

## 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)

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)

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)

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)

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)

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)

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 (0.035s 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 (0.033s latency).
All 1000 scanned ports on 192.168.1.20 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

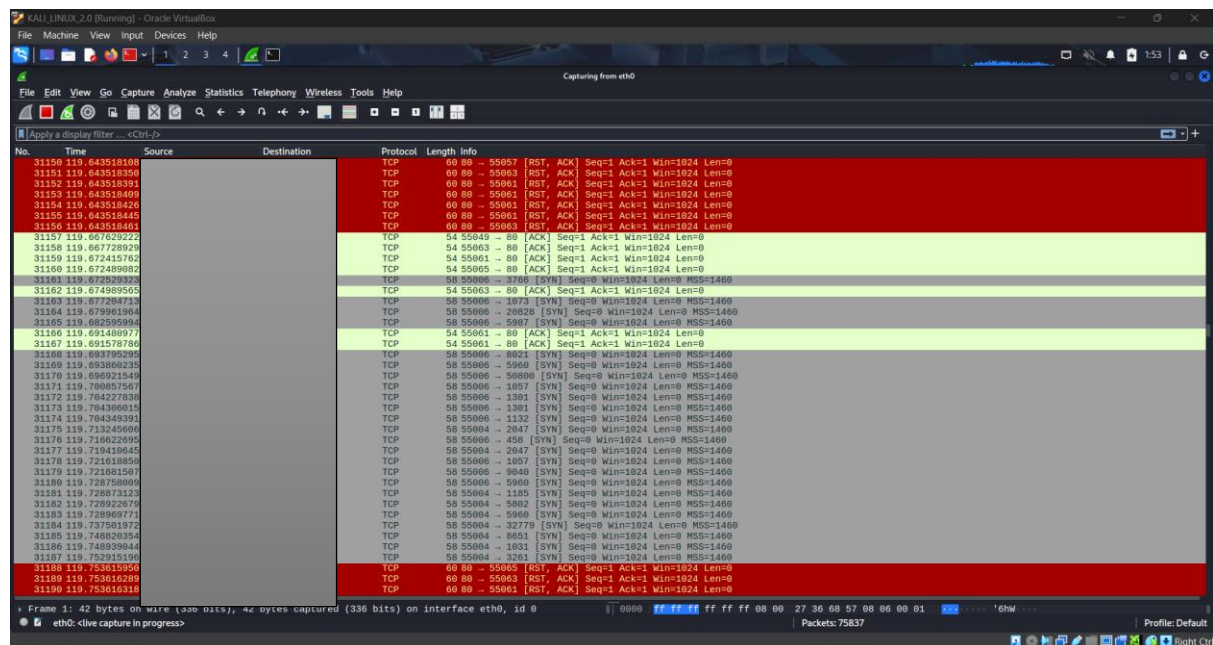
Nmap scan report for 192.168.1.21
Host is up (0.044s latency).
All 1000 scanned ports on 192.168.1.21 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

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)

