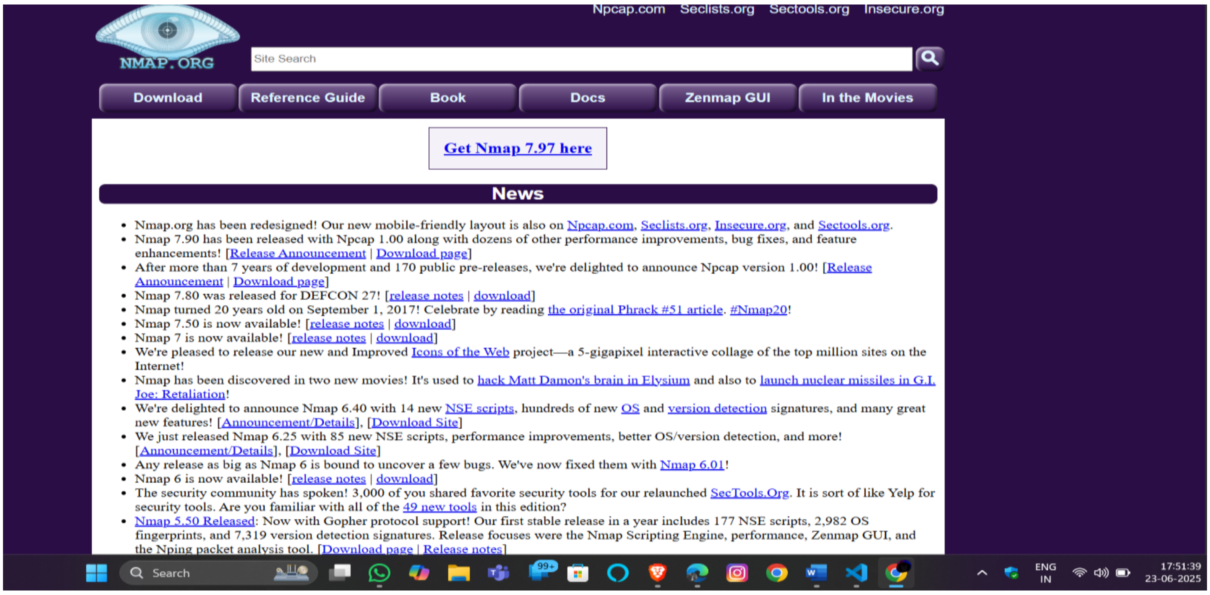
CYBER SECURITY INTERNSHIP

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.Install Nmap from official website.

