Task 1st: Scan Your Local Network for Open Ports

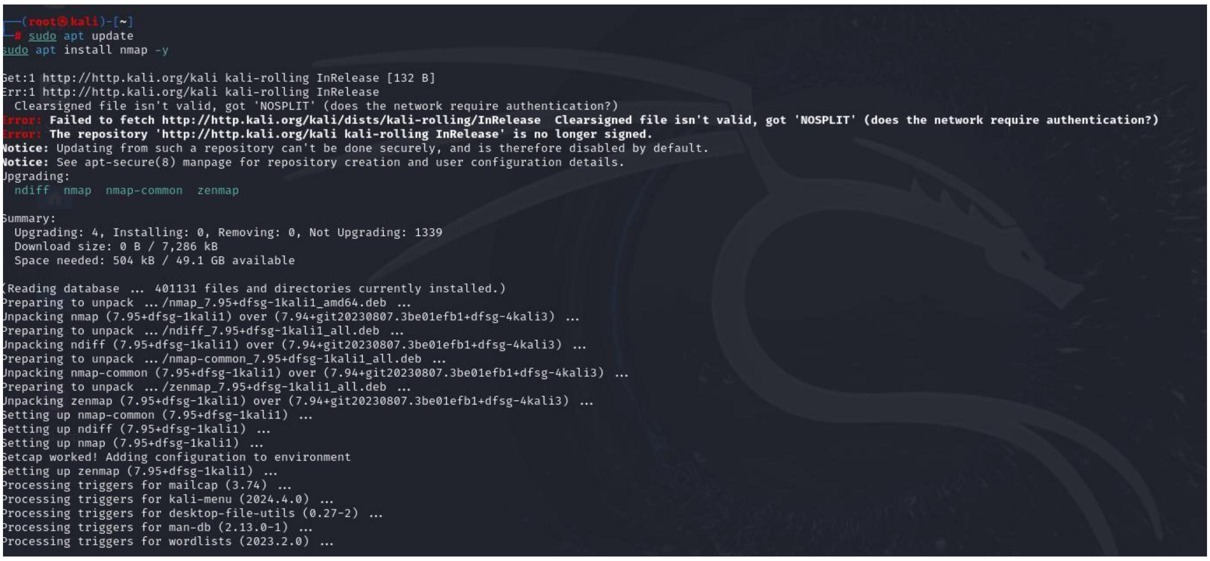
1. Install Nmap from Official Website

Kali Linux typically comes with **Nmap pre-installed**. However, to ensure it’s installed or to upgrade it:

To install or update Nmap:

