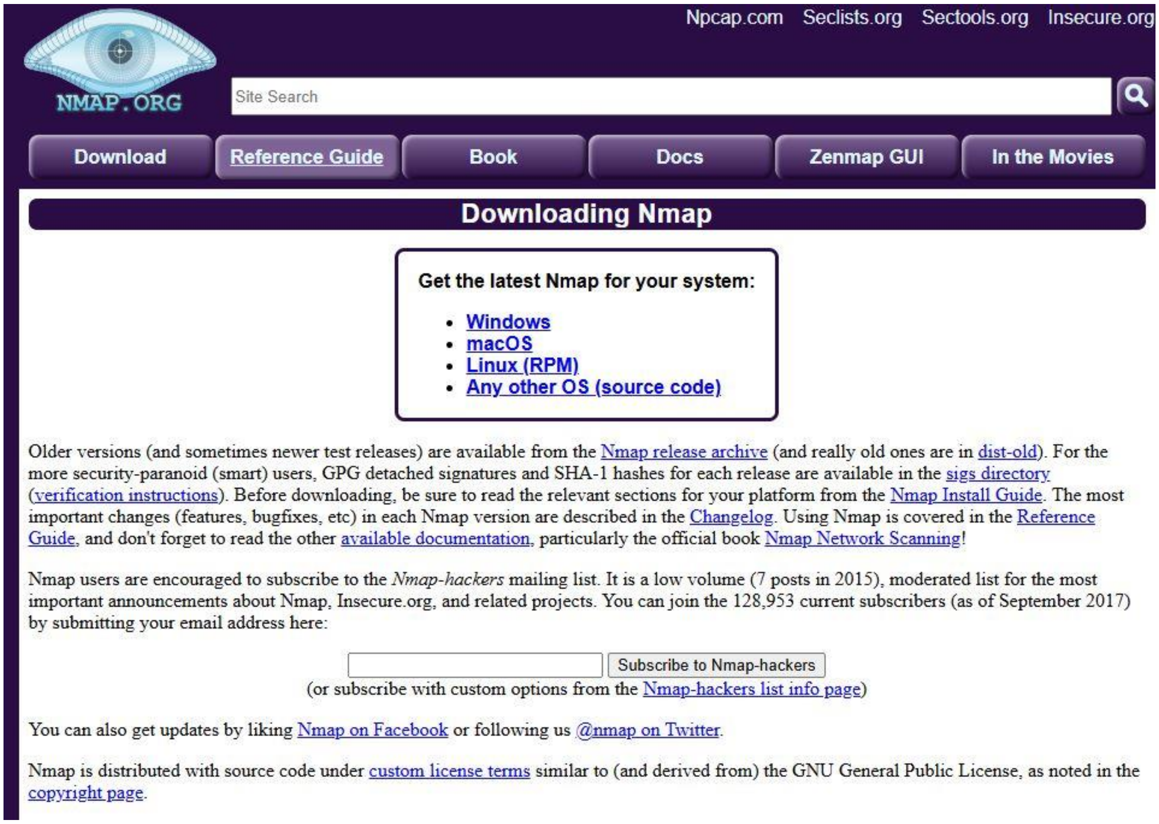
Nmap Scan Analysis

1. Install Nmap from the Official Website

Visit: https://nmap.org/download.html
Download and install Nmap for your OS (Windows, macOS, or Linux). Optionally, install Zenmap (Nmap's GUI) if you're more comfortable with a graphical interface.



Downloading Nmap

Get the latest Nmap for your system:

- Windows
- macOS
- Linux (RPM)
- Any other OS (source code)

Older versions (and sometimes newer test releases) are available from the Nmap release archive (and really old ones are in dist-old). For the more security-paranoid (smart) users, GPG detached signatures and SHA-1 hashes for each release are available in the sigs directory (verification instructions). Before downloading, be sure to read the relevant sections for your platform from the Nmap Install Guide. The most important changes (features, bugfixes, etc) in each Nmap version are described in the Changelog. Using Nmap is covered in the Reference Guide, and don't forget to read the other available documentation, particularly the official book Nmap Network Scanning!

Nmap users are encouraged to subscribe to the *Nmap-hackers* mailing list. It is a low volume (7 posts in 2015), moderated list for the most important announcements about Nmap, Insecure.org, and related projects. You can join the 128,953 current subscribers (as of September 2017) by submitting your email address here:

(or subscribe with custom options from the Nmap-hackers list info page)

You can also get updates by liking Nmap on Facebook or following us @nmap on Twitter.

Nmap is distributed with source code under custom license terms similar to (and derived from) the GNU General Public License, as noted in the copyright page.

