

ELEVATE Labs

Task 1 :- Scan Your Local Network for Open Ports

1).Find your local IP range (e.g., 192.168.1.0/24)

```
[root@Elliot]~]
# nmap 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-13 00:51 EST
Nmap scan report for 192.168.1.0
Host is up (0.041s latency).
All 1000 scanned ports on 192.168.1.0 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.1
Host is up (0.041s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.2
Host is up (0.042s latency).
All 1000 scanned ports on 192.168.1.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.3
Host is up (0.044s latency).
All 1000 scanned ports on 192.168.1.3 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.4
Host is up (0.040s latency).
All 1000 scanned ports on 192.168.1.4 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.5
Host is up (0.053s latency).
All 1000 scanned ports on 192.168.1.5 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.6
Host is up (0.051s latency).
All 1000 scanned ports on 192.168.1.6 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.7
Host is up (0.043s latency).
All 1000 scanned ports on 192.168.1.7 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.8
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.1.8 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.9
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.1.9 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.10
Host is up (0.034s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
```

```
Nmap scan report for 192.168.1.11
Host is up (0.041s latency).
All 1000 scanned ports on 192.168.1.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.12
Host is up (0.042s latency).
All 1000 scanned ports on 192.168.1.12 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.13
Host is up (0.034s latency).
All 1000 scanned ports on 192.168.1.13 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.14
Host is up (0.044s latency).
All 1000 scanned ports on 192.168.1.14 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.15
Host is up (0.048s latency).
All 1000 scanned ports on 192.168.1.15 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.16
Host is up (0.042s latency).
All 1000 scanned ports on 192.168.1.16 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.17
Host is up (0.041s latency).
All 1000 scanned ports on 192.168.1.17 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.18
Host is up (0.043s latency).
All 1000 scanned ports on 192.168.1.18 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.19
Host is up (0.047s latency).
All 1000 scanned ports on 192.168.1.19 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.20
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.1.20 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.21
Host is up (0.044s latency).
All 1000 scanned ports on 192.168.1.21 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.22
Host is up (0.043s latency).
All 1000 scanned ports on 192.168.1.22 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
```

```
Nmap scan report for 192.168.1.23
Host is up (0.042s latency).
All 1000 scanned ports on 192.168.1.23 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.24
Host is up (0.046s latency).
All 1000 scanned ports on 192.168.1.24 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.25
Host is up (0.051s latency).
All 1000 scanned ports on 192.168.1.25 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.26
Host is up (0.044s latency).
All 1000 scanned ports on 192.168.1.26 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.27
Host is up (0.052s latency).
All 1000 scanned ports on 192.168.1.27 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.28
Host is up (0.048s latency).
All 1000 scanned ports on 192.168.1.28 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.29
Host is up (0.049s latency).
All 1000 scanned ports on 192.168.1.29 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.30
Host is up (0.051s latency).
All 1000 scanned ports on 192.168.1.30 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.31
Host is up (0.045s latency).
All 1000 scanned ports on 192.168.1.31 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.32
Host is up (0.051s latency).
All 1000 scanned ports on 192.168.1.32 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.33
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.1.33 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.34
Host is up (0.041s latency).
All 1000 scanned ports on 192.168.1.34 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
```

```
Nmap scan report for 192.168.1.35
Host is up (0.049s latency).
All 1000 scanned ports on 192.168.1.35 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.36
Host is up (0.048s latency).
All 1000 scanned ports on 192.168.1.36 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.37
Host is up (0.047s latency).
All 1000 scanned ports on 192.168.1.37 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.38
Host is up (0.043s latency).
All 1000 scanned ports on 192.168.1.38 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.39
Host is up (0.042s latency).
All 1000 scanned ports on 192.168.1.39 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.40
Host is up (0.051s latency).
All 1000 scanned ports on 192.168.1.40 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.41
Host is up (0.040s latency).
All 1000 scanned ports on 192.168.1.41 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.42
Host is up (0.050s latency).
All 1000 scanned ports on 192.168.1.42 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.43
Host is up (0.058s latency).
All 1000 scanned ports on 192.168.1.43 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.44
Host is up (0.046s latency).
All 1000 scanned ports on 192.168.1.44 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.45
Host is up (0.048s latency).
All 1000 scanned ports on 192.168.1.45 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.46
Host is up (0.047s latency).
All 1000 scanned ports on 192.168.1.46 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
```