sudo apt update

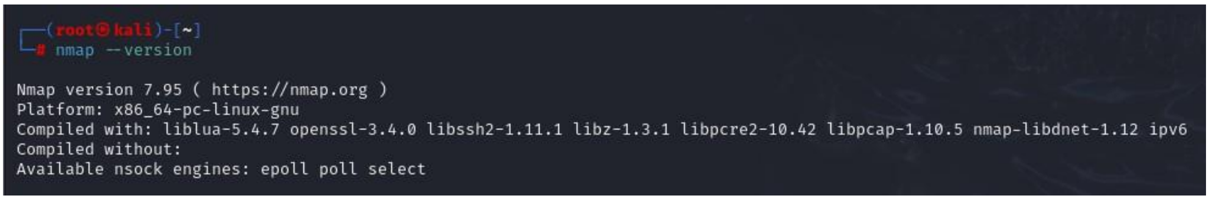
sudo apt install nmap -y



```
┌──(root㉿kali)-[~]
└─# sudo apt update
sudo apt install nmap -y

Get:1 http://http.kali.org/kali kali-rolling InRelease [132 B]
Err:1 http://http.kali.org/kali kali-rolling InRelease
  Clearsigned file isn't valid, got 'NOSPLIT' (does the network require authentication?)
Error: Failed to fetch http://http.kali.org/kali/dists/kali-rolling/InRelease  Clearsigned file isn't valid, got 'NOSPLIT' (does the network require authentication?)
Error: The repository 'http://http.kali.org/kali kali-rolling InRelease' is no longer signed.
Notice: Updating from such a repository can't be done securely, and is therefore disabled by default.
Notice: See apt-secure(8) manpage for repository creation and user configuration details.
Upgrading:
  ndiff  nmap  nmap-common  zenmap

Summary:
  Upgrading: 4, Installing: 0, Removing: 0, Not Upgrading: 1339
  Download size: 0 B / 7,286 kB
  Space needed: 504 kB / 49.1 GB available

(Reading database ... 401131 files and directories currently installed.)
Preparing to unpack .../nmap_7.95+dfsg-1kali1_amd64.deb ...
Unpacking nmap (7.95+dfsg-1kali1) over (7.94+git20230807.3be01efb1+dfsg-4kali3) ...
Preparing to unpack .../ndiff_7.95+dfsg-1kali1_all.deb ...
Unpacking ndiff (7.95+dfsg-1kali1) over (7.94+git20230807.3be01efb1+dfsg-4kali3) ...
Preparing to unpack .../nmap-common_7.95+dfsg-1kali1_all.deb ...
Unpacking nmap-common (7.95+dfsg-1kali1) over (7.94+git20230807.3be01efb1+dfsg-4kali3) ...
Preparing to unpack .../zenmap_7.95+dfsg-1kali1_all.deb ...
Unpacking zenmap (7.95+dfsg-1kali1) over (7.94+git20230807.3be01efb1+dfsg-4kali3) ...
Setting up nmap-common (7.95+dfsg-1kali1) ...
Setting up ndiff (7.95+dfsg-1kali1) ...
Setting up nmap (7.95+dfsg-1kali1) ...
Setcap worked! Adding configuration to environment
Setting up zenmap (7.95+dfsg-1kali1) ...
Processing triggers for mailcap (3.74) ...
Processing triggers for kali-menu (2024.4.0) ...
Processing triggers for desktop-file-utils (0.27-2) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for wordlists (2023.2.0) ...
```

To check if Nmap is installed:

nmap –version



```
┌──(root㉿kali)-[~]
└─# nmap --version

Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.7 openssl-3.4.0 libssh2-1.11.1 libz-1.3.1 libpcre2-10.42 libpcap-1.10.5 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```

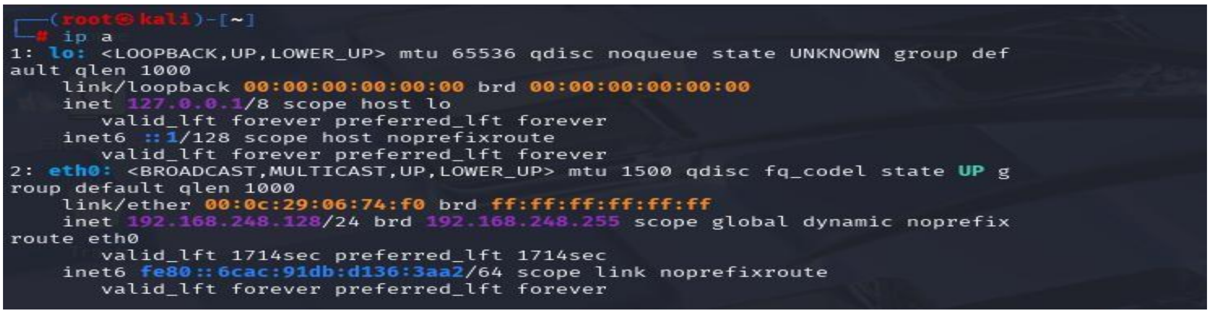
---

2. Find Your Local IP Range (e.g., 192.168.1.0/24)

To scan your local network, you need to determine the IP address and subnet.

Use the following command scan local network:

ip a



