TASK 1: SCAN YOUR LOCAL NETWORK FOR OPEN PORTS USING NMAP

Objective:

Learn to discover open ports on devices in your local network to understand potential exposure and assess risks.

Tools Used:

- Nmap (required)
- Wireshark (optional)

Procedure:

Step 1: Install Nmap

1. Visit https://nmap.org/download.html.
2. Download the **Windows self-installer**.
3. Run the installer and ensure **Npcap** is selected during setup.
4. Check wheather nmap has been installed in your PC. In command prompt type the following command:
    - nmap --version

Step 2: Find Your Local IP Range

1. Open Command Prompt and type:
    - ipconfig
2. Note your **IPv4 Address** (e.g., 192.168.149.230) and **Subnet Mask** (255.255.255.0).
3. From this, deduce your local network:
   → **IP range**: 192.168.149.0/24

Step 3: Run Nmap Scan

Start a TCP SYN scan on the entire subnet:

- nmap -sS -Pn 192.168.149.0/24
    - -sS: TCP SYN scan (stealthy and fast)

- -Pn: Skip ping; scan all devices

This will list all live hosts and their open ports.

Step 4: Note Down IP Addresses and Open Ports

Example result:

IP Address	Open Ports
192.168.149.230	80, 135, 139, 1024

Step 5 (Optional): Analyze Traffic with Wireshark

1. Open Wireshark (install Wireshark if not done in your PC).
2. Select your **active network interface** (Wi-Fi or Ethernet).
3. Start a capture.
4. While capturing, run your Nmap scan.
5. Stop the capture and apply filters like:
    - tcp.flags.syn == 1 → Show SYN packets
    - tcp.port == 445 → Show SMB traffic
    - ip.addr == 192.168.149.230 → Filter your device traffic

Step 6: Research Common Services on Open Ports

Port	Service	Use
80	HTTP	Unsecured web traffic
135	MSRPC	Windows remote procedure call
139	NetBIOS	Legacy Windows file/printer sharing
445	SMB	File sharing (commonly exploited)
1024	Dynamic Port	Often app-specific or temporary

Resources:

- nmap.org/services.html
- speedguide.net/ports.php

Step 7: Identify Security Risks

A risk analysis is performed under some basic criteria.

Risk Table:

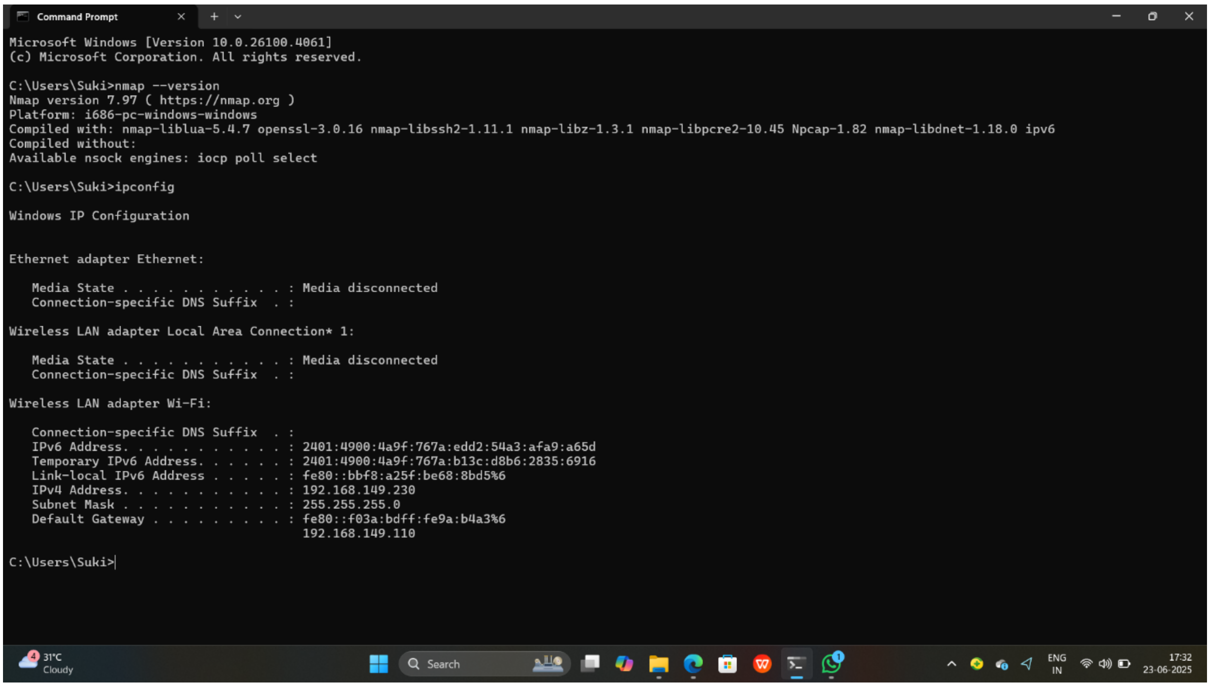
Port	Service	Needed?	Exposed?	Encrypted?	Updated?	Risk Level	Action
80	HTTP	No	No	No	Yes	Medium	Use HTTPS or disable
135	MSRPC	Yes	No	No	Yes	Medium	Internal only
139	NetBIOS	No	No	No	Yes	High	Disable NetBIOS
445	SMB	No	Yes	No	Unknown	High	Block on firewall
1024	Dynamic	Unknown	No	No	Unknown	Medium	Investigate

