Introduction

This project demonstrates a practical network reconnaissance attempt using Nmap and packet-level analysis with Wireshark. The goal was to scan a target device on a private network, analyze the results, and diagnose why all ports appeared filtered. Modern networks often use firewalls and NAT filtering, so understanding filtered scans is an essential cybersecurity skill. This project replicates a realistic situation and explains how to interpret and troubleshoot it.

Goal: Perform a full network scan on a target device using Nmap and analyze the traffic with Wireshark.
Outcome: The host was reachable, but all ports were filtered, meaning no responses were received.
Why this matters: This demonstrates a realistic scenario where devices are protected by firewalls, and analysts must understand network behavior and troubleshoot why scans fail.

Tools Used

- Nmap (Network scanning)
- Wireshark (Packet capture and analysis)
- Windows 10
- Local network

Target Setup

- **Target IP:** 192.168.12.110
- **Connection Type:**WIFI Network
  My Device: Windows laptop
- **Scan Type:** SYN Stealth Scan (`-sS`)

Nmap Commands Used

Full port scan attempted:

nmap -sS -p- 192.168.12.110

Quick diagnostic scan for Wireshark capture:

nmap -sS -p1-200 192.168.12.110

Nmap Results

```
Nmap scan report for Ghoul.lan (192.168.12.110)
Host is up (0.041s latency).
All 1000 scanned ports on Ghoul.lan (192.168.12.110) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 14:AB:C5:09:FD:62 (Intel Corporate)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

Interpretation of Results

The scan showed that the host is alive, but **all ports are filtered**, meaning:

The target received the packets but did not respond.