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

```
(root@Elliot:[~]
# nmap -sS 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-13 00:51 EST
Nmap scan report for 192.168.1.0
Host is up (0.035s latency).
All 1000 scanned ports on 192.168.1.0 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.1
Host is up (0.036s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.2
Host is up (0.038s latency).
All 1000 scanned ports on 192.168.1.2 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.3
Host is up (0.034s latency).
All 1000 scanned ports on 192.168.1.3 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.4
Host is up (0.035s latency).
All 1000 scanned ports on 192.168.1.4 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.5
Host is up (0.037s latency).
All 1000 scanned ports on 192.168.1.5 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.6
Host is up (0.035s latency).
All 1000 scanned ports on 192.168.1.6 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.7
Host is up (0.034s latency).
All 1000 scanned ports on 192.168.1.7 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.8
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.1.8 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.9
Host is up (0.037s latency).
All 1000 scanned ports on 192.168.1.9 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.10
Host is up (0.038s latency).
All 1000 scanned ports on 192.168.1.10 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.11
Host is up (0.039s latency).
All 1000 scanned ports on 192.168.1.11 are in ignored states.
```

```
Nmap scan report for 192.168.1.12
Host is up (0.033s latency).
All 1000 scanned ports on 192.168.1.12 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)      Destination

Nmap scan report for 192.168.1.13
Host is up (0.047s latency).
All 1000 scanned ports on 192.168.1.13 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)      Destination

Nmap scan report for 192.168.1.14
Host is up (0.045s latency).
All 1000 scanned ports on 192.168.1.14 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)      Destination

Nmap scan report for 192.168.1.15
Host is up (0.041s latency).
All 1000 scanned ports on 192.168.1.15 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)      Destination

Nmap scan report for 192.168.1.16
Host is up (0.043s latency).
All 1000 scanned ports on 192.168.1.16 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)      Destination

Nmap scan report for 192.168.1.17
Host is up (0.046s latency).
All 1000 scanned ports on 192.168.1.17 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)      Destination

Nmap scan report for 192.168.1.18
Host is up (0.043s latency).
All 1000 scanned ports on 192.168.1.18 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)      Destination

Nmap scan report for 192.168.1.19
Host is up (0.035s latency).
All 1000 scanned ports on 192.168.1.19 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)      Destination

Nmap scan report for 192.168.1.20
Host is up (0.033s latency).
All 1000 scanned ports on 192.168.1.20 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.21
Host is up (0.044s latency).
All 1000 scanned ports on 192.168.1.21 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.22
Host is up (0.034s latency).
All 1000 scanned ports on 192.168.1.22 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.23
Host is up (0.045s latency).
All 1000 scanned ports on 192.168.1.23 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
```