Step 8: Save Scan Results

To save the results as a text file use the following command:

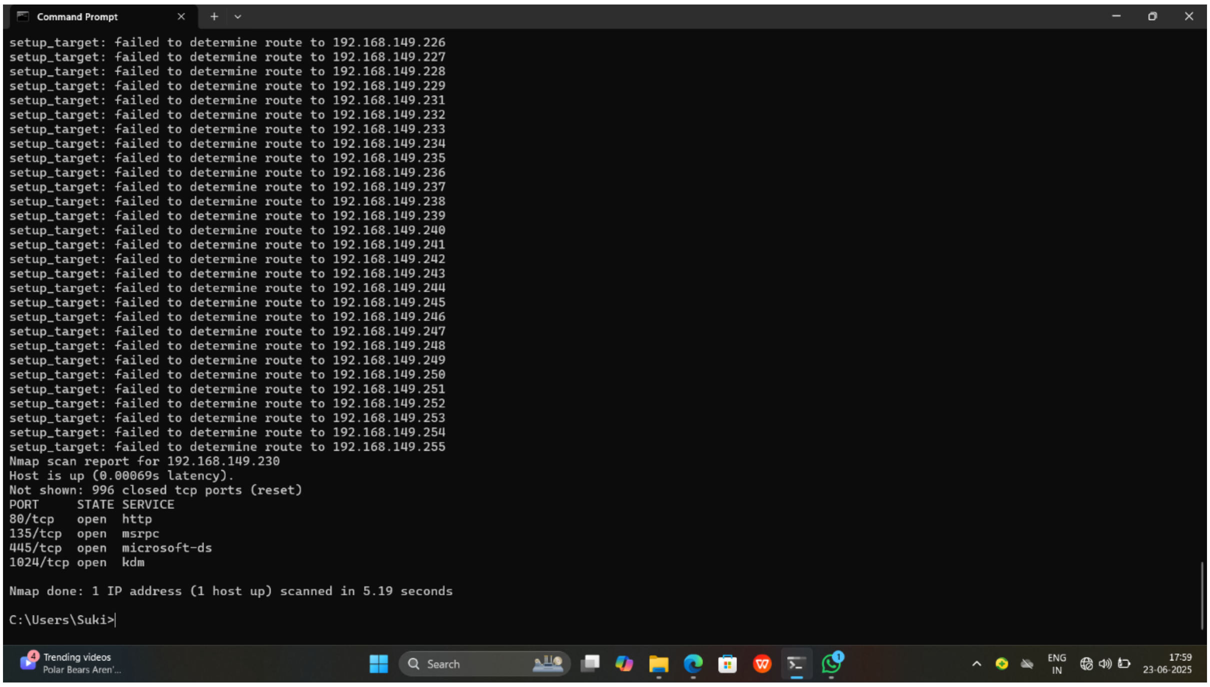
nmap -sS -Pn 192.168.149.0/24 -oN scan_result.txt

Screenshots:



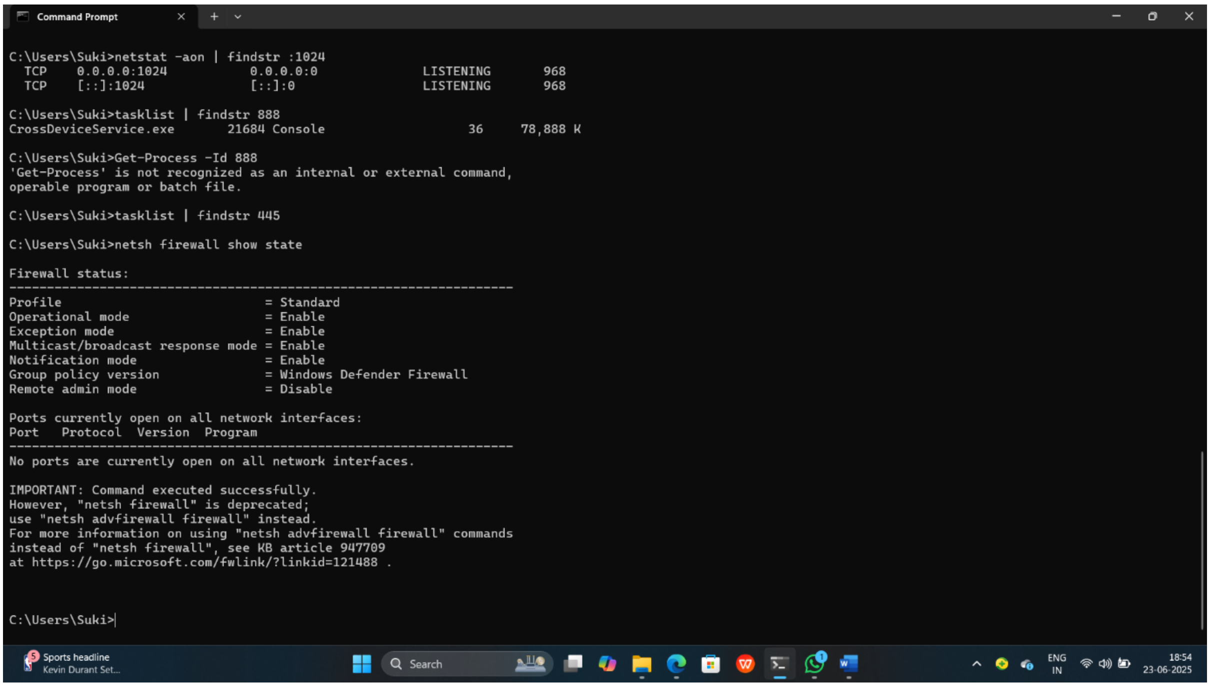
```
Microsoft Windows [Version 10.0.26100.4061]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Suki>nmap --version
Nmap version 7.97 ( https://nmap.org )
Platform: i686-pc-windows-windows
Compiled with: nmap-liblua-5.4.7 openssl-3.0.16 nmap-libssh2-1.11.1 nmap-libz-1.3.1 nmap-libpcre2-10.45 Npcap-1.82 nmap-libdnet-1.18.0 ipv6
Compiled without:
Available nsock engines: iocp poll select

C:\Users\Suki>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:4a9f:767a:edd2:54a3:afa9:a65d
   Temporary IPv6 Address. . . . . . : 2401:4900:4a9f:767a:b13c:d8b6:2835:6916
   Link-local IPv6 Address . . . . . : fe80::bbf8:a25f:be68:8bd5%6
   IPv4 Address. . . . . . . . . . . : 192.168.149.230
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::f03a:bdff:fe9a:b4a3%6
                                       192.168.149.110

C:\Users\Suki>
```