```
┌──(root㉿kali)-[~]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault 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 g
roup default qlen 1000
    link/ether 00:0c:29:06:74:f0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.248.128/24 brd 192.168.248.255 scope global dynamic noprefix
route eth0
       valid_lft 1714sec preferred_lft 1714sec
    inet6 fe80::6cac:91db:d136:3aa2/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Task 1st: Scan Your Local Network for Open Ports

Active Network Interface (eth0):

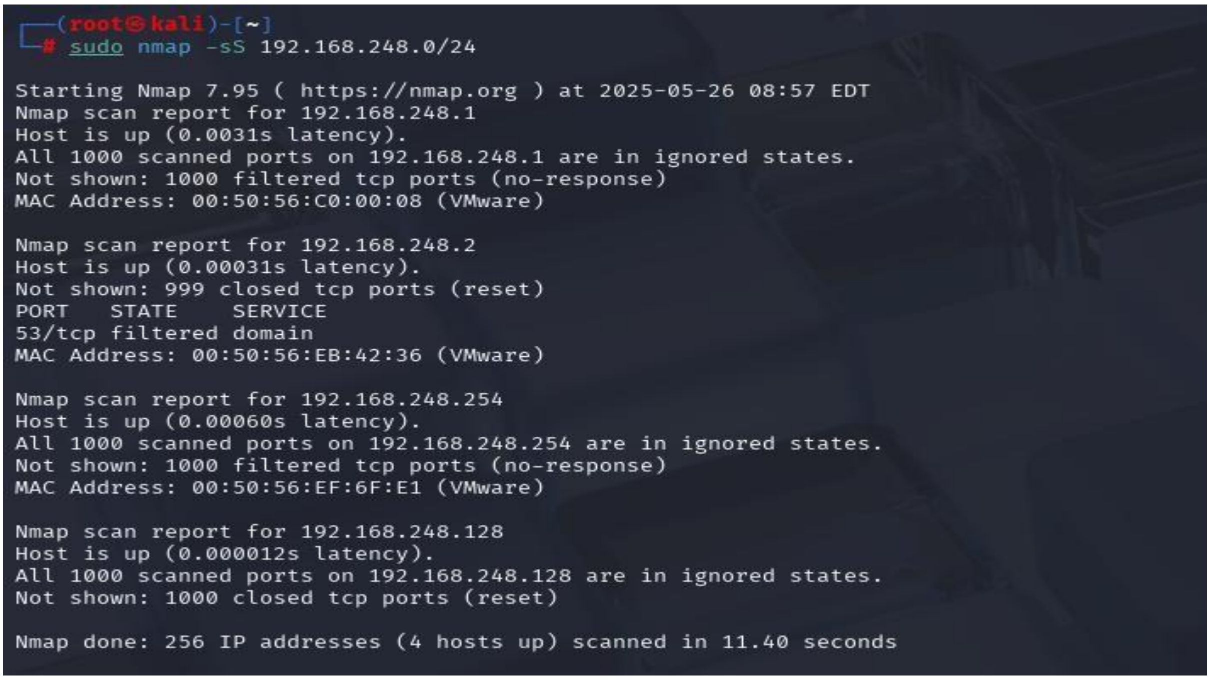
- **IP Address: 192.168.248.128**
- **Subnet Mask: /24**
- **Broadcast Address: 192.168.248.255**
- **Subnet Range: 192.168.248.0/24**

3. Run: Nmap -sS, 192.168.248.128/24 to Perform a TCP SYN Scan

The -sS flag instructs Nmap to perform a **TCP SYN (stealth) scan** which sends SYN packets and observes responses without completing TCP handshakes.

