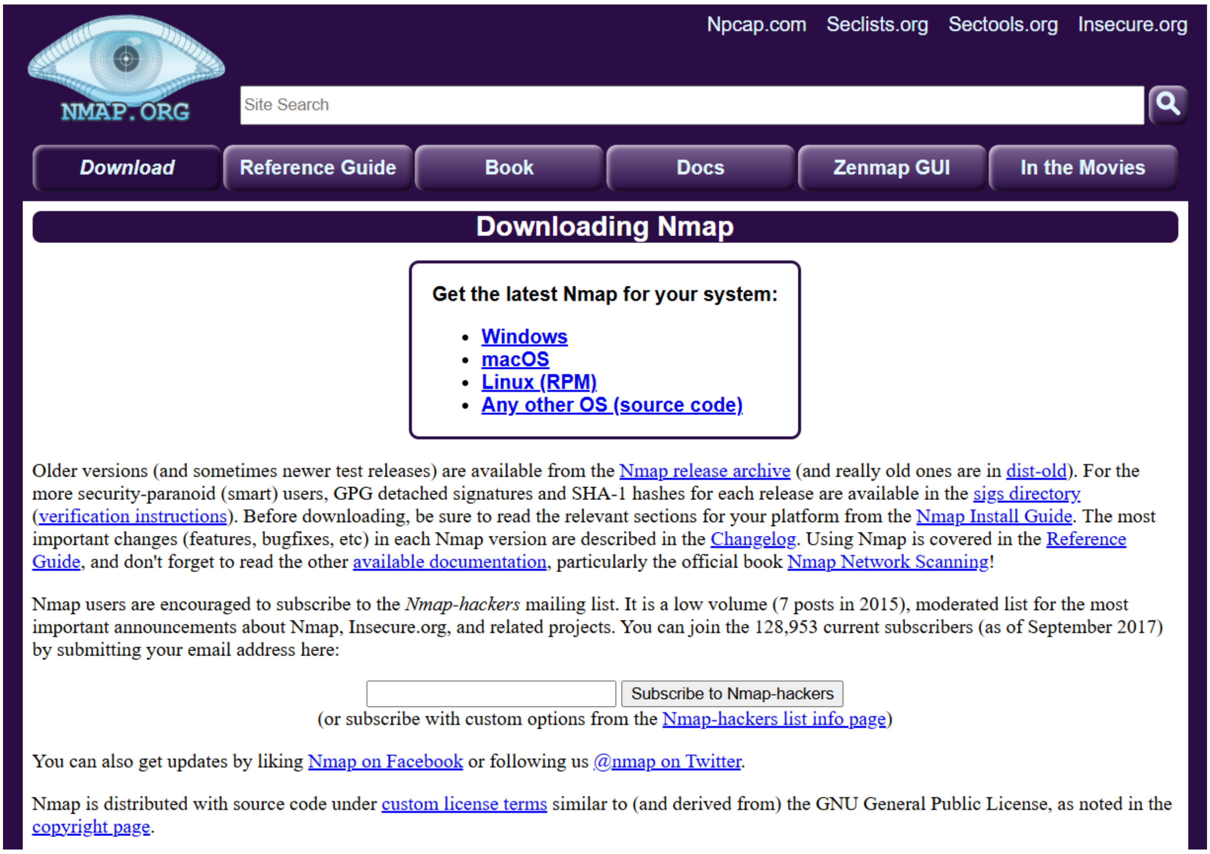
Nmap Scan & Wireshark Analysis Report

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

Tools: Nmap (free), Wireshark (optional).

1.Install Nmap from official website https://nmap.org/download.html



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:

Subscribe to Nmap-hackers
(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 (e.g., 192.168.1.0/24).

