Task -1 Scanning Local Network for open ports

Sol. – first some details about nmap for better understanding

What is Nmap?

- Nmap (Network Mapper) is a free and open-source utility for network discovery and security auditing.
- It's used by network administrators for tasks like network inventory, managing service upgrade schedules, and monitoring host or service uptime.
- It's also widely used by security professionals for penetration testing, vulnerability scanning, and security auditing.

Key Capabilities

- Host discovery (identifying active hosts on a network)
- Port scanning (determining open ports and services)
- OS detection (identifying the operating system of target hosts)
- Service version detection (identifying the application and version listening on a port)
- Scriptable interaction with the target (using Nmap Scripting Engine - NSE)

Why Nmap?

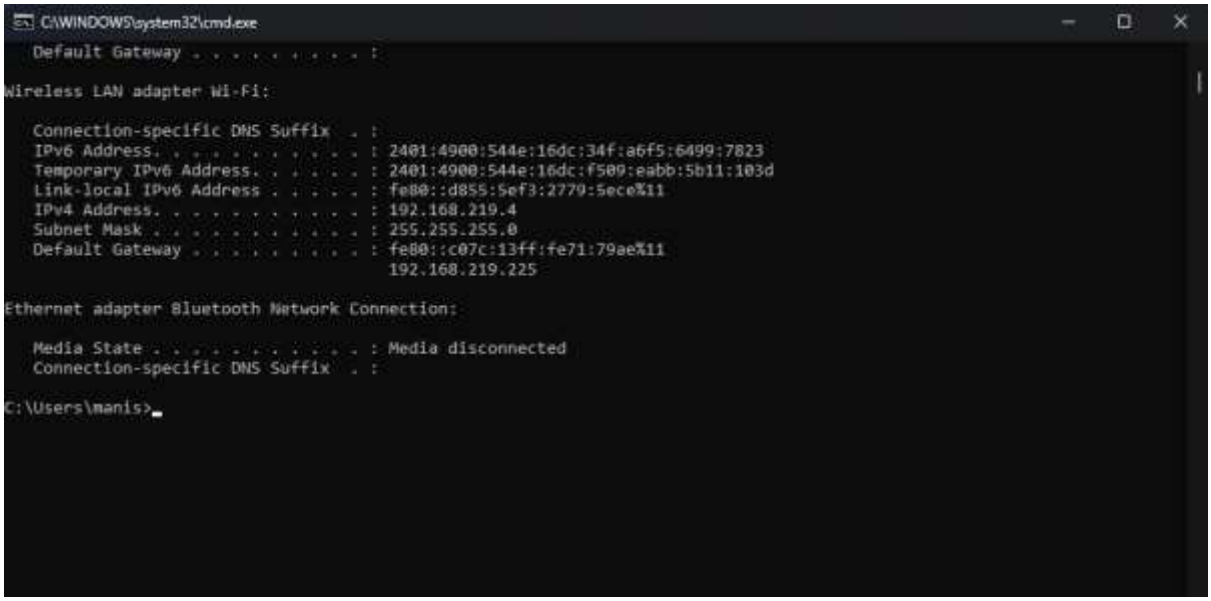
- **Comprehensive:** Offers a wide range of scanning techniques and features.
- **Flexible:** Can scan single hosts, IP ranges, or entire networks.
- **Powerful:** Capable of deep network analysis and identification of subtle vulnerabilities.
- **Cross-Platform:** Available on Linux, Windows, macOS, and other operating systems.
- **Community Support:** Large and active community, extensive documentation.