Fig. 1



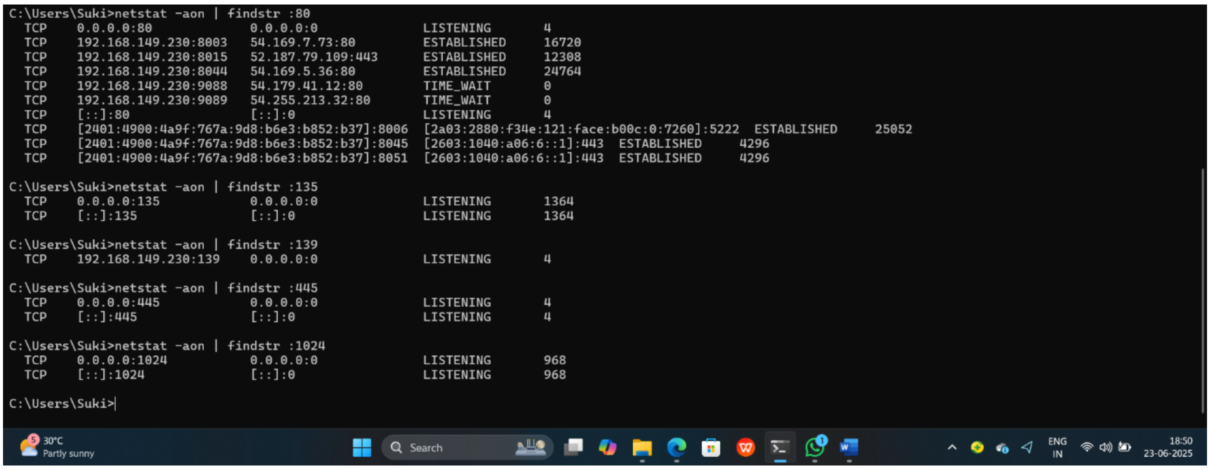
```
setup_target: failed to determine route to 192.168.149.226
setup_target: failed to determine route to 192.168.149.227
setup_target: failed to determine route to 192.168.149.228
setup_target: failed to determine route to 192.168.149.229
setup_target: failed to determine route to 192.168.149.231
setup_target: failed to determine route to 192.168.149.232
setup_target: failed to determine route to 192.168.149.233
setup_target: failed to determine route to 192.168.149.234
setup_target: failed to determine route to 192.168.149.235
setup_target: failed to determine route to 192.168.149.236
setup_target: failed to determine route to 192.168.149.237
setup_target: failed to determine route to 192.168.149.238
setup_target: failed to determine route to 192.168.149.239
setup_target: failed to determine route to 192.168.149.240
setup_target: failed to determine route to 192.168.149.241
setup_target: failed to determine route to 192.168.149.242
setup_target: failed to determine route to 192.168.149.243
setup_target: failed to determine route to 192.168.149.244
setup_target: failed to determine route to 192.168.149.245
setup_target: failed to determine route to 192.168.149.246
setup_target: failed to determine route to 192.168.149.247
setup_target: failed to determine route to 192.168.149.248
setup_target: failed to determine route to 192.168.149.249
setup_target: failed to determine route to 192.168.149.250
setup_target: failed to determine route to 192.168.149.251
setup_target: failed to determine route to 192.168.149.252
setup_target: failed to determine route to 192.168.149.253
setup_target: failed to determine route to 192.168.149.254
setup_target: failed to determine route to 192.168.149.255
Nmap scan report for 192.168.149.230
Host is up (0.00069s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1024/tcp open  kdm

Nmap done: 1 IP address (1 host up) scanned in 5.19 seconds

C:\Users\Suki>
```