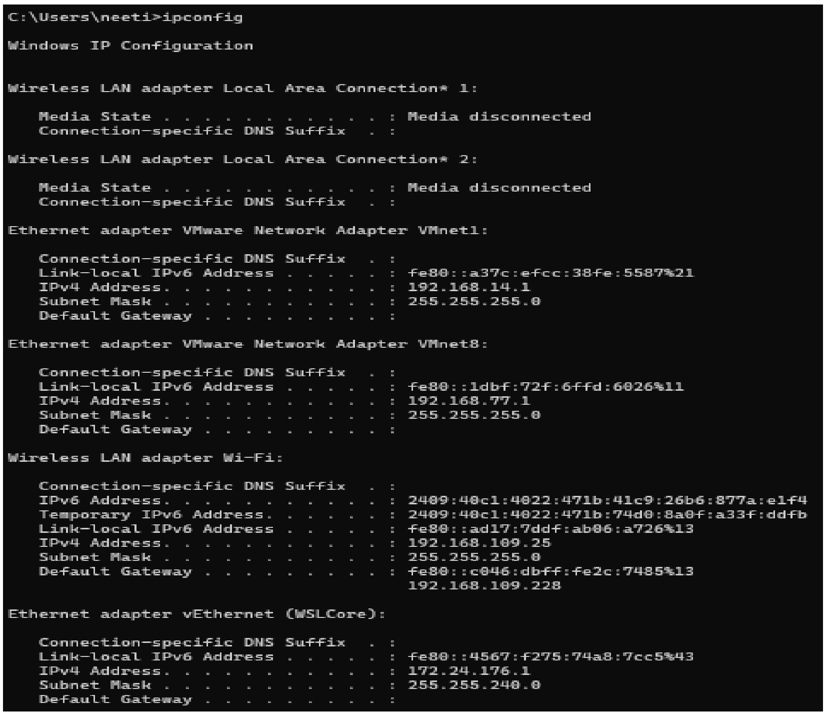


Get Nmap 7.97 here

News

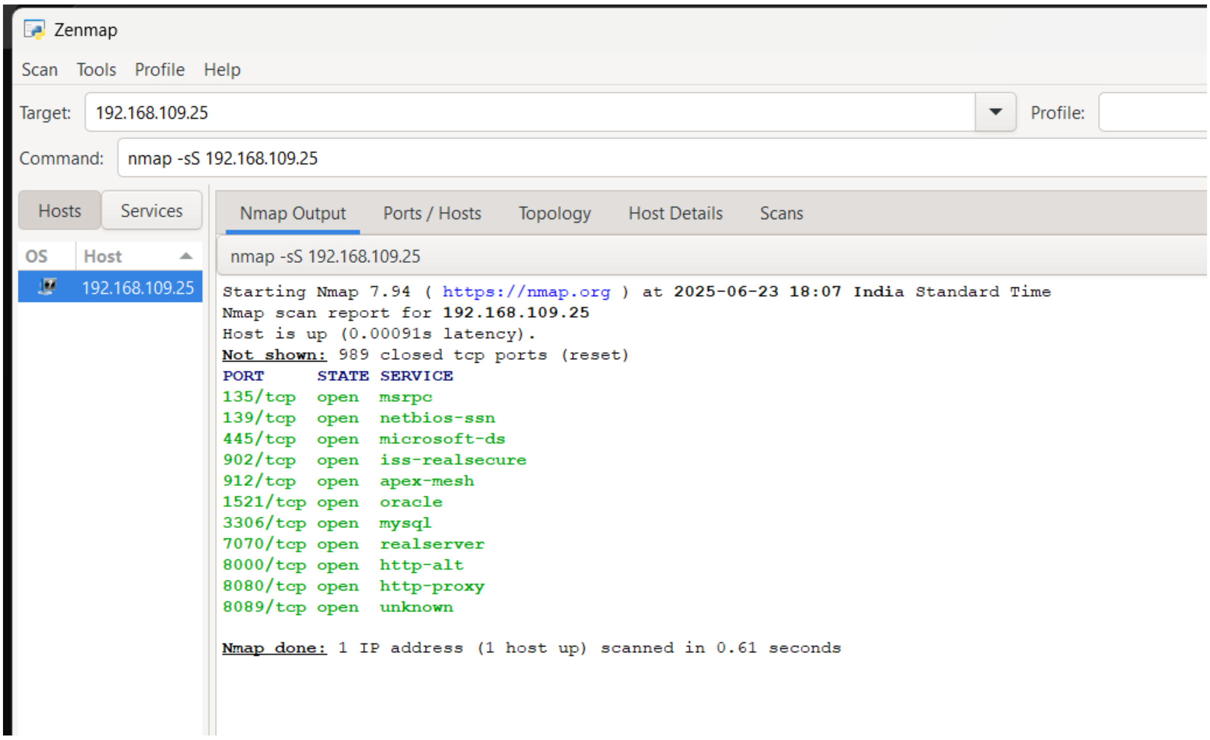
- Nmap.org has been redesigned! Our new mobile-friendly layout is also on Npcap.com, Seclists.org, Insecure.org, and Sectools.org.
- Nmap 7.90 has been released with Npcap 1.00 along with dozens of other performance improvements, bug fixes, and feature enhancements! [Release Announcement | Download page]
- After more than 7 years of development and 170 public pre-releases, we're delighted to announce Npcap version 1.00! [Release Announcement | Download page]
- Nmap 7.80 was released for DEFCON 27! [release notes | download]
- Nmap turned 20 years old on September 1, 2017! Celebrate by reading the original Phrack #51 article. #Nmap20!
- Nmap 7.50 is now available! [release notes | download]
- Nmap 7 is now available! [release notes | download]
- We're pleased to release our new and Improved Icons of the Web project—a 5-gigapixel interactive collage of the top million sites on the Internet!
- Nmap has been discovered in two new movies! It's used to hack Matt Damon's brain in Elysium and also to launch nuclear missiles in G.I. Joe: Retaliation!
- We're delighted to announce Nmap 6.40 with 14 new NSE scripts, hundreds of new OS and version detection signatures, and many great new features! [Announcement/Details], [Download Site]
- We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! [Announcement/Details], [Download Site]
- Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with Nmap 6.01!
- Nmap 6 is now available! [release notes | download]
- The security community has spoken! 3,000 of you shared favorite security tools for our relaunched SecTools.Org. It is sort of like Yelp for security tools. Are you familiar with all of the 49 new tools in this edition?
- Nmap 5.50 Released: Now with Gopher protocol support! Our first stable release in a year includes 177 NSE scripts, 2,982 OS fingerprints, and 7,319 version detection signatures. Release focuses were the Nmap Scripting Engine, performance, Zenmap GUI, and the Nping packet analysis tool. [Download page | Release notes]

