

## Task 1: Scan Your Local Network for Open Ports

**Objective:** Learn to discover open ports on devices in your local network to understand network exposure.

**Tools:** Nmap (free), Wireshark (optional).

**Machine:** Kali (Linux).

### 1. Install Nmap from official website.

**Nmap on Kali Linux** is usually **pre-installed**. However, we can check it. If it is missing or not by running following commands:

**nmap --version** or **nmap --help**

**--version** show the installed version of nmap and **--help** is nmap commands help book.



```
kali@kali: ~$ nmap --help
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] [Target Specification]
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilenames>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1,host2[,host3],...>: Exclude hosts/networks
  --exclude-file <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL List Scan - simply list targets to scan
  -sn Ping Scan - disable port scan
  -Pn Treat all hosts as online - skip host discovery
  -Pp/Pp/Pn/Pn[portlist]: TCP SYN/ACK, UDP or SCIP discovery to given ports
  -PE/PP/PM: [OS echo, timestamp, and network request discovery probes]
  -PO[protocol list]: IP Protocol PING
  -n/S: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1,serv2[,...]>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/T/P/A/X/M: TCP SYN/Connect()/ACK/Window/Maxmin scans
  -sU: UDP Scan
  -nM/sf/AX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sV/Z: SCIP INIT/CONCL-IGMP scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN OPTIONS:
  -p <port ranges>: Only scan specified ports
  Ex: -p22 -p1-65535; -p U55,111,137,721-25,16,129,8080,819
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -i: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan numbers most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
```

And to ensure it's up to date; you can install or reinstall it by using the following commands:

**sudo apt update nmap**

**sudo aptget update nmap**

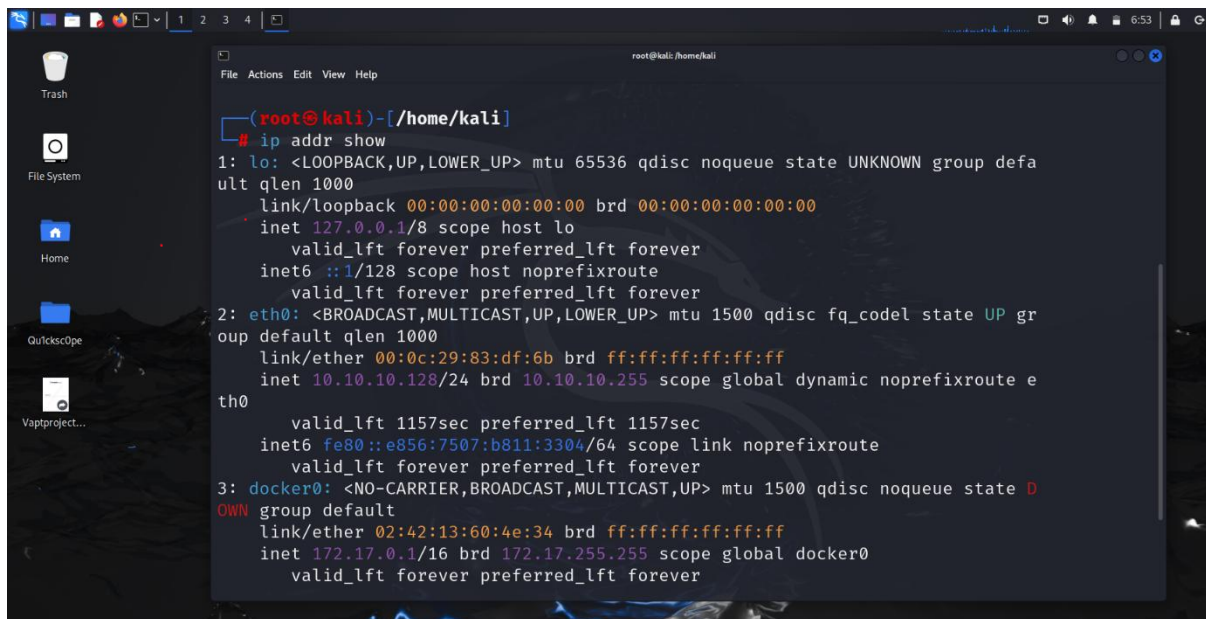
**sudo apt install nmap**

**apt** or **aptget** for package handling tool so you can install/update/remove nmap by using **sudo** for root privileges.

