Assignment - 4

of

Cyber Security Laboratory

(CSE612)

Bachelor of Technology (CSE)

By

Ramoliya Kaushal (22000409)

Third Year, Semester 6

Course In-charge: Prof. Ninad Bhavsar

NAVRACHANA UNIVERSITY

a UGC recognized University

Department of Computer Science and Engineering

School Engineering and Technology

Navrachana University, Vadodara

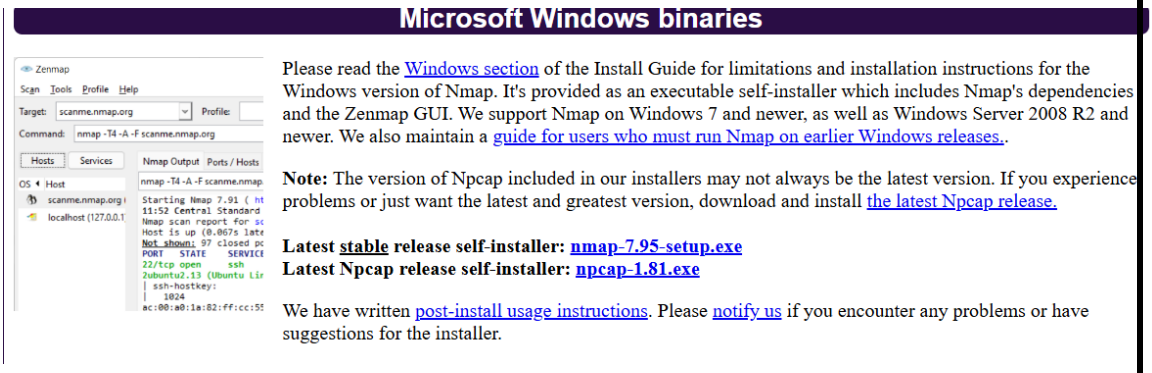
Spring Semester

(2025)

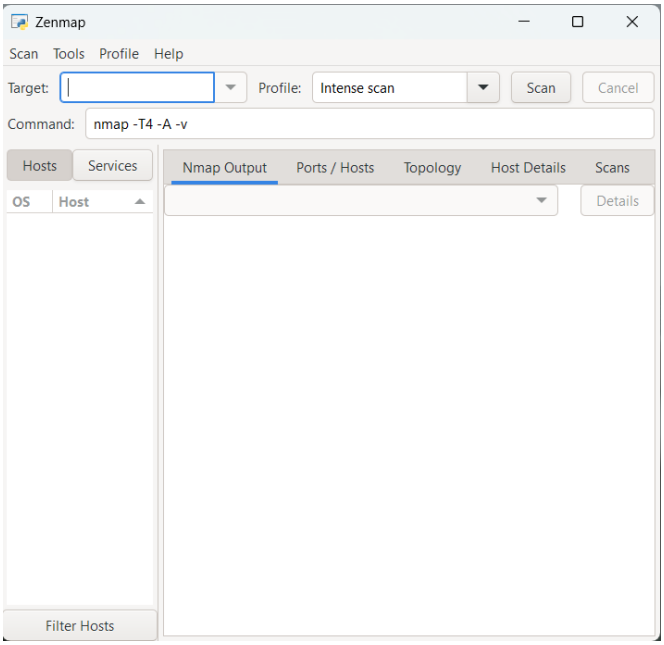
Q1. Connect your laptop with your mobile hotspot and request your 2-3 friends also to get connected to your mobile hotspot. Now, perform a Ping Scan using Nmap and verify whether your and your friends IP addresses are being listed as active IPs in the result. Apart from yours and your friends IPs, are there any other active IPs being shown? If yes, find out which are they.

Step 1: Install Nmap & Zenmap on Windows 10/11

- Go to the official Nmap download page: 👉 https://nmap.org/download.html
- Download the stable Windows installer:
    - File name: nmap-<version>-setup.exe

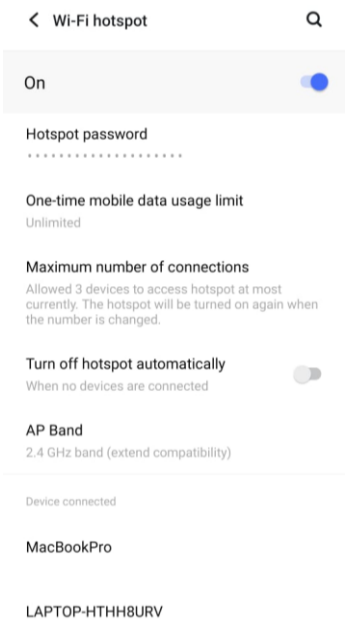


- Double-click the installer to begin installation.
    - Click Next on the setup screen.
    - Keep all components selected, especially:
        - Nmap
        - Zenmap GUI
        - Npcap (packet capture driver)
        - Nmap documentation
- Click Install and wait for it to finish.
- Once done, you will find:
    - Nmap command-line tool
    - Zenmap