2. Find Your Local IP Range

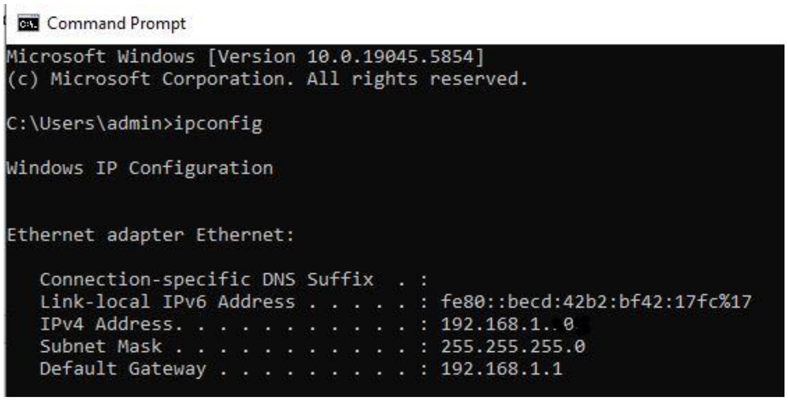
Windows:
  Open CMD and run:

```
ipconfig
```

  Look for your IPv4 address and subnet (e.g., 192.168.1.5, subnet 255.255.255.0 → range is 192.168.1.0/24)

Linux/macOS:
  Run:

```
ifconfig
```



```
Microsoft Windows [Version 10.0.19045.5854]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::becd:42b2:bf42:17fc%17
   IPv4 Address. . . . . . . . . . . : 192.168.1.[redacted]0
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

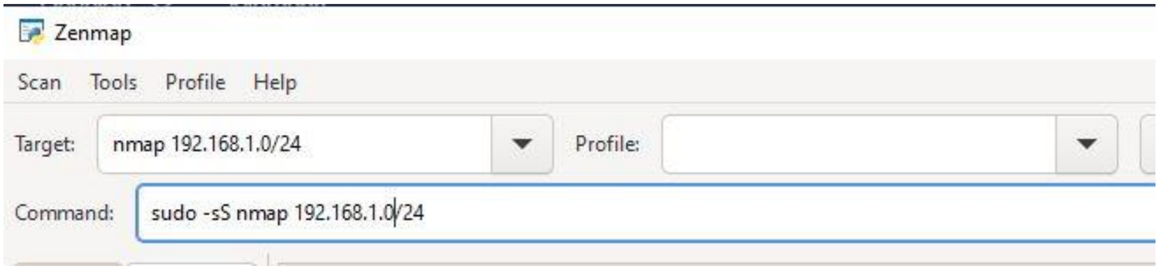
3. Run the Nmap TCP SYN Scan

Open a terminal or CMD and type:

```
nmap -sS 192.168.1.0/24
```

On Linux/macOS, use sudo:

```
sudo nmap -sS 192.168.1.0/24
```



Target: nmap 192.168.1.0/24

Profile:

Command: sudo -sS nmap 192.168.1.0/24

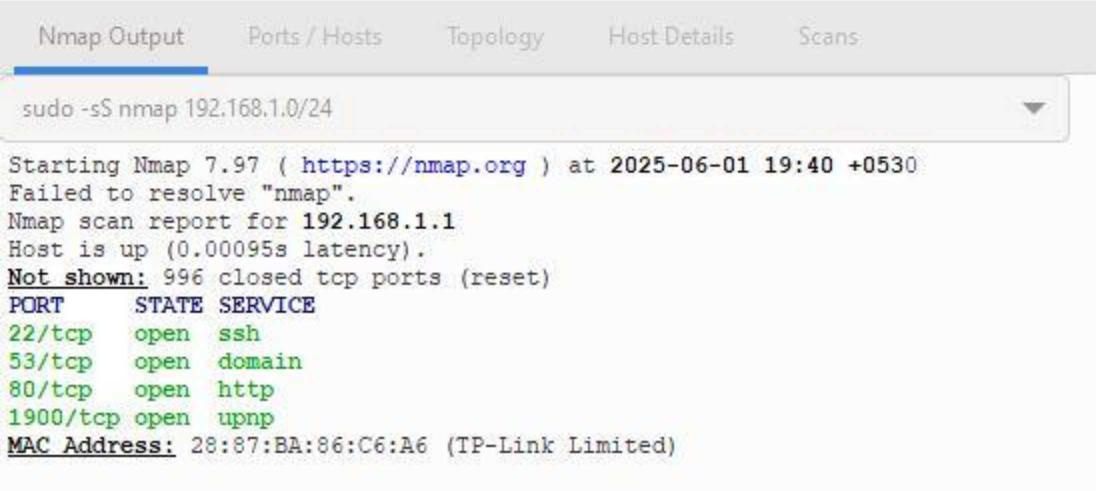
4. Note IP Addresses and Open Ports

Nmap output example:

```
Nmap scan report for 192.168.1.10
Host is up.
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
```

Save the result:

```
nmap -sS 192.168.1.0/24 -oN scan_results.txt
```



```
sudo -sS nmap 192.168.1.0/24
```

```
Starting Nmap 7.97 ( https://nmap.org ) at 2025-06-01 19:40 +0530
Failed to resolve "nmap".
Nmap scan report for 192.168.1.1
Host is up (0.00095s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
1900/tcp open  upnp
MAC Address: 28:87:BA:86:C6:A6 (TP-Link Limited)
```