Run the command:

sudo nmap -sS 192.168.248.128/24



```
┌──(root㉿kali)-[~]
└─# sudo nmap -sS 192.168.248.0/24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 08:57 EDT
Nmap scan report for 192.168.248.1
Host is up (0.0031s latency).
All 1000 scanned ports on 192.168.248.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.248.2
Host is up (0.00031s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE    SERVICE
53/tcp filtered domain
MAC Address: 00:50:56:EB:42:36 (VMware)

Nmap scan report for 192.168.248.254
Host is up (0.00060s latency).
All 1000 scanned ports on 192.168.248.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:EF:6F:E1 (VMware)

Nmap scan report for 192.168.248.128
Host is up (0.000012s latency).
All 1000 scanned ports on 192.168.248.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 11.40 seconds
```

This scan identifies:

- **Live devices** (hosts that respond)
- **Open TCP ports**
- **Running services (if identifiable)**

IP Address	Status	Open Ports	Notes
192.168.248.1	Up	None (filtered)	Host responded, no open port
192.168.248.2	Up	53 (filtered)	DNS service, filtered
192.168.248.254	Up	None (filtered)	Host responded, no open port
192.168.248.128	Up (Kali)	None (reset)	This is the scanning machine

Task 1st: Scan Your Local Network for Open Ports

Observations

- Only port 53 (DNS) on 192.168.248.2 was detected, and it is **filtered**.
- Other hosts had **all ports filtered or reset**, indicating strong firewall rules or inactive services.
- The scan completed in **11.40 seconds**.

4. Note Down IP Addresses and Open Ports Found

From the scan output,

IP Address	Status	Open Ports	Service	Remarks
192.168.248.1	Up	None	—	All 1000 TCP ports filtered
192.168.248.2	Up	53/tcp	Filtered (domain)	Likely running DNS service
192.168.248.254	Up	None	—	All ports filtered
192.168.248.128	Up	None	—	This is the Kali machine itself

Additional Notes:

- **192.168.248.2** is the only host with a detected **filtered port (53/tcp)**, which commonly indicates a DNS service—possibly a DNS server or firewall filtering responses.
- Other hosts responded to the scan but showed **no open ports**, meaning they may be protected by firewalls or not running services on standard TCP ports.
- **Filtered ports** suggest that a firewall is blocking Nmap from determining the actual state (open/closed).

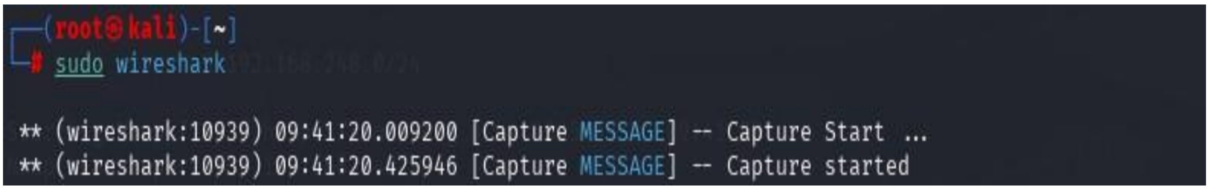
5. Optionally Analyze Packet Capture with Wireshark

Wireshark helps visualize the traffic generated during a scan and understand how devices respond.

Steps:

1. **Open Wireshark in Kali:**

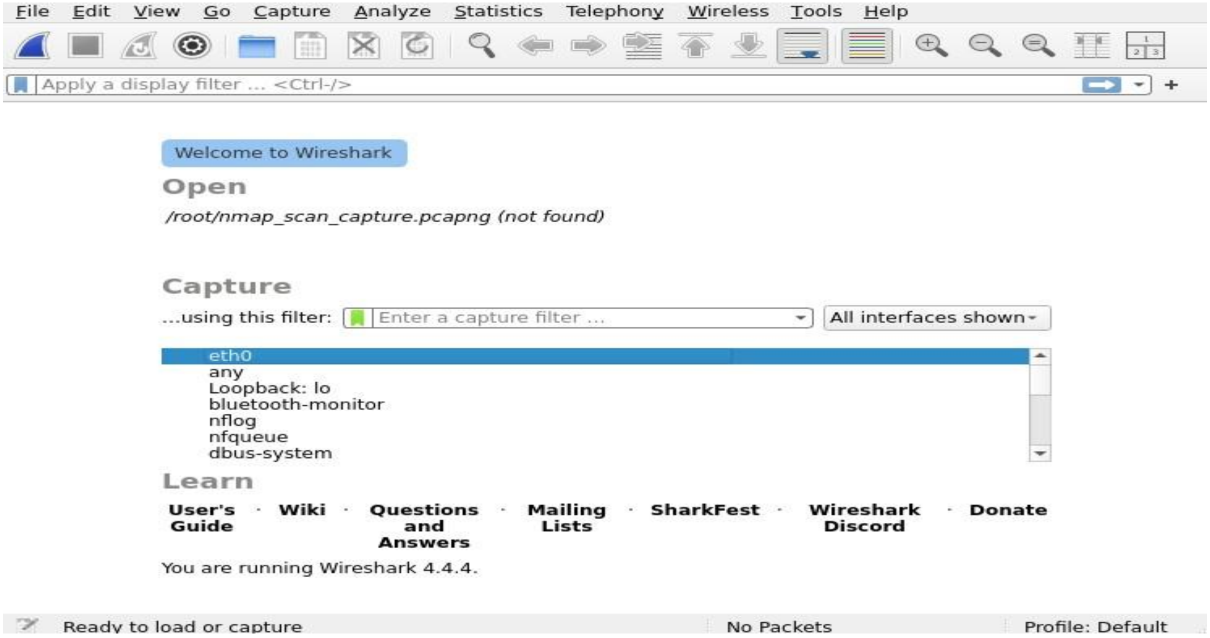
sudo wireshark



```
┌──(root㉿kali)-[~]
└─# sudo wireshark

** (wireshark:10939) 09:41:20.009200 [Capture MESSAGE] -- Capture Start ...
** (wireshark:10939) 09:41:20.425946 [Capture MESSAGE] -- Capture started
```

2. **Chooses active interface (likely eth0 for wired or bridged).**

Task 1st: Scan Your Local Network for Open Ports


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

Welcome to Wireshark

Open

/root/nmap_scan_capture.pcapng (not found)

Capture

...using this filter: Enter a capture filter … All interfaces shown

```
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
```

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

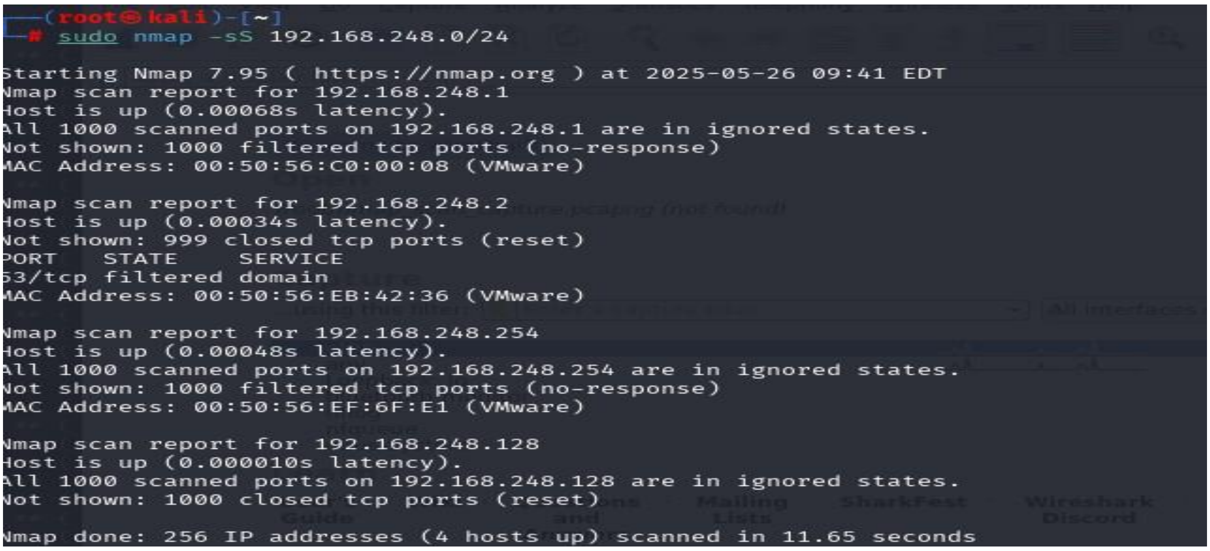
You are running Wireshark 4.4.4.