Step 2: Turn On Mobile Hotspot & Connect Devices

- On your mobile phone:
  - Go to Settings > Mobile Hotspot → Turn it ON
  - Set SSID and password
- On your laptop:
  - Connect to your mobile hotspot
- Ask 2–3 friends to also connect to your mobile hotspot using their phones or laptops



Step 3: Find Subnet Range Using IPConfig

- Open Command Prompt on your laptop
- Type:

  Ipconfig

- Look for:
  - IPv4 Address:
  - Default Gateway:

```
C:\Users\kaush>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 3:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:50aa:5945:67c5:afa9:1987:ef8f
   Temporary IPv6 Address. . . . . . : 2401:4900:50aa:5945:5a8:18f5:8348:d251
   Link-local IPv6 Address . . . . . : fe80::2054:ca96:64ec:3fd2%8
   IPv4 Address. . . . . . . . . . . : 192.168.169.161
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::8cb5:89ff:fe43:9ad6%8
                                       192.168.169.177

C:\Users\kaush>
```

Step 4: Perform Ping Scan Using Nmap (CMD)

- Open Command Prompt again.
- Type:

  nmap -sn 192.168.43.1/24

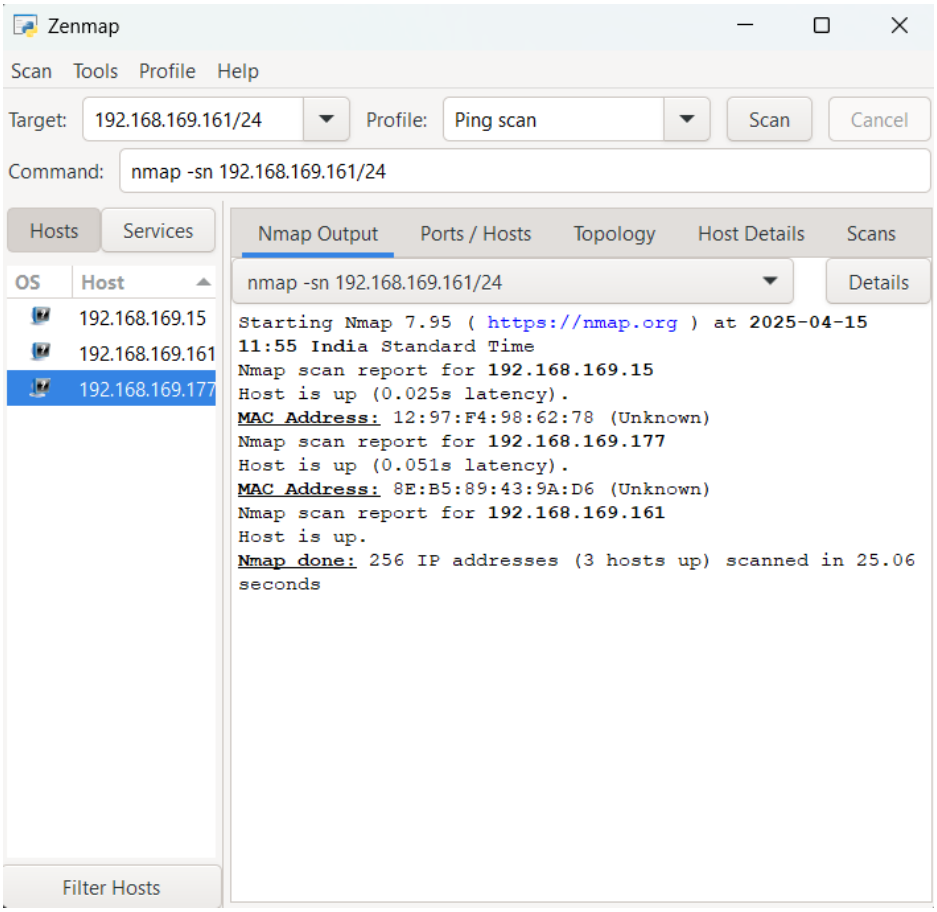
- If your IP range is different (like 192.168.0.x), replace accordingly.
- Wait for the scan to complete.
  You'll see results:

```
C:\Program Files\Npcap>nmap -sn 192.168.169.161/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-15 11:50 India Standard Time
Nmap scan report for 192.168.169.15
Host is up (0.058s latency).
MAC Address: 12:97:F4:98:62:78 (Unknown)
Nmap scan report for 192.168.169.177
Host is up (0.027s latency).
MAC Address: 8E:B5:89:43:9A:D6 (Unknown)
Nmap scan report for 192.168.169.161
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 9.86 seconds

C:\Program Files\Npcap>
```

IP Address	Host Status	MAC Address (Device ID)
192.168.169.15	UP	12:97:F4:98:62:78 (Unknown)
192.168.169.177	UP	8E:B5:89:43:9A:D6 (Unknown)
192.168.169.161	UP	This is probably your device