Fig. 2



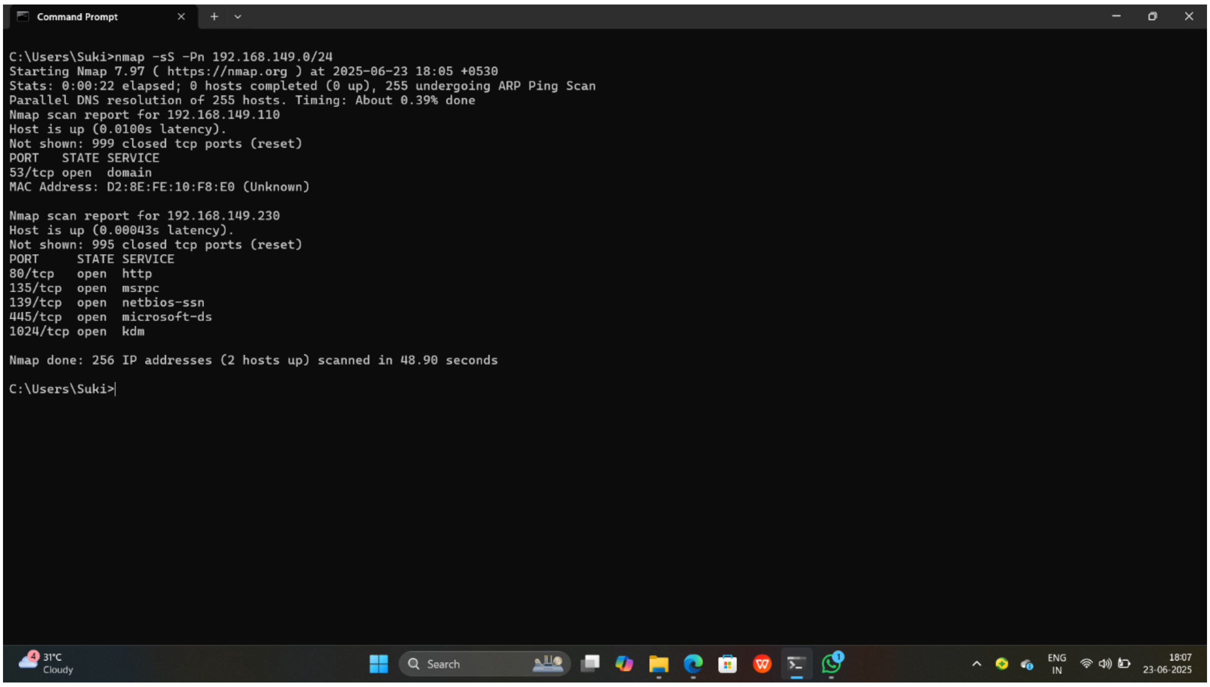
```
C:\Users\Suki>netstat -aon | findstr :1024
  TCP    0.0.0.0:1024           0.0.0.0:0              LISTENING       968
  TCP    [::]:1024              [::]:0                 LISTENING       968

C:\Users\Suki>tasklist | findstr 888
CrossDeviceService.exe       21684 Console                   36     78,888 K

C:\Users\Suki>Get-Process -Id 888
'Get-Process' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Suki>tasklist | findstr 445

C:\Users\Suki>netsh firewall show state

Firewall status:
-------------------------------------------------------------------
Profile                           = Standard
Operational mode                  = Enable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Enable
Group policy version              = Windows Defender Firewall
Remote admin mode                 = Disable

Ports currently open on all network interfaces:
Port   Protocol  Version  Program
-------------------------------------------------------------------
No ports are currently open on all network interfaces.

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at https://go.microsoft.com/fwlink/?linkid=121488 .


C:\Users\Suki>
```

