

**Note:** All the commands, outputs, and configurations in this document are demonstrated on Kali Linux.

## **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)

### **Hints/Mini Guide:**

1. Install Nmap from official website.
2. Find your local IP range (192.168.62.130/24).
3. Run: `nmap -sS 192.168.1.0/24` to perform TCP SYN scan.
4. Note down IP addresses and open ports found.
5. Optionally analyze packet capture with Wireshark.
6. Research common services running on those ports.
7. Identify potential security risks from open ports.
8. Save scan results as a text or HTML file.

### **1. Install Nmap from official website.**

Step 1: Update your system package list - `sudo apt update`

Step 2: Install Nmap - `sudo apt install nmap -y`

Step 3: Verify the installation - `nmap --version`

### **2. Find your local IP range (192.168.62.130/24).**

- **ip a Command Output**

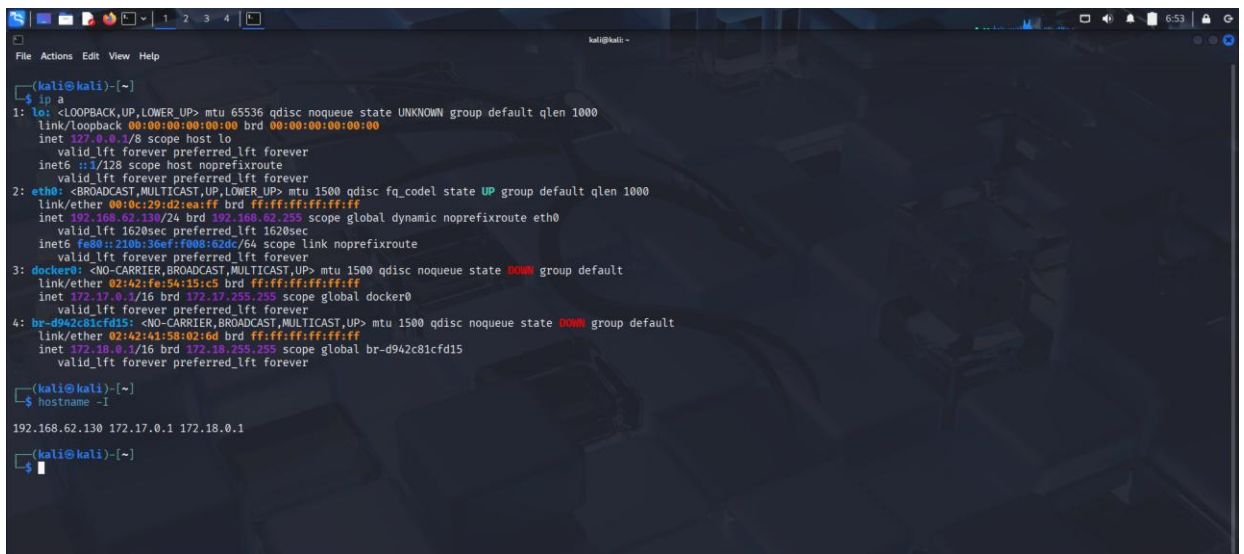
The `ip a` (or `ip addr`) command displays all network interfaces and their IP addresses.

- **Active Network Interface – eth0**

The interface eth0 is UP and has the IP address 192.168.62.130/24.

- **Private IP Addresses**

The system uses private IPs like 192.168.62.130, 172.17.0.1, and 172.18.0.1. These are used within internal networks and are not accessible directly from the internet.



