ELEVATE LABS

SCAN YOUR LOCAL NETWORK FOR OPEN PORTS

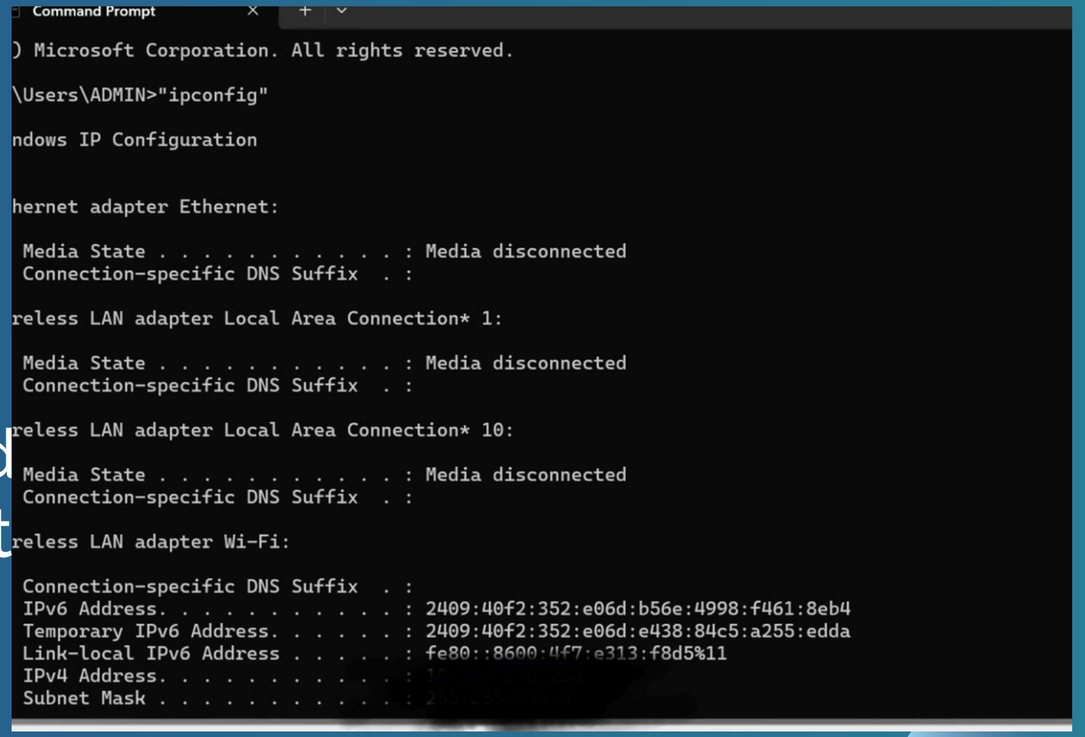
Learn to discover open ports on devices in your local network to understand network exposure.

1. INSTAL NMAP FROM OFFICIAL WEBSITE.

I downloaded the Nmap application from a Google search and successfully installed it on my system.

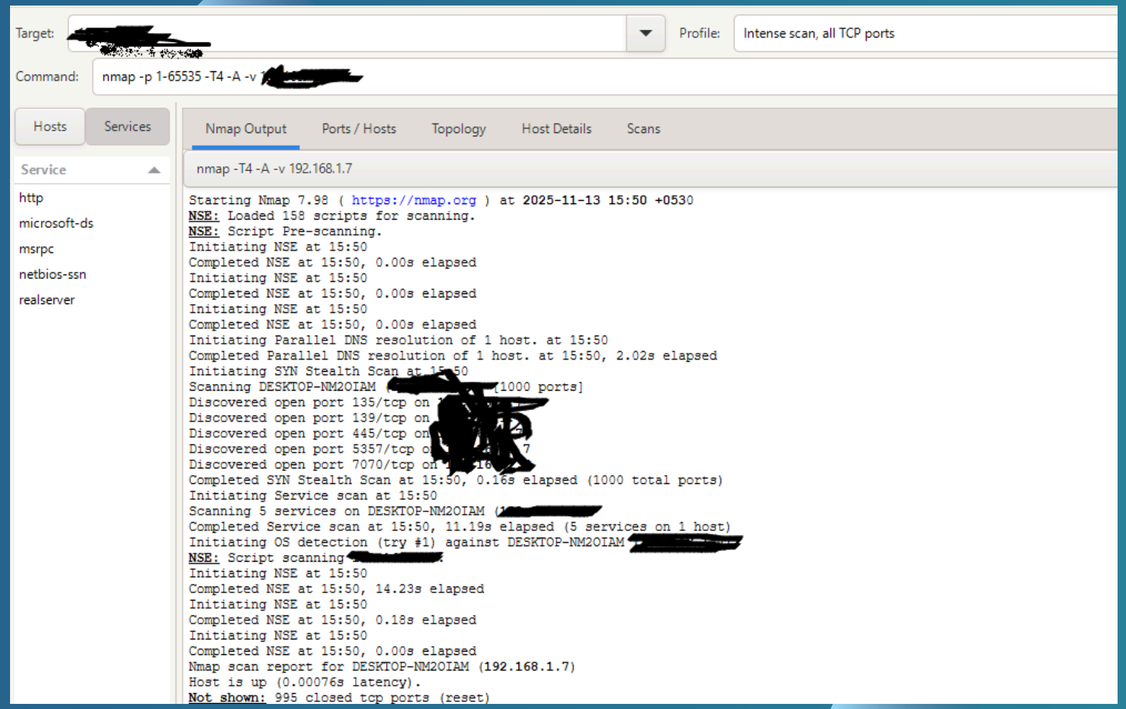
3.FIND YOUR LOCAL IP RANGE (E.G., 192.168.1.0/24).