## 2. Find your local IP range (e.g., 192.168.1.0/24).

On terminal use command to find local IP range:

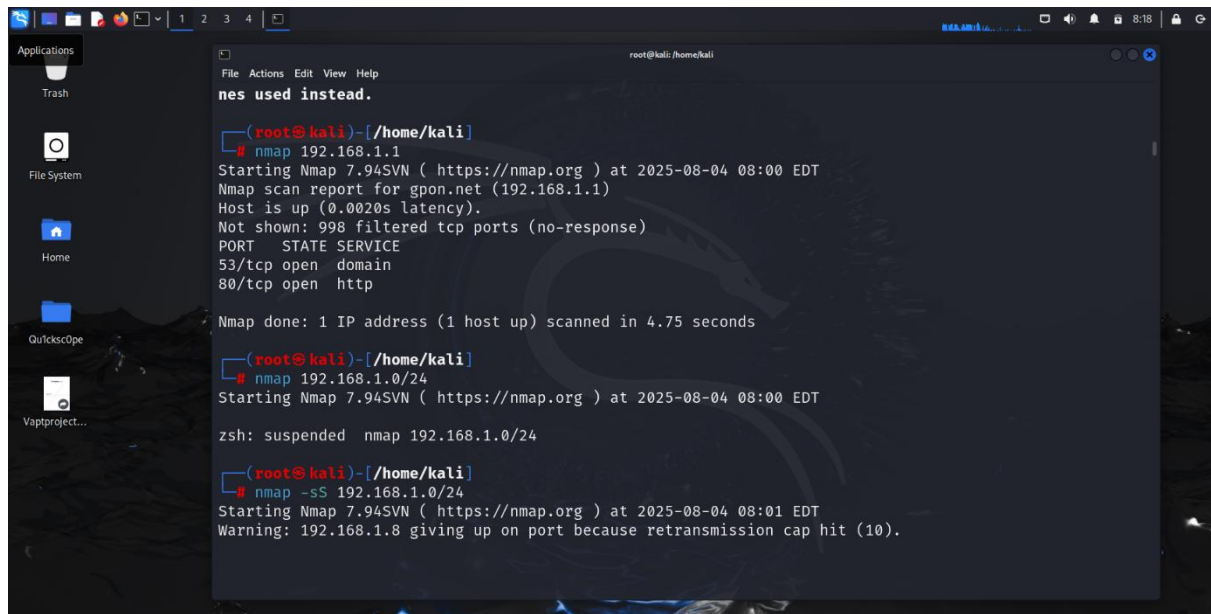
- **ip addr show** is a Linux command to determine your **local subnet and IP address**, from which you can infer the range.
- Ip address given below is **10.10.10.128/24** **ip of my VM**



```
(root@kali)-[/home/kali]
# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:83:df:6b brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.128/24 brd 10.10.10.255 scope global dynamic noprefixroute eth0
        valid_lft 1157sec preferred_lft 1157sec
    inet6 fe80::e856:7507:b811:3304/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:13:60:4e:34 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
```