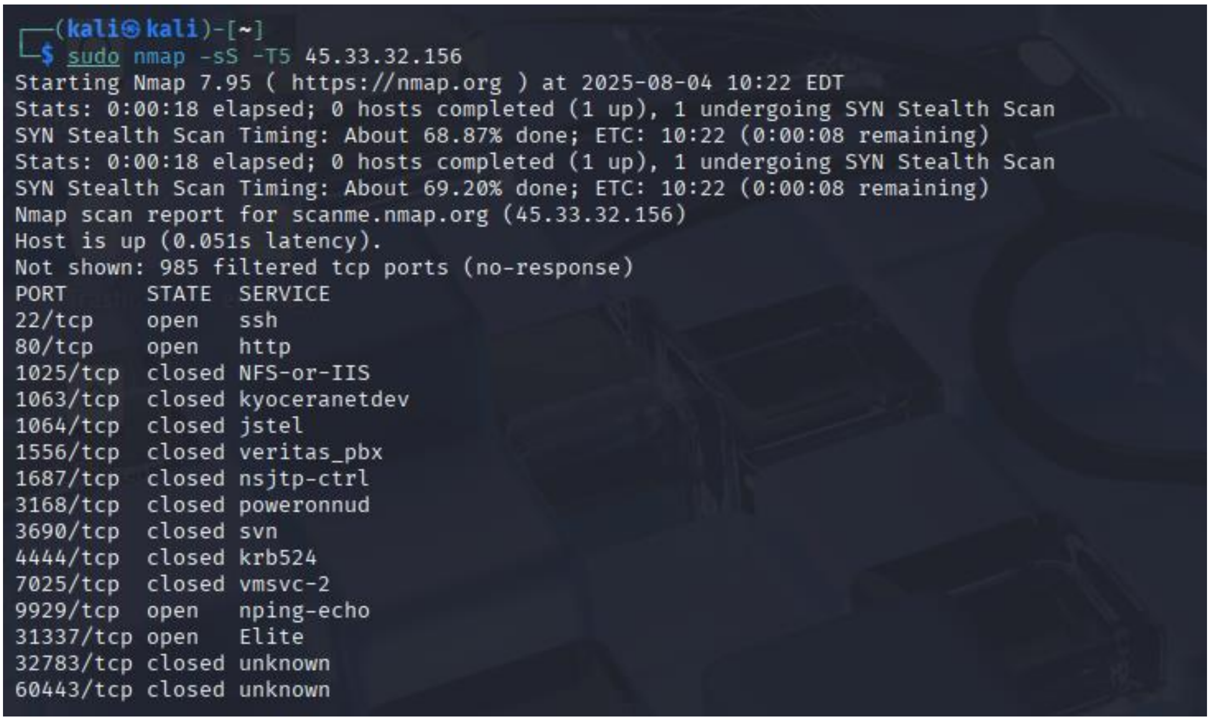
Command to check IP:

