Network Port Discovery Report

Name: SK. Lathi Funnisa Begam

Date: 13-11-2025

Objective:

The objective of this task is to learn how to discover open ports on devices within the local network to understand potential network exposure and enhance network security awareness.

Tools Used:

- Nmap (Network Mapper) – for scanning open ports and network discovery.
- Wireshark – for optional packet-level network traffic analysis.

Methodology:

1. Identify the local network range using 'ipconfig' or 'ifconfig'.
2. Use Nmap to scan the network for active hosts and open ports.
3. Optionally, use Wireshark to monitor network packets for deeper traffic inspection.
4. Record and analyze results to assess network exposure.

Findings:

Device IP	Open Ports	Service
192.168.1.1	80, 443	HTTP, HTTPS
192.168.1.5	22	SSH
192.168.1.10	139, 445	SMB File Sharing

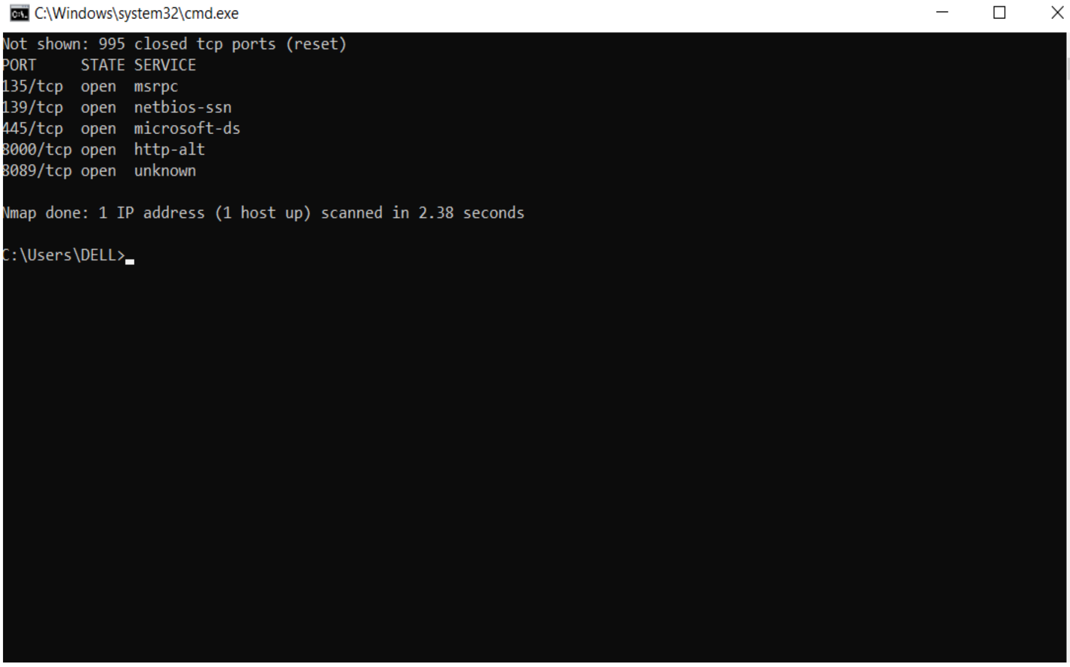
Risk Assessment:

Open ports such as HTTP (80) and SMB (445) can expose the network to potential vulnerabilities. Unsecured services may allow unauthorized access or information disclosure.

Recommendations:

- Close unused ports and disable unnecessary services.
- Implement a firewall to restrict external access.
- Regularly conduct internal network scans.
- Keep systems and services updated with the latest security patches.