Ready to load or capture   No Packets   Profile: Default

WE HAVE CHOOSES eth0 and then Start capturing before running the Nmap scan.

3. **In a new terminal, run:**

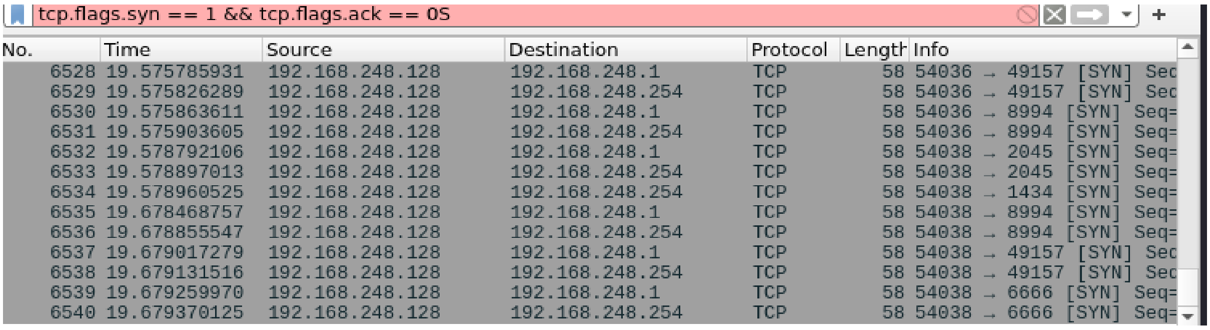
   sudo nmap -sS 192.168.248.0/24



```
┌──(root㉿kali)-[~]
└─# sudo nmap -sS 192.168.248.0/24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 09:41 EDT
Nmap scan report for 192.168.248.1
Host is up (0.00068s latency).
All 1000 scanned ports on 192.168.248.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.248.2
Host is up (0.00034s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE    SERVICE
53/tcp filtered domain
MAC Address: 00:50:56:EB:42:36 (VMware)

Nmap scan report for 192.168.248.254
Host is up (0.00048s latency).
All 1000 scanned ports on 192.168.248.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:EF:6F:E1 (VMware)

Nmap scan report for 192.168.248.128
Host is up (0.000010s latency).
All 1000 scanned ports on 192.168.248.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 11.65 seconds
```

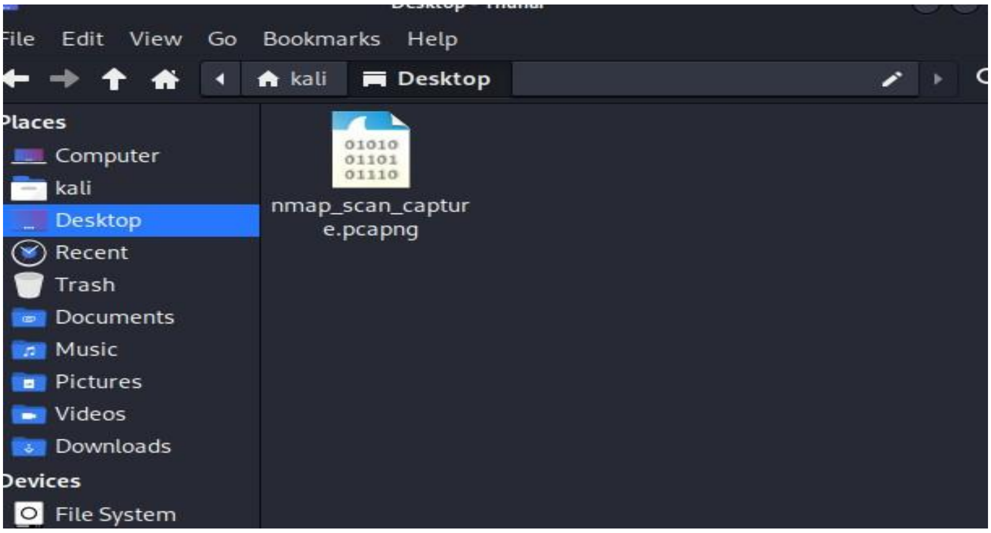
4. **Return to Wireshark and apply this filter to see SYN packets:**