Fig. 3



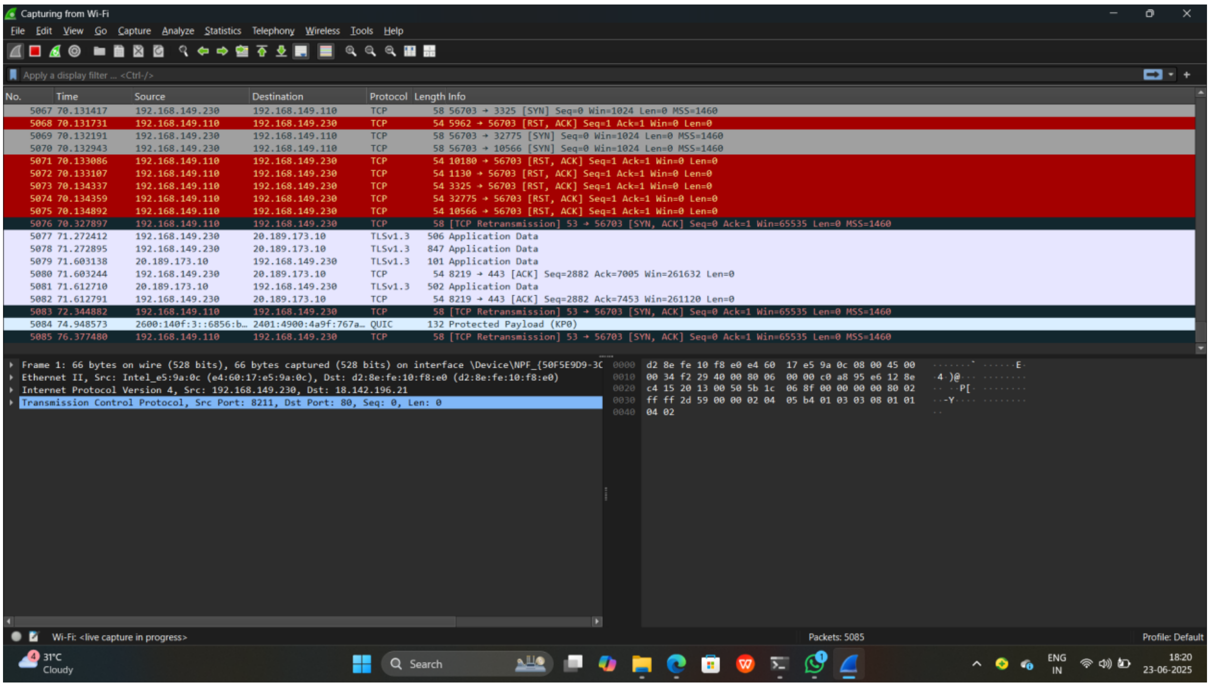
```
C:\Users\Suki>netstat -aon | findstr :80
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    192.168.149.230:8003   54.169.7.73:80         ESTABLISHED     16720
  TCP    192.168.149.230:8015   52.187.79.109:443      ESTABLISHED     12308
  TCP    192.168.149.230:8044   54.169.5.36:80         ESTABLISHED     24764
  TCP    192.168.149.230:9088   54.179.41.12:80        TIME_WAIT       0
  TCP    192.168.149.230:9089   54.255.213.32:80       TIME_WAIT       0
  TCP    [::]:80                [::]:0                 LISTENING       4
  TCP    [2401:4900:4a9f:767a:9d8:b6e3:b852:b37]:8006  [2a03:2880:f34e:121:face:b00c:0:7260]:5222  ESTABLISHED     25052
  TCP    [2401:4900:4a9f:767a:9d8:b6e3:b852:b37]:8045  [2603:1040:a06:6::1]:443  ESTABLISHED     4296
  TCP    [2401:4900:4a9f:767a:9d8:b6e3:b852:b37]:8051  [2603:1040:a06:6::1]:443  ESTABLISHED     4296

C:\Users\Suki>netstat -aon | findstr :135
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1364
  TCP    [::]:135               [::]:0                 LISTENING       1364

C:\Users\Suki>netstat -aon | findstr :139
  TCP    192.168.149.230:139    0.0.0.0:0              LISTENING       4

C:\Users\Suki>netstat -aon | findstr :445
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    [::]:445               [::]:0                 LISTENING       4

C:\Users\Suki>netstat -aon | findstr :1024
  TCP    0.0.0.0:1024           0.0.0.0:0              LISTENING       968
  TCP    [::]:1024              [::]:0                 LISTENING       968

C:\Users\Suki>
```

Fig. 4



```
C:\Users\Suki>nmap -sS -Pn 192.168.149.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2025-06-23 18:05 +0530
Stats: 0:00:22 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
Parallel DNS resolution of 255 hosts. Timing: About 0.39% done
Nmap scan report for 192.168.149.110
Host is up (0.0100s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: D2:8E:FE:10:F8:E0 (Unknown)

Nmap scan report for 192.168.149.230
Host is up (0.00043s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1024/tcp open  kdm

Nmap done: 256 IP addresses (2 hosts up) scanned in 48.90 seconds

C:\Users\Suki>
```

Fig. 5



Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
31°C
Cloudy
Search
ENG
IN
18:20
23-06-2025