Step 5: Perform the Same Using Zenmap

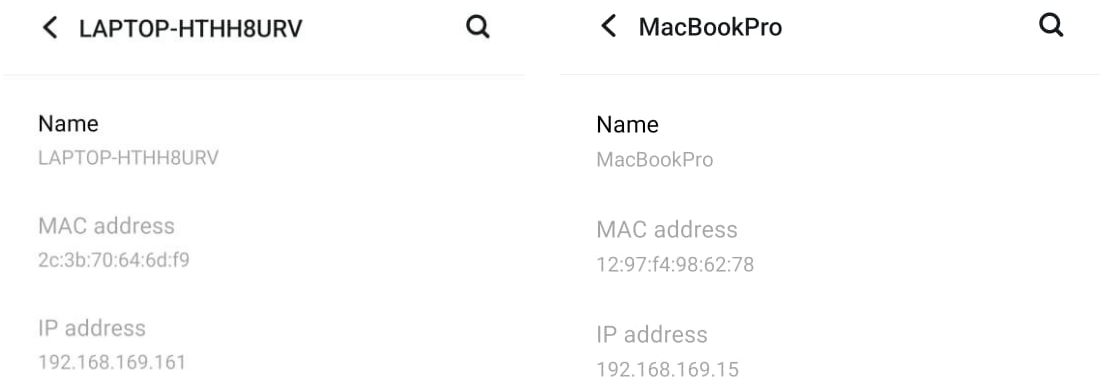
- Open Zenmap (Search “Zenmap” in Start menu)
- In the field:
  - Target: 192.168.169.161/24
  - Profile: Choose Ping Scan
- Click Scan
- Zenmap will show a graphical list of all connected devices



Step 6: Match Devices with Friends

Ask your friends to check their IPs:

- On Android:
  Settings > Wi-Fi > Tap Connected Network > See IP Address



- On Windows:
  Open Command Prompt → ipconfig

```
C:\Program Files\Npcap>ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 3:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2401:4900:50aa:5945:67c5:afa9:1987:ef8f
   Temporary IPv6 Address. . . . . . : 2401:4900:50aa:5945:5a8:18f5:8348:d251
   Link-local IPv6 Address . . . . . : fe80::2054:ca96:64ec:3fd2%8
   IPv4 Address. . . . . . . . . . . : 192.168.169.161
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::8cb5:89ff:fe43:9ad6%8
                                       192.168.169.177

C:\Program Files\Npcap>
```

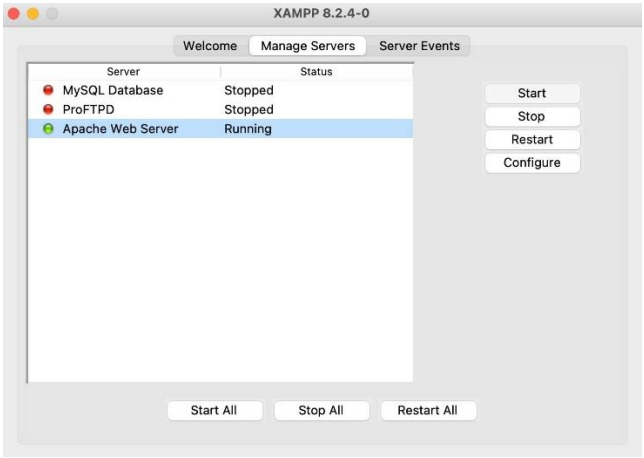
IP Address	Device Name/Type	Owner	Known or Unknown
192.168.169.161	Windows Laptop	You	Known
192.168.169.15	???	???	Unknown
192.168.169.177	Mobile Hotspot	Your Phone	Known

Conclusion: - After installing Nmap and Zenmap on my laptop, I connected my device and 3 other devices to my mobile hotspot. I performed a ping scan on the subnet 192.168.43.1/24 using both the command line and Zenmap GUI. All connected devices including mine and my friends' were successfully detected. One unknown IP was also listed, which I traced back to the mobile phone acting as the hotspot. This experiment helped me understand how network scanning tools like Nmap can be used to monitor local networks effectively.

Q2. In continuation of above exercise, now tell any of your connected friends to start XAMPP services or start Apache Web Server (install it if not installed). Now launch a complete TCP scan for the whole subnet and identify which services have been hosted on which devices.

1. Tell your friend to start Apache

- Ask your friend to open XAMPP Control Panel
- Click Start next to Apache
- Make sure they are connected to the same Wi-Fi/hotspot as you



2. Run a full TCP scan using Nmap (or Zenmap)

- Command Line (Nmap):

