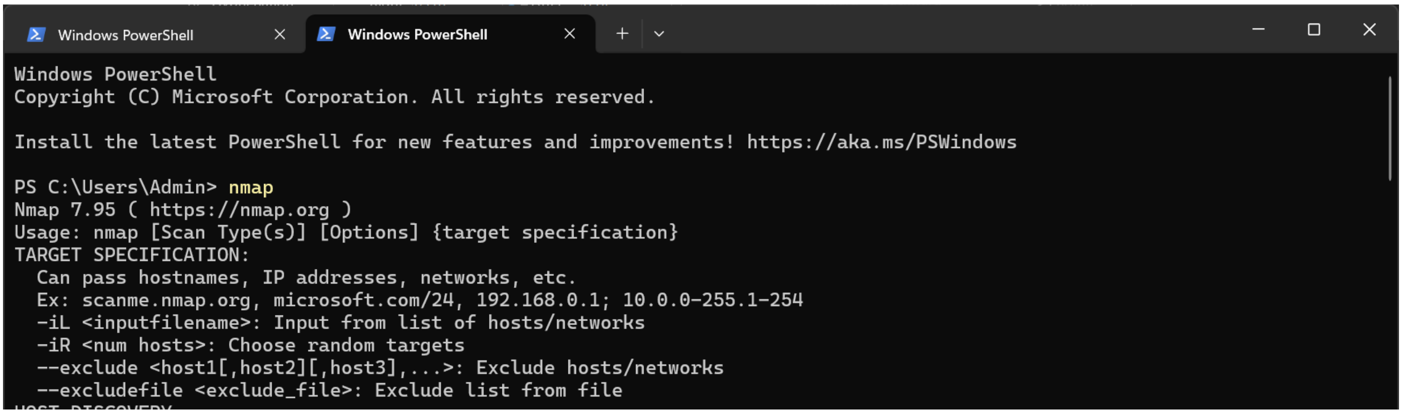
Task 1:

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

Tools Used: Nmap

1.Install Nmap from official website.

