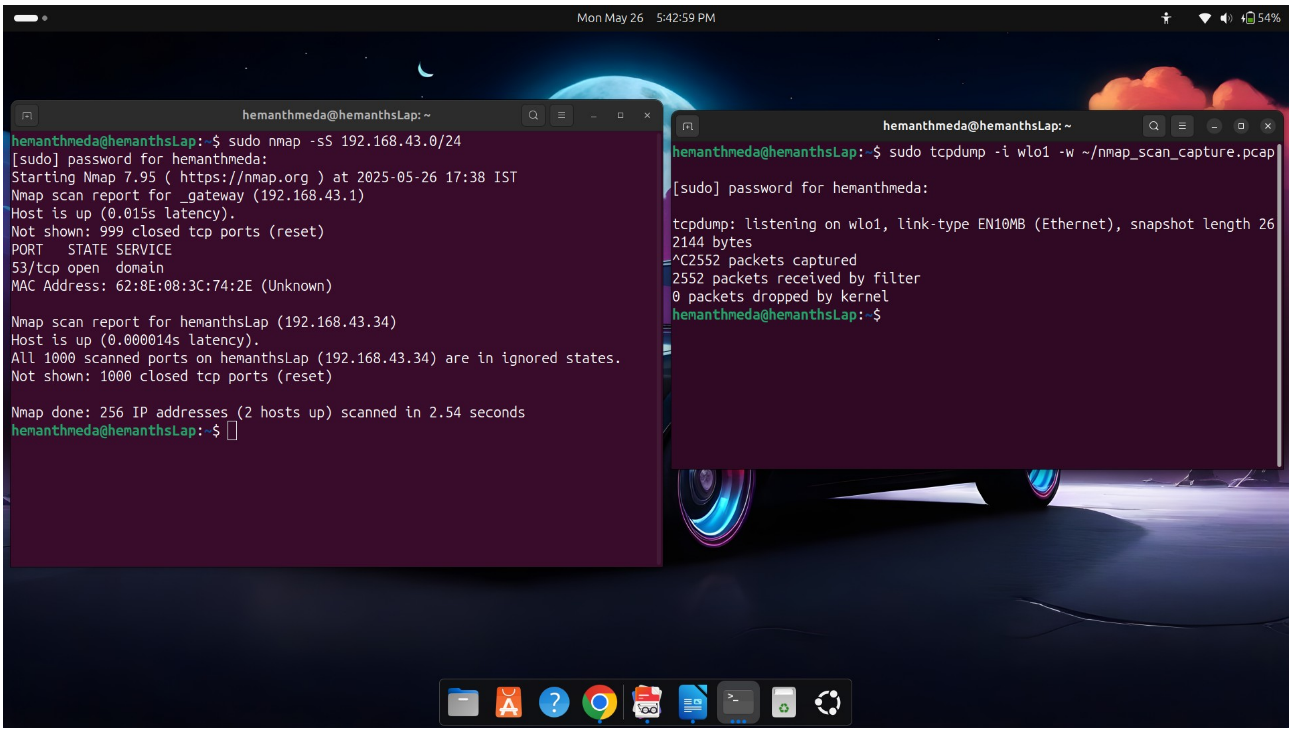
Wireshark accepts .pcap files but nmap can’t generate directly these files so here I have used another tool called **tcpdump**