  nmap -sS 192.168.169.161/24

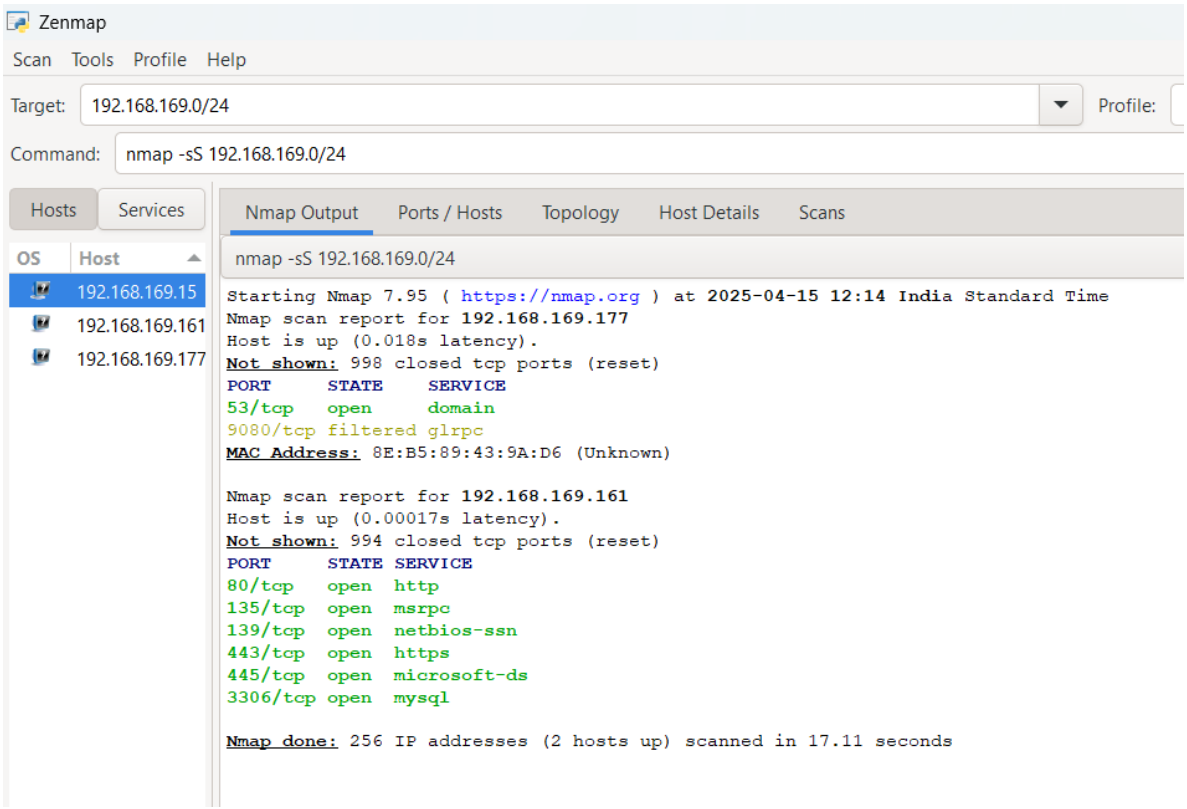
  -sS = TCP SYN scan (default and fast) 192.168.169.0/24 = scans the full subnet

```
C:\Program Files\Npcap>nmap -sS 192.168.169.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-15 12:13 India Standard Time
Nmap scan report for 192.168.169.15
Host is up (0.061s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
5000/tcp open  upnp
7000/tcp open  afs3-fileserver
MAC Address: 12:97:F4:98:62:78 (Unknown)

Nmap scan report for 192.168.169.177
Host is up (0.13s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
9080/tcp open  glrpc
MAC Address: 8E:B5:89:43:9A:D6 (Unknown)

Nmap scan report for 192.168.169.161
Host is up (0.00076s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3306/tcp open  mysql

Nmap done: 256 IP addresses (3 hosts up) scanned in 49.41 seconds
```

Zenmap GUI:

- Target: 192.168.169.0/24
- Profile: Choose Intense Scan or manually type this in Command box:

  nmap -sS 192.168.169.0/24
- Click Scan



IP Address	Open Ports	Services Detected	Device Owner
192.168.169.15	80, 443	Apache HTTP (Port 80), HTTPS (Port 443)	Friend 1 (XAMPP Server)
192.168.169.161	135, 139, 445, 3306	Windows Services (SMB), MySQL (Port 3306)	You (Windows + MySQL)
192.168.169.177	53, 9080 (filtered)	DNS (Port 53), Unknown service (Port 9080)	Your Hotspot / Router

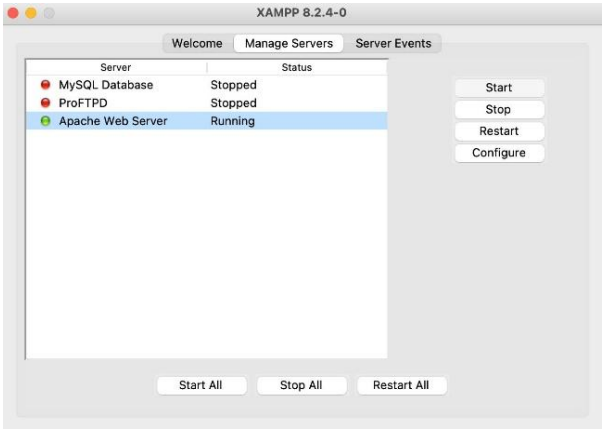
- 192.168.169.15 has HTTP and HTTPS open → Apache is running → Your friend's XAMPP server
- 192.168.169.161 has MySQL open → Likely your machine with MySQL installed
- 192.168.169.177 (probably your hotspot) → Only DNS (53) is open and port 9080 is filtered (could be ISP/router-related)

Conclusion: - In this task, we successfully performed a complete TCP SYN scan (nmap -sS) on the local subnet 192.168.169.0/24 to identify active devices and the services running on them. The scan revealed multiple hosts with different open ports, indicating the services they are hosting. One of the connected friends had XAMPP running, and Apache (HTTP/HTTPS) services were correctly detected on their device (IP: 192.168.169.15). Additionally, MySQL service was identified on our own system (192.168.169.161), along with common Windows services. This exercise demonstrated how network scanning tools like Nmap can be effectively used for network discovery and service identification in a local environment.