Firewalls are silently dropping packets.

No SYN/ACK or RST responses were returned.

Nmap cannot determine if ports are open or closed.

Likely causes include:

Windows Firewall blocking inbound requests

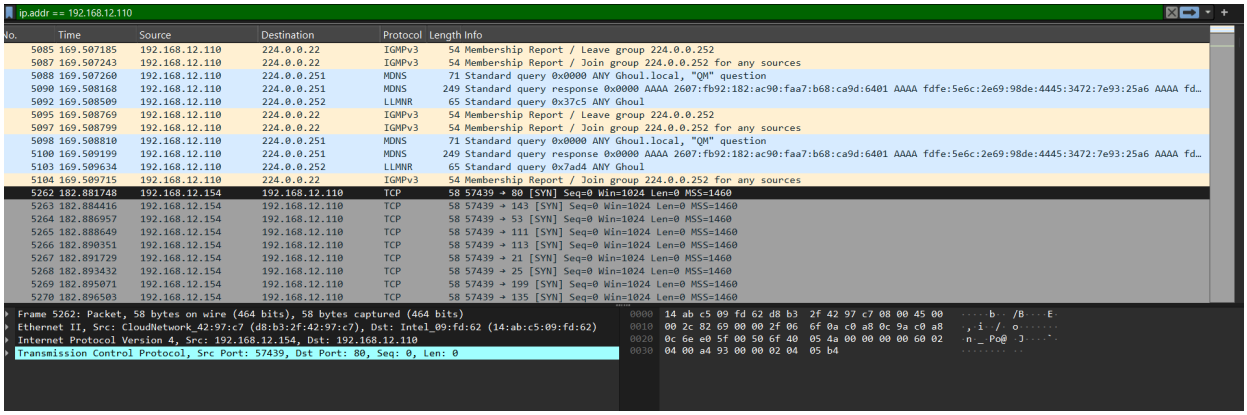
Phone hotspot device isolation

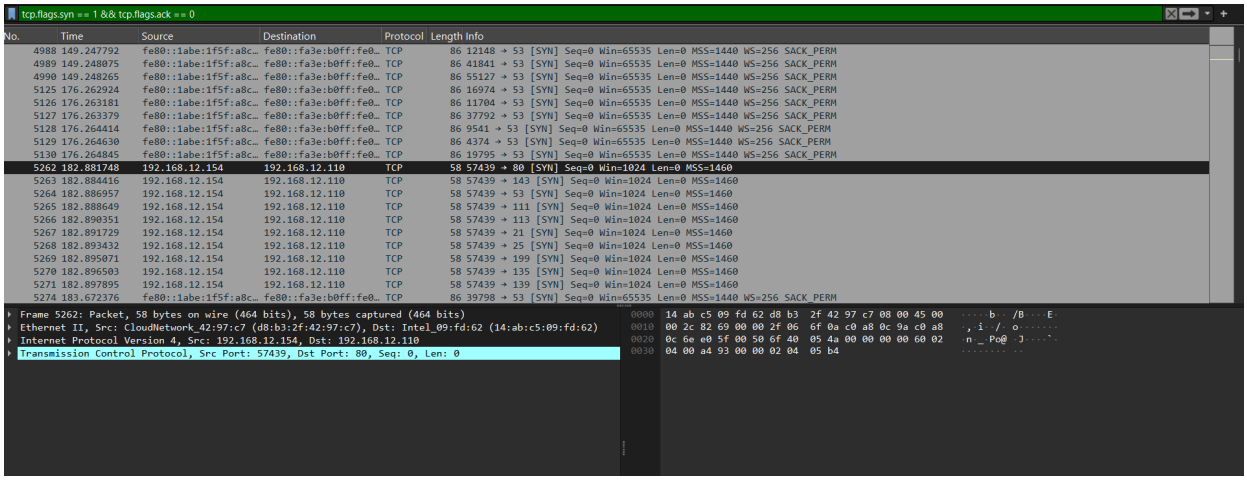
NAT preventing direct host-to-host communication

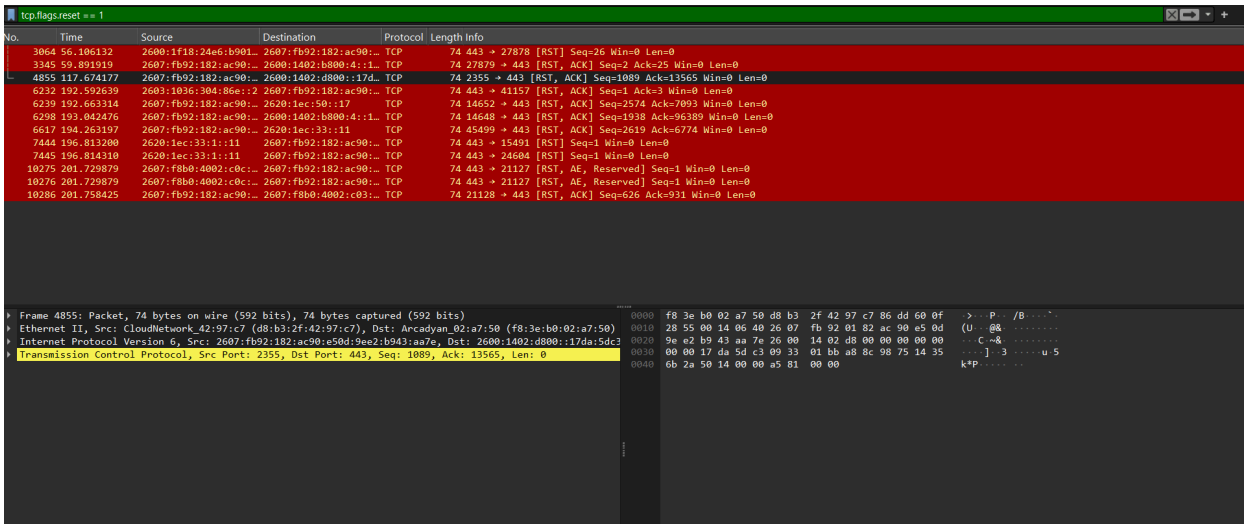
ISP-level filtering

This behavior is common in protected networks.

Wireshark Packet Capture Analysis







Key Observations:

Outgoing SYN packets were visible.

No SYN/ACK or RST packets were returned.

ARP broadcasts may appear, confirming network presence.

Confirms Nmap’s "filtered" interpretation.

Filters Used:

ip.addr == 192.168.12.110 (View only traffic between you and target)

tcp.flags.syn == 1 && tcp.flags.ack == 0 (View only SYN probes)

tcp.flags.reset == 1 (For RST packets)

Troubleshooting & Root Cause Analysis

Ensured you and the target were on the same network.

Confirmed NAT behavior prevents external port scans.

Verified Windows Firewall likely blocks unsolicited requests.

These findings explain the lack of response packets.

What I Learned

This project taught me:

How SYN scans work and why ports appear filtered.

How firewalls silently drop packets.

How NAT and hotspots affect network visibility.

How to use Wireshark filters to isolate packets.

How to analyze expected vs unexpected network behavior.

Full Project Workflow

Step 1 — Installing Tools

Installed **Nmap** on Windows.

Installed **Wireshark** for packet capture.

Verified Nmap installation using: nmap --version

Step 2 — Map the Network (LAN Discovery)

nmap -sn 192.168.1.0/24
Discovered multiple devices:
Phone
Laptops
(controlled environment)