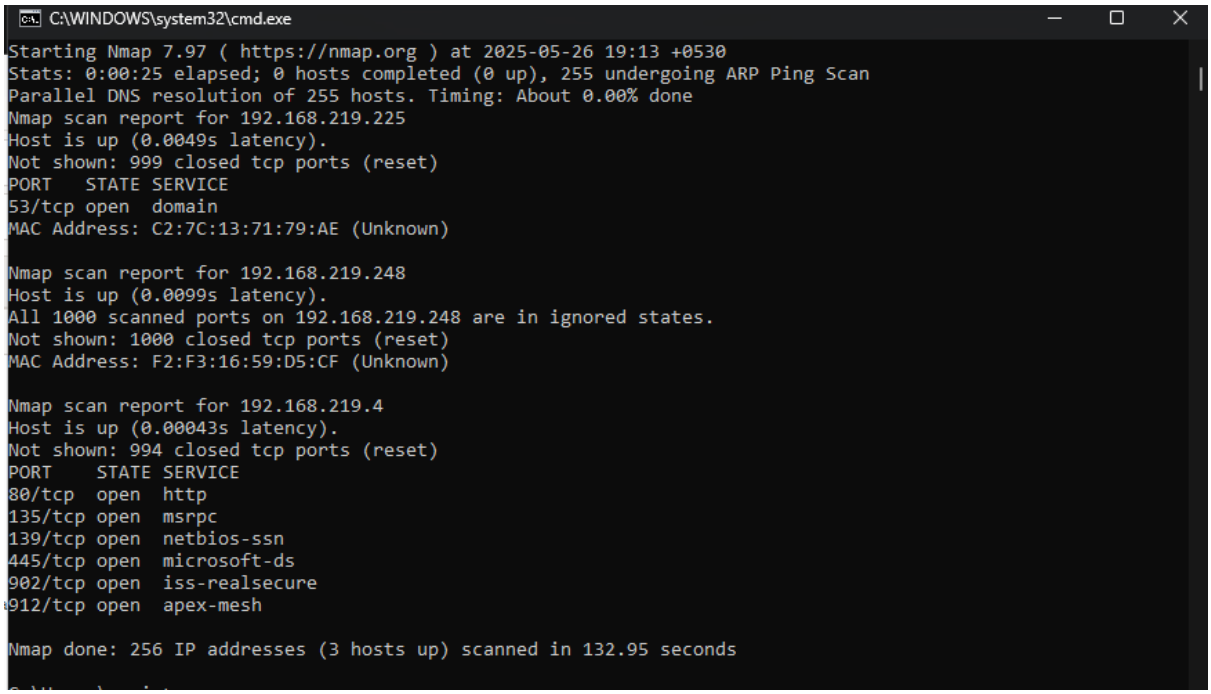
Downloaded Nmap from his official website

[Download the Free Nmap Security Scanner for Linux/Mac/Windows]

Next : find the local ip range

So use the command of **ipconfig** for ip.





Starting Nmap 7.97 (https://nmap.org) at 2025-05-26 19:15 +0530

Nmap scan report for 192.168.219.4

Host is up (0.0014s latency).

Not shown: 994 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

902/tcp open iss-realsecure

912/tcp open apex-mesh

There are total 6 open ports in my local network.

Next Step : -

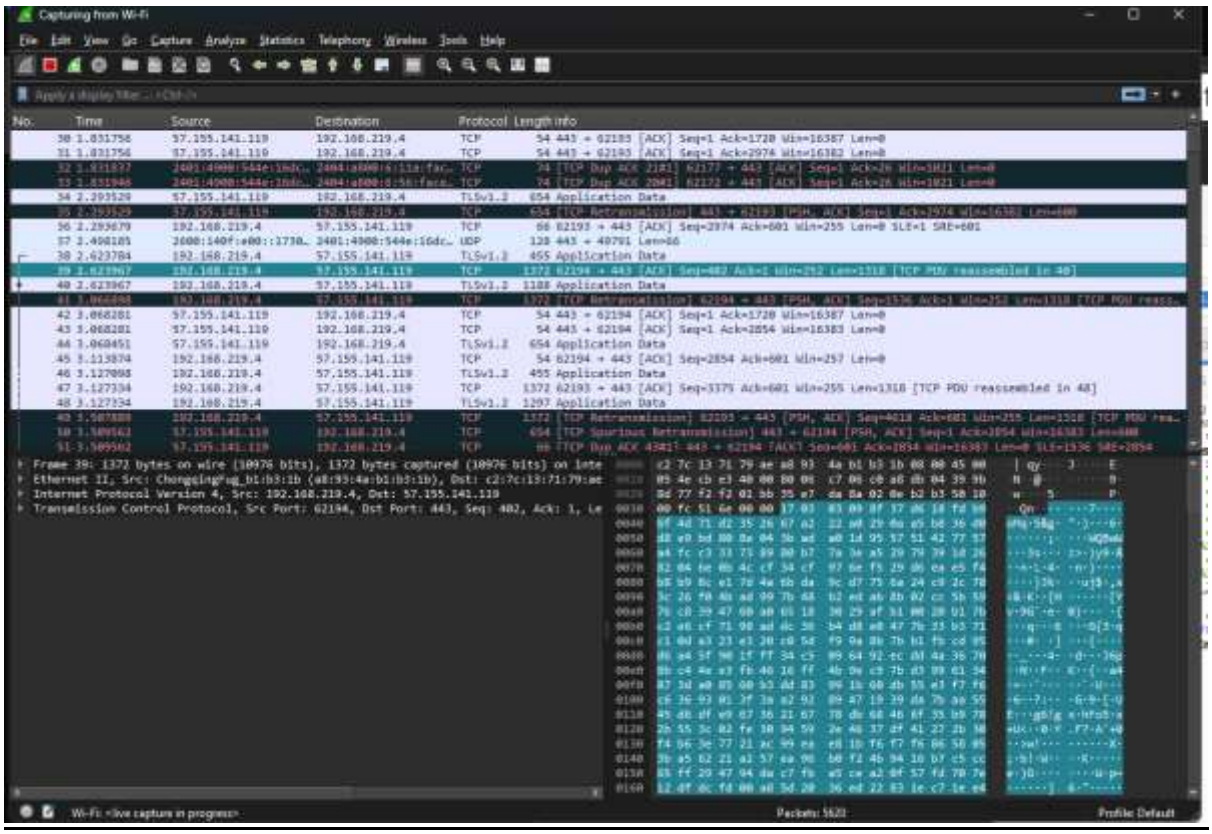
There is some services running in open ports and their versions

```
C:\Windows\System32>nmap -sS -sV 192.168.219.4
Starting Nmap 7.97 ( https://nmap.org ) at 2025-05-26 19:19 +0530
Nmap scan report for 192.168.219.4
Host is up (0.00076s latency).
Not shown: 994 closed tcp ports (reset)
PORT    STATE SERVICE         VERSION
80/tcp  open  http            Microsoft IIS httpd 10.0
135/tcp open  msrpc           Microsoft Windows RPC
139/tcp open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
902/tcp open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 8.39 seconds

C:\Windows\System32>
```