2.Find your local IP range.



```
C:\Users\neeti>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a37c:efcc:38fe:5587%21
   IPv4 Address. . . . . . . . . . . : 192.168.14.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1dbf:72f:6ffd:6026%11
   IPv4 Address. . . . . . . . . . . : 192.168.77.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:40c1:4022:471b:41c9:26b6:877a:e1f4
   Temporary IPv6 Address. . . . . . : 2409:40c1:4022:471b:74d0:8a0f:a33f:ddfb
   Link-local IPv6 Address . . . . . : fe80::ad17:7ddf:ab06:a726%13
   IPv4 Address. . . . . . . . . . . : 192.168.109.25
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::c046:dbff:fe2c:7485%13
                                       192.168.109.228

Ethernet adapter vEthernet (WSLCore):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4567:f275:74a8:7cc5%43
   IPv4 Address. . . . . . . . . . . : 172.24.176.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :
```

3.Run: nmap -sS 192.168.109.25 to perform TCP SYN scan.



Target: 192.168.109.25

Profile:

Command: nmap -sS 192.168.109.25

192.168.109.25

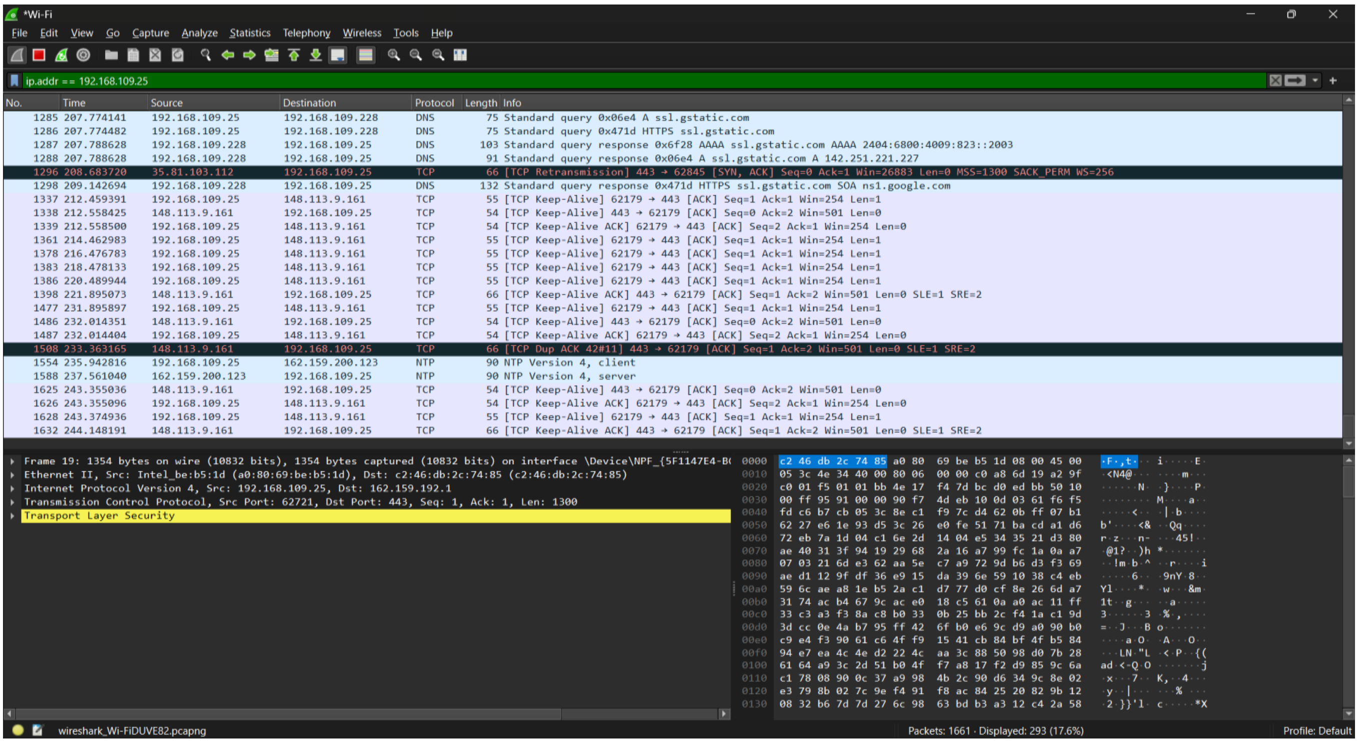
```
nmap -sS 192.168.109.25

Starting Nmap 7.94 ( https://nmap.org ) at 2025-06-23 18:07 India Standard Time
Nmap scan report for 192.168.109.25
Host is up (0.00091s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1521/tcp open  oracle
3306/tcp open  mysql
7070/tcp open  realserver
8000/tcp open  http-alt
8080/tcp open  http-proxy
8089/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.61 seconds
```

4.IP addresses and open ports found.

