

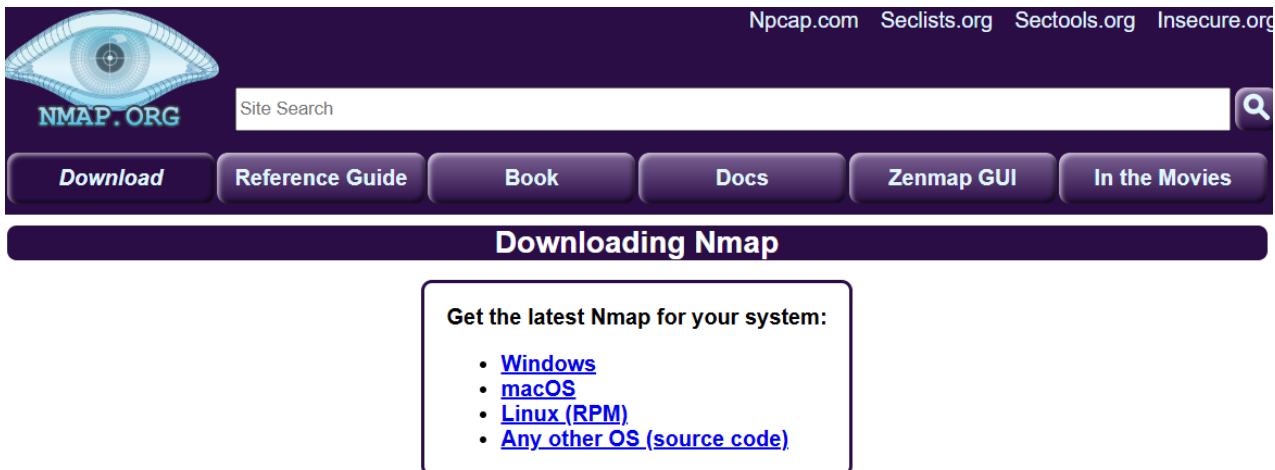
Vaibhav Dhonde

Cyber Security

Nmap Scan & Wireshark Analysis Report

1. Install Nmap:

Download and install Nmap from official website: <https://nmap.org/download.html>



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!](#)

2. Find Local IP Range:

Command to check IP:

- ipconfig (Windows)
- ifconfig or ip addr (Linux)

```
(Lucifer@Windows) - [~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.14.170 netmask 255.255.224.0 broadcast 10.10.31.255
    inet6 fe80::6fef:bde:d0d2:aa02 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:d1:f8:5d txqueuelen 1000 (Ethernet)
    RX packets 3830 bytes 921030 (899.4 KiB)
    RX errors 0 dropped 2072 overruns 0 frame 0
    TX packets 77 bytes 10202 (9.9 KiB)
    TX errors 0 dropped 1 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Example: 10.10.0.0/19

3. Perform TCP SYN Scan:

Command:

`nmap -sS [Target ip-address]`

```
(Lucifer@Windows)-[~]
$ sudo nmap -sS 10.10.18.168
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 09:48 EDT
Nmap scan report for 10.10.18.168
Host is up (0.0042s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:69:AD:3C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

4. Scan Results:

10.10.14.116 - Ports: 21(FTP), 22 (SSH) and 80 (HTTP)

```
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:69:AD:3C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
```

5. Wireshark Analysis:

Captured packets during scan.

