

# PROJECT REPORT

## LOCAL NETWORK PORT SCANNING USING NMAP

(Scanning and Analyzing Open Ports in a Local Network using Nmap on Windows)

### 1. Objective

To identify open ports and active services running on devices within the local network using Nmap, in order to assess potential network exposure and security risks.

### 2. Tools Used

- **Nmap** (Network Mapper)
- **Zenmap GUI** (optional)
- **Wireshark** (for packet-level traffic analysis – optional)
- **Operating System:** Windows 10/11

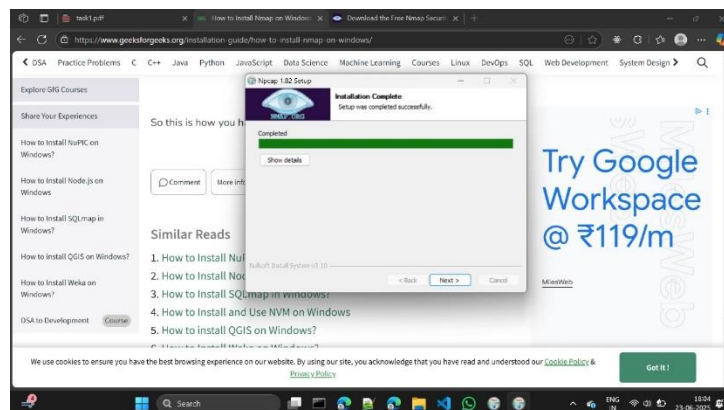
### 3. Network Details

- **IPv4 Address:** 192.168.208.160
- **Subnet Mask:** 255.255.255.0
- **Network Range (CIDR):** 192.168.208.0/24
- **Usable IP Range:** 192.168.208.1 – 192.168.208.254

### 4. Procedure

#### Step 1: Installed Nmap

- Downloaded from <https://nmap.org/download.html>
- Installed using the Windows self-installer
- Verified installation via Command Prompt (nmap -version)



#### Step 2: Identified Local Network Range

- Ran ipconfig to find IPv4 address and subnet mask

- Calculated network range: 192.168.208.0/24

```

Administrator: Command Prompt
E:\cyber_intern>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : 
Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . : 
   Link-local IPv6 Address . . . . . : fe80::282c:fd17:883b:5dcd%17
   IPv4 Address. . . . . : 192.168.255.1
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 
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  . : 
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : 
   IPv6 Address. . . . . : 2401:4900:6080:7c6d:8f8:1599:daff:6d07
   Temporary IPv6 Address. . . . . : 2401:4900:6080:7c6d:85c0:1e5f:3a24:221f
   Link-local IPv6 Address . . . . . : fe80::401:1bb4:d984:8393%10
   IPv4 Address. . . . . : 192.168.183.160
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : fe80::6835:edff:fe54:5653%10
                               192.168.183.71
E:\cyber_intern>

```

### Step 3: Performed Port Scan

- Opened Command Prompt as Administrator
- Executed the scan:  
**nmap -sS 192.168.208.0/24**
- Recorded all active hosts and open ports from the output

```

C:\Windows\System32>nmap -sS 192.168.208.0/24
Starting Nmap 7.97 ( https://nmap.org ) at 2025-06-23 18:26 +0530
Nmap scan report for 192.168.208.159
Host is up (0.0050s latency).
All 1000 scanned ports on 192.168.208.159 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 7C:A4:49:9A:21:7B (Xiaomi Communications)

Nmap scan report for 192.168.208.199
Host is up (0.0058s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: C6:A0:FD:EF:70:CD (Unknown)

Nmap scan report for 192.168.208.160
Host is up (0.0015s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
8080/tcp   open  http-proxy

Nmap done: 256 IP addresses (3 hosts up) scanned in 62.15 seconds
C:\Windows\System32>

```

### Step 4: Analyzed Traffic with Wireshark

- Captured packet data during scan
- Filtered TCP SYN and response packets
- Identified scan behavior and response types

Wireshark shows **thousands of packets**, so you need to **filter** to focus.