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

Example: 192.168.1.0/24

3. Perform TCP SYN Scan:

Command: nmap -sS 45.33.32.156



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -T5 45.33.32.156
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 10:22 EDT
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 68.87% done; ETC: 10:22 (0:00:08 remaining)
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 69.20% done; ETC: 10:22 (0:00:08 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.051s latency).
Not shown: 985 filtered tcp ports (no-response)
PORT      STATE  SERVICE
22/tcp    open   ssh
80/tcp    open   http
1025/tcp  closed NFS-or-IIS
1063/tcp  closed kyoceranetdev
1064/tcp  closed jstel
1556/tcp  closed veritas_pbx
1687/tcp  closed nsjtp-ctrl
3168/tcp  closed poweronnud
3690/tcp  closed svn
4444/tcp  closed krb524
7025/tcp  closed vmsvc-2
9929/tcp  open   nping-echo
31337/tcp open   Elite
32783/tcp closed unknown
60443/tcp closed unknown
```

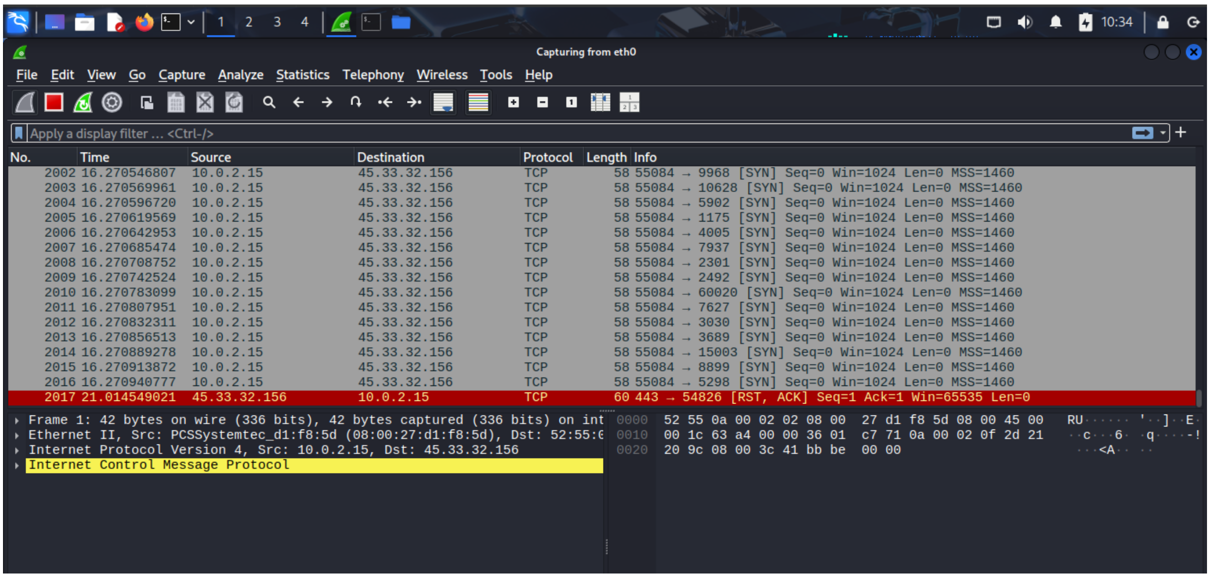
4. Scan Results:

Example:

192.168.1.10 - Ports: 80 (HTTP), 22 (SSH)

5. Wireshark Analysis:

Captured packets during scan.



```
No.   Time          Source         Destination    Protocol Length Info
 2002 16.270546807  10.0.2.15      45.33.32.156   TCP      58 55084 → 9968 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2003 16.270569961  10.0.2.15      45.33.32.156   TCP      58 55084 → 10628 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2004 16.270596720  10.0.2.15      45.33.32.156   TCP      58 55084 → 5902 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2005 16.270619569  10.0.2.15      45.33.32.156   TCP      58 55084 → 1175 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2006 16.270642953  10.0.2.15      45.33.32.156   TCP      58 55084 → 4005 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2007 16.270685474  10.0.2.15      45.33.32.156   TCP      58 55084 → 7937 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2008 16.270708752  10.0.2.15      45.33.32.156   TCP      58 55084 → 2301 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2009 16.270742524  10.0.2.15      45.33.32.156   TCP      58 55084 → 2492 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2010 16.270783099  10.0.2.15      45.33.32.156   TCP      58 55084 → 60020 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2011 16.270807951  10.0.2.15      45.33.32.156   TCP      58 55084 → 7627 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2012 16.270832311  10.0.2.15      45.33.32.156   TCP      58 55084 → 3030 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2013 16.270856513  10.0.2.15      45.33.32.156   TCP      58 55084 → 3689 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2014 16.270889278  10.0.2.15      45.33.32.156   TCP      58 55084 → 15003 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2015 16.270913872  10.0.2.15      45.33.32.156   TCP      58 55084 → 8899 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2016 16.270940777  10.0.2.15      45.33.32.156   TCP      58 55084 → 5298 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2017 21.014549021  45.33.32.156   10.0.2.15      TCP      60 443 → 54826 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0

▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on int
▸ Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: 52:55:0
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 45.33.32.156
▸ Internet Control Message Protocol