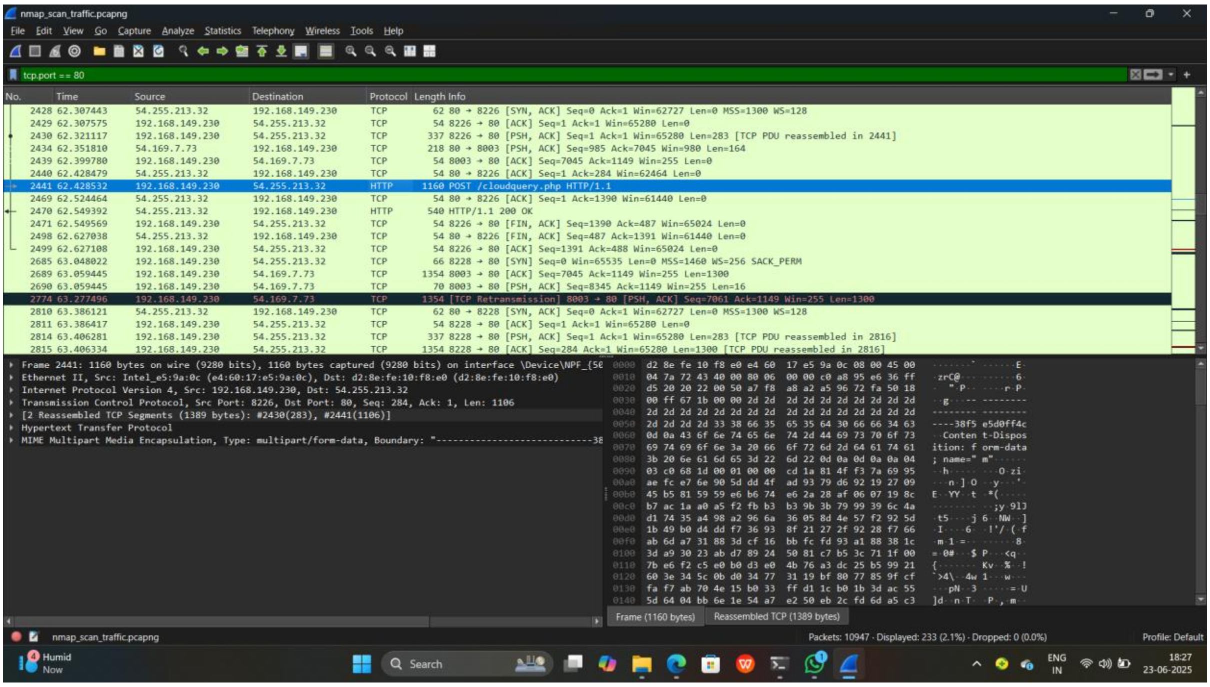
```
No.   Time       Source              Destination       Protocol Length Info
 5067 70.131417  192.168.149.230     192.168.149.110   TCP        58 56703 → 3325 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 5068 70.131731  192.168.149.110     192.168.149.230   TCP        54 5962 → 56703 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 5069 70.132191  192.168.149.230     192.168.149.110   TCP        58 56703 → 32775 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 5070 70.132943  192.168.149.230     192.168.149.110   TCP        58 56703 → 10566 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 5071 70.133086  192.168.149.110     192.168.149.230   TCP        54 10180 → 56703 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 5072 70.133107  192.168.149.110     192.168.149.230   TCP        54 1130 → 56703 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 5073 70.134337  192.168.149.110     192.168.149.230   TCP        54 3325 → 56703 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 5074 70.134359  192.168.149.110     192.168.149.230   TCP        54 32775 → 56703 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 5075 70.134892  192.168.149.110     192.168.149.230   TCP        54 10566 → 56703 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 5076 70.327897  192.168.149.110     192.168.149.230   TCP        58 [TCP Retransmission] 53 → 56703 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
 5077 71.272412  192.168.149.230     20.189.173.10     TLSv1.3   506 Application Data
 5078 71.272895  192.168.149.230     20.189.173.10     TLSv1.3   847 Application Data
 5079 71.603138  20.189.173.10       192.168.149.230   TLSv1.3   101 Application Data
 5080 71.603244  192.168.149.230     20.189.173.10     TCP        54 8219 → 443 [ACK] Seq=2882 Ack=7005 Win=261632 Len=0
 5081 71.612710  20.189.173.10       192.168.149.230   TLSv1.3   502 Application Data
 5082 71.612791  192.168.149.230     20.189.173.10     TCP        54 8219 → 443 [ACK] Seq=2882 Ack=7453 Win=261120 Len=0
 5083 72.344882  192.168.149.110     192.168.149.230   TCP        58 [TCP Retransmission] 53 → 56703 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
 5084 74.948573  2600:140f:3::6856:b… 2401:4900:4a9f:767a… QUIC 132 Protected Payload (KP0)
 5085 76.377480  192.168.149.110     192.168.149.230   TCP        58 [TCP Retransmission] 53 → 56703 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
```

```
▸ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{50F5E9D9-3C
▸ Ethernet II, Src: Intel_e5:9a:0c (e4:60:17:e5:9a:0c), Dst: d2:8e:fe:10:f8:e0 (d2:8e:fe:10:f8:e0)
▸ Internet Protocol Version 4, Src: 192.168.149.230, Dst: 18.142.196.21
▸ Transmission Control Protocol, Src Port: 8211, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  d2 8e fe 10 f8 e0 e4 60  17 e5 9a 0c 08 00 45 00   ·······` ······E·
0010  00 34 f2 29 40 00 80 06  00 00 c0 a8 95 e6 12 8e   ·4·)@··· ········
0020  c4 15 20 13 00 50 5b 1c  06 8f 00 00 00 00 80 02   ·· ··P[· ········
0030  ff ff 2d 59 00 00 02 04  05 b4 01 03 03 08 01 01   ··-Y···· ········
0040  04 02                                              ··
```

Wi-Fi: <live capture in progress>   Packets: 5085   Profile: Default

Fig. 6



nmap_scan_traffic.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Frame (1160 bytes)
Reassembled TCP (1389 bytes)
Humid
Now
Search
ENG
IN
18:27
23-06-2025

