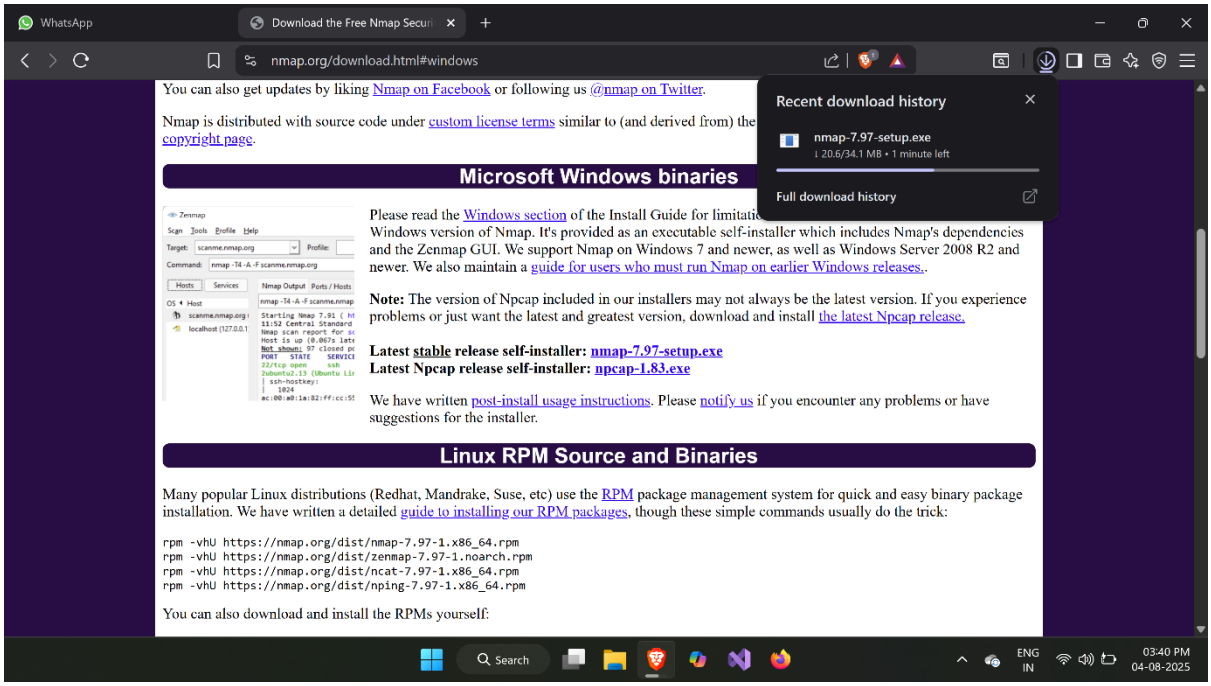
# Task 1:- Scan Your Local Network for Open Ports

## Step 1: Download Nmap for Windows

Refer to the image below for the official Nmap download page:

Navigate to the official Nmap website: https://nmap.org/download.html#windows

1. Click on the link `` to download the latest stable version for Windows.
2. Also download **Npcap** if not included: ``.




---

## Step 2: Verify Installation

Use Command Prompt to verify that Nmap has been installed successfully:

nmap -v

This will output the Nmap version and other runtime information.

```
C:\Users\Eshwara K>nmap -v
Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-04 16:27 +0530
Read data files from: C:\Program Files (x86)\Nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds
           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```

---

## Step 3: Find Local IP Configuration

To determine your system's IP address:

ipconfig

```
C:\Users\Eshwara K>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ae13:6782:f833:c484%8
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Unknown adapter Local Area Connection:

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

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. . . . . . . . . . . : 2409:40f4:2102:a29:ff12:204f:3d8d:9719
```

Locate the **IPv4 Address** under the active network adapter (e.g., Ethernet or Wi-Fi).

---

**Step 4: Run a Basic Scan**

Perform a TCP SYN scan on a known IP address (e.g., your default gateway):

nmap -sS 192.168.56.1

This reveals open ports and associated services.

```
C:\Users\Eshwara K>nmap -sS 192.168.56.1
Starting Nmap 7.97 ( https://nmap.org ) at 2025-08-04 16:30 +0530
Nmap scan report for 192.168.56.1
Host is up (0.00020s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
808/tcp  open  ccproxy-http
9001/tcp open  tor-orport

Nmap done: 1 IP address (1 host up) scanned in 0.76 seconds
```

Example output shows open ports like:

- 135/tcp (msrpc)
    - Port 135 is used as a service control manager (SCM). It acts as a dispatcher that lets client applications locate various services running on a Windows machine, such as:

- DCOM (Distributed Component Object Model)
- WMI (Windows Management Instrumentation)
- Remote administration tools
- File and printer sharing

- 139/tcp (netbios-ssn)
    - File sharing
    - Printer sharing
    - Windows network discovery (browsing shared folders)
    - Remote administration

- 445/tcp (microsoft-ds)
    - File and printer sharing
    - Accessing shared drives/folders
    - Remote administration (via SMB)
    - Windows domain authentication
    - Active Directory communication
    - WMI and PowerShell remoting

- 808/tcp (ccproxy-http)
    - Web applications for development or testing (e.g., Tomcat, Jenkins)
    - IoT devices and routers (web interface over port 808)
    - Transparent proxy services (like CCProxy)

- 9001/tcp (tor-orport)
    - Tor Relay Communication
      Port 9001 is used by **Tor relays (also called onion routers)** to communicate with one another.
      It's the **ORPort (Onion Routing Port)** in Tor's terminology.

---

**Step 5: Save Scan Results to HTML**

You can save the scan output to a file for reports or documentation:

nmap -sS 192.168.56.1 >output.html  # Save as HTML

```
C:\Users\Eshwara K>nmap -sS 192.168.56.1 > output.html
```