Open ports are 135,139,445,902,912,1521,3306,7070,8000,8080,8089

5.Analyze packet capture with Wireshark. (Optionally)

- Use the filter ip.addr==<ip address>



ip.addr == 192.168.109.25

```
No.   Time       Source           Destination      Protocol Length Info
 1285 207.774141 192.168.109.25   192.168.109.228  DNS       75 Standard query 0x06e4 A ssl.gstatic.com
 1286 207.774482 192.168.109.25   192.168.109.228  DNS       75 Standard query 0x471d HTTPS ssl.gstatic.com
 1287 207.788628 192.168.109.228  192.168.109.25   DNS      103 Standard query response 0x6f28 AAAA ssl.gstatic.com AAAA 2404:6800:4009:823::2003
 1288 207.788628 192.168.109.228  192.168.109.25   DNS       91 Standard query response 0x06e4 A ssl.gstatic.com A 142.251.221.227
 1296 208.683720 35.81.103.112    192.168.109.25   TCP       66 [TCP Retransmission] 443 → 62845 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1300 SACK_PERM WS=256
 1298 209.142694 192.168.109.228  192.168.109.25   DNS      132 Standard query response 0x471d HTTPS ssl.gstatic.com SOA ns1.google.com
 1337 212.459391 192.168.109.25   148.113.9.161    TCP       55 [TCP Keep-Alive] 62179 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
 1338 212.558425 148.113.9.161    192.168.109.25   TCP       54 [TCP Keep-Alive] 443 → 62179 [ACK] Seq=0 Ack=2 Win=501 Len=0
 1339 212.558500 192.168.109.25   148.113.9.161    TCP       54 [TCP Keep-Alive ACK] 62179 → 443 [ACK] Seq=2 Ack=1 Win=254 Len=0
 1361 214.462983 192.168.109.25   148.113.9.161    TCP       55 [TCP Keep-Alive] 62179 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
 1378 216.476783 192.168.109.25   148.113.9.161    TCP       55 [TCP Keep-Alive] 62179 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
 1383 218.478133 192.168.109.25   148.113.9.161    TCP       55 [TCP Keep-Alive] 62179 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
 1386 220.489944 192.168.109.25   148.113.9.161    TCP       55 [TCP Keep-Alive] 62179 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
 1398 221.895073 148.113.9.161    192.168.109.25   TCP       66 [TCP Keep-Alive ACK] 443 → 62179 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
 1477 231.895897 192.168.109.25   148.113.9.161    TCP       55 [TCP Keep-Alive] 62179 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
 1486 232.014351 148.113.9.161    192.168.109.25   TCP       54 [TCP Keep-Alive] 443 → 62179 [ACK] Seq=0 Ack=2 Win=501 Len=0
 1487 232.014404 192.168.109.25   148.113.9.161    TCP       54 [TCP Keep-Alive ACK] 62179 → 443 [ACK] Seq=2 Ack=1 Win=254 Len=0
 1508 233.363165 148.113.9.161    192.168.109.25   TCP       66 [TCP Dup ACK 42#11] 443 → 62179 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
 1554 235.942816 192.168.109.25   162.159.200.123  NTP       90 NTP Version 4, client
 1588 237.561040 162.159.200.123  192.168.109.25   NTP       90 NTP Version 4, server
 1625 243.355036 148.113.9.161    192.168.109.25   TCP       54 [TCP Keep-Alive] 443 → 62179 [ACK] Seq=0 Ack=2 Win=501 Len=0
 1626 243.355096 192.168.109.25   148.113.9.161    TCP       54 [TCP Keep-Alive ACK] 62179 → 443 [ACK] Seq=2 Ack=1 Win=254 Len=0
 1628 243.374936 192.168.109.25   148.113.9.161    TCP       55 [TCP Keep-Alive] 62179 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
 1632 244.148191 148.113.9.161    192.168.109.25   TCP       66 [TCP Keep-Alive ACK] 443 → 62179 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
```

```
> Frame 19: 1354 bytes on wire (10832 bits), 1354 bytes captured (10832 bits) on interface \Device\NPF_{5F1147E4-B(
> Ethernet II, Src: Intel_be:b5:1d (a0:80:69:be:b5:1d), Dst: c2:46:db:2c:74:85 (c2:46:db:2c:74:85)
> Internet Protocol Version 4, Src: 192.168.109.25, Dst: 162.159.192.1
> Transmission Control Protocol, Src Port: 62721, Dst Port: 443, Seq: 1, Ack: 1, Len: 1300
> Transport Layer Security
```