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

```

[KALI_LINUX_2.0 (Running) - Oracle VirtualBox
File Machine View Input Devices Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
[Apply a display filter... <Ctrl-/>
No. Time Source Destination Protocol Length Info
31150 119.643518108 TCP 60 80 - 55057 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0
31151 119.643518356 TCP 60 80 - 55063 [RST, ACK] Seq=3 Ack=1 Win=1024 Len=0
31152 119.643518391 TCP 60 80 - 55061 [RST, ACK] Seq=3 Ack=1 Win=1024 Len=0
31153 119.643518409 TCP 60 80 - 55063 [RST, ACK] Seq=3 Ack=1 Win=1024 Len=0
31154 119.643518426 TCP 60 80 - 55063 [RST, ACK] Seq=3 Ack=1 Win=1024 Len=0
31155 119.643518445 TCP 60 80 - 55063 [RST, ACK] Seq=3 Ack=1 Win=1024 Len=0
31156 119.643518461 TCP 60 80 - 55063 [RST, ACK] Seq=3 Ack=1 Win=1024 Len=0
31157 119.643518478 TCP 54 55063 - 88 [ACK] Seq=1 Ack=1 Win=1024 Len=0
31158 119.667728029 TCP 54 55063 - 88 [ACK] Seq=1 Ack=1 Win=1024 Len=0
31159 119.672415762 TCP 54 55063 - 88 [ACK] Seq=1 Ack=1 Win=1024 Len=0
31160 119.672489882 TCP 54 55065 - 88 [ACK] Seq=1 Ack=1 Win=1024 Len=0
31161 119.672489928 TCP 54 55063 - 88 [ACK] Seq=1 Ack=1 Win=1024 Len=0
31162 119.674985765 TCP 54 55063 - 88 [ACK] Seq=1 Ack=1 Win=1024 Len=0
31163 119.677947113 TCP 58 55068 - 1973 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31164 119.679961964 TCP 58 55068 - 2882 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31165 119.680001994 TCP 58 55068 - 2887 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31166 119.691480973 TCP 54 55063 - 88 [ACK] Seq=1 Ack=1 Win=1024 Len=0
31167 119.691578786 TCP 54 55063 - 88 [ACK] Seq=1 Ack=1 Win=1024 Len=0
31168 119.693795295 TCP 58 55068 - 8921 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31169 119.693860235 TCP 58 55068 - 5966 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31170 119.693860249 TCP 58 55068 - 5966 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31171 119.708857567 TCP 58 55068 - 1857 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31172 119.708278586 TCP 58 55068 - 1381 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31173 119.704300195 TCP 58 55068 - 1381 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31174 119.704300199 TCP 58 55068 - 1381 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31175 119.713245666 TCP 58 55064 - 2847 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31176 119.716622695 TCP 58 55064 - 458 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31177 119.719410645 TCP 58 55064 - 2847 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31178 119.721681590 TCP 58 55064 - 42 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31179 119.721681597 TCP 58 55064 - 9846 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31180 119.728758069 TCP 58 55068 - 5966 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31181 119.728873123 TCP 58 55068 - 1185 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31182 119.728900229 TCP 58 55068 - 5966 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31183 119.728900771 TCP 58 55068 - 5966 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31184 119.737591572 TCP 58 55064 - 32779 [SYN] Seq=9 Win=1024 Len=0 MSS=1460
31185 119.744820354 TCP 58 55064 - 8851 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31186 119.750883049 TCP 58 55064 - 1831 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31187 119.750883199 TCP 58 55064 - 1831 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31188 119.753615956 TCP 60 80 - 55063 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0
31189 119.753616289 TCP 60 80 - 55063 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0
31190 119.753616318

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
[ 0000 ff ff ff ff ff ff ff 00 00 27 36 68 57 08 06 00 01 ] '6hw...
Packets: 75837 | Profile: Default
eth0: <live capture in progress>