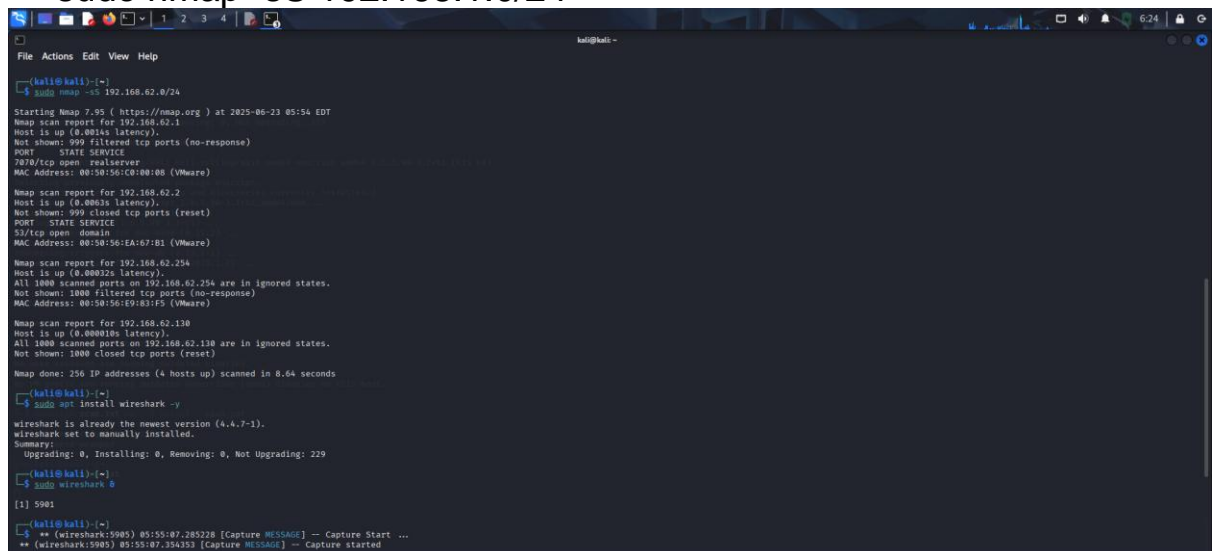
```
(kali@kali)~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        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:d2:ea:ff brd ff:ff:ff:ff:ff:ff
    inet 192.168.62.130/24 brd 192.168.62.255 scope global dynamic noprefixroute eth0
        valid_lft 1620sec preferred_lft 1620sec
    inet6 fe80::210b:36ef:f000:62d7/64 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:fe:54:15:c5 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
4: br-d942c81cfd15: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:43:58:02:6d brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.1/16 brd 172.18.255.255 scope global br-d942c81cfd15
        valid_lft forever preferred_lft forever

(kali@kali)~$ hostname -I
192.168.62.130 172.17.0.1 172.18.0.1

(kali@kali)~$
```

### 3. Run: **nmap -sS 192.168.62.130/24** to perform TCP SYN scan.

- **sudo nmap -sS 192.168.1.0/24**



```
(kali@kali)~$ sudo nmap -sS 192.168.62.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 05:54 EDT
Nmap scan report for 192.168.62.1
Host is up (0.0013s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
7870/tcp  open  realserver
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.62.2
Host is up (0.0003s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:EA:07:01 (VMware)

Nmap scan report for 192.168.62.254
Host is up (0.0002s latency).
All 1000 scanned ports on 192.168.62.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:10:83:15 (VMware)

Nmap scan report for 192.168.62.130
Host is up (0.000010s latency).
All 1000 scanned ports on 192.168.62.130 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 0.64 seconds

(kali@kali)~$ sudo apt install wireshark -y
wireshark is already the newest version (4.4.7-1).
wireshark set to manually installed.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 229

(kali@kali)~$ sudo wireshark &
[1] 5901

(kali@kali)~$ ** (wireshark:5905) 05:55:07.285228 [Capture M05SA00] -- Capture Start ...
** (wireshark:5905) 05:55:07.354353 [Capture M05SA00] -- Capture started
```

- The command `sudo nmap -sS 192.168.1.0/24` is used to perform a TCP SYN scan across all devices in the local network range from 192.168.1.1 to 192.168.1.254.
- The `sudo` prefix runs the command with administrative privileges, which is required because the scan needs access to raw network packets.