Command: sudo tcpdump -i wlo1 -w ~/nmap_scan_capture.pcap

start it and open another terminal to run nmap script

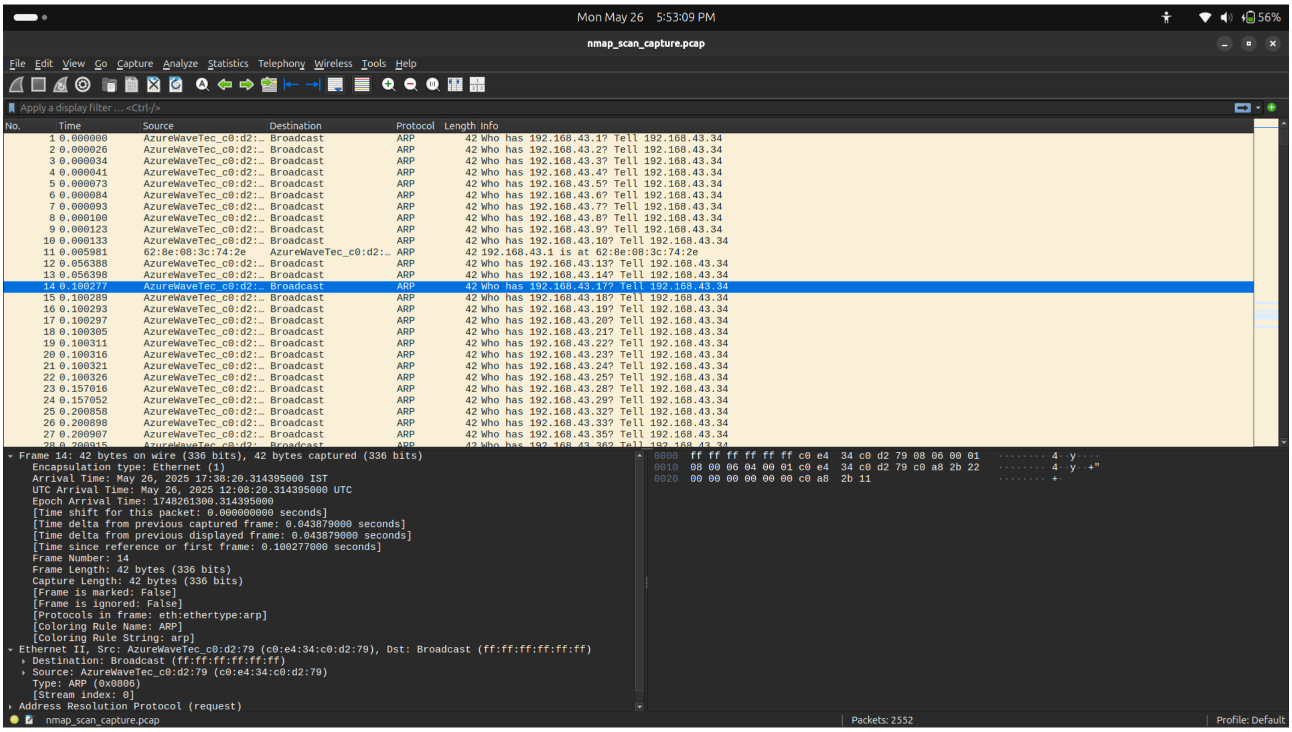
Command:sudo nmap -sS 192.168.43.0/24

start it and after completion of nmap scan stop the tcpdump scan also by typing ^c then open the capture file with Wireshark.



```
hemanthmeda@hemanthsLap:~$ sudo nmap -sS 192.168.43.0/24
[sudo] password for hemanthmeda:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 17:38 IST
Nmap scan report for _gateway (192.168.43.1)
Host is up (0.015s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 62:8E:08:3C:74:2E (Unknown)

Nmap scan report for hemanthsLap (192.168.43.34)
Host is up (0.000014s latency).
All 1000 scanned ports on hemanthsLap (192.168.43.34) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (2 hosts up) scanned in 2.54 seconds
hemanthmeda@hemanthsLap:~$
```

```
hemanthmeda@hemanthsLap:~$ sudo tcpdump -i wlo1 -w ~/nmap_scan_capture.pcap

[sudo] password for hemanthmeda:

tcpdump: listening on wlo1, link-type EN10MB (Ethernet), snapshot length 26
2144 bytes
^C2552 packets captured
2552 packets received by filter
0 packets dropped by kernel
hemanthmeda@hemanthsLap:~$
```



Mon May 26 5:53:09 PM
56%
nmap_scan_capture.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
nmap_scan_capture.pcap
Packets: 2552
Profile: Default

```
No.     Time      Source                 Destination            Protocol  Length Info
      1 0.000000  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.1? Tell 192.168.43.34
      2 0.000026  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.2? Tell 192.168.43.34
      3 0.000034  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.3? Tell 192.168.43.34
      4 0.000041  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.4? Tell 192.168.43.34
      5 0.000073  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.5? Tell 192.168.43.34
      6 0.000084  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.6? Tell 192.168.43.34
      7 0.000093  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.7? Tell 192.168.43.34
      8 0.000100  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.8? Tell 192.168.43.34
      9 0.000123  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.9? Tell 192.168.43.34
     10 0.000133  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.10? Tell 192.168.43.34
     11 0.005981  62:8e:08:3c:74:2e     AzureWaveTec_c0:d2:…   ARP          42 192.168.43.1 is at 62:8e:08:3c:74:2e
     12 0.056388  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.13? Tell 192.168.43.34
     13 0.056398  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.14? Tell 192.168.43.34
     14 0.100277  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.17? Tell 192.168.43.34
     15 0.100289  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.18? Tell 192.168.43.34
     16 0.100293  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.19? Tell 192.168.43.34
     17 0.100297  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.20? Tell 192.168.43.34
     18 0.100305  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.21? Tell 192.168.43.34
     19 0.100311  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.22? Tell 192.168.43.34
     20 0.100316  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.23? Tell 192.168.43.34
     21 0.100321  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.24? Tell 192.168.43.34
     22 0.100326  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.25? Tell 192.168.43.34
     23 0.157016  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.28? Tell 192.168.43.34
     24 0.157052  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.29? Tell 192.168.43.34
     25 0.200858  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.32? Tell 192.168.43.34
     26 0.200898  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.33? Tell 192.168.43.34
     27 0.200907  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.35? Tell 192.168.43.34
     28 0.200915  AzureWaveTec_c0:d2:…  Broadcast              ARP          42 Who has 192.168.43.36? Tell 192.168.43.34
```

```
▾ Frame 14: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: May 26, 2025 17:38:20.314395000 IST
    UTC Arrival Time: May 26, 2025 12:08:20.314395000 UTC
    Epoch Arrival Time: 1748261300.314395000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.043879000 seconds]
    [Time delta from previous displayed frame: 0.043879000 seconds]
    [Time since reference or first frame: 0.100277000 seconds]
    Frame Number: 14
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
▾ Ethernet II, Src: AzureWaveTec_c0:d2:79 (c0:e4:34:c0:d2:79), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: AzureWaveTec_c0:d2:79 (c0:e4:34:c0:d2:79)
    Type: ARP (0x0806)
    [Stream index: 0]
▸ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff c0 e4  34 c0 d2 79 08 06 00 01   ········ 4··y····
0010  08 00 06 04 00 01 c0 e4  34 c0 d2 79 c0 a8 2b 22   ········ 4··y··+"
0020  00 00 00 00 00 00 c0 a8  2b 11                     ········ +·
```