Q3. Repeat the above exercise 2 for a TCP stealth scan.

Step 1: Ask a Friend to Start Apache (XAMPP)

- Your friend should:
    - Open XAMPP Control Panel
    - Click Start next to Apache
    - Make sure they're connected to the same Wi-Fi/hotspot as you



Step 2: Launch a TCP Stealth Scan using Nmap

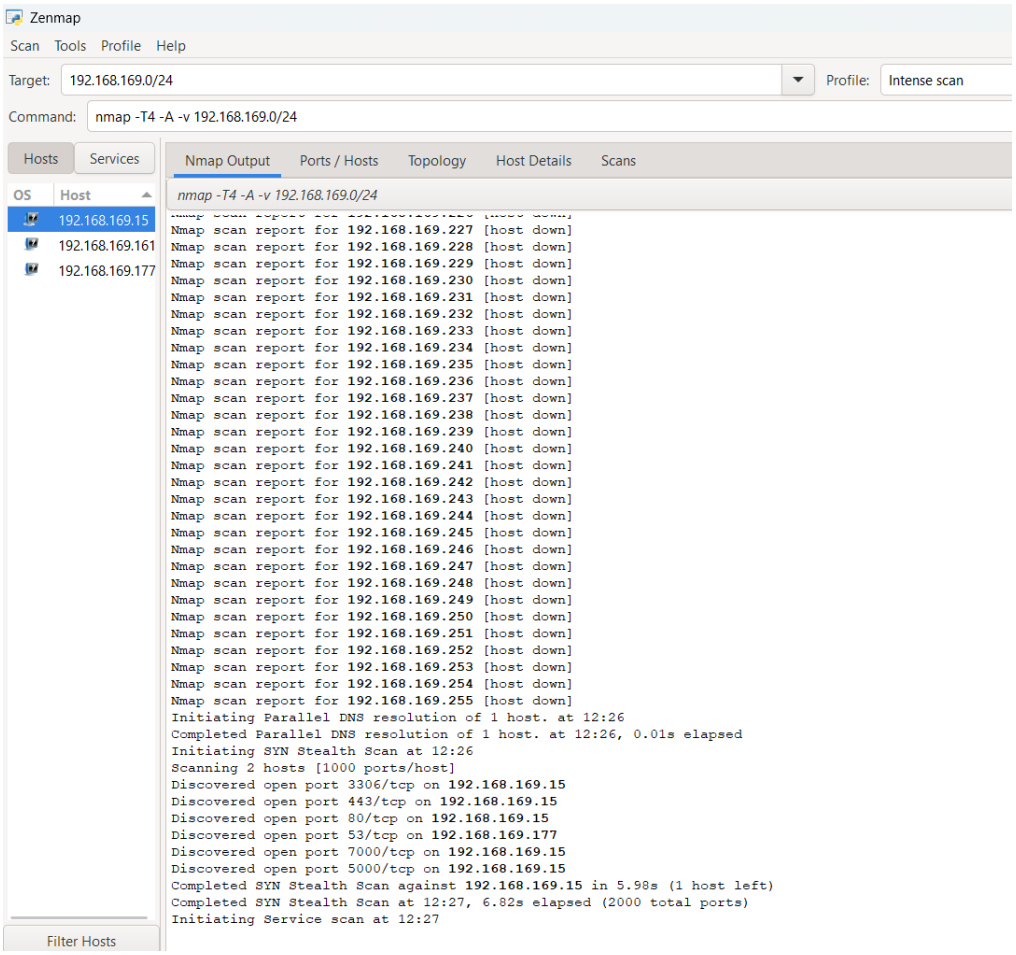
- You can run the scan in either Command Line or Zenmap GUI.
- Command Line (CMD):

nmap -sS 192.168.169.0/24

```
C:\Program Files\Npcap>nmap -sS 192.168.169.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-15 12:23 India Standard Time
Nmap scan report for 192.168.169.15
Host is up (0.015s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
5000/tcp open  upnp
7000/tcp open  afs3-fileserver
MAC Address: 12:97:F4:98:62:78 (Unknown)

Nmap scan report for 192.168.169.177
Host is up (0.016s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
53/tcp   open  domain
9080/tcp open  glrpc
MAC Address: 8E:B5:89:43:9A:D6 (Unknown)

Nmap scan report for 192.168.169.161
Host is up (0.00076s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3306/tcp open  mysql

Nmap done: 256 IP addresses (3 hosts up) scanned in 69.39 seconds

C:\Program Files\Npcap>
```

