

NMAP AND WIRESHARK

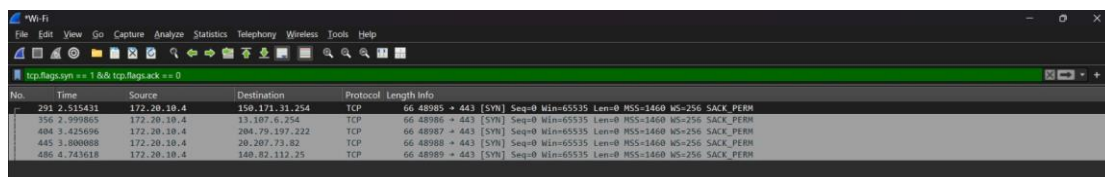
```
C:\Users\Athre>nmap -sS 192.168.56.0/24 -oN scan-results.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 18:27 India Standard Time
Nmap scan report for 192.168.56.1
Host is up (0.00098s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
808/tcp    open  ccproxy-http
1521/tcp   open  oracle
3306/tcp   open  mysql
8080/tcp   open  http-proxy
25734/tcp  open  unknown

Nmap done: 256 IP addresses (1 host up) scanned in 11.28 seconds
```

Nmap TCP SYN scan on local network
(192.168.56.0/24)

It found 8 open ports.

These open ports indicate which services are exposed and could be potential attacks.



The image shows a Wireshark packet capture window with a filter applied: `tcp.flags.syn == 1 && tcp.flags.ack == 0`. The packet list shows several SYN packets from source 172.20.10.4 to various destinations. The packet details pane shows the structure of a SYN packet.

No.	Time	Source	Destination	Protocol	Length	Info
291	2.515431	172.20.10.4	150.171.31.254	TCP	66	48985 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
356	2.998865	172.20.10.4	13.107.0.254	TCP	66	48986 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
404	3.425696	172.20.10.4	204.79.197.222	TCP	66	48987 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
445	3.800808	172.20.10.4	28.207.73.82	TCP	66	48988 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
486	4.743618	172.20.10.4	140.82.132.25	TCP	66	48989 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM

The applied filter (`tcp.flags.syn == 1 && tcp.flags.ack == 0`) isolates SYN packets.

It proves that **Nmap was actively sending scan requests**, and Wireshark successfully captured those packets.