# 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)**

1. Checking the version of Nmap by using following command:
   nmap -v

```
└─# nmap -v
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 17:11 IST
Read data files from: /usr/share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.09 seconds
           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```

2. Local Ip address is 192.168.1.4

```
 Connection-specific DNS Suffix  . :
 IPv6 Address. . . . . . . . . . . : 2401:4900:1c34:1557:9c3:cf7f:614b:5db5
 Temporary IPv6 Address. . . . . . : 2401:4900:1c34:1557:6177:2879:3150:13f2
 Link-local IPv6 Address . . . . . : fe80::415d:71a2:d23c:917b%3
 IPv4 Address. . . . . . . . . . . : 192.168.1.4
 Subnet Mask . . . . . . . . . . . : 255.255.255.0
 Default Gateway . . . . . . . . . : fe80::1%3
                                     192.168.1.1
```

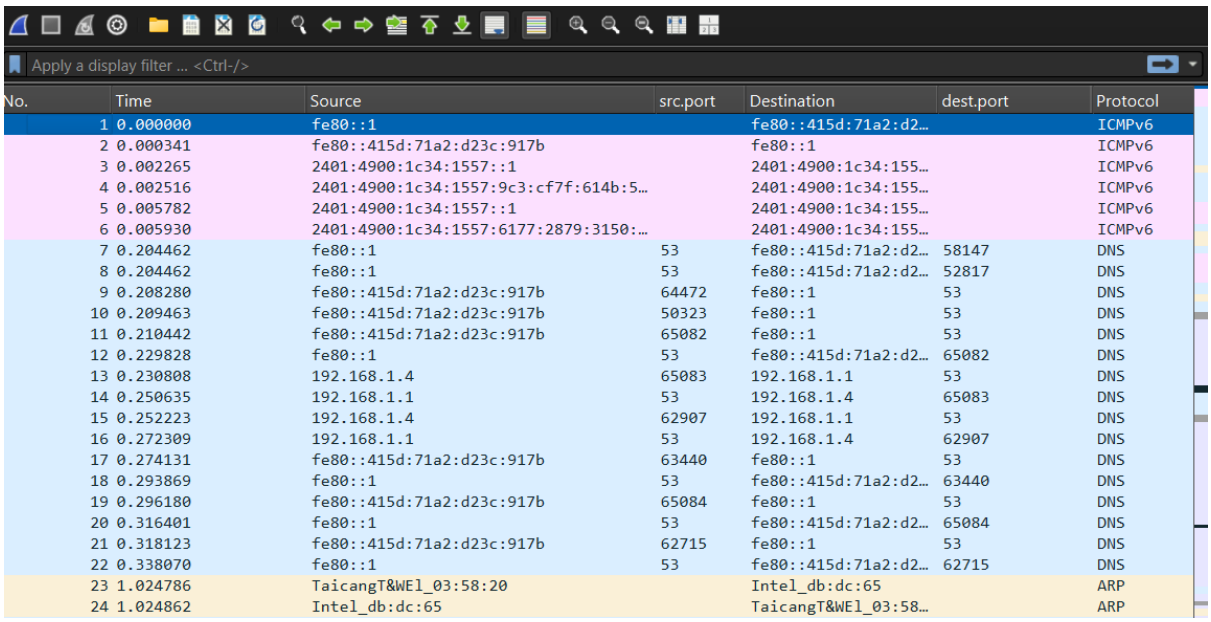
3. Scan the network by using the following command:
   nmap -sS -Pn -T4 192.168.1.4

```
└─# nmap -sS -T4 -Pn 192.168.1.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 17:16 IST
Nmap scan report for 192.168.1.4
Host is up (0.0019s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
903/tcp  open  iss-console-mgr
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 56.46 seconds
```

4. Open ports found are:
   i. 903/tcp - open - iss-console-mgr
   ii. 5357/tcp - open - wsdapi

5. Capturing packets using wireshark:



Apply a display filter ... <Ctrl-/>

| No. | Time | Source | src.port | Destination | dest.port | Protocol |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | fe80::1 | | fe80::415d:71a2:d2… | | ICMPv6 |
| 2 | 0.000341 | fe80::415d:71a2:d23c:917b | | fe80::1 | | ICMPv6 |
| 3 | 0.002265 | 2401:4900:1c34:1557::1 | | 2401:4900:1c34:155… | | ICMPv6 |
| 4 | 0.002516 | 2401:4900:1c34:1557:9c3:cf7f:614b:5… | | 2401:4900:1c34:155… | | ICMPv6 |
| 5 | 0.005782 | 2401:4900:1c34:1557::1 | | 2401:4900:1c34:155… | | ICMPv6 |
| 6 | 0.005930 | 2401:4900:1c34:1557:6177:2879:3150:… | | 2401:4900:1c34:155… | | ICMPv6 |
| 7 | 0.204462 | fe80::1 | 53 | fe80::415d:71a2:d2… | 58147 | DNS |
| 8 | 0.204462 | fe80::1 | 53 | fe80::415d:71a2:d2… | 52817 | DNS |
| 9 | 0.208280 | fe80::415d:71a2:d23c:917b | 64472 | fe80::1 | 53 | DNS |
| 10 | 0.209463 | fe80::415d:71a2:d23c:917b | 50323 | fe80::1 | 53 | DNS |
| 11 | 0.210442 | fe80::415d:71a2:d23c:917b | 65082 | fe80::1 | 53 | DNS |
| 12 | 0.229828 | fe80::1 | 53 | fe80::415d:71a2:d2… | 65082 | DNS |
| 13 | 0.230808 | 192.168.1.4 | 65083 | 192.168.1.1 | 53 | DNS |
| 14 | 0.250635 | 192.168.1.1 | 53 | 192.168.1.4 | 65083 | DNS |
| 15 | 0.252223 | 192.168.1.4 | 62907 | 192.168.1.1 | 53 | DNS |
| 16 | 0.272309 | 192.168.1.1 | 53 | 192.168.1.4 | 62907 | DNS |
| 17 | 0.274131 | fe80::415d:71a2:d23c:917b | 63440 | fe80::1 | 53 | DNS |
| 18 | 0.293869 | fe80::1 | 53 | fe80::415d:71a2:d2… | 63440 | DNS |
| 19 | 0.296180 | fe80::415d:71a2:d23c:917b | 65084 | fe80::1 | 53 | DNS |
| 20 | 0.316401 | fe80::1 | 53 | fe80::415d:71a2:d2… | 65084 | DNS |
| 21 | 0.318123 | fe80::415d:71a2:d23c:917b | 62715 | fe80::1 | 53 | DNS |
| 22 | 0.338070 | fe80::1 | 53 | fe80::415d:71a2:d2… | 62715 | DNS |
| 23 | 1.024786 | TaicangT&WEl_03:58:20 | | Intel_db:dc:65 | | ARP |
| 24 | 1.024862 | Intel_db:dc:65 | | TaicangT&WEl_03:58… | | ARP |

6. Saving scan as text file using the following command:

   nmap -oN task1_output.txt -Pn 192.168.1.4

```
└─# cat task1_output.txt
# Nmap 7.95 scan initiated Mon May 26 17:25:39 2025 as: /usr/lib/nmap/nmap -oN task1_output.txt -Pn 192.168.1.4
Nmap scan report for 192.168.1.4
Host is up (0.0015s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE
903/tcp  open  iss-console-mgr
5357/tcp open  wsdapi

# Nmap done at Mon May 26 17:26:36 2025 -- 1 IP address (1 host up) scanned in 56.50 seconds
```