```

```

[KALI_LINUX_2.0 (Running) - Oracle VirtualBox
File Machine View Input Devices Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
[Apply a display filter... <Ctrl-/>
No. Time Source Destination Protocol Length Info
31210 119.778535688 TCP 58 55064 - 49175 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31211 119.778958314 TCP 58 55064 - 28928 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31212 119.780000029 TCP 58 55064 - 28928 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31213 119.804314656 TCP 58 55064 - 5967 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31214 119.809083263 TCP 58 55064 - 8851 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31215 119.804225675 TCP 60 80 - 55063 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0
31216 119.808716273 TCP 58 55064 - 42 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31217 119.808869635 TCP 58 55064 - 5965 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31218 119.808869688 TCP 58 55064 - 5967 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31219 119.808918137 TCP 58 55064 - 5968 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31220 119.824122326 TCP 58 55064 - 1844 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31221 119.824122349 TCP 58 55064 - 1844 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31222 119.832984946 TCP 58 55064 - 3281 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31223 119.840660806 TCP 54 55063 - 89 [ACK] Seq=1 Ack=1 Win=1024 Len=0
31224 119.854382883 TCP 54 55063 - 88 [ACK] Seq=1 Ack=1 Win=1024 Len=0
31225 119.860876498 TCP 58 55064 - 3281 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31226 119.860876693 TCP 58 55064 - 3281 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31227 119.868572545 TCP 60 80 - 55063 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0
31228 119.868564998 TCP 54 55063 - 89 [ACK] Seq=1 Ack=1 Win=1024 Len=0
31229 119.880159615 TCP 58 55064 - 28928 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31230 119.888737326 TCP 60 80 - 55063 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0
31231 119.888737326 TCP 60 80 - 55063 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0
31232 119.889185308 TCP 60 80 - 55063 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0
31233 119.889185697 TCP 58 55064 - 76 [Time to live exceeded in transit]
31234 119.889185698 TCP 53 55064 - 3880 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31235 119.889185699 TCP 58 55064 - 1381 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31236 119.889185700 TCP 58 55064 - 1381 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31237 119.894289619 TCP 58 55064 - 2042 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31238 119.894349532 TCP 58 55064 - 42 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31239 119.894349562 TCP 58 55064 - 42 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31240 119.894448983 TCP 58 55064 - 481 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31241 119.897461493 TCP 58 55064 - 1831 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31242 119.897461497 TCP 58 55064 - 1831 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31243 119.905890753 TCP 58 55064 - 1831 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31244 119.905211712 TCP 58 55064 - 1947 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31245 119.905211712 TCP 58 55064 - 5968 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31246 119.905211712 TCP 58 55064 - 5968 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31247 119.909861118 TCP 58 55064 - 2847 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31248 119.909779327 TCP 58 55064 - 42 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31249 119.909862065 TCP 58 55064 - 2047 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31250 119.909923430 TCP 58 55064 - 417 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
[ 0000 ff ff ff ff ff ff ff 00 00 27 36 68 57 08 06 00 01 ] '6hw...
Packets: 87704 | Profile: Default
eth0: <live capture in progress>

```

.Research common services running on those ports.

```
(root@Elliot)~] # nmap -p 21 -sV -o Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 02:59 EDT Nmap scan report for 10.252.120.5 Host is up (0.0014s latency). PORT      STATE SERVICE VERSION 21/tcp    open  ftp      vsftpd 2.3.4 MAC Address: 08:00:27:F7:A2:3D (PCS Systemtechnik/Oracle VirtualBox virtual NIC) Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port Device type: general purpose Running: Linux 2.6.X | keyword searching of CVE Records (with limitations) is now available in the s OS CPE: cpe:/o:linux:linux_kernel:2.6 OS details: Linux 2.6.9 - 2.6.33 Network Distance: 1 hop Service Info: OS: Unix
```

```
(root@Elliot)~] # ls -l /usr/share/nmap/scripts | grep ftp -rw-r--r-- 1 root root 4530 May 15 11:37 ftp-anon.nse -rw-r--r-- 1 root root 3253 May 15 11:37 ftp-bounce.nse -rw-r--r-- 1 root root 3108 May 15 11:37 ftp-brute.nse -rw-r--r-- 1 root root 3272 May 15 11:37 ftp-libopie.nse -rw-r--r-- 1 root root 3290 May 15 11:37 ftp-proftp-backdoor.nse -rw-r--r-- 1 root root 3768 May 15 11:37 ftp-syst.nse -rw-r--r-- 1 root root 6021 May 15 11:37 ftp-vsftpd-backdoor.nse -rw-r--r-- 1 root root 5923 May 15 11:37 ftp-vuln-cve2010-4221.nse -rw-r--r-- 1 root root 5736 May 15 11:37 tftp-enum.nse -rw-r--r-- 1 root root 10034 May 15 11:37 tftp-version.nse
```

```
(root@Elliot)~] # searchsploit vsftpd 2.3.4 Exploit Title | Path vsftpd 2.3.4 - Backdoor Command Execution | unix/remote/49757.py vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb Shellcodes: No Results
```

Impact:

- Unauthorized access to files.
- Data modification or theft.
- System compromise.

