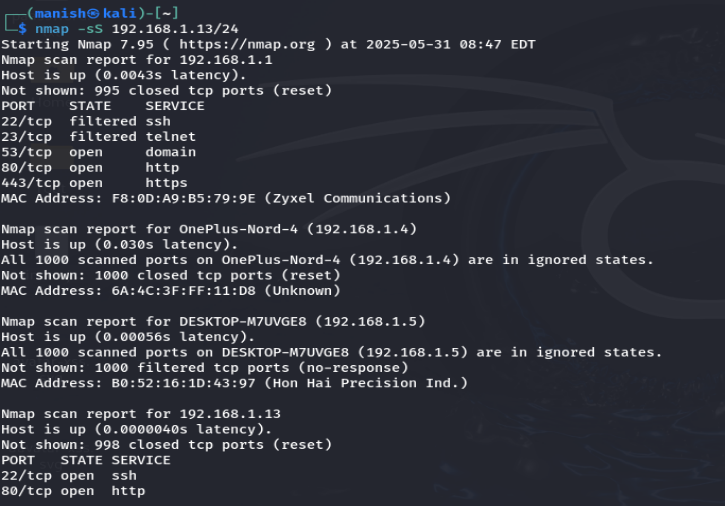
1. **Running nmap to perform TCP SYN scan**



(manish㉿kali)-[~]

└─$ nmap -sS 192.168.1.13/24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-31 08:47 EDT

Nmap scan report for 192.168.1.1

Host is up (0.0043s latency).

Not shown: 995 closed tcp ports (reset)

PORT STATE SERVICE

22/tcp filtered ssh

23/tcp filtered telnet

53/tcp open domain

80/tcp open http

443/tcp open https

MAC Address: F8:0D:A9:B5:79:9E (Zyxel Communications)

Nmap scan report for OnePlus-Nord-4 (192.168.1.4)

Host is up (0.030s latency).

All 1000 scanned ports on OnePlus-Nord-4 (192.168.1.4) are in ignored states.

Not shown: 1000 closed tcp ports (reset)

MAC Address: 6A:4C:3F:FF:11:D8 (Unknown)

Nmap scan report for DESKTOP-M7UVGE8 (192.168.1.5)

Host is up (0.00056s latency).

All 1000 scanned ports on DESKTOP-M7UVGE8 (192.168.1.5) are in ignored states.

Not shown: 1000 filtered tcp ports (no-response)

MAC Address: B0:52:16:1D:43:97 (Hon Hai Precision Ind.)

Nmap scan report for 192.168.1.13

Host is up (0.0000040s latency).

Not shown: 998 closed tcp ports (reset)

PORT STATE SERVICE

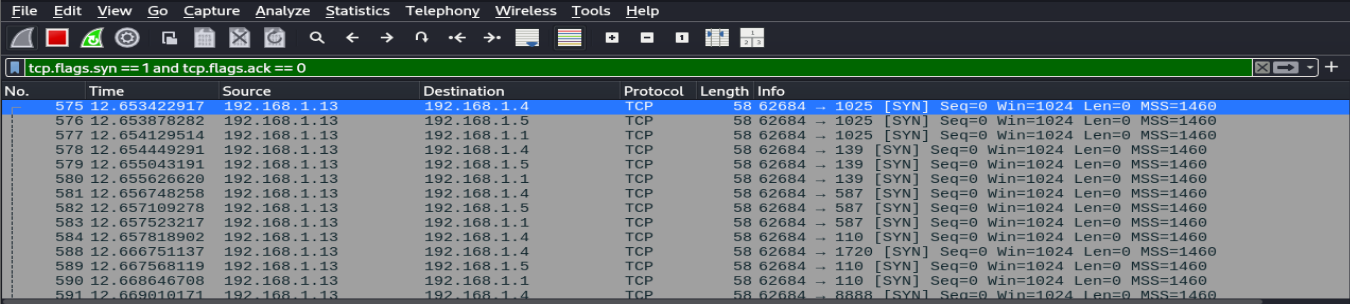
22/tcp open ssh

80/tcp open http

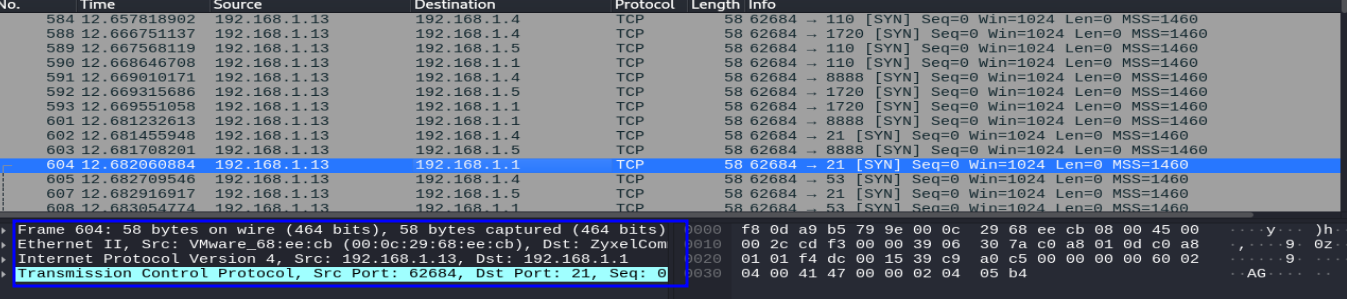
Nmap done: 256 IP addresses (4 hosts up) scanned in 6.55 seconds

1. Analyze packet capture with Wireshark.

Open wireshark, start packet capturing



See the Tcp packets, services running om ports etc..



1. **Services running on ports**

22/tcp ssh

23/tcp telnet

53/tcp domain

80/tcp http

443/tcp https

1. Potential security risk from open ports

| **Port** | **Protocol** | **Service** | **Risk Level** | **Description of Risk** | **Recommendations** |
| --- | --- | --- | --- | --- | --- |
| 22 | TCP | SSH | Low–Medium | Secure shell for remote login. Risk if default credentials or password-based auth is used. | Disable password login, use SSH key auth, change default port, and enable fail2ban or firewall rules. |
| 23 | TCP | Telnet | High | Transmits data (including passwords) in plaintext. Easily exploited. | **Disable Telnet**, use SSH instead. Remove service if not needed. |
| 53 | TCP/UDP | DNS | Medium | Can be exploited for DNS tunneling (data exfiltration) or spoofing if misconfigured. | Use secure DNS configurations (e.g., DNSSEC), monitor for unusual traffic, and restrict zone transfers. |
| 80 | TCP | HTTP | High | Unencrypted web traffic; allows MITM attacks, sniffing, and credential theft. | Enforce HTTPS with redirection; disable HTTP if not needed. |
| 443 | TCP | HTTPS | Low | Encrypted traffic, but may be vulnerable if using weak SSL/TLS configurations. | Use TLS 1.2 or 1.3, disable older protocols (SSLv3), and regularly scan with SSL tools. |