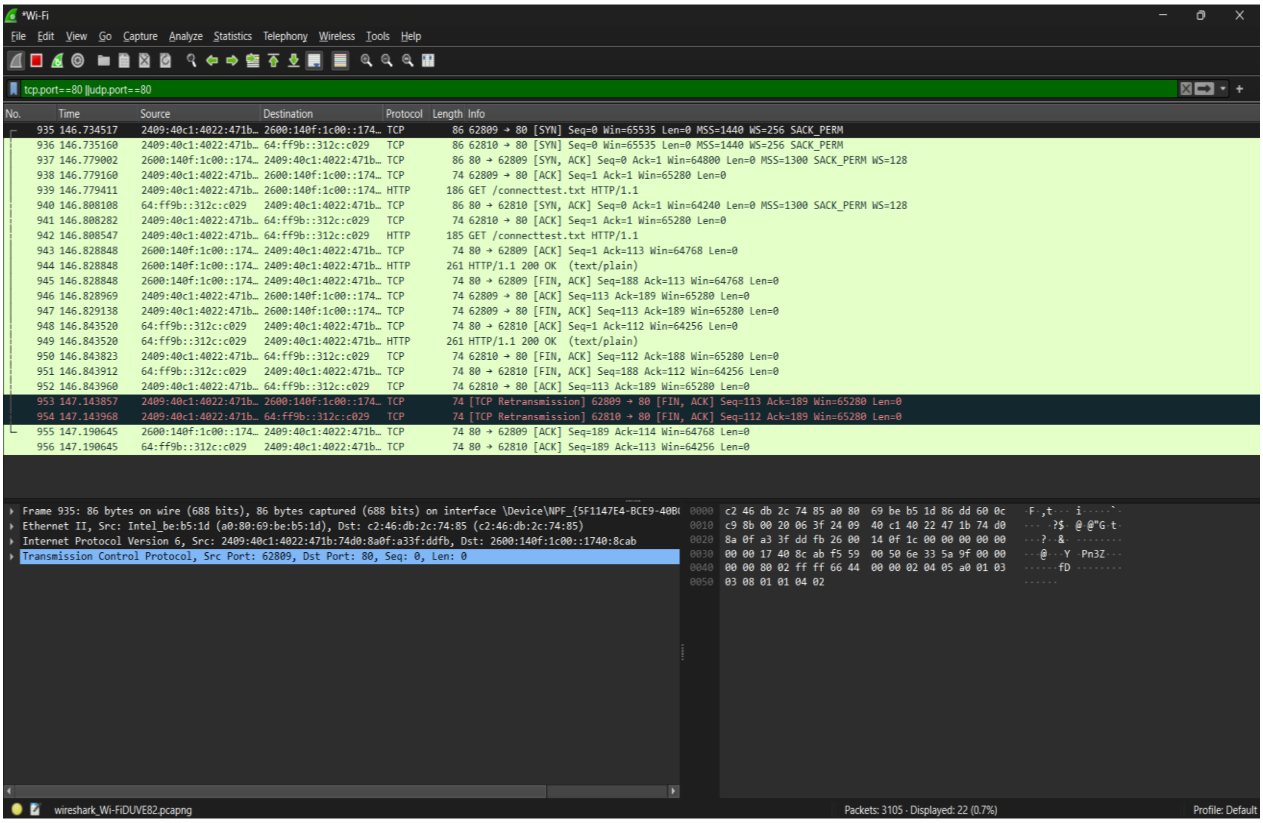
```
0000  c2 46 db 2c 74 85 a0 80  69 be b5 1d 08 00 45 00
0010  05 3c 4e 34 40 00 80 06  00 00 c0 a8 6d 19 a2 9f
0020  c0 01 f5 01 01 bb 4e 17  f4 7d bc d0 ed bb 50 10
0030  00 ff 95 91 00 00 90 f7  4d eb 10 0d 03 61 f6 f5
0040  fd c6 b7 cb 05 3c 8e c1  f9 7c d4 62 0b ff 07 b1
0050  62 27 e6 1e 93 d5 3c 26  e0 fe 51 71 ba cd a1 d6
0060  72 eb 7a 1d 04 c1 6e 2d  14 04 e5 34 35 21 d3 80
0070  ae 40 31 3f 94 19 29 68  2a 16 a7 99 fc 1a 0a a7
0080  07 03 21 6d e3 62 aa 5e  c7 a9 72 9d b6 d3 f3 69
0090  ae d1 12 9f df 36 e9 15  da 39 6e 59 10 38 c4 eb
00a0  59 6c ae a8 1e b5 2a c1  d7 77 d0 cf 8e 26 6d a7
00b0  31 74 ac b4 67 9c ac e0  18 c5 61 0a a0 ac 11 ff
00c0  33 c3 a3 f3 8a c8 b0 33  0b 25 bb 2c f4 1a c1 9d
00d0  3d cc 0e 4a b7 95 ff 42  6f b0 e6 9c d9 a0 90 b0
00e0  c9 e4 f3 90 61 c6 4f f9  15 41 cb 84 bf 4f b5 84
00f0  94 e7 ea 4c 4e d2 22 4c  aa 3c 88 50 98 d0 7b 28
0100  61 64 a9 3c 2d 51 b0 4f  f7 a8 17 f2 d9 85 9c 6a
0110  c1 78 08 90 0c 37 a9 98  4b 2c 90 d6 34 9c 8e 02
0120  e3 79 8b 02 7c 9e f4 91  f8 ac 84 25 20 82 9b 12
0130  08 32 b6 7d 7d 27 6c 98  63 bd b3 a3 12 c4 2a 58
```