tcp.port == 80

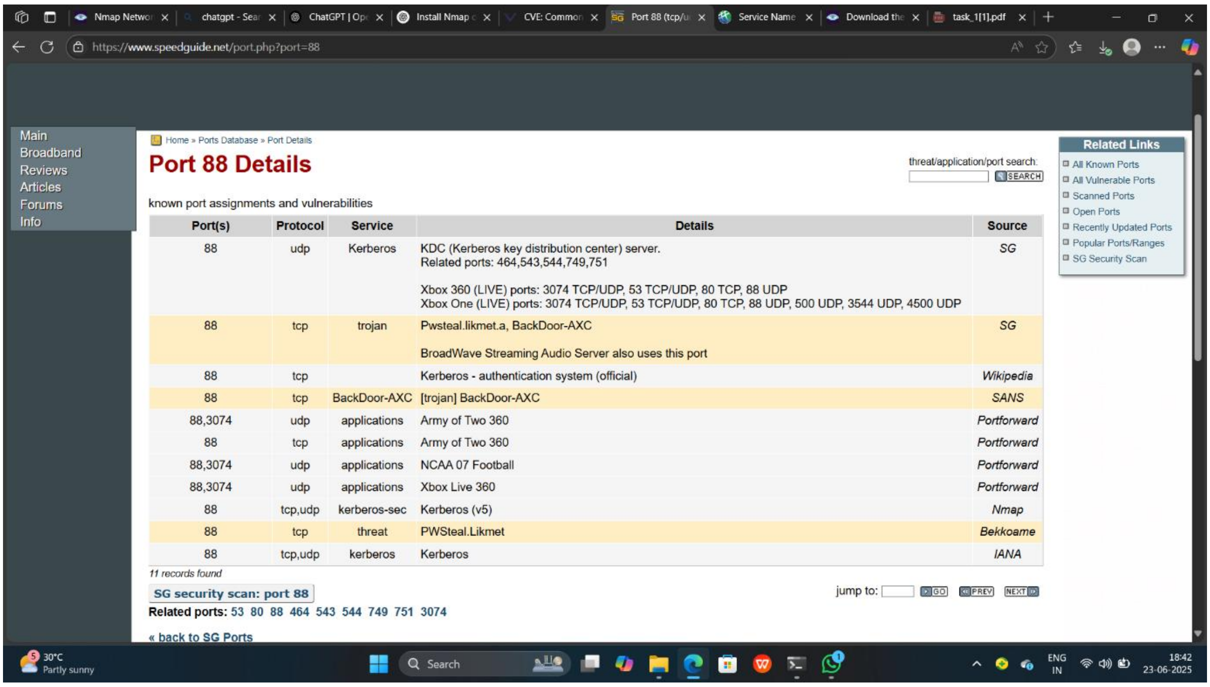
```
No.   Time       Source           Destination      Protocol Length Info
 2428 62.307443  54.255.213.32    192.168.149.230  TCP        62 80 → 8226 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1300 WS=128
 2429 62.307575  192.168.149.230  54.255.213.32    TCP        54 8226 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
 2430 62.321117  192.168.149.230  54.255.213.32    TCP       337 8226 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=283 [TCP PDU reassembled in 2441]
 2434 62.351810  54.169.7.73      192.168.149.230  TCP       218 80 → 8003 [PSH, ACK] Seq=985 Ack=7045 Win=980 Len=164
 2439 62.399780  192.168.149.230  54.169.7.73      TCP        54 8003 → 80 [ACK] Seq=7045 Ack=1149 Win=255 Len=0
 2440 62.428479  54.255.213.32    192.168.149.230  TCP        54 80 → 8226 [ACK] Seq=1 Ack=284 Win=62464 Len=0
 2441 62.428532  192.168.149.230  54.255.213.32    HTTP     1160 POST /cloudquery.php HTTP/1.1
 2469 62.524464  54.255.213.32    192.168.149.230  TCP        54 80 → 8226 [ACK] Seq=1 Ack=1390 Win=61440 Len=0
 2470 62.549392  54.255.213.32    192.168.149.230  HTTP      540 HTTP/1.1 200 OK
 2471 62.549569  192.168.149.230  54.255.213.32    TCP        54 8226 → 80 [FIN, ACK] Seq=1390 Ack=487 Win=65024 Len=0
 2498 62.627038  54.255.213.32    192.168.149.230  TCP        54 80 → 8226 [FIN, ACK] Seq=487 Ack=1391 Win=61440 Len=0
 2499 62.627108  192.168.149.230  54.255.213.32    TCP        54 8226 → 80 [ACK] Seq=1391 Ack=488 Win=65024 Len=0
 2685 63.048022  192.168.149.230  54.255.213.32    TCP        66 8228 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 2689 63.059445  192.168.149.230  54.169.7.73      TCP      1354 8003 → 80 [ACK] Seq=7045 Ack=1149 Win=255 Len=1300
 2690 63.059445  192.168.149.230  54.169.7.73      TCP        70 8003 → 80 [PSH, ACK] Seq=8345 Ack=1149 Win=255 Len=16
 2774 63.277496  192.168.149.230  54.169.7.73      TCP      1354 [TCP Retransmission] 8003 → 80 [PSH, ACK] Seq=7061 Ack=1149 Win=255 Len=1300
 2810 63.386121  54.255.213.32    192.168.149.230  TCP        62 80 → 8228 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1300 WS=128
 2811 63.386417  192.168.149.230  54.255.213.32    TCP        54 8228 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
 2814 63.406281  192.168.149.230  54.255.213.32    TCP       337 8228 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=283 [TCP PDU reassembled in 2816]
 2815 63.406334  192.168.149.230  54.255.213.32    TCP      1354 8228 → 80 [ACK] Seq=284 Ack=1 Win=65280 Len=1300 [TCP PDU reassembled in 2816]
```

```
▸ Frame 2441: 1160 bytes on wire (9280 bits), 1160 bytes captured (9280 bits) on interface \Device\NPF_{5E
▸ Ethernet II, Src: Intel_e5:9a:0c (e4:60:17:e5:9a:0c), Dst: d2:8e:fe:10:f8:e0 (d2:8e:fe:10:f8:e0)
▸ Internet Protocol Version 4, Src: 192.168.149.230, Dst: 54.255.213.32
▸ Transmission Control Protocol, Src Port: 8226, Dst Port: 80, Seq: 284, Ack: 1, Len: 1106
▸ [2 Reassembled TCP Segments (1389 bytes): #2430(283), #2441(1106)]
▸ Hypertext Transfer Protocol
▸ MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "---------------------------38
```

```
0000  d2 8e fe 10 f8 e0 e4 60  17 e5 9a 0c 08 00 45 00   ·······` ······E·
0010  04 7a 72 43 40 00 80 06  00 00 c0 a8 95 e6 36 ff   ·zrC@··· ······6·
0020  d5 20 20 22 00 50 a7 f8  a8 a2 a5 96 72 fa 50 18   ·  "·P·· ····r·P·
0030  00 ff 67 1b 00 00 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   ··g···-- --------
0040  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0050  2d 2d 2d 2d 33 38 66 35  65 35 64 30 66 66 34 63   ----38f5 e5d0ff4c
0060  0d 0a 43 6f 6e 74 65 6e  74 2d 44 69 73 70 6f 73   ··Conten t-Dispos
0070  69 74 69 6f 6e 3a 20 66  6f 72 6d 2d 64 61 74 61   ition: f orm-data
0080  3b 20 6e 61 6d 65 3d 22  6d 22 0d 0a 0d 0a 0a 04   ; name=" m"······
0090  03 c0 68 1d 00 01 00 00  cd 1a 81 4f f3 7a 69 95   ··h····· ···O·zi·
00a0  ae fc e7 6e 90 5d dd 4f  ad 93 79 d6 92 19 27 09   ···n·]·O ··y···'·
00b0  45 b5 81 59 59 e6 b6 74  e6 2a 28 af 06 07 19 8c   E··YY··t ·*(·····
00c0  b7 ac 1a a0 a5 f2 fb b3  b3 9b 3b 79 99 39 6c 4a   ········ ··;y·9lJ
00d0  d1 74 35 a4 98 a2 96 6a  36 05 8d 4e 57 f2 92 5d   ·t5····j 6··NW··]
00e0  1b 49 b0 d4 dd f7 36 93  8f 21 27 2f 92 28 f7 66   ·I····6· ·!'/·(·f
00f0  ab 6d a7 31 88 3d cf 16  bb fc fd 93 a1 88 38 1c   ·m·1·=·· ······8·
0100  3d a9 30 23 ab d7 89 24  50 81 c7 b5 3c 71 1f 00   =·0#···$ P···<q··
0110  7b e6 f2 c5 e0 b0 d3 e0  4b 76 a3 dc 25 b5 99 21   {······· Kv··%··!
0120  60 3e 34 5c 0b d0 34 77  31 19 bf 80 77 85 9f cf   `>4\··4w 1···w···
0130  fa f7 ab 70 4e 15 b0 33  ff d1 1c b0 1b 3d ac 55   ···pN··3 ·····=·U
0140  5d 64 04 bb 6e 1e 54 a7  e2 50 eb 2c fd 6d a5 c3   ]d··n·T· ·P·,·m··
```