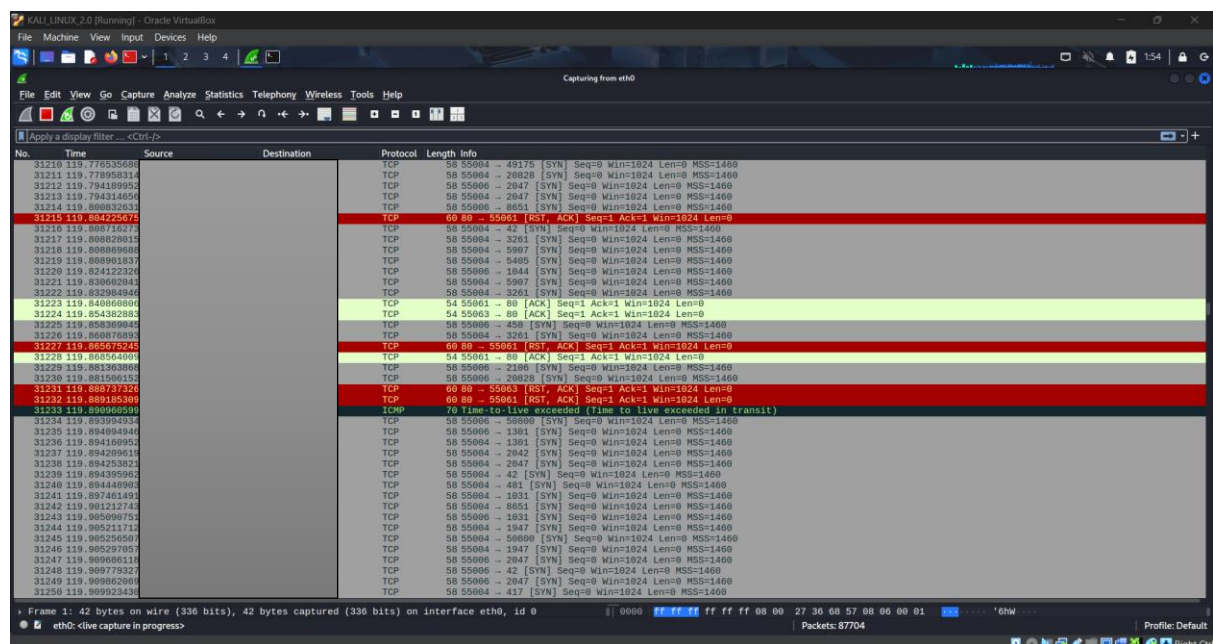
Nmap scan report for 192.168.1.23
Host is up (0.045s latency).
All 1000 scanned ports on 192.168.1.23 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

```

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



| No.   | Time          | Source        | Destination   | Protocol | Length | Info   |
|-------|---------------|---------------|---------------|----------|--------|--|
| 31150 | 119.643518108 | 192.168.1.119 | 192.168.1.119 | TCP      | 60     | 60 89 - 55057 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0  |
| 31151 | 119.643518399 | 192.168.1.119 | 192.168.1.119 | TCP      | 60     | 60 89 - 55061 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0  |
| 31152 | 119.643518391 | 192.168.1.119 | 192.168.1.119 | TCP      | 60     | 60 89 - 55061 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0  |
| 31153 | 119.643518409 | 192.168.1.119 | 192.168.1.119 | TCP      | 60     | 60 89 - 55061 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0  |
| 31154 | 119.643518426 | 192.168.1.119 | 192.168.1.119 | TCP      | 60     | 60 89 - 55061 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0  |
| 31155 | 119.643518446 | 192.168.1.119 | 192.168.1.119 | TCP      | 60     | 60 89 - 55061 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0  |
| 31156 | 119.643518461 | 192.168.1.119 | 192.168.1.119 | TCP      | 60     | 60 89 - 55063 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0  |
| 31157 | 119.667629222 | 192.168.1.119 | 192.168.1.119 | TCP      | 54     | 54 55043 - 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0       |
| 31158 | 119.667729929 | 192.168.1.119 | 192.168.1.119 | TCP      | 54     | 54 55063 - 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0       |
| 31159 | 119.672415762 | 192.168.1.119 | 192.168.1.119 | TCP      | 54     | 54 55061 - 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0       |
| 31160 | 119.672489882 | 192.168.1.119 | 192.168.1.119 | TCP      | 54     | 54 55065 - 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0       |
| 31161 | 119.672893928 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 3786 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31162 | 119.674989565 | 192.168.1.119 | 192.168.1.119 | TCP      | 54     | 54 55063 - 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0       |
| 31163 | 119.677204713 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 1873 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31164 | 119.678961366 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 20828 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 31165 | 119.682595994 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 5987 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31166 | 119.691488977 | 192.168.1.119 | 192.168.1.119 | TCP      | 54     | 54 55061 - 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0       |
| 31167 | 119.691578786 | 192.168.1.119 | 192.168.1.119 | TCP      | 54     | 54 55061 - 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0       |
| 31168 | 119.693795298 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 8021 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31169 | 119.693868235 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 5986 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31170 | 119.696921546 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 58880 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 31171 | 119.708057567 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 1057 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31172 | 119.704227839 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 1301 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31173 | 119.704386815 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 1301 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31174 | 119.704349391 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 1132 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31175 | 119.713245686 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 2847 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31176 | 119.716627695 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 458 [SYN] Seq=0 Win=1024 Len=0 MSS=1460   |
| 31177 | 119.718410845 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 2847 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31178 | 119.721618859 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 1057 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31179 | 119.721681507 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 8048 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31180 | 119.728758809 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 5960 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31181 | 119.728873123 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 1185 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31182 | 119.728922678 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 5882 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31183 | 119.728969771 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 5960 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31184 | 119.737501872 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 32779 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 31185 | 119.748029354 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 8051 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31186 | 119.748939844 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 1031 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31187 | 119.752313196 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 2313 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  |
| 31188 | 119.753619550 | 192.168.1.119 | 192.168.1.119 | TCP      | 60     | 60 89 - 55065 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0  |
| 31189 | 119.753616289 | 192.168.1.119 | 192.168.1.119 | TCP      | 60     | 60 89 - 55063 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0  |
| 31190 | 119.753616318 | 192.168.1.119 | 192.168.1.119 | TCP      | 60     | 60 89 - 55061 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0  |



| No.   | Time          | Source        | Destination   | Protocol | Length | Info  |