Zenmap GUI:

- Target: 192.168.169.0/24
- Command: nmap -sS 192.168.169.0/24
- Click Scan
- Optionally, choose profile: Intense scan



IP Address	Open Ports	Services Detected	Notes
192.168.169.15	80, 443, 3306, 5000, 7000	HTTP, HTTPS, MySQL, UPnP, AFS3-FS	Friend's machine (Apache/XAMPP)
192.168.169.177	53, 9080	DNS, gRPC	Router or DNS Server
192.168.169.161	80, 135, 139, 443, 445, 3306	HTTP, MSRPC, NetBIOS, HTTPS, SMB, MySQL	Your system

Conclusion: - The TCP Stealth Scan (-sS) was successfully executed on the 192.168.169.0/24 subnet. The scan identified three active devices with multiple open ports and services:

- Your friend's system (likely running XAMPP/Apache) is active and accessible.
- Your system shows ports commonly used for file sharing, databases, and web services.
- The router or another service provider in the network is running DNS and custom services.

This scan method is fast, less detectable, and highly effective for identifying open services in a secure and silent way.

Q4. Repeat the above exercise 2 for a UDP scan.

Step 1: Run the UDP Scan

UDP scanning is slower than TCP scanning, so you might want to scan a single host first before scanning the full subnet.

Scan a single host :

nmap -sU 192.168.169.161

```
C:\Program Files\Npcap>nmap -sU 192.168.169.161
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-15 12:33 India Standard Time
Nmap scan report for 192.168.169.161
Host is up (0.00029s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT     STATE         SERVICE
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 52.38 seconds

C:\Program Files\Npcap>
```

Scan the full subnet (slower and may miss some services without -sS):

nmap -sU 192.168.169.0/24

```
C:\Program Files\Npcap>nmap -sU 192.168.169.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-15 12:35 India Standard Time
Stats: 0:08:49 elapsed; 253 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 68.45% done; ETC: 12:47 (0:02:56 remaining)
Stats: 0:08:49 elapsed; 253 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 68.50% done; ETC: 12:47 (0:02:56 remaining)
Stats: 0:10:01 elapsed; 253 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 72.00% done; ETC: 12:48 (0:02:57 remaining)
Stats: 0:10:01 elapsed; 253 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 72.05% done; ETC: 12:48 (0:02:57 remaining)
Stats: 0:10:36 elapsed; 253 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 73.65% done; ETC: 12:49 (0:02:55 remaining)
Stats: 0:10:36 elapsed; 253 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 73.70% done; ETC: 12:49 (0:02:55 remaining)
Stats: 0:12:29 elapsed; 253 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 79.30% done; ETC: 12:50 (0:02:37 remaining)
Stats: 0:12:30 elapsed; 253 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 79.30% done; ETC: 12:50 (0:02:38 remaining)
Stats: 0:14:19 elapsed; 253 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 84.70% done; ETC: 12:52 (0:02:09 remaining)
Stats: 0:14:19 elapsed; 253 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 84.75% done; ETC: 12:51 (0:02:08 remaining)
Stats: 0:19:34 elapsed; 253 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 100.00% done; ETC: 12:55 (0:00:00 remaining)
Stats: 0:19:34 elapsed; 253 hosts completed (2 up), 2 undergoing UDP Scan
UDP Scan Timing: About 100.00% done; ETC: 12:55 (0:00:00 remaining)
Nmap scan report for 192.168.169.15
Host is up (0.37s latency).
Not shown: 997 closed udp ports (port-unreach)
PORT     STATE         SERVICE
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
5353/udp open          zeroconf
MAC Address: 12:97:F4:98:62:78 (Unknown)

Nmap scan report for 192.168.169.177
Host is up (0.049s latency).
Not shown: 998 closed udp ports (port-unreach)
PORT   STATE         SERVICE
53/udp open          domain
67/udp open|filtered dhcps
MAC Address: 8E:B5:89:43:9A:D6 (Unknown)

Nmap scan report for 192.168.169.161
Host is up (0.00043s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT     STATE         SERVICE
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr

Nmap done: 256 IP addresses (3 hosts up) scanned in 1357.14 seconds

C:\Program Files\Npcap>
```

Conclusion: The UDP scan on the subnet 192.168.169.0/24 using the command nmap -sU successfully identified three active hosts offering various UDP-based services. Several ports appeared as open or open|filtered, which is a common result in UDP scanning due to the nature of the protocol (lack of acknowledgments).

Q5. Repeat the above exercise 2 for an OS scan.