wireshark_Wi-FiDUVE82.pcapng

Packets: 1661 · Displayed: 293 (17.6%)

Profile: Default

- Use the filter tcp.port==<port> ||udp.port==<port>



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.port==80 ||udp.port==80
```

```
No.  Time        Source                  Destination             Protocol Length Info
 935 146.734517  2409:40c1:4022:471b…  2600:140f:1c00::174…  TCP       86 62809 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
 936 146.735160  2409:40c1:4022:471b…  64:ff9b::312c:c029     TCP       86 62810 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
 937 146.779002  2600:140f:1c00::174…  2409:40c1:4022:471b…  TCP       86 80 → 62809 [SYN, ACK] Seq=0 Ack=1 Win=64800 Len=0 MSS=1300 SACK_PERM WS=128
 938 146.779160  2409:40c1:4022:471b…  2600:140f:1c00::174…  TCP       74 62809 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
 939 146.779411  2409:40c1:4022:471b…  2600:140f:1c00::174…  HTTP     186 GET /connecttest.txt HTTP/1.1
 940 146.808108  64:ff9b::312c:c029     2409:40c1:4022:471b…  TCP       86 80 → 62810 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1300 SACK_PERM WS=128
 941 146.808282  2409:40c1:4022:471b…  64:ff9b::312c:c029     TCP       74 62810 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
 942 146.808547  2409:40c1:4022:471b…  64:ff9b::312c:c029     HTTP     185 GET /connecttest.txt HTTP/1.1
 943 146.828848  2600:140f:1c00::174…  2409:40c1:4022:471b…  TCP       74 80 → 62809 [ACK] Seq=1 Ack=113 Win=64768 Len=0
 944 146.828848  2600:140f:1c00::174…  2409:40c1:4022:471b…  HTTP     261 HTTP/1.1 200 OK  (text/plain)
 945 146.828848  2600:140f:1c00::174…  2409:40c1:4022:471b…  TCP       74 80 → 62809 [FIN, ACK] Seq=188 Ack=113 Win=64768 Len=0
 946 146.828969  2409:40c1:4022:471b…  2600:140f:1c00::174…  TCP       74 62809 → 80 [ACK] Seq=113 Ack=189 Win=65280 Len=0
 947 146.829138  2409:40c1:4022:471b…  2600:140f:1c00::174…  TCP       74 62809 → 80 [FIN, ACK] Seq=113 Ack=189 Win=65280 Len=0
 948 146.843520  64:ff9b::312c:c029     2409:40c1:4022:471b…  TCP       74 80 → 62810 [ACK] Seq=1 Ack=112 Win=64256 Len=0
 949 146.843520  64:ff9b::312c:c029     2409:40c1:4022:471b…  HTTP     261 HTTP/1.1 200 OK  (text/plain)
 950 146.843823  2409:40c1:4022:471b…  64:ff9b::312c:c029     TCP       74 62810 → 80 [FIN, ACK] Seq=112 Ack=188 Win=65280 Len=0
 951 146.843912  64:ff9b::312c:c029     2409:40c1:4022:471b…  TCP       74 80 → 62810 [FIN, ACK] Seq=188 Ack=112 Win=64256 Len=0
 952 146.843960  2409:40c1:4022:471b…  64:ff9b::312c:c029     TCP       74 62810 → 80 [ACK] Seq=113 Ack=189 Win=65280 Len=0
 953 147.143857  2409:40c1:4022:471b…  2600:140f:1c00::174…  TCP       74 [TCP Retransmission] 62809 → 80 [FIN, ACK] Seq=113 Ack=189 Win=65280 Len=0
 954 147.143968  2409:40c1:4022:471b…  64:ff9b::312c:c029     TCP       74 [TCP Retransmission] 62810 → 80 [FIN, ACK] Seq=112 Ack=189 Win=65280 Len=0
 955 147.190645  2600:140f:1c00::174…  2409:40c1:4022:471b…  TCP       74 80 → 62809 [ACK] Seq=189 Ack=114 Win=64768 Len=0
 956 147.190645  64:ff9b::312c:c029     2409:40c1:4022:471b…  TCP       74 80 → 62810 [ACK] Seq=189 Ack=113 Win=64256 Len=0
```