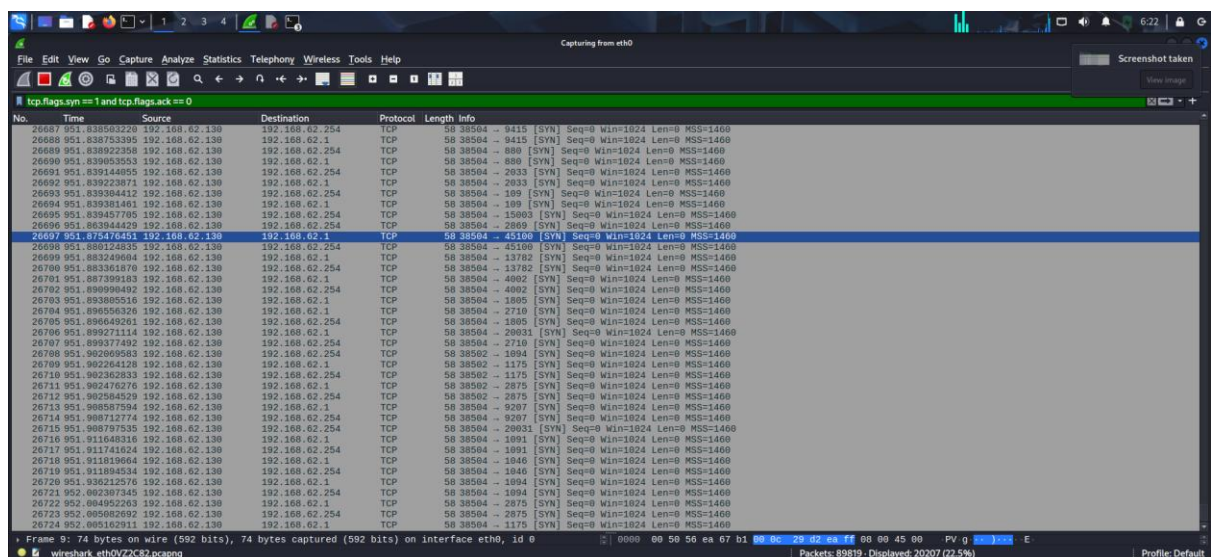
## 5. Analyze packet capture with Wireshark.

```
(kali㉿kali)-[~]
$ sudo wireshark &

[1] 5901

(kali㉿kali)-[~]
$ ** (wireshark:5905) 05:55:07.285228 [Capture MESSAGE] -- Capture Start ...
** (wireshark:5905) 05:55:07.354353 [Capture MESSAGE] -- Capture started
```

- Command used is “**sudo wireshark &**”.
- **sudo** is used to run Wireshark with root privileges, which is needed to capture packets.
- **&** runs it in the background so your terminal stays usable.







192.168.62.254 and 192.168.62.130, had no open ports; all 1000 scanned ports were either filtered or closed.

- This scan helps in identifying potentially exposed services in the network and sets the foundation for further analysis such as vulnerability detection or access control verification.

```
# Nmap 7.95 scan initiated Mon Jun 23 06:12:25 2025 as: /usr/lib/nmap/nmap -sS -oN /home/kali/scan.txt 192.168.62.0/24
Nmap scan report for 192.168.62.1
Host is up (0.0053s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
7070/tcp  open  realserver
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.62.2
Host is up (0.00021s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:EA:67:B1 (VMware)

Nmap scan report for 192.168.62.254
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.62.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:E9:83:F5 (VMware)

Nmap scan report for 192.168.62.130
Host is up (0.0000090s latency).
All 1000 scanned ports on 192.168.62.130 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

# Nmap done at Mon Jun 23 06:12:34 2025 -- 256 IP addresses (4 hosts up) scanned in 9.31 seconds
```