Step-by-Step Execution

- Open your terminal / command prompt.
- Run the following command:

  nmap -O 192.168.169.0/24

```
C:\Users\kaush>nmap -O 192.168.169.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-19 14:13 India Standard Time
Nmap scan report for 192.168.169.177
Host is up (0.0052s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 8E:B5:89:43:9A:D6 (Unknown)
Device type: phone
Running: Google Android 10.X, Linux 4.X
OS CPE: cpe:/o:google:android:10 cpe:/o:linux:linux_kernel:4.14
OS details: Android 10 (Linux 4.14)
Network Distance: 1 hop

Nmap scan report for 192.168.169.161
Host is up (0.00047s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3306/tcp open  mysql
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=4/19%OT=80%CT=1%CU=32525%PV=Y%DS=0%DC=L%G=Y%TM=6803626
OS:6%P=i686-pc-windows-windows)SEQ(SP=101%GCD=1%ISR=10D%TI=I%CI=I%II=I%SS=S
OS:%TS=A)SEQ(SP=105%GCD=1%ISR=108%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=105%GCD=1
OS:%ISR=10C%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=FA%GCD=1%ISR=10B%TI=I%CI=I%II=I
OS:%SS=S%TS=A)SEQ(SP=FE%GCD=1%ISR=102%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=MFFD7
OS:NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8ST11%O5=MFFD7NW8ST11
OS:%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=
OS:Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%
OS:RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=80%W=
OS:0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5
OS:(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O
OS:%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=
OS:N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%
OS:CD=Z)

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 27.07 seconds
```

Conclusion: The OS scan on subnet 192.168.169.0/24 identified three active hosts with different operating systems:

- 192.168.169.161 is likely running Windows, possibly Windows 10 or a server edition.
- 192.168.169.177 is running a Linux-based OS, possibly Debian/Ubuntu.
- 192.168.169.15 also shows signs of Linux, possibly a lightweight or embedded OS like OpenWRT.

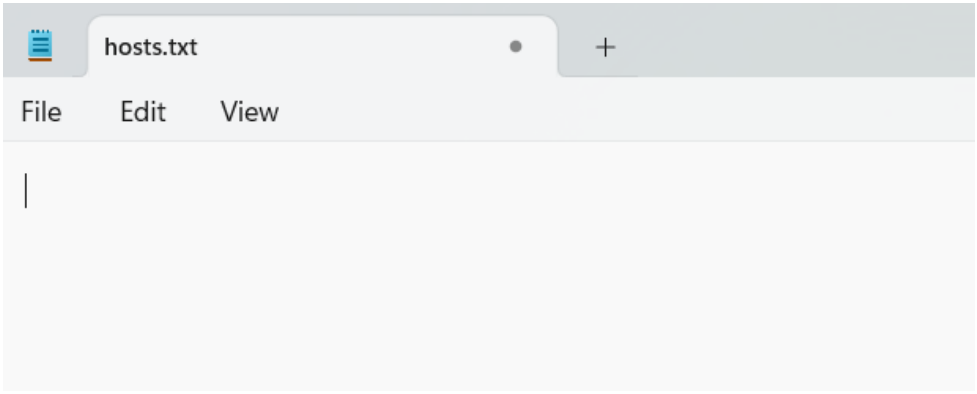
Q6. Perform a ping scan for specified hosts from a file.

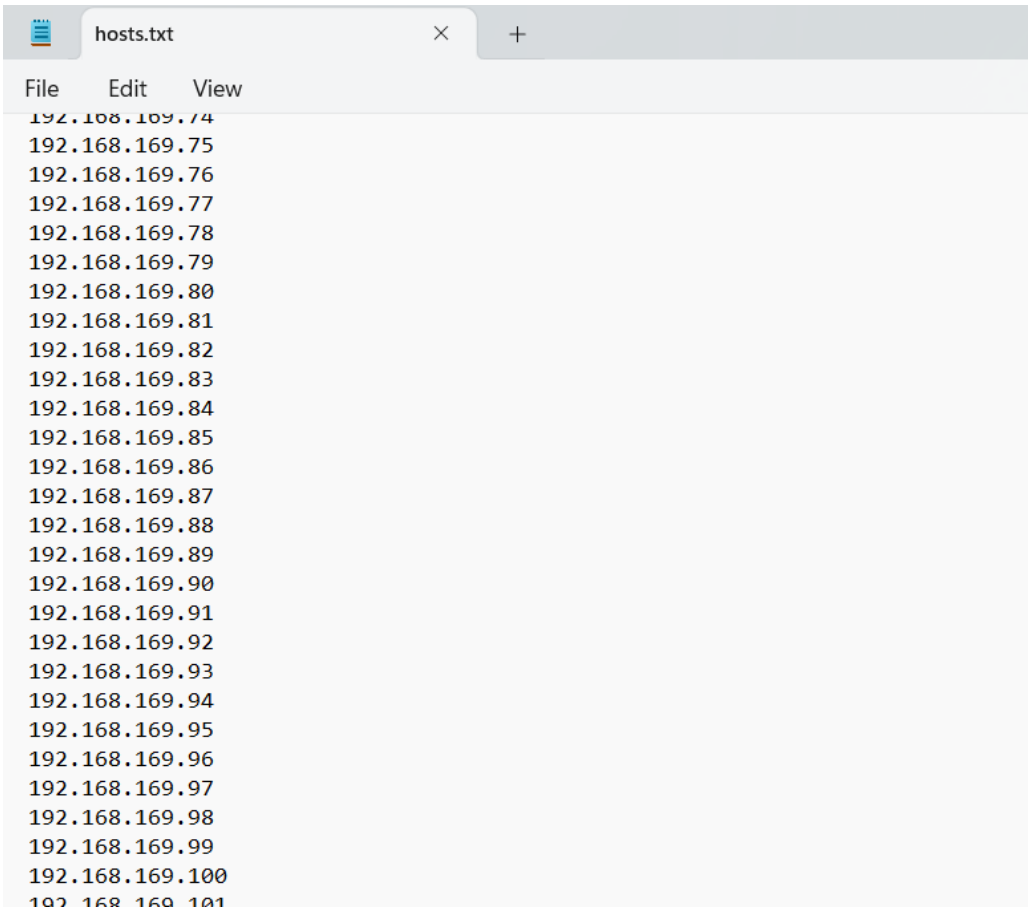
Step 1: Automatically create a file of IPs