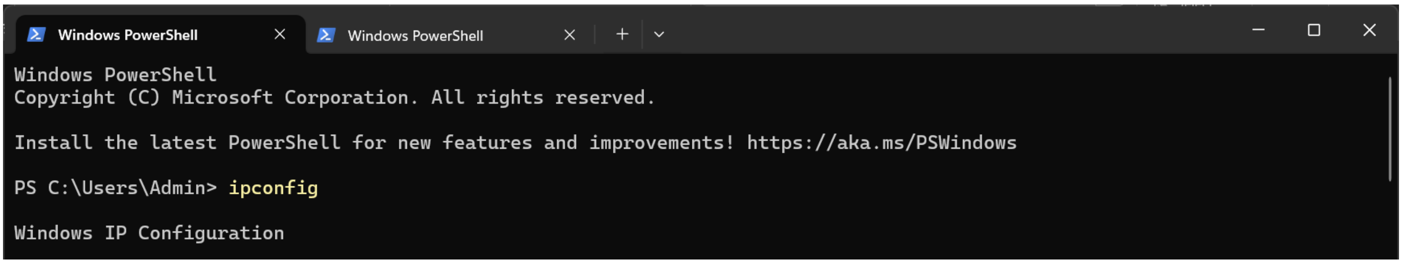


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Admin> nmap
Nmap 7.95 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
```

2.Find your local IP range.

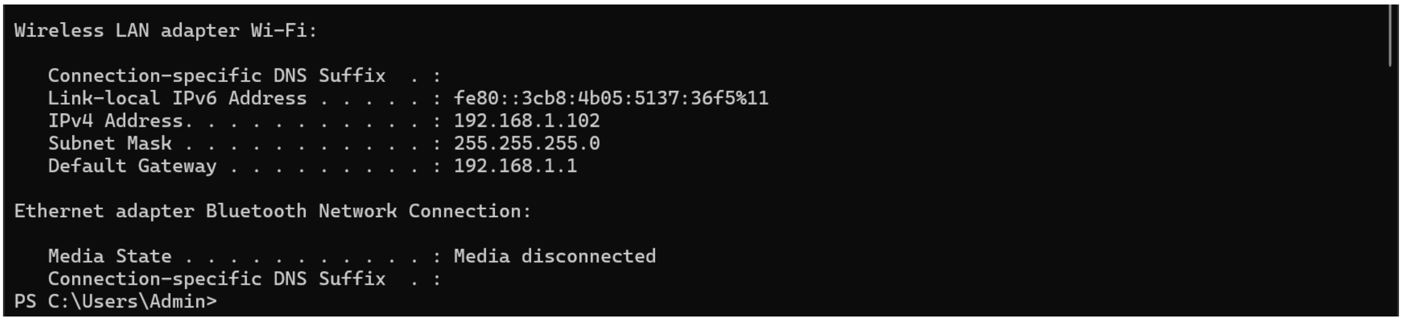


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Admin> ipconfig

Windows IP Configuration
```



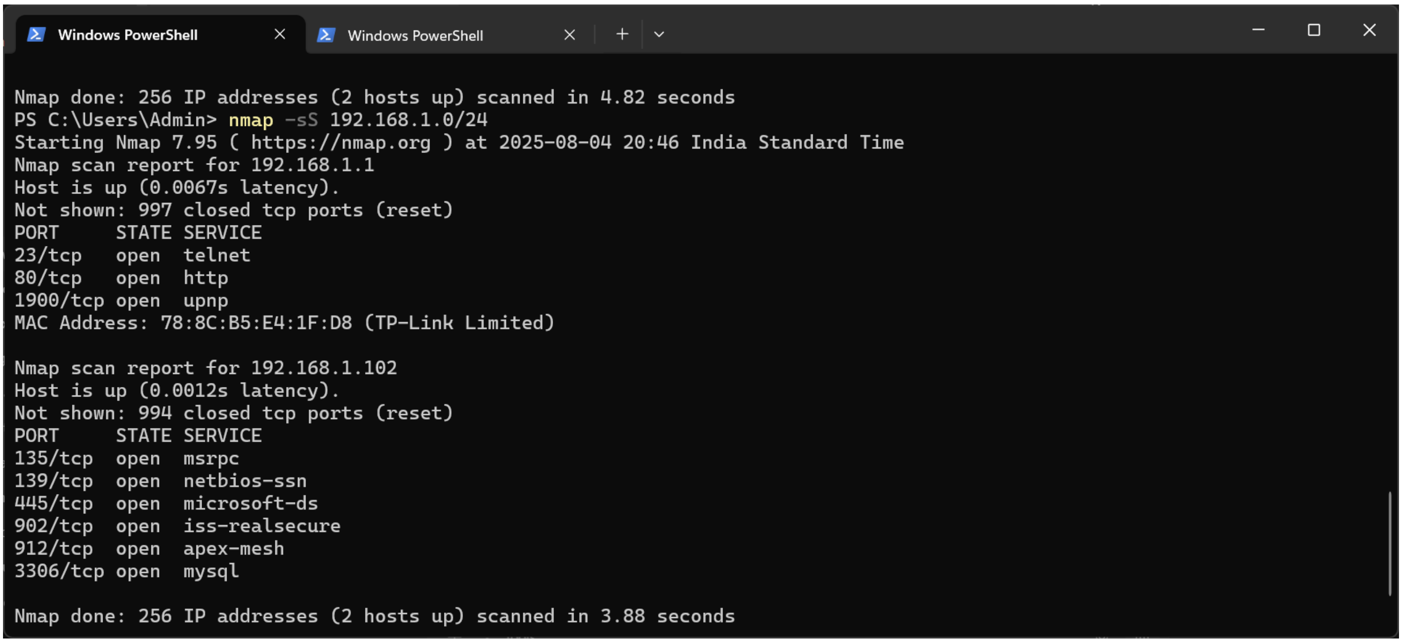
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3cb8:4b05:5137:36f5%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
PS C:\Users\Admin>
```

3. Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan.

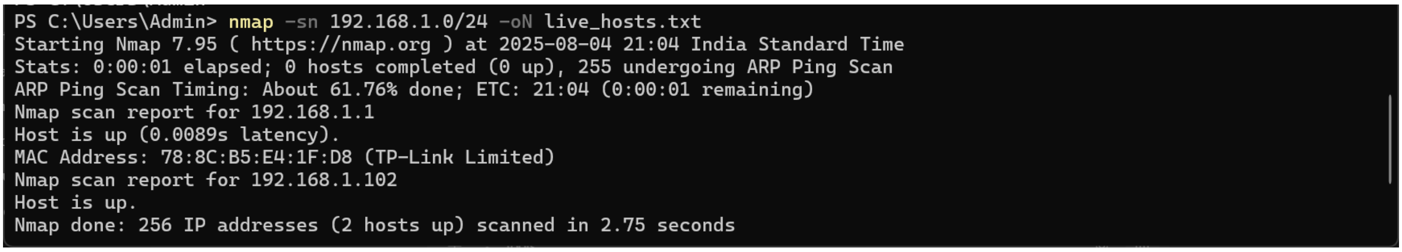