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

- **Nmap -sS 192.168.1.0/24** -sS switch performs a TCP SYN scan, which is one of the most common and stealthy types of port scans. It's often referred to as a "half-open" scan because it doesn't complete the full TCP handshake.
- TCP SYN packets sent by a tool (like Nmap) to a target system to check if specific TCP ports are open. These packets are part of TCP SYN scans and are used for probing—testing how a system responds.
- Send a **SYN packet** to a port.
- The target system replies:
  - **SYN-ACK** → Port is **open**
  - **RST** → Port is **closed**
  - **No response** or **ICMP error** → Port is **filtered** (likely by a firewall)
  - You send **RST** (reset) instead of ACK to avoid a full connection.
- Mostly used to avoid detection



```
root@kali: /home/kali
File Actions Edit View Help
nes used instead.

(root@kali)-[/home/kali]
# nmap 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 08:00 EDT
Nmap scan report for gpon.net (192.168.1.1)
Host is up (0.0020s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http

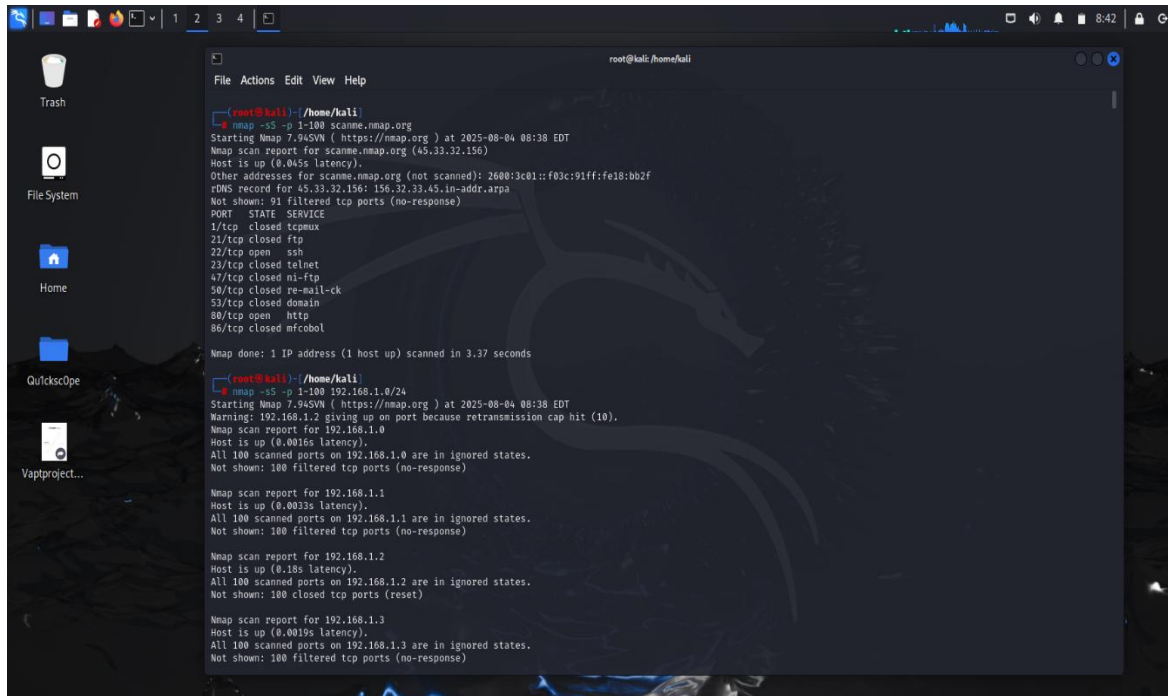
Nmap done: 1 IP address (1 host up) scanned in 4.75 seconds

(root@kali)-[/home/kali]
# nmap 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 08:00 EDT

zsh: suspended nmap 192.168.1.0/24

(root@kali)-[/home/kali]
# nmap -sS 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 08:01 EDT
Warning: 192.168.1.8 giving up on port because retransmission cap hit (10).
```