```
C:\Users\Khan>nmap -sn 192.168.12.0/24
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-13 19:08 -0700
Nmap scan report for TMO-G4AR.lan (192.168.12.1)
Host is up (0.029s latency).
MAC Address: F8:3E:B0:02:A7:50 (Unknown)
Nmap scan report for Ghoul.lan (192.168.12.110)
Host is up (0.068s latency).
MAC Address: 14:AB:C5:09:FD:62 (Intel Corporate)
Nmap scan report for iPhone.lan (192.168.12.150)
Host is up (0.088s latency).
MAC Address: 06:FA:74:54:94:CE (Unknown)
Nmap scan report for DESKTOP-1BVSU7G.lan (192.168.12.154)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.73 seconds
```

Step 3 — Attempt Full Port Scan on Multiple Devices

Phone

```
PS C:\Users\Khan> nmap -sV -O 192.168.12.150
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-13 19:21 -0700
Nmap scan report for iPhone.lan (192.168.12.150)
Host is up (0.014s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE    VERSION
49152/tcp open  tcpwrapped
62078/tcp open  tcpwrapped
MAC Address: 06:FA:74:54:94:CE (Unknown)
Device type: phone
Running: Apple iOS 15.X
OS CPE: cpe:/o:apple:iphone_os:15
OS details: Apple iOS 15.0 - 15.6 (Darwin 21.1.0 - 21.6.0)
Network Distance: 1 hop
```

Router

```
PS C:\Users\Khan> nmap -sV -O 192.168.12.0/24 -oN network_scan.txt
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-13 19:22 -0700
Nmap scan report for TMO-G4AR.lan (192.168.12.1)
Host is up (0.0042s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE    SERVICE    VERSION
23/tcp   filtered telnet
53/tcp   open     domain     dnsmasq 2.85
80/tcp   open     http       lighttpd 1.4.69
8080/tcp open     http-proxy
```

(Target laptop)

```
PS C:\Users\Khan> nmap -sT -p 22,80,443,139,445,3389 192.168.12.110
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-14 18:57 -0700
Nmap scan report for Ghoul.lan (192.168.12.110)
Host is up (0.080s latency).

PORT     STATE    SERVICE
22/tcp   filtered ssh
80/tcp   filtered http
139/tcp  filtered netbios-ssn
443/tcp  filtered https
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server
MAC Address: 14:AB:C5:09:FD:62 (Intel Corporate)
```

User desktop

```
Nmap scan report for DESKTOP-1BVSU7G.lan (192.168.12.154)
Host is up (0.00061s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds?
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.98%E=4%D=11/13%OT=135%CT=1%CU=30453%PV=Y%DS=0%DC=L%G=Y%TM=69169
OS:29E%P=i686-pc-windows-windows)SEQ(SP=100%GCD=1%ISR=106%TI=I%CI=I%II=I%SS
OS:=S%TS=A)SEQ(SP=103%GCD=1%ISR=107%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=105%GCD
OS:=1%ISR=10B%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=106%GCD=1%ISR=109%TI=I%CI=I%I
OS:I=I%SS=S%TS=A)SEQ(SP=106%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=M
OS:FFD7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8ST11%O5=MFFD7NW8
OS:ST11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)EC
OS:N(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F
OS:=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=8
OS:0%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q
OS:=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A
OS:%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y
OS:%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T
OS:=80%CD=Z)