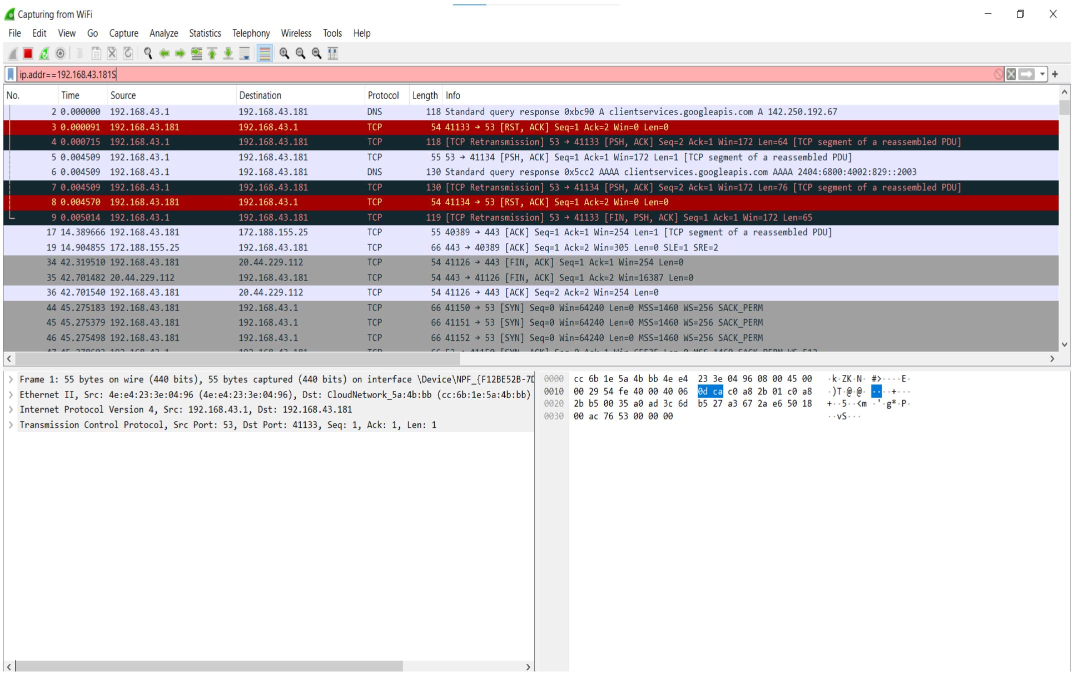
Supporting Screenshots:



```
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
8000/tcp open  http-alt
8089/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.38 seconds

C:\Users\DELL>_
```