- After running `nmap -sS 192.168.1.0/24` command keep getting retransmission cap hit because of firewall filtration, so I narrowed it down by using specific ports range using nmap switch **-p 1-100**.



```
root@kali: /home/kali
File Actions Edit View Help

root@kali: /home/kali
nmap -sS -p 1-100 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 08:38 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.045s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: 156.32.33.45.in-addr.arpa
Not shown: 91 filtered tcp ports (no-response)
PORT      STATE SERVICE
1/tcp     closed tcpxmx
21/tcp    closed ftp
22/tcp    open  ssh
23/tcp    closed telnet
47/tcp    closed ni-ftp
50/tcp    closed re-mail-ck
53/tcp    closed domain
80/tcp    open  http
86/tcp    closed mircobol

Nmap done: 1 IP address (1 host up) scanned in 3.37 seconds

root@kali: /home/kali
nmap -sS -p 1-100 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 08:38 EDT
Warning: 192.168.1.2 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.1.0
Host is up (0.0016s latency).
All 100 scanned ports on 192.168.1.0 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)

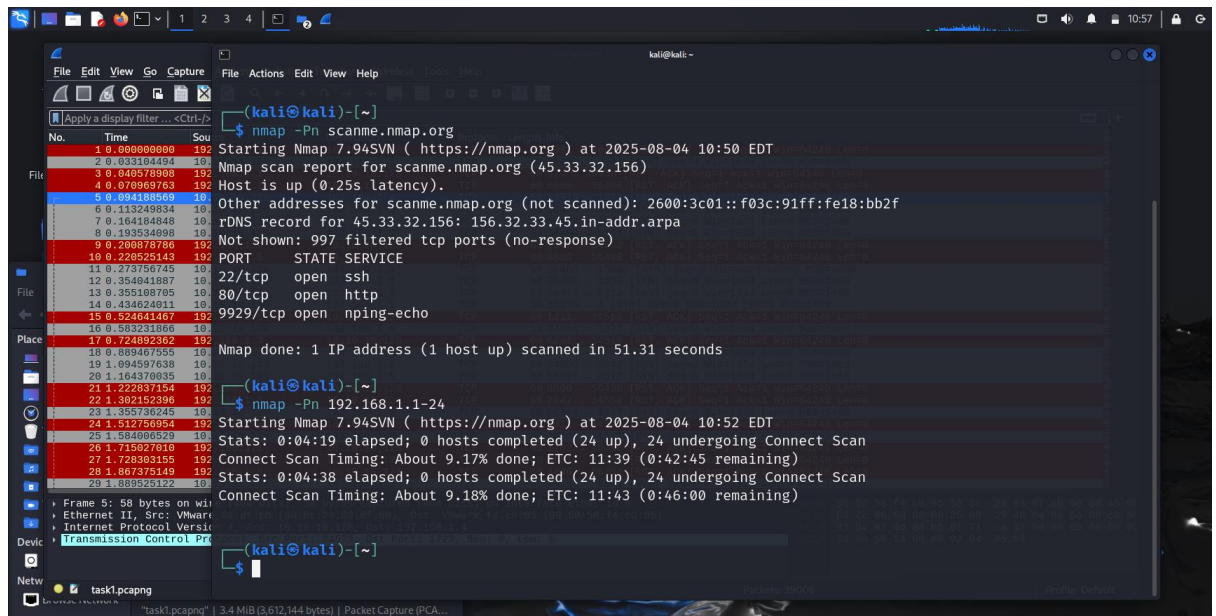
Nmap scan report for 192.168.1.1
Host is up (0.0032s latency).
All 100 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)

Nmap scan report for 192.168.1.2
Host is up (0.18s latency).
All 100 scanned ports on 192.168.1.2 are in ignored states.
Not shown: 100 closed tcp ports (reset)

Nmap scan report for 192.168.1.3
Host is up (0.0019s latency).
All 100 scanned ports on 192.168.1.3 are in ignored states.
Not shown: 100 filtered tcp ports (no-response)
```