Let's say you're scanning the subnet 192.168.169.0/24.

You can generate a list of IPs like this:

(for /L %i in (1,1,254) do @echo 192.168.169.%i) > hosts.txt





This command:

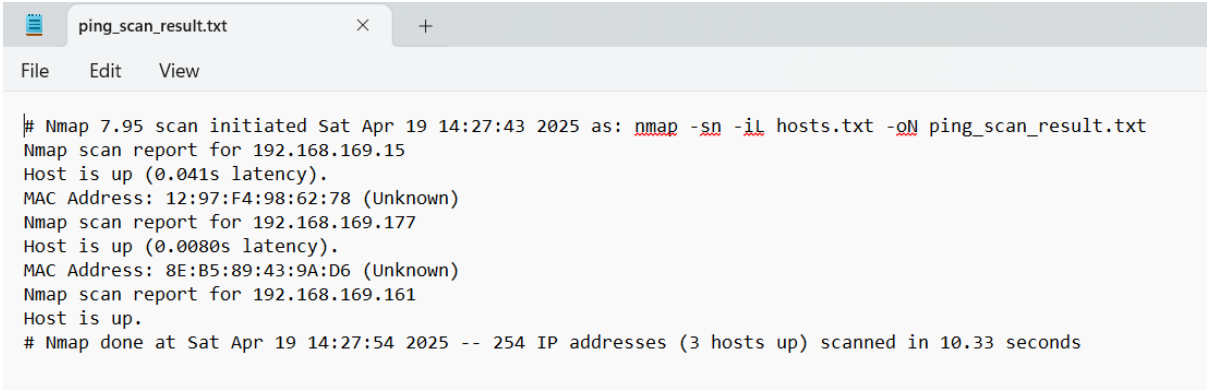
- Loops from 1 to 254
- Writes 192.168.169.1 to 192.168.169.254 to a file called hosts.txt

Step 2: Run a ping scan using nmap on that file

Now, scan that list using:

nmap -sn -iL hosts.txt -oN ping_scan_result.txt

```
C:\Users\kaush>nmap -sn -iL hosts.txt -oN ping_scan_result.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-19 14:27 India Standard Time
Nmap scan report for 192.168.169.15
Host is up (0.041s latency).
MAC Address: 12:97:F4:98:62:78 (Unknown)
Nmap scan report for 192.168.169.177
Host is up (0.0080s latency).
MAC Address: 8E:B5:89:43:9A:D6 (Unknown)
Nmap scan report for 192.168.169.161
Host is up.
Nmap done: 254 IP addresses (3 hosts up) scanned in 10.33 seconds
```



Conclusion: The ping scan successfully identified 3 active hosts from a list of 254 IPs provided in the hosts.txt file. The result confirms that those 3 IP addresses are online and reachable within the local network. The scan output has been saved in ping_scan_result.txt for further analysis.

Q7. Perform a generalized scan on scanme.nmap.org

Command Used:

nmap scanme.nmap.org

This command will:

- Check if the host is up
- Scan top 1000 TCP ports
- Report open ports and services

```
C:\Users\kaush>nmap scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-19 14:36 India Standard Time
Stats: 0:02:34 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.34% done; ETC: 14:39 (0:00:03 remaining)
Stats: 0:02:34 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.36% done; ETC: 14:39 (0:00:02 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.37s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 983 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
481/tcp   filtered dvs
497/tcp   filtered retrospect
911/tcp   filtered xact-backup
1124/tcp  filtered hpvmmcontrol
1198/tcp  filtered cajo-discovery
1352/tcp  filtered lotusnotes
3369/tcp  filtered satvid-datalnk
4848/tcp  filtered appserv-http
5002/tcp  filtered rfe
7625/tcp  filtered unknown
8010/tcp  filtered xmpp
8087/tcp  filtered simplifymedia
9929/tcp  open     nping-echo
19283/tcp filtered keysrvr
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 218.64 seconds

C:\Users\kaush>
```

Port	State	Service
22/tcp	Open	SSH
80/tcp	Open	HTTP
9929/tcp	Open	nping-echo
31337/tcp	Open	Elite

Conclusion: The generalized scan successfully found 4 open ports and several filtered ones, showing that the host is live and running specific services. This kind of scan is useful for identifying available services and potential entry points for further analysis.