Mitigation:

- Use a secure alternative like SFTP or FTPS.
- Enforce strong password policies.
- Restrict access with firewall rules.

```
[root@Elliot:~]
# nmap -p 23 -sV -oNmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 09:13 EDT
Nmap scan report for 10.252.120.5
Host is up (0.0021s latency).

PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linux telnetd
MAC Address: 08:00:27:F7:A2:3D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.26 seconds
```

```
[root@Elliot:~]
# ls -l /usr/share/nmap/scripts | grep telnet
-rw-r--r-- 1 root root 20216 May 15 11:37 telnet-brute.nse
-rw-r--r-- 1 root root 3008 May 15 11:37 telnet-encryption.nse
-rw-r--r-- 1 root root 4564 May 15 11:37 telnet-ntlm-info.nse
```

Exploit Title		Path
netkit-telnet-0.17	telnetd (Fedora 31) - 'BraveStarr' Remote Code Execution	linux/remote/48170.py
TelnetD	encrypt_keyid - Function Pointer Overwrite	linux/remote/18280.c
Shellcode Title		Path
Linux/MIPS (Little Endian) - system(telnetd -l /bin/sh) Shellcode (80 bytes)		linux_mips/27132.txt

Impact

- Unencrypted Communication
- Remote Unauthorized Access
- Network Pivoting

Mitigation:

- Disable this service immediately
- Replace with a secure protocol like SSH.

```
[root@Elliot:~]# nmap -p 80 -sV -oN /tmp/nmap_out.nmap
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 13:05 EDT
Nmap scan report for 10.252.120.5
Host is up (0.0012s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 08:00:27:F7:A2:3D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.29 seconds
```

```
[root@Elliot:~]# ls -l /usr/share/nmap/scripts | grep http
-rw-r--r-- 1 root root 2153 May 15 11:37 http-adobe-coldfusion-apsa1301.nse
-rw-r--r-- 1 root root 5149 May 15 11:37 http-affiliate-id.nse
-rw-r--r-- 1 root root 1950 May 15 11:37 http-apache-negotiation.nse
-rw-r--r-- 1 root root 4499 May 15 11:37 http-apache-server-status.nse
-rw-r--r-- 1 root root 1805 May 15 11:37 http-aspnet-debug.nse
-rw-r--r-- 1 root root 3959 May 15 11:37 http-auth-finder.nse
-rw-r--r-- 1 root root 3187 May 15 11:37 http-auth.nse
-rw-r--r-- 1 root root 2865 May 15 11:37 http-avaya-ipoffice-users.nse
-rw-r--r-- 1 root root 4372 May 15 11:37 http-awstatstotals-exec.nse
-rw-r--r-- 1 root root 6872 May 15 11:37 http-axis2-dir-traversal.nse
-rw-r--r-- 1 root root 5484 May 15 11:37 http-backup-finder.nse
-rw-r--r-- 1 root root 6387 May 15 11:37 http-barracuda-dir-traversal.nse
-rw-r--r-- 1 root root 2038 May 15 11:37 http-bigip-cookie.nse
-rw-r--r-- 1 root root 4920 May 15 11:37 http-brute.nse
-rw-r--r-- 1 root root 4436 May 15 11:37 http-cakephp-version.nse
-rw-r--r-- 1 root root 4927 May 15 11:37 http-chrono.nse
-rw-r--r-- 1 root root 1695 May 15 11:37 http-cisco-anyconnect.nse
-rw-r--r-- 1 root root 5520 May 15 11:37 http-coldfusion-subzero.nse
-rw-r--r-- 1 root root 4150 May 15 11:37 http-comments-displayer.nse
-rw-r--r-- 1 root root 7251 May 15 11:37 http-config-backup.nse
-rw-r--r-- 1 root root 5139 May 15 11:37 http-cookie-flags.nse
-rw-r--r-- 1 root root 2577 May 15 11:37 http-cors.nse
-rw-r--r-- 1 root root 13803 May 15 11:37 http-cross-domain-policy.nse
-rw-r--r-- 1 root root 5418 May 15 11:37 http-csrf.nse
-rw-r--r-- 1 root root 1718 May 15 11:37 http-date.nse
-rw-r--r-- 1 root root 17388 May 15 11:37 http-default-accounts.nse
-rw-r--r-- 1 root root 4288 May 15 11:37 http-devframework.nse
```

Impacts

- Session Hijacking & Cookie Theft
- Content Tampering
- Man-in-the-Middle (MITM) Risks

Mitigation:

- Migrate all traffic to HTTPS (port 443) using SSL/TLS encryption.
- Implement HTTP Strict Transport Security (HSTS).