#### 4. Note down IP addresses and open ports found.

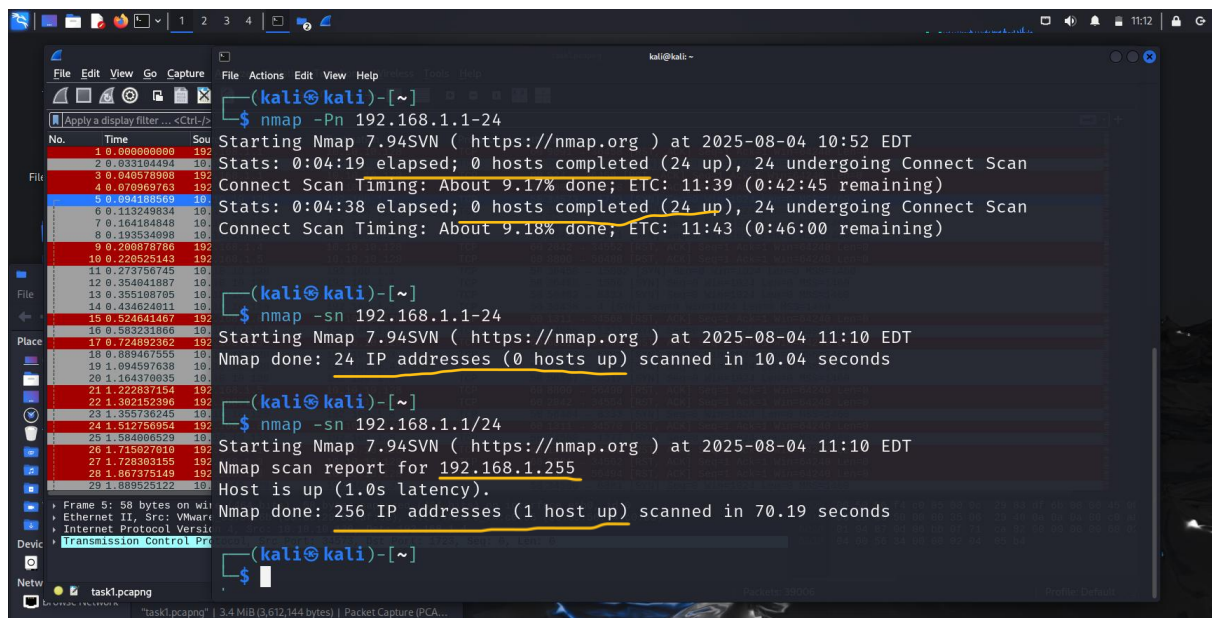
- Most common open/filtered ports are 21, 22, 23, 53, 80, 443, 123.
- Since pinging probes are getting blocked by firewall, I used `nmap -Pn 192.168.1-24` to minimize the time put the IP range but still not discovered the live host yet.



```
(kali@kali)-[~]
$ nmap -Pn scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 10:50 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: 156.32.33.45.in-addr.arpa
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp   open  nping-echo
Nmap done: 1 IP address (1 host up) scanned in 51.31 seconds

(kali@kali)-[~]
$ nmap -Pn 192.168.1-24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 10:52 EDT
Stats: 0:04:19 elapsed; 0 hosts completed (24 up), 24 undergoing Connect Scan
Connect Scan Timing: About 9.17% done; ETC: 11:39 (0:42:45 remaining)
Stats: 0:04:38 elapsed; 0 hosts completed (24 up), 24 undergoing Connect Scan
Connect Scan Timing: About 9.18% done; ETC: 11:43 (0:46:00 remaining)
```

- Try it with only host discovery switch by using `nmap -sn 192.168.1.0/24`



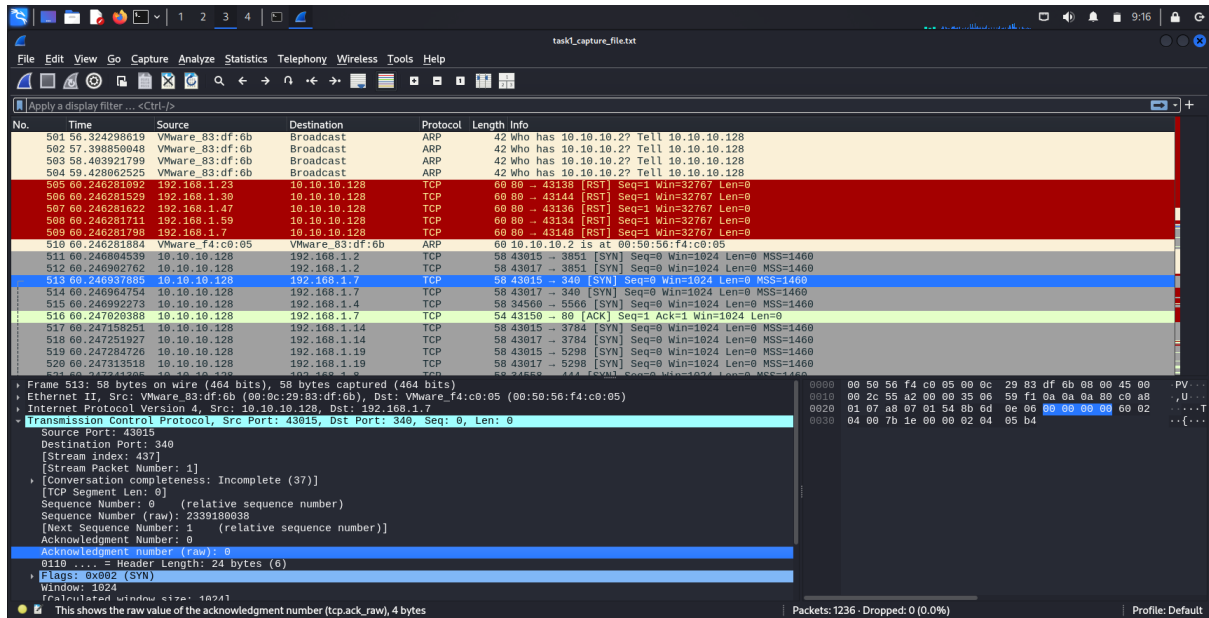
```
(kali@kali)-[~]
$ nmap -Pn 192.168.1.1-24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 10:52 EDT
Stats: 0:04:19 elapsed; 0 hosts completed (24 up), 24 undergoing Connect Scan
Connect Scan Timing: About 9.17% done; ETC: 11:39 (0:42:45 remaining)
Stats: 0:04:38 elapsed; 0 hosts completed (24 up), 24 undergoing Connect Scan
Connect Scan Timing: About 9.18% done; ETC: 11:43 (0:46:00 remaining)

(kali@kali)-[~]
$ nmap -sn 192.168.1.1-24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 11:10 EDT
Nmap done: 24 IP addresses (0 hosts up) scanned in 10.04 seconds

(kali@kali)-[~]
$ nmap -sn 192.168.1.1/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-04 11:10 EDT
Nmap scan report for 192.168.1.255
Host is up (1.0s latency).
Nmap done: 256 IP addresses (1 host up) scanned in 70.19 seconds
```