```
Frame 935: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{5F1147E4-BCE9-40B(
Ethernet II, Src: Intel_be:b5:1d (a0:80:69:be:b5:1d), Dst: c2:46:db:2c:74:85 (c2:46:db:2c:74:85)
Internet Protocol Version 6, Src: 2409:40c1:4022:471b:74d0:8a0f:a33f:ddfb, Dst: 2600:140f:1c00::1740:8cab
Transmission Control Protocol, Src Port: 62809, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  c2 46 db 2c 74 85 a0 80  69 be b5 1d 86 dd 60 0c   ·F·,t···i·····`·
0010  c9 8b 00 20 06 3f 24 09  40 c1 40 22 47 1b 74 d0   ··· ·?$·@·@"G·t·
0020  8a 0f a3 3f dd fb 26 00  14 0f 1c 00 00 00 00 00   ···?··&·········
0030  00 00 17 40 8c ab f5 59  00 50 6e 33 5a 9f 00 00   ···@···Y·Pn3Z···
0040  00 00 80 02 ff ff 66 44  00 00 02 04 05 a0 01 03   ······fD········
0050  03 08 01 01 04 02                                  ······
```

```
wireshark_Wi-FiDUVE82.pcapng    Packets: 3105 · Displayed: 22 (0.7%)    Profile: Default
```

6.Research common services running on those ports.

Port	State	Service	Description
135	open	msrpc	Microsoft RPC services, common in Windows networks.
139	open	netbios-ssn	NetBIOS Session Service; used in Windows file sharing.
445	open	microsoft-ds	SMB over TCP, also used for Windows file sharing.
902	open	iss-realsecure	Often VMware-related (used by VMware Server Console).
912	open	apex-mesh	Often related to VMware (VM communication interface).
1521	open	oracle	Oracle database default listener port.
3306	open	mysql	MySQL database service.
7070	open	realserver	RealNetworks streaming media server.
8000	open	http-alt	Alternate HTTP service port; could be a web service.
8080	open	http-proxy	Commonly used for web servers or proxies.
8089	open	unknown	Unknown service — needs further investigation.

7.Identify potential security risks from open ports.

Open ports can introduce a range of security risks, especially if the services listening on them are misconfigured, outdated, or unnecessary.

General Risks of Open Ports

1. **Unauthorized Access**
    - Open ports expose services to anyone on the network (or the internet), increasing the attack surface.
    - Attackers may attempt brute-force logins or exploit weak authentication.