Network Distance: 0 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 42.07 seconds
```

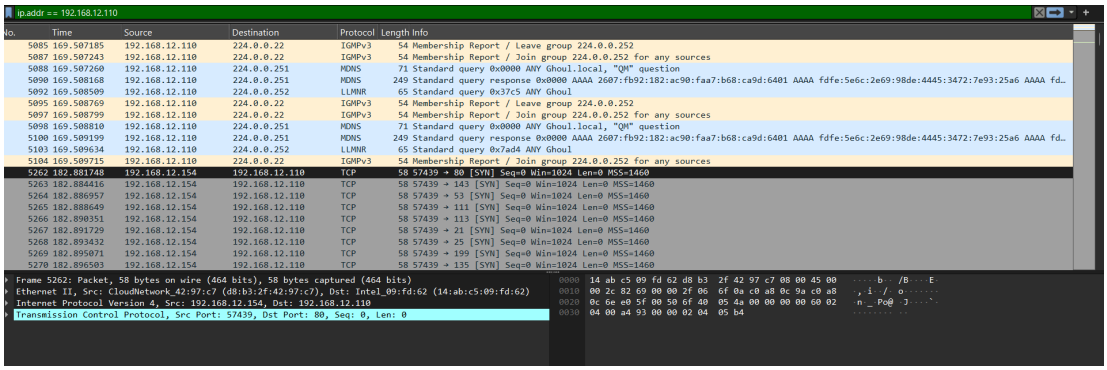
Step 4 — Analyze Behavior

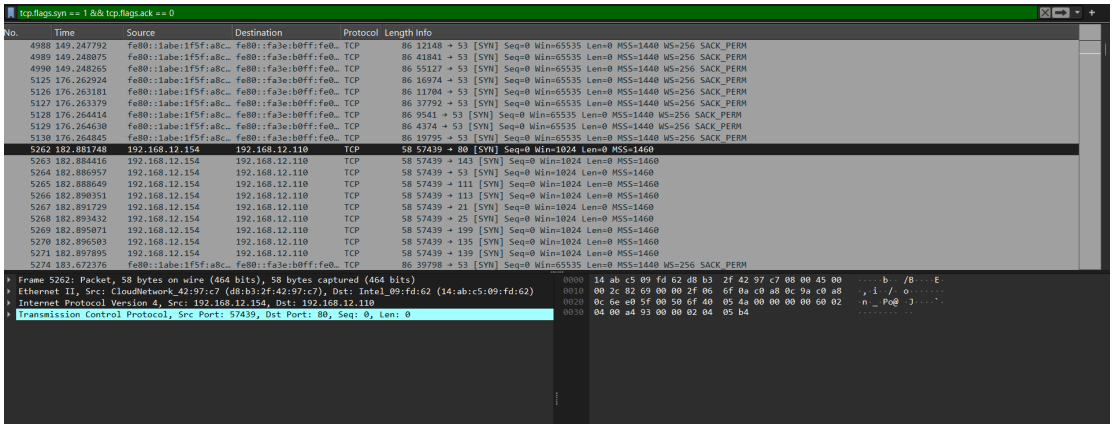
Realized home Wi-Fi:

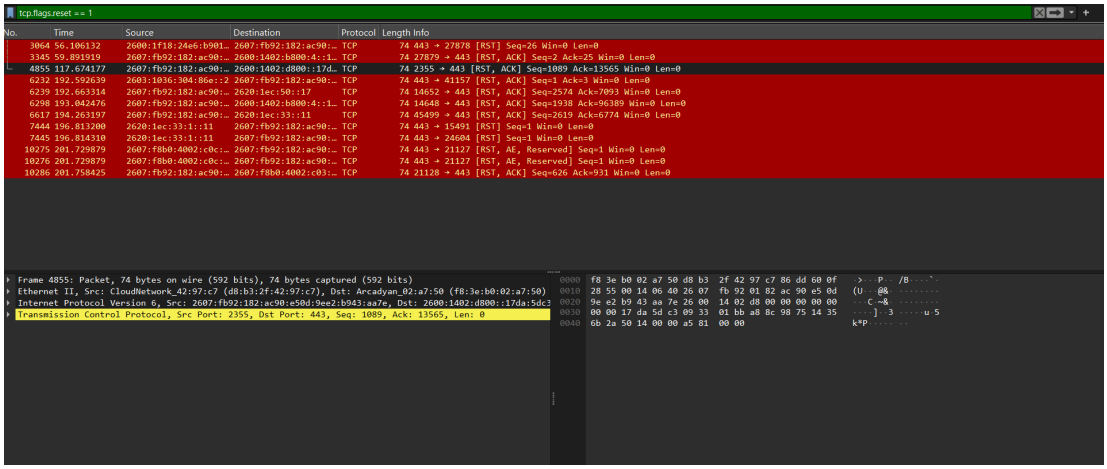
Blocks unsolicited connections
Uses NAT + firewall rules
Devices run strong OS firewalls

Step 5 — Wireshark Verification

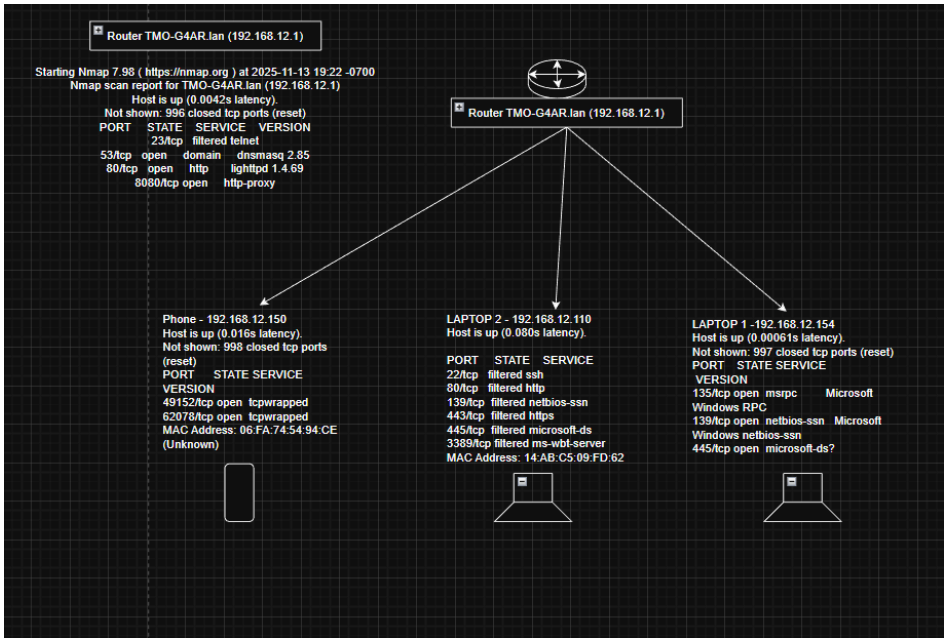
Captured traffic during Nmap scan.
Saw only:
No SYN/ACK or RST
Outgoing SYN
Confirmed router/device dropped packets.




tcp.flags.syn == 1 && tcp.flags.ack == 0
No. Time Source Destination Protocol Length Info
4988 149.247792 fe80::1abe:1f5f:a8c… fe80::fa3e:b0ff:fe0… TCP 86 12148 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
4989 149.248075 fe80::1abe:1f5f:a8c… fe80::fa3e:b0ff:fe0… TCP 86 41841 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
4990 149.248265 fe80::1abe:1f5f:a8c… fe80::fa3e:b0ff:fe0… TCP 86 55127 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
5125 176.262924 fe80::1abe:1f5f:a8c… fe80::fa3e:b0ff:fe0… TCP 86 16974 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
5126 176.263181 fe80::1abe:1f5f:a8c… fe80::fa3e:b0ff:fe0… TCP 86 11704 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
5127 176.263379 fe80::1abe:1f5f:a8c… fe80::fa3e:b0ff:fe0… TCP 86 37792 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
5128 176.264414 fe80::1abe:1f5f:a8c… fe80::fa3e:b0ff:fe0… TCP 86 9541 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
5129 176.264630 fe80::1abe:1f5f:a8c… fe80::fa3e:b0ff:fe0… TCP 86 4374 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
5130 176.264845 fe80::1abe:1f5f:a8c… fe80::fa3e:b0ff:fe0… TCP 86 19795 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
5262 182.881748 192.168.12.154 192.168.12.110 TCP 58 57439 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5263 182.884416 192.168.12.154 192.168.12.110 TCP 58 57439 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5264 182.886957 192.168.12.154 192.168.12.110 TCP 58 57439 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5265 