

local IP range :

- Ip a
- Ip route

```
~$ ip route
192.168.56.0/24 dev eth0 proto kernel scope link src 192.168.56.102 metric 100
```

TCP SYN scan:

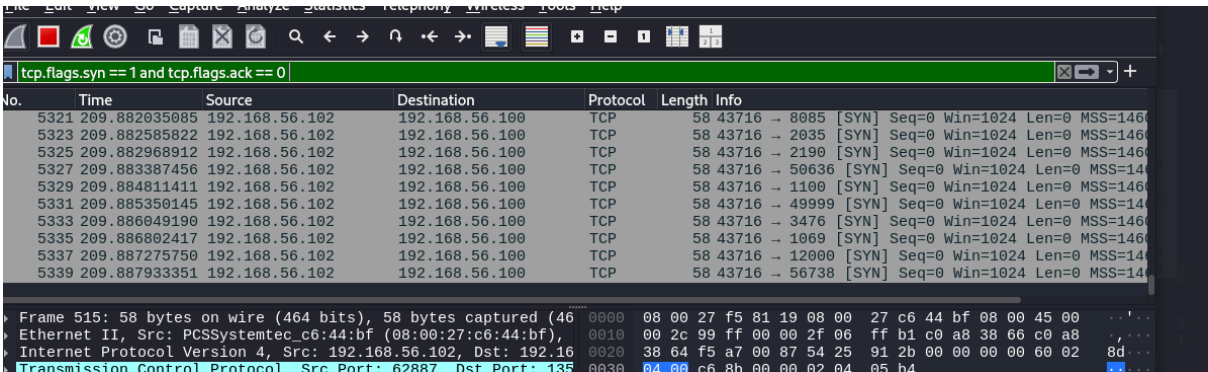
```
(dj@kali)-[~]
$ sudo nmap -sS 192.168.56.0/24


Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 20:06 IST
Nmap scan report for 192.168.56.100
Host is up (0.00046s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:F5:81:19 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.000010s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
25/tcp    open  smtp
53/tcp    open  domain

Nmap done: 256 IP addresses (2 hosts up) scanned in 30.36 seconds
```

Wireshark.



Port	Protocol	Common Service	Description	 Security Risks
25	TCP	SMTP (Simple Mail Transfer Protocol)	Used for sending emails between mail servers	- Open Relay Attacks: If misconfigured, attackers can send spam using your server.- Brute-force Login Attempts on mail accounts.- Banner Grabbing can reveal mail server version (useful for attackers).- Email Spoofing if SPF/DKIM not set.
53	TCP/UDP	DNS (Domain Name System)	Resolves hostnames to IPs	- DNS Amplification Attacks (DDoS). - Cache Poisoning / Spoofing.- Zone Transfers if TCP/53 is exposed and AXFR is enabled.- Data Exfiltration via DNS tunneling.

HTML file:

Nmap Scan Report - Scanned at Mon Jun 23 20:21:23 2025

Scan Summary | 192.168.56.100 | 192.168.56.102

Scan Summary

Nmap 7.95 was initiated at Mon Jun 23 20:21:23 2025 with these arguments:
`sudo nmap -sS -oX scan_results.xml 192.168.56.0/24`

Verbosity: 0; Debug level 0

Nmap done at Mon Jun 23 20:21:56 2025; 256 IP addresses (2 hosts up) scanned in 33.00 seconds

192.168.56.100

Address

- 192.168.56.100 (IPv4)
- 08:00:27:F5:81:19 - PCS Systemtechnik/Oracle VirtualBox virtual NIC (mac)

Ports

The 1000 ports scanned but not shown below are in state: **filtered**

- 1000 ports replied with: **proto-unreach**

Misc Metrics (click to expand)

192.168.56.102

Address

- 192.168.56.102 (IPv4)

Ports

The 998 ports scanned but not shown below are in state: **closed**

- 998 ports replied with: **reset**

Port	State (toggle closed [0] filtered [0])	Service	Reason	Product	Version	Extra Info
25	tcp open	smtp	syn-ack			
53	tcp open	domain	syn-ack			

Misc Metrics (click to expand)

Go to top

Toggle Closed Ports

Toggle Filtered Ports