Wireshark Packet Analyser –

Download wireshark from it’s official Website

[Wireshark · Download]



Here some packets where the connection establishing via 3 way handshaking

Some Raw Application data showing on above image.

Next Steps :

Some common services which most running locally on ports

Like- http, https, Microsoft DB

Port 135 –

MSRPC is a protocol used by Microsoft Windows systems to allow software components to communicate over a network. It's commonly used for various Windows services like file sharing, printer sharing, and remote management. MSRPC typically runs over TCP port 135.

Port 139 –

NetBIOS Session Service (NetBIOS SSN) runs over TCP port 139 and is part of the NetBIOS over TCP/IP protocol suite. It provides session-layer services for Windows networking, enabling file sharing, printer sharing, and other network communication between Windows machines in a local network.

Port 445 –

Port 445 is commonly used for Microsoft-DS (Directory Services) over TCP/IP, primarily for SMB (Server Message Block) protocol communication. SMB allows file sharing, printer sharing, and various network services in Windows environments. Port 445 is used for direct hosting of SMB over TCP without the older NetBIOS layer.

Port 902 –

Port 902 is commonly associated with VMware services, specifically VMware Server and VMware ESX/ESXi hosts. It is used for the VMware Remote Console and VMware Authentication Daemon, facilitating remote management and communication between the VMware client and the host.

Port 912 –

Port 912 is not one of the most commonly known or standardized ports. It is officially registered with IANA for the "apex-mesh" service, which relates to Apex Mesh, a network management or mesh networking protocol.

Identify Potential Security risks from Open Ports –

Open ports can expose services that might have vulnerabilities or misconfigurations, creating potential security risks. Common risks include outdated software with known exploits, services running with excessive privileges, weak authentication, or unnecessary services that increase the attack surface.

To identify risks, start by scanning open ports with Nmap using service and version detection (**-sV**) and script scanning (**-sC**) to gather detailed info. Then, cross-reference the discovered services and versions against vulnerability databases like CVE or exploit databases to find known issues.

For example, an open port running an outdated version of an FTP server might be vulnerable to anonymous access or buffer overflow exploits. Similarly, open management ports (like SSH, RDP, or database ports) without proper access controls can be entry points for attackers.

if port 21 (FTP) is open and running an outdated FTP server version, it might allow anonymous login or be vulnerable to buffer overflow attacks, letting attackers upload or execute malicious files. Similarly, an open port 3389 (RDP) without strong authentication could allow unauthorized remote desktop access, leading to full system compromise.

Another example is port 80 or 443 running a web server with outdated software that has known vulnerabilities like remote code execution or SQL injection, which attackers can exploit to take control or steal data.