182.888649 192.168.12.154 192.168.12.110 TCP 58 57439 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5266 182.890351 192.168.12.154 192.168.12.110 TCP 58 57439 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5267 182.891729 192.168.12.154 192.168.12.110 TCP 58 57439 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5268 182.893432 192.168.12.154 192.168.12.110 TCP 58 57439 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5269 182.895071 192.168.12.154 192.168.12.110 TCP 58 57439 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5270 182.896503 192.168.12.154 192.168.12.110 TCP 58 57439 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5271 182.897895 192.168.12.154 192.168.12.110 TCP 58 57439 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5274 183.672376 fe80::1abe:1f5f:a8c… fe80::fa3e:b0ff:fe0… TCP 86 39798 → 53 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
Frame 5262: Packet, 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
Ethernet II, Src: CloudNetwork_42:97:c7 (d8:b3:2f:42:97:c7), Dst: Intel_09:fd:62 (14:ab:c5:09:fd:62)
Internet Protocol Version 4, Src: 192.168.12.154, Dst: 192.168.12.110
Transmission Control Protocol, Src Port: 57439, Dst Port: 80, Seq: 0, Len: 0
0000 14 ab c5 09 fd 62 d8 b3 2f 42 97 c7 08 00 45 00 ·····b·· /B····E·
0010 00 2c 82 69 00 00 2f 06 6f 0a c0 a8 0c 9a c0 a8 ·,·i··/· o·······
0020 0c 6e e0 5f 00 50 6f 40 05 4a 00 00 00 00 60 02 ·n·_·Po@ ·J····`·
0030 04 00 a4 93 00 00 02 04 05 b4 ···· ···· ··


tcp.flags.reset == 1
No. Time Source Destination Protocol Length Info
3064 56.106132 2600:1f18:24a6:b901… 2607:fb92:182:ac90:… TCP 74 443 → 27878 [RST] Seq=26 Win=0 Len=0
3345 59.891919 2607:fb92:182:ac90:… 2600:1402:b800:4::1… TCP 74 27879 → 443 [RST, ACK] Seq=2 Ack=25 Win=0 Len=0
4855 117.674177 2607:fb92:182:ac90:… 2600:1402:d800::17d… TCP 74 2355 → 443 [RST, ACK] Seq=1089 Ack=13565 Win=0 Len=0
6232 192.592639 2603:103c:304:86e::2 2607:fb92:182:ac90:… TCP 74 443 → 41157 [RST, ACK] Seq=1 Ack=3 Win=0 Len=0
6239 192.663314 2607:fb92:182:ac90:… 2620:1ec:50::17 TCP 74 14652 → 443 [RST, ACK] Seq=2574 Ack=7093 Win=0 Len=0