7. Common services running on ports

port 53/tcp → domain(DNS) → DNS(Domain Name System) services translates domain names to IP addresses. Usually runs on routers pr dedicated DNS servers.

Commnon related ports and services:

80/tcp → HTTP → Web servers
443/tcp → HTTPS → Secure Web servers
22/tcp → SSH → Secure Shell for remote management
25/tcp → SMTP → Email sending service
53/udp → DNS → UDP variant for DNS queries (fast and connectionless)
21/tcp → FTP → File transfer protocol

445/tcp → SMB → Windows file sharing
23/tcp → telnet → Unencrypted remote login

8. Potential security risks from open ports.

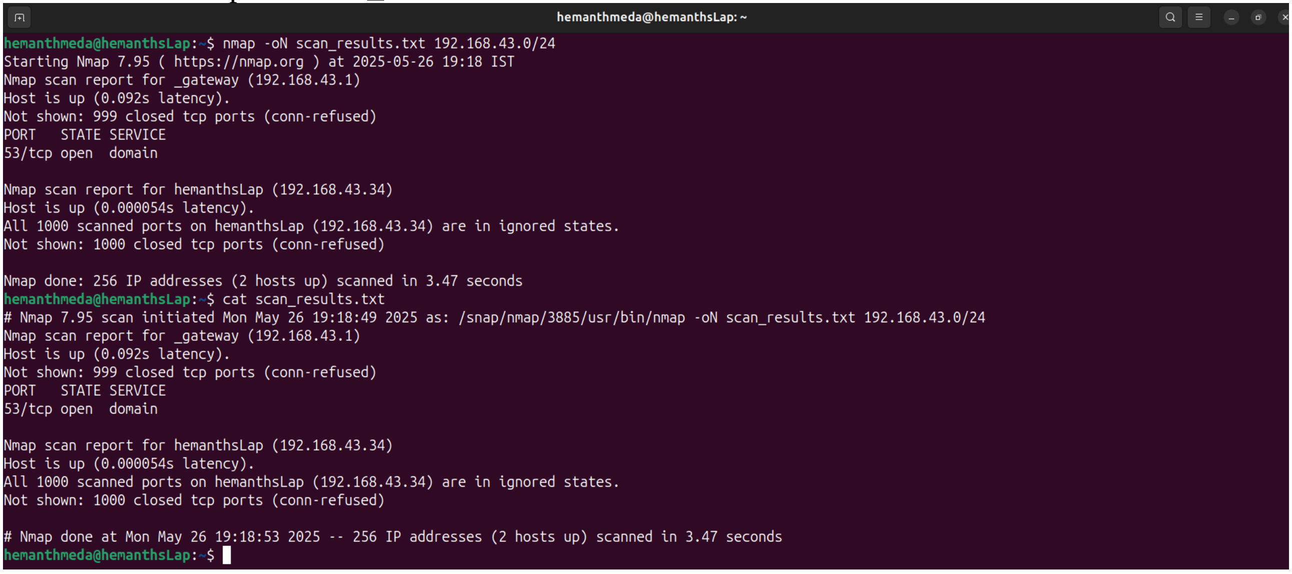
1) Port 53/tcp (DNS):

- if exposed externally or misconfigured, can be exploited fro DNS amplification/ reflection attacks (DdoS)
- Can leak network infrastructure information if zone transfers are allowed without restrictions.
- Internal exposure is usually less risky but still worth monitoring

No other open ports found with the this IP.