0000  52 55 0a 00 02 02 08 00  27 d1 f8 5d 08 00 45 00   RU······'··]··E·
0010  00 1c 63 a4 00 00 36 01  c7 71 0a 00 02 0f 2d 21   ··c···6··q····-!
0020  20 9c 08 00 3c 41 bb be  00 00                     ····<A····
```

6. Common Services on Ports:

Port 80 → HTTP (Web Server)

Port 22 → SSH (Secure Shell)

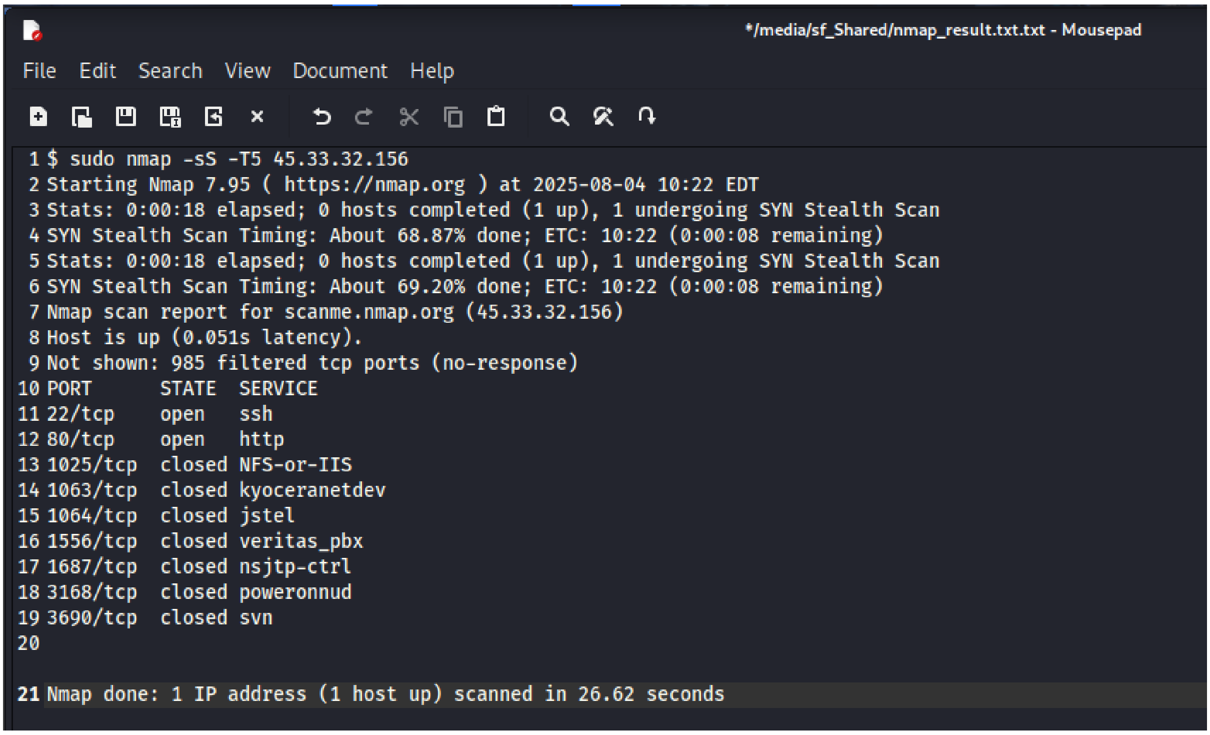
7. Potential Security Risks:

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

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

8. Save Scan Results:

Exported scan results as text or HTML.


*/media/sf_Shared/nmap_result.txt.txt - Mousepad
File Edit Search View Document Help

```
$ sudo nmap -sS -T5 45.33.32.156
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 10:22 EDT
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 68.87% done; ETC: 10:22 (0:00:08 remaining)
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 69.20% done; ETC: 10:22 (0:00:08 remaining)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.051s latency).
Not shown: 985 filtered tcp ports (no-response)
PORT      STATE  SERVICE
22/tcp    open   ssh
80/tcp    open   http
1025/tcp  closed NFS-or-IIS
1063/tcp  closed kyoceranetdev
1064/tcp  closed jstel
1556/tcp  closed veritas_pbx
1687/tcp  closed nsjtp-ctrl
3168/tcp  closed poweronnud
3690/tcp  closed svn

Nmap done: 1 IP address (1 host up) scanned in 26.62 seconds
```