nmap_scan_traffic.pcapng   Packets: 10947 · Displayed: 233 (2.1%) · Dropped: 0 (0.0%)   Profile: Default

Fig. 7



Port 88 Details

known port assignments and vulnerabilities

Port(s)	Protocol	Service	Details	Source
88	udp	Kerberos	KDC (Kerberos key distribution center) server. Related ports: 464,543,544,749,751 Xbox 360 (LIVE) ports: 3074 TCP/UDP, 53 TCP/UDP, 80 TCP, 88 UDP Xbox One (LIVE) ports: 3074 TCP/UDP, 53 TCP/UDP, 80 TCP, 88 UDP, 500 UDP, 3544 UDP, 4500 UDP	SG
88	tcp	trojan	Pwsteal.likmet.a, BackDoor-AXC BroadWave Streaming Audio Server also uses this port	SG
88	tcp		Kerberos - authentication system (official)	Wikipedia
88	tcp	BackDoor-AXC	[trojan] BackDoor-AXC	SANS
88,3074	udp	applications	Army of Two 360	Portforward
88	tcp	applications	Army of Two 360	Portforward
88,3074	udp	applications	NCAA 07 Football	Portforward
88,3074	udp	applications	Xbox Live 360	Portforward
88	tcp,udp	kerberos-sec	Kerberos (v5)	Nmap
88	tcp	threat	PWSteal.Likmet	Bekkoame
88	tcp,udp	kerberos	Kerberos	IANA

11 records found

SG security scan: port 88

jump to: GO PREV NEXT

Related ports: 53 80 88 464 543 544 749 751 3074

« back to SG Ports

Fig. 8

Key Points to remember:

- Always run **Nmap as Administrator** for accurate results.
- Never scan networks you don’t own or have permission to scan.
- Keep Nmap, Wireshark, and system software updated.

Conclusion:

The task provided hands-on experience in scanning of Local Network for Open Ports using Nmap. Additionally, traffic analysis using Wireshark was done and the results were obtained. The key concepts are Port scanning, TCP SYN scan, IP ranges, network reconnaissance, open ports, network security basics.

References:

- https://nmap.org/download.html
- https://www.cyberly.org/en/how-do-you-install-nmap-on-windows/index.html
- https://www.wireshark.org/
- How to Install Wireshark on Windows? - GeeksforGeeks
- https://chatgpt.com/