9. Scanning results as text files

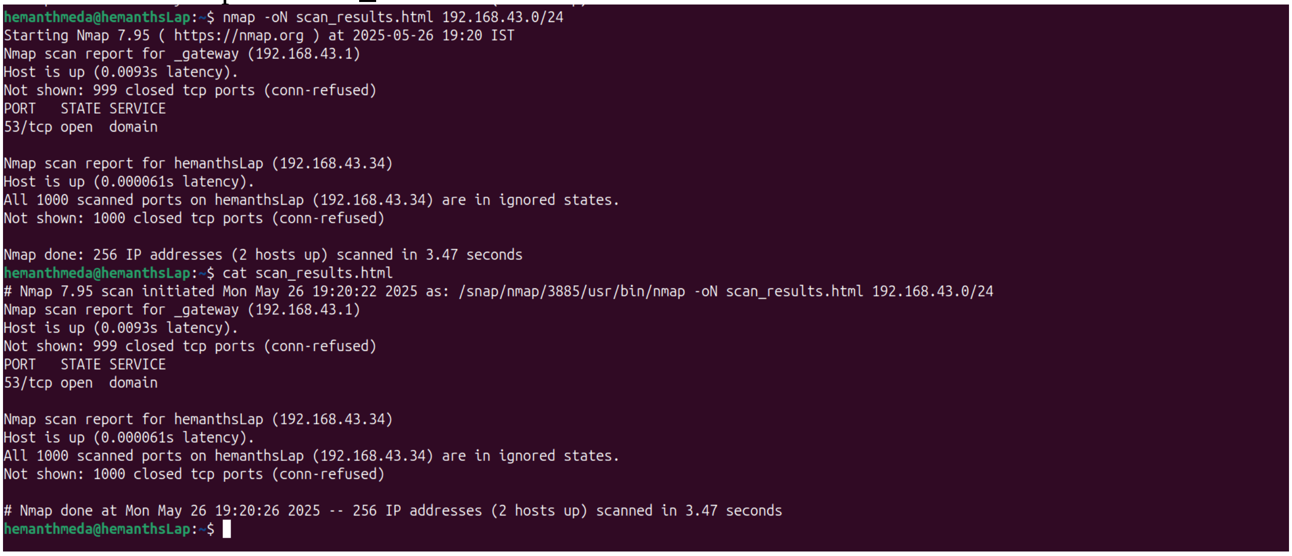
Command: nmap -oN scan_results.txt 192.168.43.0/24



```
hemanthmeda@hemanthsLap:~$ nmap -oN scan_results.txt 192.168.43.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 19:18 IST
Nmap scan report for _gateway (192.168.43.1)
Host is up (0.092s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for hemanthsLap (192.168.43.34)
Host is up (0.000054s latency).
All 1000 scanned ports on hemanthsLap (192.168.43.34) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (2 hosts up) scanned in 3.47 seconds
hemanthmeda@hemanthsLap:~$ cat scan_results.txt
# Nmap 7.95 scan initiated Mon May 26 19:18:49 2025 as: /snap/nmap/3885/usr/bin/nmap -oN scan_results.txt 192.168.43.0/24
Nmap scan report for _gateway (192.168.43.1)
Host is up (0.092s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for hemanthsLap (192.168.43.34)
Host is up (0.000054s latency).
All 1000 scanned ports on hemanthsLap (192.168.43.34) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

# Nmap done at Mon May 26 19:18:53 2025 -- 256 IP addresses (2 hosts up) scanned in 3.47 seconds
hemanthmeda@hemanthsLap:~$ 
```

10. Scanning results in HTML format

Command: nmap -oN scan_results.html 192.168.43.0/24



```
hemanthmeda@hemanthsLap:~$ nmap -oN scan_results.html 192.168.43.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 19:20 IST
Nmap scan report for _gateway (192.168.43.1)
Host is up (0.0093s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for hemanthsLap (192.168.43.34)
Host is up (0.000061s latency).
All 1000 scanned ports on hemanthsLap (192.168.43.34) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (2 hosts up) scanned in 3.47 seconds
hemanthmeda@hemanthsLap:~$ cat scan_results.html
# Nmap 7.95 scan initiated Mon May 26 19:20:22 2025 as: /snap/nmap/3885/usr/bin/nmap -oN scan_results.html 192.168.43.0/24
Nmap scan report for _gateway (192.168.43.1)
Host is up (0.0093s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for hemanthsLap (192.168.43.34)
Host is up (0.000061s latency).
All 1000 scanned ports on hemanthsLap (192.168.43.34) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

# Nmap done at Mon May 26 19:20:26 2025 -- 256 IP addresses (2 hosts up) scanned in 3.47 seconds
hemanthmeda@hemanthsLap:~$ 
```