## 5. Optionally analyze packet capture with Wireshark.

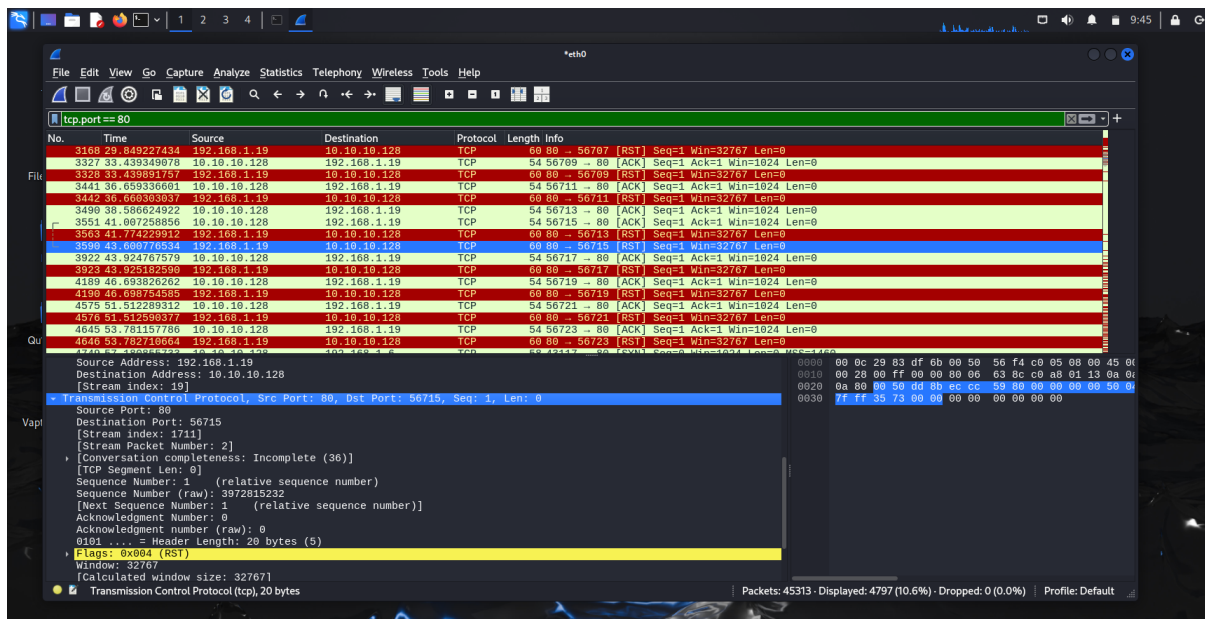
- We can analyze the transmitting packets by using filters tcp, tcp.port, tcp.port == 80, udp, dns, http, http2, http3 and do on.
- It provides packets in- depth detail how system actually sent/receive data over connected networks.