No.	Time	Source	Destination	Protocol	Length	Info
123	11.530227861	10.10.14.170	10.10.18.168	TCP	58	61479 → 113 [SYN] Seq=
124	11.530474640	10.10.14.170	10.10.18.168	TCP	58	61479 → 5900 [SYN] Seq=
125	11.530744102	10.10.18.168	10.10.14.170	TCP	60	113 → 61479 [RST, AC
126	11.530744360	10.10.18.168	10.10.14.170	TCP	60	5900 → 61479 [RST, AC
127	11.531197128	10.10.14.170	10.10.18.168	TCP	58	61479 → 8080 [SYN] Seq=
128	11.531376466	10.10.14.170	10.10.18.168	TCP	58	61479 → 111 [SYN] Seq=
129	11.531511701	10.10.18.168	10.10.14.170	TCP	60	8080 → 61479 [RST, AC
130	11.531511798	10.10.18.168	10.10.14.170	TCP	60	111 → 61479 [RST, AC
131	11.531627198	10.10.14.170	10.10.18.168	TCP	58	61479 → 21 [SYN] Seq=
132	11.531773295	10.10.18.168	10.10.14.170	TCP	60	21 → 61479 [SYN, ACK
133	11.531839534	10.10.14.170	10.10.18.168	TCP	54	61479 → 21 [RST] Seq=
134	11.531940402	10.10.14.170	10.10.18.168	TCP	58	61479 → 443 [SYN] Seq=
135	11.532124110	10.10.14.170	10.10.18.168	TCP	58	61479 → 1720 [SYN] Seq=
136	11.532264581	10.10.18.168	10.10.14.170	TCP	60	443 → 61479 [RST, AC
137	11.532264676	10.10.18.168	10.10.14.170	TCP	60	1720 → 61479 [RST, AC
138	11.532376291	10.10.14.170	10.10.18.168	TCP	58	61479 → 1025 [SYN] Seq=
139	11.532521856	10.10.18.168	10.10.14.170	TCP	60	1025 → 61479 [RST, AC
140	11.532612582	10.10.14.170	10.10.18.168	TCP	58	61479 → 995 [SYN] Seq=
141	11.532750438	10.10.18.168	10.10.14.170	TCP	60	995 → 61479 [RST, AC
142	11.532829214	10.10.14.170	10.10.18.168	TCP	58	61479 → 3306 [SYN] Seq=
143	11.533130074	10.10.18.168	10.10.14.170	TCP	60	3306 → 61479 [RST, AC
144	11.533270427	10.10.14.170	10.10.18.168	TCP	58	61479 → 100 [SYN] Seq=

Frame 123: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0
Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:00:10:2c), Dst: 08:00:27:00:10:2c
Internet Protocol Version 4, Src: 10.10.14.170, Destination: 10.10.18.168
Transmission Control Protocol, Src Port: 61479, Destination Port: 113

6. Common Services on Ports:

Port 80 → HTTP (Web Server)

Port 22 → SSH (Secure Shell)

Port 21 → FTP (File Transfer Protocol)

7. Potential Security Risks:

Port 80 (HTTP): No encryption, vulnerable to sniffing.

Port 22 (SSH): Brute-force risk with weak passwords.

Port 21 (FTP): Transmits data in plain text, making it vulnerable to sniffing, credential theft, and man-in-the-middle attacks.

8. Save Scan Results:

Exported scan results as text or HTML.

```
File Edit Search View Document Help
1 # Nmap 7.95 scan initiated Thu Jul 31 05:17:20 2025 as: /usr/lib/nmap/nmap --privileged -sV -A -p22,80 -T4 -oN
  nmap_scan.txt 10.10.123.113
2 Nmap scan report for 10.10.123.113
3 Host is up (0.17s latency).
4
5 PORT      STATE SERVICE VERSION
6 22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
7 | ssh-hostkey:
8 |   3072 d6:2f:c4:d3:6d:5b:b2:c2:65:4b:ff:00:de:1b:ea:80 (RSA)
9 |   256  84:f5:80:cc:77:a1:74:cd:a6:cd:ac:3e:9c:d5:46:05 (ECDSA)
10 |_  256  33:27:6a:c2:af:3c:0e:f0:de:76:89:07:22:30:d5:71 (ED25519)
11 80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
12 |_http-server-header: Apache/2.4.41 (Ubuntu)
13 |_http-title: Did not follow redirect to http://www.smol.thm
14 Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
15 Device type: general purpose
16 Running: Linux 4.X
17 OS CPE: cpe:/o:linux:linux_kernel:4.15
18 OS details: Linux 4.15
19 Network Distance: 2 hops
20 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
21
22 TRACEROUTE (using port 443/tcp)
23 HOP RTT      ADDRESS
24 1   218.01 ms 10.9.0.1
25 2   218.85 ms 10.10.123.113
26
27 OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
28 # Nmap done at Thu Jul 31 05:17:39 2025 -- 1 IP address (1 host up) scanned in 19.30 seconds
29
```