

TASK1: Local Network Open Port Scan Report

◆ Objective:

To discover open ports on devices within the local network using Nmap, and assess potential exposure risks.

◆ Tools Used:

- **Nmap**
- **Wireshark** (for packet capture)
- **Python3 HTTP server**
- **Netcat**
- **VirtualBox (Kali Linux VM)**

◆ Target:

Device IP: 192.168.0.105

◆ Procedure:

1. Installed Nmap and identified the local IP (192.168.0.105).
2. Ran various Nmap scans, initially found all ports closed.

```
[root@kali)-[~]
# nmap -p 80,1234 192.168.0.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 18:22 IST
Nmap scan report for 192.168.0.105
Host is up (0.000036s latency).

PORT      STATE    SERVICE
80/tcp    open     http
1234/tcp  closed   hotline

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds

[root@kali)-[~]
# nmap -sS -sV 192.168.0.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 18:24 IST
Nmap scan report for 192.168.0.105
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.0.105 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds

[root@kali)-[~]
# nmap -sS 192.168.0.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 18:24 IST
Nmap scan report for 192.168.0.105
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.0.105 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds

[root@kali)-[~]
# _
```

3. Started temporary services:

- o python3 -m http.server 80 → Opened **port 80**
- o nc -lvpn 1234 → Opened **port 1234**

```
[root@kali]# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
[sudo] nc -lvpn 1234
```

4. Performed scans:

nmap -p 80,1234 192.168.0.105

```
[root@kali]# nmap -p 80,1234 192.168.0.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 18:22 IST
Nmap scan report for 192.168.0.105
Host is up (0.000036s latency).

PORT      STATE SERVICE
80/tcp    open  http
1234/tcp  closed hotline

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

5. Also performed multiple scans on different IP:

```
[root@kali]# nmap 148.72.90.78 -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-06 00:43 IST
Nmap scan report for 78.90.72.148.host.secureserver.net (148.72.90.78)
Host is up (0.13s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftpd
30/tcp    open  http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
443/tcp   open  https?
3443/tcp open  ssl/http Microsoft IIS httpd 10.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.07 seconds
```



```
[root@kali]# nmap 148.72.90.78 -sS
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-06 00:44 IST
Nmap scan report for 78.90.72.148.host.secureserver.net (148.72.90.78)
Host is up (0.11s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
30/tcp    open  http
443/tcp   open  https
3443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 18.65 seconds
```

```

└──(root㉿kali)-[~]
  # nmap 148.72.90.78 -sn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-06 00:45 IST
Nmap scan report for 78.90.72.148.host.secureserver.net (148.72.90.78)
Host is up (0.064s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds

└──(root㉿kali)-[~]
  # nmap 148.72.90.78 -o
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-06 00:45 IST
Nmap scan report for 78.90.72.148.host.secureserver.net (148.72.90.78)
Host is up (0.14s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
8443/tcp  open  https-alt
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10 (92%)
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Windows Server 2019 (92%), Microsoft Windows 10 1903 - 21H1 (85%)
No exact OS matches for host (test conditions non-ideal).

```

6. Observed open ports using both Nmap and Wireshark.

◆ Results:

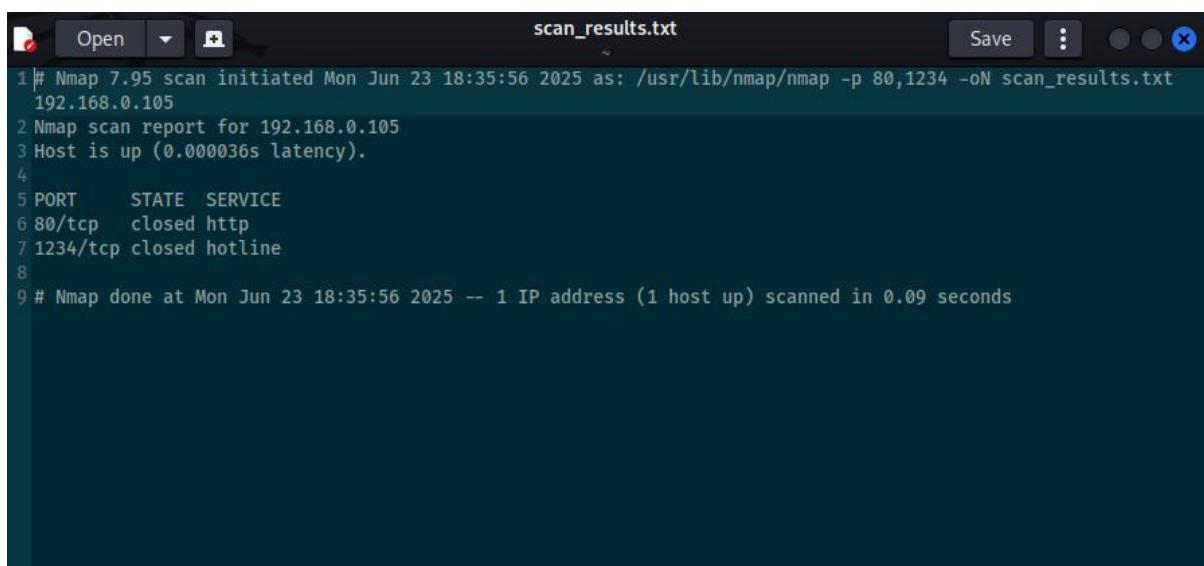
Port State Service Details

80 open http Python HTTP server

1234 open unknown Netcat listener

Scan saved as:

- Text: scan_result.txt
- HTML: scan.html



```

scan_results.txt
1 # Nmap 7.95 scan initiated Mon Jun 23 18:35:56 2025 as: /usr/lib/nmap/nmap -p 80,1234 -oN scan_results.txt
192.168.0.105
2 Nmap scan report for 192.168.0.105
3 Host is up (0.000036s latency).
4
5 PORT      STATE SERVICE
6 80/tcp    closed http
7 1234/tcp  closed hotline
8
9 # Nmap done at Mon Jun 23 18:35:56 2025 -- 1 IP address (1 host up) scanned in 0.09 seconds

```

◆ Wireshark Observation:

TCP 3-way handshake observed:

- SYN → SYN-ACK → ACK on port 80 and 1234

Filter used:

```
tcp.port == 80 || tcp.port == 1234
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000	192.168.0.105	192.168.0.105	>=> TCP	SYN = s 0, Win 63J 642<	
2	0.01771	192.168.0.105	192.168.0.105	=> TCP	SYN-ACK = [50] 5eq;	
3	0.34223	192.168.0.104	192.168.0.105	>=> TCP	ACK = s 1, Ack=1 60	
4	0.24997	192.168.0.104	192.168.0.105	40 TCP	SYN = 50, port 80 80	
5	0.55232	192.168.0.104	192.168.0.105	>=> TCP	SYN-ACK = [50] Seq.	
6	0.65231	192.168.0.104	192.168.0.105	60 TCP	ACK = s 1, Ack=12 60	
7	0.49973	192.168.0.105	192.168.0.105	134 TCP	ACK = s 1, ack=12 1234	

◆ Risk Analysis:

Port	Risk	Mitigation
80	Unencrypted HTTP, info leakage	Use HTTPS or close when unused
1234	Custom port — could be exploited	Monitor or close

◆ Conclusion:

Nmap and Wireshark effectively helped identify and monitor open ports and traffic. Services running on ports should always be monitored to prevent unauthorized access.