   tcp.flags.syn == 1 && tcp.flags.ack == 0



```
tcp.flags.syn == 1 && tcp.flags.ack == 0S

No.     Time         Source           Destination      Protocol Length Info
   6528 19.575785931 192.168.248.128  192.168.248.1    TCP        58 54036 → 49157 [SYN] Sec
   6529 19.575826289 192.168.248.128  192.168.248.254  TCP        58 54036 → 49157 [SYN] Sec
   6530 19.575863611 192.168.248.128  192.168.248.1    TCP        58 54036 → 8994 [SYN] Seq=
   6531 19.575903605 192.168.248.128  192.168.248.254  TCP        58 54036 → 8994 [SYN] Seq=
   6532 19.578792106 192.168.248.128  192.168.248.1    TCP        58 54038 → 2045 [SYN] Seq=
   6533 19.578897013 192.168.248.128  192.168.248.254  TCP        58 54038 → 2045 [SYN] Seq=
   6534 19.578960525 192.168.248.128  192.168.248.254  TCP        58 54038 → 1434 [SYN] Seq=
   6535 19.678468757 192.168.248.128  192.168.248.1    TCP        58 54038 → 8994 [SYN] Seq=
   6536 19.678855547 192.168.248.128  192.168.248.254  TCP        58 54038 → 8994 [SYN] Seq=
   6537 19.679017279 192.168.248.128  192.168.248.1    TCP        58 54038 → 49157 [SYN] Sec
   6538 19.679131516 192.168.248.128  192.168.248.254  TCP        58 54038 → 49157 [SYN] Sec
   6539 19.679259970 192.168.248.128  192.168.248.1    TCP        58 54038 → 6666 [SYN] Seq=
   6540 19.679370125 192.168.248.128  192.168.248.254  TCP        58 54038 → 6666 [SYN] Seq=
```

5. **Observe That:**
   - ○ **How SYN packets are sent.**
   - ○ **Responses like SYN-ACK (open port) or RST (closed) are received.**
6. **Then Stop the capture and save it:**
   - ○ **File → Save As → nmap_scan_capture.pcapng**



---

6. Research Common Services Running on Those Ports

From scan:

- **Only 192.168.248.2 has a detected open (filtered) port:**
  - ○ **Port 53/tcp → Service: domain**
  - ○ **This refers to the DNS (Domain Name System) service.**

About Port 53:

Port	Protocol	Service	Description
53	TCP/UDP	DNS	Resolves domain names (e.g., google.com → IP address). Typically runs on DNS servers.

---

7. Identify Potential Security Risks from Open Ports

Risks of Exposing Port 53 (DNS):

Threat	Description
DNS Amplification Attacks	Can be abused for DDoS attacks by spoofing requests.