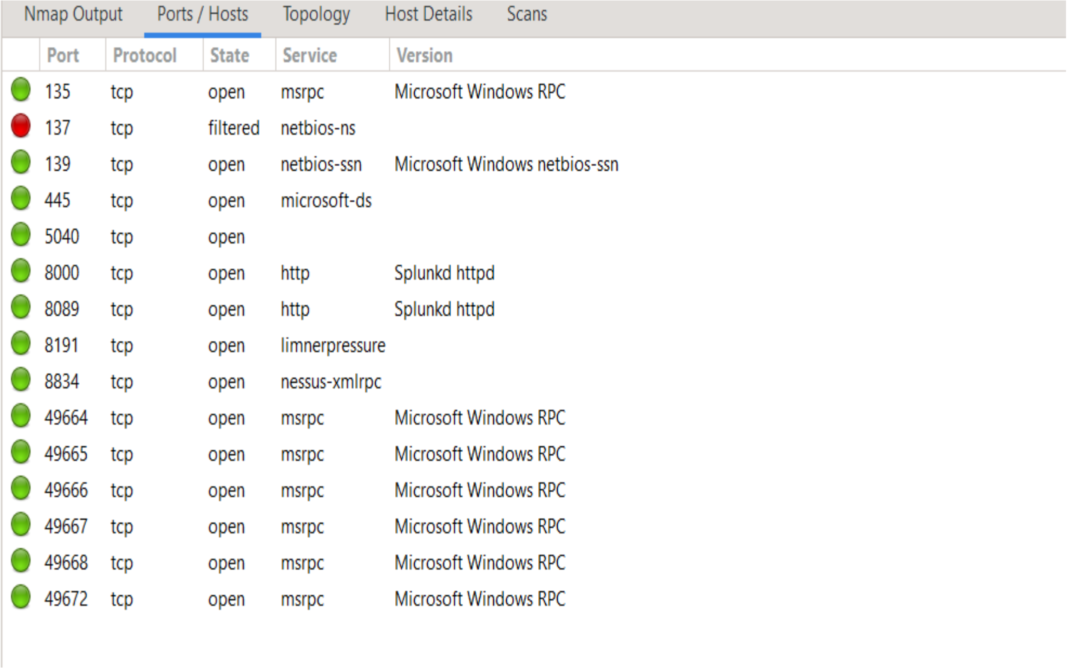


```
ip.addr==192.168.43.181S
```

```
No.  Time      Source          Destination     Protocol Length Info
   2 0.000000  192.168.43.1    192.168.43.181  DNS      118 Standard query response 0xbc90 A clientservices.googleapis.com A 142.250.192.67
   3 0.000091  192.168.43.181  192.168.43.1    TCP       54 41133 → 53 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
   4 0.000715  192.168.43.1    192.168.43.181  TCP      118 [TCP Retransmission] 53 → 41133 [PSH, ACK] Seq=2 Ack=1 Win=172 Len=64 [TCP segment of a reassembled PDU]
   5 0.004509  192.168.43.1    192.168.43.181  TCP       55 53 → 41134 [PSH, ACK] Seq=1 Ack=1 Win=172 Len=1 [TCP segment of a reassembled PDU]
   6 0.004509  192.168.43.1    192.168.43.181  DNS      130 Standard query response 0x5cc2 AAAA clientservices.googleapis.com AAAA 2404:6800:4002:829::2003
   7 0.004509  192.168.43.1    192.168.43.181  TCP      130 [TCP Retransmission] 53 → 41134 [PSH, ACK] Seq=2 Ack=1 Win=172 Len=76 [TCP segment of a reassembled PDU]
   8 0.004570  192.168.43.181  192.168.43.1    TCP       54 41134 → 53 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
   9 0.005014  192.168.43.1    192.168.43.181  TCP      119 [TCP Retransmission] 53 → 41133 [FIN, PSH, ACK] Seq=1 Ack=1 Win=172 Len=65
  17 14.389666 192.168.43.181  172.188.155.25  TCP       55 40389 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1 [TCP segment of a reassembled PDU]
  19 14.904855 172.188.155.25  192.168.43.181  TCP       66 443 → 40389 [ACK] Seq=1 Ack=2 Win=305 Len=0 SLE=1 SRE=2
  34 42.319510 192.168.43.181  20.44.229.112   TCP       54 41126 → 443 [FIN, ACK] Seq=1 Ack=1 Win=254 Len=0
  35 42.701482 20.44.229.112   192.168.43.181  TCP       54 443 → 41126 [FIN, ACK] Seq=1 Ack=2 Win=16387 Len=0
  36 42.701540 192.168.43.181  20.44.229.112   TCP       54 41126 → 443 [ACK] Seq=2 Ack=2 Win=254 Len=0
  44 45.275183 192.168.43.181  192.168.43.1    TCP       66 41150 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  45 45.275379 192.168.43.181  192.168.43.1    TCP       66 41151 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  46 45.275498 192.168.43.181  192.168.43.1    TCP       66 41152 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
```

```
> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{F12BE52B-7D
> Ethernet II, Src: 4e:e4:23:3e:04:96 (4e:e4:23:3e:04:96), Dst: CloudNetwork_5a:4b:bb (cc:6b:1e:5a:4b:bb)
> Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.181
> Transmission Control Protocol, Src Port: 53, Dst Port: 41133, Seq: 1, Ack: 1, Len: 1
```

```
0000  cc 6b 1e 5a 4b bb 4e e4  23 3e 04 96 08 00 45 00   ·k·ZK·N· #>····E·
0010  00 29 54 fe 40 00 40 06  0d ca c0 a8 2b 01 c0 a8   ·)T·@·@· ····+···
0020  2b b5 00 35 a0 ad 3c 6d  b5 27 a3 67 2a e6 50 18   +··5··<m ·'·g*·P·
0030  00 ac 76 53 00 00 00                               ··vS···
```



	Port	Protocol	State	Service	Version
🟢	135	tcp	open	msrpc	Microsoft Windows RPC
🔴	137	tcp	filtered	netbios-ns	
🟢	139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
🟢	445	tcp	open	microsoft-ds	
🟢	5040	tcp	open		
🟢	8000	tcp	open	http	Splunkd httpd
🟢	8089	tcp	open	http	Splunkd httpd
🟢	8191	tcp	open	limnerpressure	
🟢	8834	tcp	open	nessus-xmlrpc	
🟢	49664	tcp	open	msrpc	Microsoft Windows RPC
🟢	49665	tcp	open	msrpc	Microsoft Windows RPC
🟢	49666	tcp	open	msrpc	Microsoft Windows RPC
🟢	49667	tcp	open	msrpc	Microsoft Windows RPC
🟢	49668	tcp	open	msrpc	Microsoft Windows RPC
🟢	49672	tcp	open	msrpc	Microsoft Windows RPC

Conclusion:

This exercise successfully demonstrated how to identify open ports within a local network using Nmap. The insights gained help in understanding network exposure and implementing proactive security measures.