|-------|---------------|---------------|---------------|----------|--------|---|
| 31210 | 119.776535688 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 45178 [SYN] Seq=0 Win=1024 Len=0 MSS=1460        |
| 31211 | 119.778950314 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 20828 [SYN] Seq=0 Win=1024 Len=0 MSS=1460        |
| 31212 | 119.794189952 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 2047 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31213 | 119.794314856 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 2847 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31214 | 119.808835353 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 8051 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31215 | 119.804223678 | 192.168.1.119 | 192.168.1.119 | TCP      | 60     | 60 89 - 55061 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0         |
| 31216 | 119.808710273 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 42 [SYN] Seq=0 Win=1024 Len=0 MSS=1460           |
| 31217 | 119.808820815 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 3261 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31218 | 119.808869688 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 5987 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31219 | 119.808901837 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 5485 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31220 | 119.824122326 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 1044 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31221 | 119.830662841 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 5987 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31222 | 119.832984846 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 3261 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31223 | 119.840680806 | 192.168.1.119 | 192.168.1.119 | TCP      | 54     | 54 55061 - 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0              |
| 31224 | 119.854382881 | 192.168.1.119 | 192.168.1.119 | TCP      | 54     | 54 55063 - 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0              |
| 31225 | 119.858309845 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 458 [SYN] Seq=0 Win=1024 Len=0 MSS=1460          |
| 31226 | 119.866876893 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 3261 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31227 | 119.865675245 | 192.168.1.119 | 192.168.1.119 | TCP      | 60     | 60 89 - 55061 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0         |
| 31228 | 119.869564009 | 192.168.1.119 | 192.168.1.119 | TCP      | 54     | 54 55061 - 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0              |
| 31229 | 119.881263869 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 2180 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31230 | 119.881506152 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 20828 [SYN] Seq=0 Win=1024 Len=0 MSS=1460        |
| 31231 | 119.888737328 | 192.168.1.119 | 192.168.1.119 | TCP      | 60     | 60 89 - 55063 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0         |
| 31232 | 119.888816309 | 192.168.1.119 | 192.168.1.119 | TCP      | 60     | 60 89 - 55061 [RST, ACK] Seq=1 Ack=1 Win=1024 Len=0         |
| 31233 | 119.898960599 | 192.168.1.119 | 192.168.1.119 | ICMP     | 70     | 70 Time-to-live exceeded (Time to live exceeded in transit) |
| 31234 | 119.893994934 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 58880 [SYN] Seq=0 Win=1024 Len=0 MSS=1460        |
| 31235 | 119.894094944 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 1301 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31236 | 119.894160952 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 1301 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31237 | 119.894299619 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 2842 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31238 | 119.894253821 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 2847 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31239 | 119.894395962 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 42 [SYN] Seq=0 Win=1024 Len=0 MSS=1460           |
| 31240 | 119.894448993 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 481 [SYN] Seq=0 Win=1024 Len=0 MSS=1460          |
| 31241 | 119.897463149 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 1031 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31242 | 119.901212743 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 8051 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31243 | 119.905099753 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 1031 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31244 | 119.905211713 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 1947 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31245 | 119.905250567 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 58880 [SYN] Seq=0 Win=1024 Len=0 MSS=1460        |
| 31246 | 119.905297857 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 1947 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31247 | 119.908680118 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 2847 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31248 | 119.909779327 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 42 [SYN] Seq=0 Win=1024 Len=0 MSS=1460           |
| 31249 | 119.909862868 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55086 - 2847 [SYN] Seq=0 Win=1024 Len=0 MSS=1460         |
| 31250 | 119.909923436 | 192.168.1.119 | 192.168.1.119 | TCP      | 58     | 58 55084 - 417 [SYN] Seq=0 Win=1024 Len=0 MSS=1460          |

.Research common services running on those ports.

```
(root@Elliot)-[~]
# nmap -p 21 -sV -O 10.252.120.5
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
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-proftpd-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 -O 10.252.120.5
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
```

```
(root@Elliot)-[~]
# searchsploit Linux telnetd
```

| 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 -O 10.252.120.5
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-apsal301.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).