Task 1st: Scan Your Local Network for Open Ports

DNS Cache Poisoning	**Attacker manipulates DNS cache to redirect traffic to malicious sites.**

Zone Transfers (if misconfigured)	**May reveal internal domain details to attackers.**
Information Leakage	**Poor DNS configuration might expose subdomains or hostnames.**

Mitigation:

- **Restrict DNS access to trusted IPs.**
- **Disable zone transfers unless absolutely necessary.**
- **Keep DNS server software updated.**
- **Monitor DNS traffic for anomalies.**

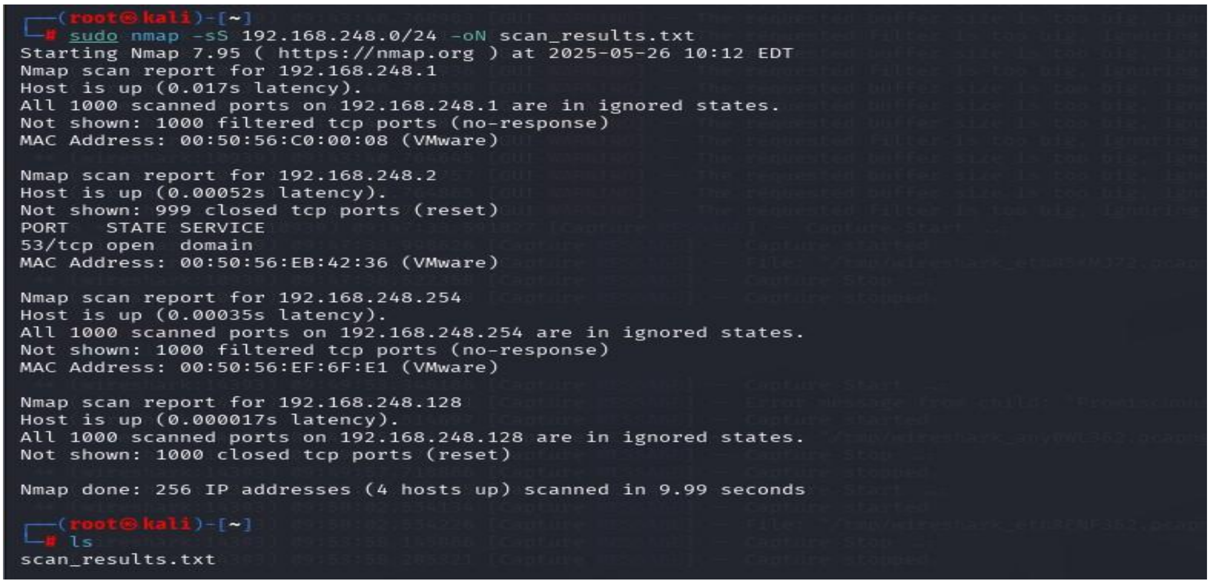
8. Save Scan Results as a Text or HTML File

To document your work and submit it as part of your internship or GitHub task, here are two ways to save your Nmap results:

Option 1: Save as Plain Text (.txt)

sudo nmap -sS 192.168.248.0/24 -oN scan_results.txt

- **-oN = Normal text format**
- **Output will be saved as scan_results.txt in your current directory.**



```
┌──(root㉿kali)-[~]
└─# sudo nmap -sS 192.168.248.0/24 -oN scan_results.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-26 10:12 EDT
Nmap scan report for 192.168.248.1
Host is up (0.017s latency).
All 1000 scanned ports on 192.168.248.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.248.2
Host is up (0.00052s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:EB:42:36 (VMware)

Nmap scan report for 192.168.248.254
Host is up (0.00035s latency).
All 1000 scanned ports on 192.168.248.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:EF:6F:E1 (VMware)

Nmap scan report for 192.168.248.128
Host is up (0.000017s latency).
All 1000 scanned ports on 192.168.248.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 9.99 seconds

┌──(root㉿kali)-[~]
└─# ls
scan_results.txt
```

GitHub Repository Link

All files, documentation, and supporting evidence for Task 1 have been uploaded to the following GitHub repository:

Repository URL:
https://github.com/CyberSIDH/Task-1-

Repository Contents:

Task 1st: Scan Your Local Network for Open Ports

- README.md – Full explanation of the task
- scan_results.txt – Output from the Nmap TCP SYN scan
- nmap_scan_capture.pcapng – Wireshark packet capture file