```
Nmap done: 256 IP addresses (2 hosts up) scanned in 4.82 seconds
PS C:\Users\Admin> nmap -sS 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 20:46 India Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.0067s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
1900/tcp open  upnp
MAC Address: 78:8C:B5:E4:1F:D8 (TP-Link Limited)

Nmap scan report for 192.168.1.102
Host is up (0.0012s latency).
Not shown: 994 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
3306/tcp open  mysql

Nmap done: 256 IP addresses (2 hosts up) scanned in 3.88 seconds
```

4. Note down IP addresses and open ports found.



```
PS C:\Users\Admin> nmap -sn 192.168.1.0/24 -oN live_hosts.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 21:04 India Standard Time
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 61.76% done; ETC: 21:04 (0:00:01 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.0089s latency).
MAC Address: 78:8C:B5:E4:1F:D8 (TP-Link Limited)
Nmap scan report for 192.168.1.102
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.75 seconds
```

6.Research common services running on those ports.

1. Host: 192.168.1.1 (TP-Link Router)

Port	Service	Description
23	Telnet	An old, unencrypted remote login protocol, security risk if enabled.
80	HTTP	Web interface for router configuration, likely the admin panel.
1900	uPnP	Universal Plug and Play, allows devices to auto-configure port forwarding, often abused in attacks.

2. Host: 192.168.1.102 (Windows Machine)

Port	Service	Description
135	MSRPC	Windows Remote Procedure Call, used by Windows for internal communication.
139	NetBIOS-SSN	Supports file sharing and network browsing, legacy protocol, can be exploited.
445	Microsoft-DS (SMB)	Main port for Windows file and printer sharing (SMB), often targeted in ransomware attacks.
902	ISS-Realsecure	Typically used by VMware for remote management (used in virtualized environments).
912	Apex-Mesh	Less common; possibly related to local applications or services.
3306	MySQL	Default port for MySQL database, ensure it's not exposed externally.

7.Identify potential security risks from open ports.

Port 23 (Telnet)

- Telnet sends data in plain text, making it easy for attackers to intercept credentials.