2. **Exploitation of Vulnerabilities**
    - Services listening on open ports might have known vulnerabilities that attackers can exploit (e.g., buffer overflows, remote code execution).
3. **Information Leakage**
    - Some services may disclose version info or system details, aiding attackers in reconnaissance.
4. **Lateral Movement**
    - Once inside a network, attackers can use open ports to move laterally to other systems.
5. **Malware Communication (C2)**
    - Open ports can be used by malware to establish **Command & Control (C2)** channels, allowing remote control of the compromised system.

The specific security risks associated with the open ports found in Nmap scan

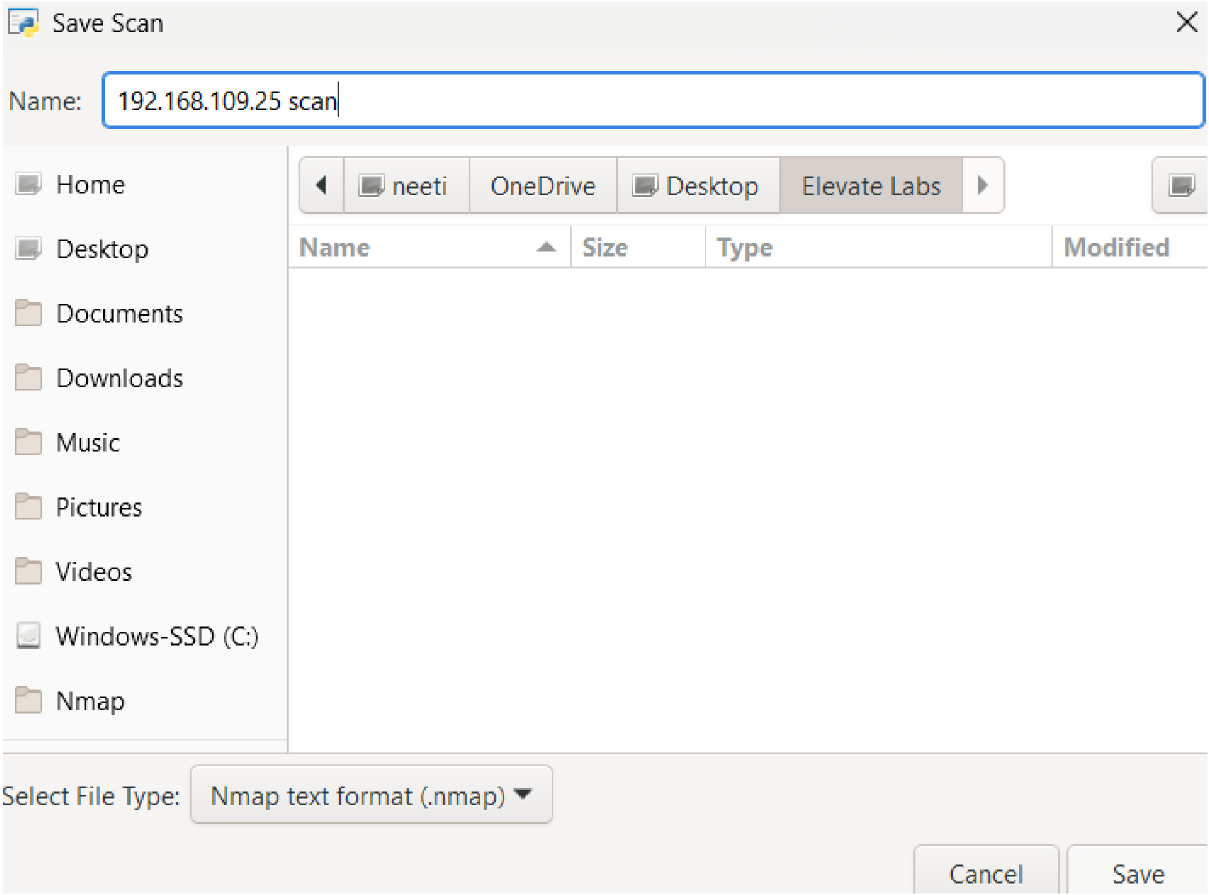
Ports 135, 139, and 445 are commonly used in Windows networking for services like Microsoft RPC, NetBIOS, and SMB. These ports are frequent targets for malware and attackers due to historical vulnerabilities like EternalBlue, which enabled widespread attacks such as WannaCry. If exposed, they can be used for remote code execution, credential theft, or lateral movement within a network.

Ports 902 and 912 are typically associated with VMware services, and if left exposed, they could potentially allow unauthorized access to virtual machine controls or facilitate data leakage between host and guest systems

Port 1521, used by Oracle databases, and 3306, used by MySQL, pose a significant risk when accessible from untrusted networks, as attackers could exploit vulnerabilities or weak credentials to perform SQL injection, data extraction, or even take control of the database server.

Web-related ports like 8000, 8080, and 8089 often host development or alternative HTTP services, which may be less hardened, exposing them to common web application attacks such as cross-site scripting (XSS), remote code execution (RCE), or misconfigured admin panels. Notably, port 8089 is unclassified in the scan and should be investigated further, as unknown services can pose stealthy or custom threats that are harder to detect and defend against.

8.Save scan results as a text or HTML file.



Save Scan

Name: 192.168.109.25 scan

Select File Type: Nmap text format (.nmap)