To find my local IP address, I opened the Command Prompt from the Start menu, typed “ipconfig”, and got the IPv4 address details.

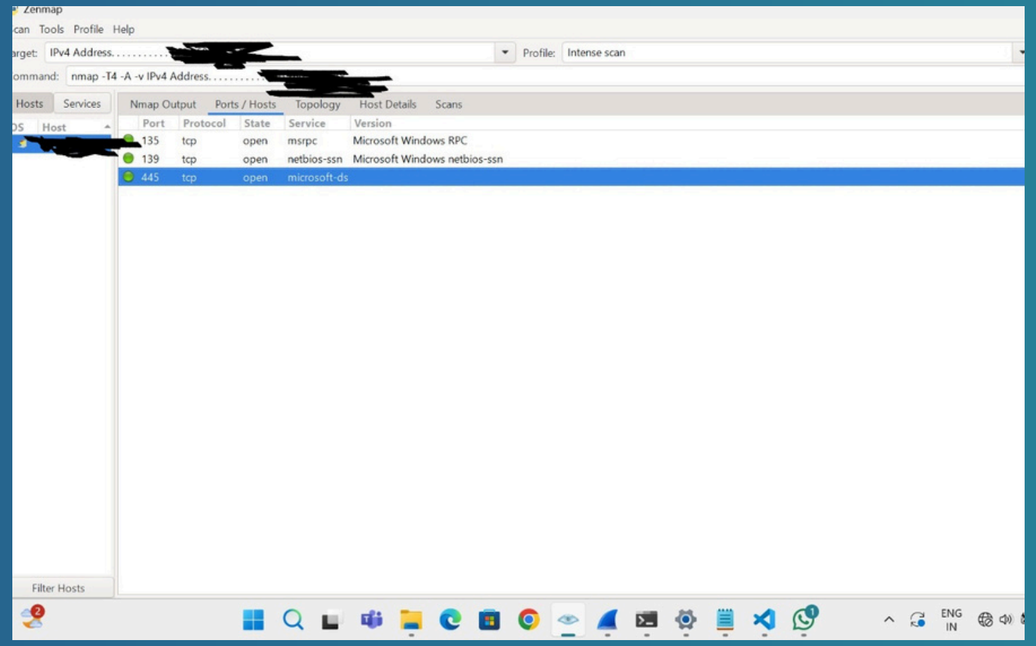


4.RUN: NMAP -SS 192.168.1.0/24 TO PERFORM TCP SYN SCAN.

To perform a TCP SYN scan, I opened the Nmap application and entered the IPv4 address in the target section. Then, in the profile section, I selected ‘Intense scan, all TCP ports’ and started the scan.



5.NOTE DOWN IP ADDRESSES AND OPEN PORTS FOUND.




```
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
No exact OS matches for host (If you know what OS is runni
TCP/IP fingerprint:
```

6.RESEARCH COMMON SERVICES RUNNING ON THOSE PORTS.

Port 135/tcp — MSRPC (Microsoft RPC)

- Used for Remote Procedure Calls in Windows.
- Supports services like DCOM, WMI, and remote management.

Port 139/tcp — NetBIOS Session Service

- Used for file sharing and printer sharing on older Windows systems.
- Supports SMB over NetBIOS.

6.RESEARCH COMMON SERVICES RUNNING ON THOSE PORTS.

Port 445/tcp — Microsoft-DS (SMB Direct)

- Used by SMB (Server Message Block) protocol.
- Handles:
  - file sharing
  - printer sharing
  - Windows authentication
  - Active Directory communication

7.IDENTIFY POTENTIAL SECURITY RISKS FROM OPEN PORTS.

Port 135 – MSRPC

Risk:

- Frequently targeted for DDoS amplification and remote code execution attacks.
- Historically vulnerable (e.g., MS Blaster worm).

Recommendation:

- Block externally on firewall
- Allow only inside LAN if necessary

7.IDENTIFY POTENTIAL SECURITY RISKS FROM OPEN PORTS.

Port 139 – NetBIOS
Risk:

- Can expose:
  - computer name
  - domain
  - network shares
- Vulnerable to:
  - NBNS poisoning
  - SMB relay attacks

Recommendation:

- Disable if not needed
- Use SMBv2/SMBv3 instead

7.IDENTIFY POTENTIAL SECURITY RISKS FROM OPEN PORTS.

Port 445 – SMB

Risk:

This is one of the most dangerous ports to leave open.

- Used in:
  - WannaCry ransomware
  - EternalBlue exploit
  - SMB relay attacks
  - Unauthorized file access
- Allows attackers to enumerate:
  - shared folders
  - users
  - passwords (via SMB brute force)

Recommendation:

- NEVER expose 445 to the internet
- Apply Windows patches
- Enable SMB signing

THANK YOU!