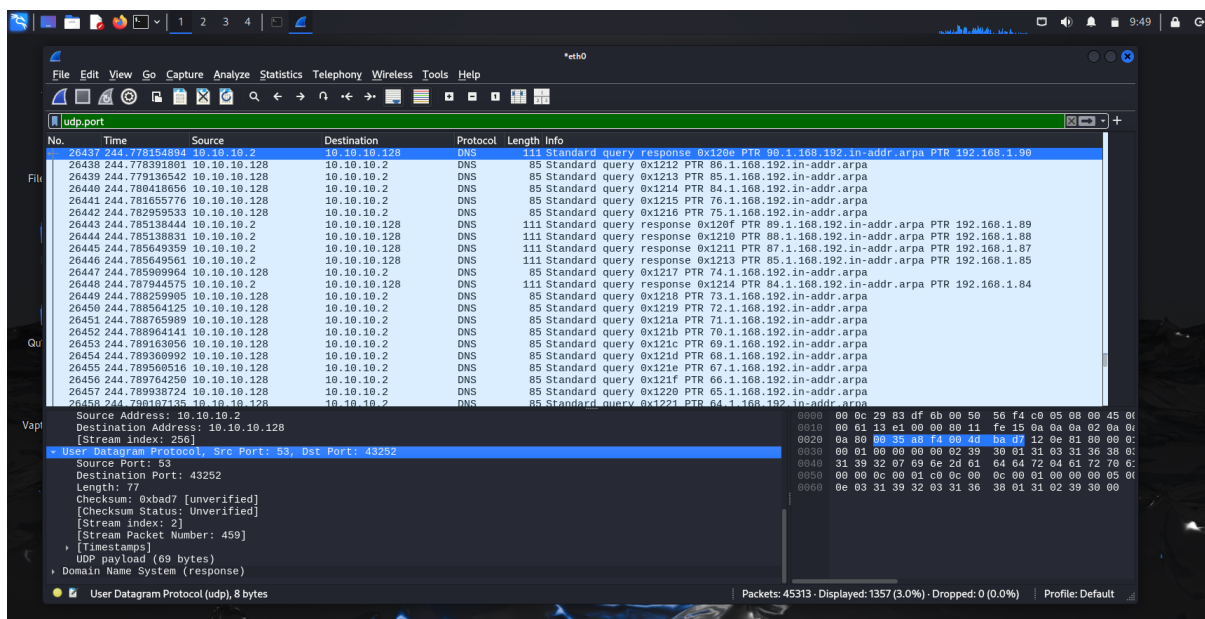


## 6. Research common services running on those ports.

- Most commonly probes are TCP SYN packets are sent by the nmap to check whether the target system is running or not then it sends back SYN-ACK but since we are doing half open scan it only sends SYN packets and don't wait for the ACK to establish connection.
- RST flag is sent back when the probes are getting blocked or unreachable.



- Most common open/filtered ports are 21 ftp, 22 ssh, 23 telnet, 80 http, 443 https, 123 udp, 53 dns.



## 7. Identify potential security risks from open ports.

- They represent potential entry points into your system. If a service listening on a port is misconfigured, outdated, or vulnerable, it could be exploited by an attacker.
- Exposed Vulnerable Services
  - Old or unpatched services may contain known vulnerabilities.
    - Open port 21 (FTP) → Might allow anonymous access or be vulnerable to brute-force.
    - Open port 445 (SMB) → Could be vulnerable to exploits like EternalBlue.
- Information Leakage
  - Services often leak system info:
    - Web servers (port 80/443) may expose server versions, frameworks, and internal paths.
    - SSH (port 22) banners can reveal OS and version.
- Brute-force and Credential Attacks
  - Open ports like:
    - 22 (SSH) → Targeted with brute-force password attempts.
    - 3389 (RDP) → Common in ransomware attacks.
- Denial-of-Service (DoS) Attacks
  - Some services are vulnerable to resource exhaustion or flooding.
  - Even if not exploited, they can be overwhelmed and crash.
- Backdoors or Rogue Services
  - Malware may open ports for remote access (e.g., reverse shells).
  - Unauthorized open ports may indicate compromise.
- Increased Attack Surface
  - The more ports you leave open, the more opportunities attackers have to:
    - Scan your network
    - Find misconfigurations
    - Exploit vulnerabilities