**tcp.port == 80**

To filter all traffic to/from a specific IP:

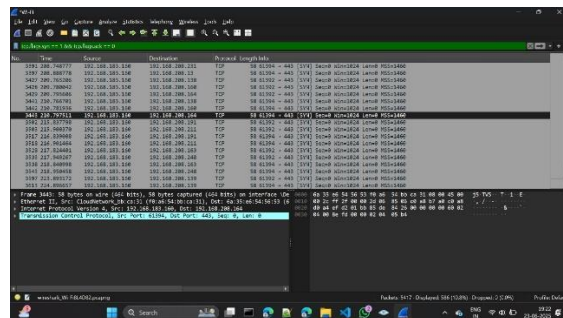
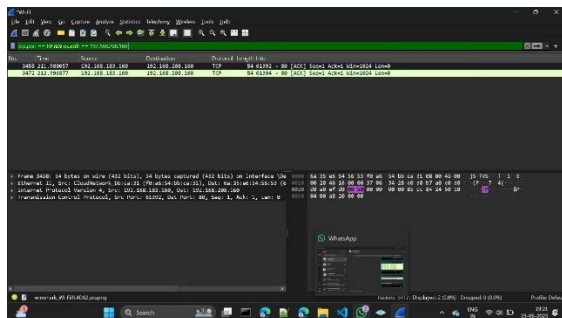
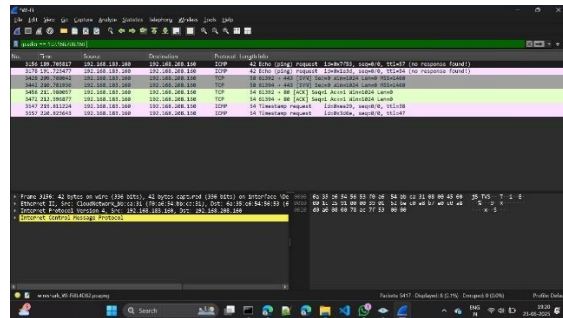
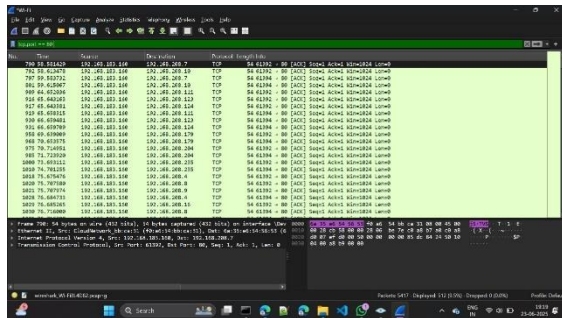
**ip.addr == 192.168.208.160**

Combine both:

**tcp.port == 80 && ip.addr == 192.168.208.160**

To filter Nmap SYN scan traffic:

**tcp.flags.syn == 1 && tcp.flags.ack == 0**



## 5. Saved Scan Output

- Used the following command to save:

**nmap -sS 192.168.208.0/24 > scan\_results.txt**

## 6. Save Nmap Results as a .html File (Using Zenmap GUI)

- Installed **Zenmap** (comes with Nmap installer)

### 1. Set Up the Scan:

- In **Target**, type: **192.168.208.0/24**
- In **Profile**, choose: **Intense scan**
- Click the **Scan** button

### 2. Wait for Scan to Complete:

- Zenmap will scan all IPs in your network and display the results in the bottom pane
  - IP addresses

- Hostnames (if found)
  - Open ports and the service names
3. **Save the Results:**
- Go to the menu bar: File → Save Scan
  - Choose a folder and name your file (e.g., nmap\_report.html)
  - Set the file type as: **.html**
  - Click **Save**

## 7. Risk Analysis

Port	Service	Security Risk	Recommendation
135	MS RPC (Microsoft Remote Procedure Call)	High – Often exploited for lateral movement in Windows networks (e.g., DCOM attacks, EternalBlue variants)	Disable if not used; restrict to trusted IPs only
139	NetBIOS Session Service	High – Legacy file/printer sharing; vulnerable to enumeration and attacks	Disable NetBIOS over TCP/IP; use SMBv2/v3 instead
445	SMB (Server Message Block)	High – Target for ransomware and exploits like EternalBlue	Disable if not needed; patch system and restrict via firewall
8080	HTTP Alternate (Web services)	Medium – Used for development/web servers; may run unprotected apps	Ensure apps on this port are authenticated and secured

## 8. Conclusion

Through this task, I gained practical experience in using Nmap to scan local networks and identify open ports and active services. This helped me understand basic cybersecurity principles such as network exposure, potential vulnerabilities, and the importance of minimizing unnecessary services.

## 9. References

- <https://nmap.org/download.html>
- [How to Install Nmap on Windows? - GeeksforGeeks](#)
- <https://www.wireshark.org/>
- [How to Install Wireshark on Windows? - GeeksforGeeks](#)