- It's outdated and vulnerable to brute-force attacks.

Port 80 (HTTP)

- HTTP traffic is unencrypted, which can expose login details and sensitive data.
- If the web interface uses default credentials, it can be easily compromised.

Port 1900 (UPnP)

- UPnP can be exploited by malware to open ports automatically without user consent.
- Often used in botnet attacks like Mirai.

Port 135 (MSRPC)

- Used for internal Windows communication; attackers can exploit it for enumeration or lateral movement.
- May reveal sensitive service information.

Port 139 and 445 (NetBIOS/SMB)

- Commonly exploited in ransomware attacks (e.g., WannaCry).
- Exposes file sharing, which can allow attackers to access or modify files on the system.

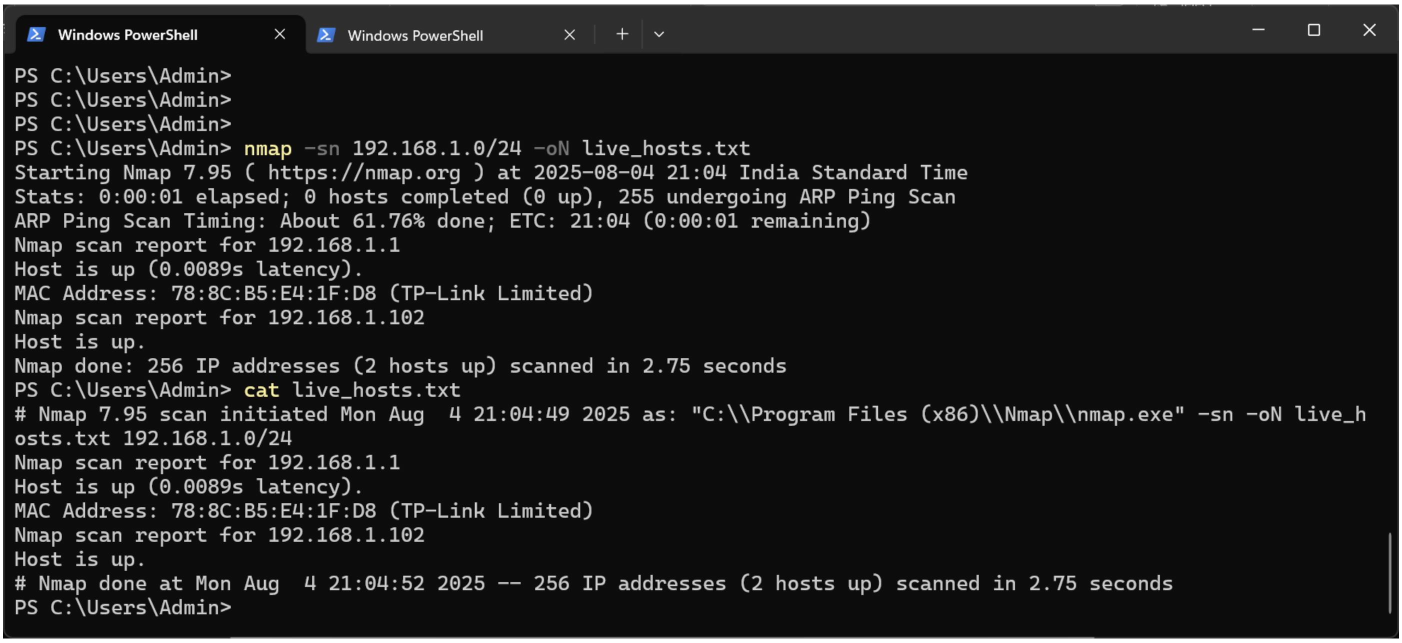
Port 902 and 912 (VMware / custom services)

- These ports may be linked to virtual machine management or unknown services.
- If not secured or monitored, they can become unnoticed entry points.

Port 3306 (MySQL)

- If exposed, attackers can attempt to access the database and steal or delete data.
- Databases should never be exposed to the internet without proper restrictions.

8.Save scan results as a text file.



```
PS C:\Users\Admin>
PS C:\Users\Admin>
PS C:\Users\Admin>
PS C:\Users\Admin> nmap -sn 192.168.1.0/24 -oN live_hosts.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 21:04 India Standard Time
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 61.76% done; ETC: 21:04 (0:00:01 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.0089s latency).
MAC Address: 78:8C:B5:E4:1F:D8 (TP-Link Limited)
Nmap scan report for 192.168.1.102
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.75 seconds
PS C:\Users\Admin> cat live_hosts.txt
# Nmap 7.95 scan initiated Mon Aug  4 21:04:49 2025 as: "C:\\Program Files (x86)\\Nmap\\nmap.exe" -sn -oN live_h
osts.txt 192.168.1.0/24
Nmap scan report for 192.168.1.1
Host is up (0.0089s latency).
MAC Address: 78:8C:B5:E4:1F:D8 (TP-Link Limited)
Nmap scan report for 192.168.1.102
Host is up.
# Nmap done at Mon Aug  4 21:04:52 2025 -- 256 IP addresses (2 hosts up) scanned in 2.75 seconds
PS C:\Users\Admin>
```