6298 193.042476 2607:fb92:182:ac90:… 2600:1402:b800:4::1… TCP 74 14648 → 443 [RST, ACK] Seq=1938 Ack=96389 Win=0 Len=0
6617 194.263197 2607:fb92:182:ac90:… 2620:1ec:33::11 TCP 74 45499 → 443 [RST, ACK] Seq=2619 Ack=6774 Win=0 Len=0
7444 196.813200 2620:1ec:33:1::11 2607:fb92:182:ac90:… TCP 74 443 → 15491 [RST] Seq=1 Win=0 Len=0
7445 196.814310 2620:1ec:33:1::11 2607:fb92:182:ac90:… TCP 74 443 → 24604 [RST] Seq=1 Win=0 Len=0
10275 201.729879 2607:f8b0:4002:c0c:… 2607:fb92:182:ac90:… TCP 74 443 → 21127 [RST, AE, Reserved] Seq=1 Win=0 Len=0
10276 201.729879 2607:f8b0:4002:c0c:… 2607:fb92:182:ac90:… TCP 74 443 → 21127 [RST, AE, Reserved] Seq=1 Win=0 Len=0
10286 201.758425 2607:fb92:182:ac90:… 2607:f8b0:4002:c03:… TCP 74 21128 → 443 [RST, ACK] Seq=626 Ack=931 Win=0 Len=0
Frame 4855: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: CloudNetwork_42:97:c7 (d8:b3:2f:42:97:c7), Dst: Arcadyan_02:a7:50 (f8:3e:b0:02:a7:50)
Internet Protocol Version 6, Src: 2607:fb92:182:ac90:e50d:9ee2:b943:aa7e, Dst: 2600:1402:d800::17da:5dc3
Transmission Control Protocol, Src Port: 2355, Dst Port: 443, Seq: 1089, Ack: 13565, Len: 0
0000 f8 3e b0 02 a7 50 d8 b3 2f 42 97 c7 86 dd 60 0f ·>···P·· /B····`·
0010 28 55 00 14 06 40 26 07 fb 92 01 82 ac 90 e5 0d (U···@&· ········
0020 9e e2 b9 43 aa 7e 26 00 14 02 d8 00 00 00 00 00 ···C·~&· ········
0030 00 00 17 da 5d c3 09 33 01 bb a8 8c 98 75 14 35 ····]··3 ·····u·5
0040 6b 2a 50 14 00 00 a5 81 00 00 k*P····· ··

Updated Network Topology (Wi-Fi)



Key Properties:

NAT prevents external scans
Router firewall blocks internal scans
Devices have OS-level firewalls

Devices Found Earlier:

Device	IP	MAC Vendor	Notes
Laptop	192.168.12.110	Intel	Filtered
Laptop	192.168.12.154	AMD	Filtered
Phone	192.168.12.150	Iphone	Responded only to ARP
Router	192.168.12.1	T- mobile	Filtered

Conclusion

This project demonstrates:

Realistic network scanning behavior on home Wi-Fi
How to analyze filtered ports
How to use Wireshark to validate Nmap results
How NAT and firewalls protect modern networks