

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**

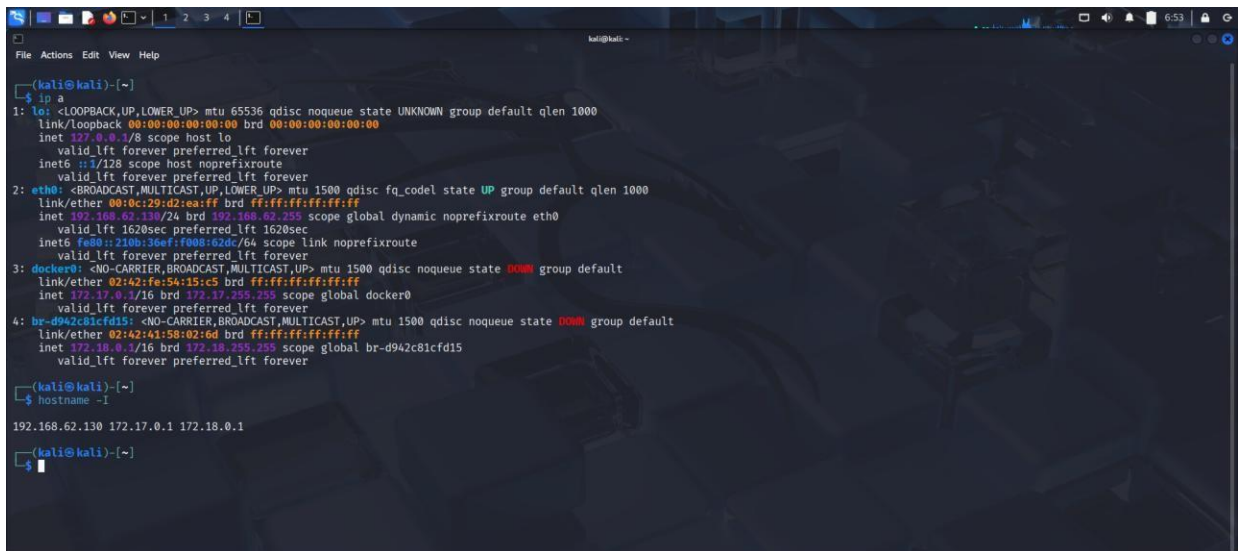
The `ip a` (or `ip addr`) command displays all network interfaces and their IP addresses.

- **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.



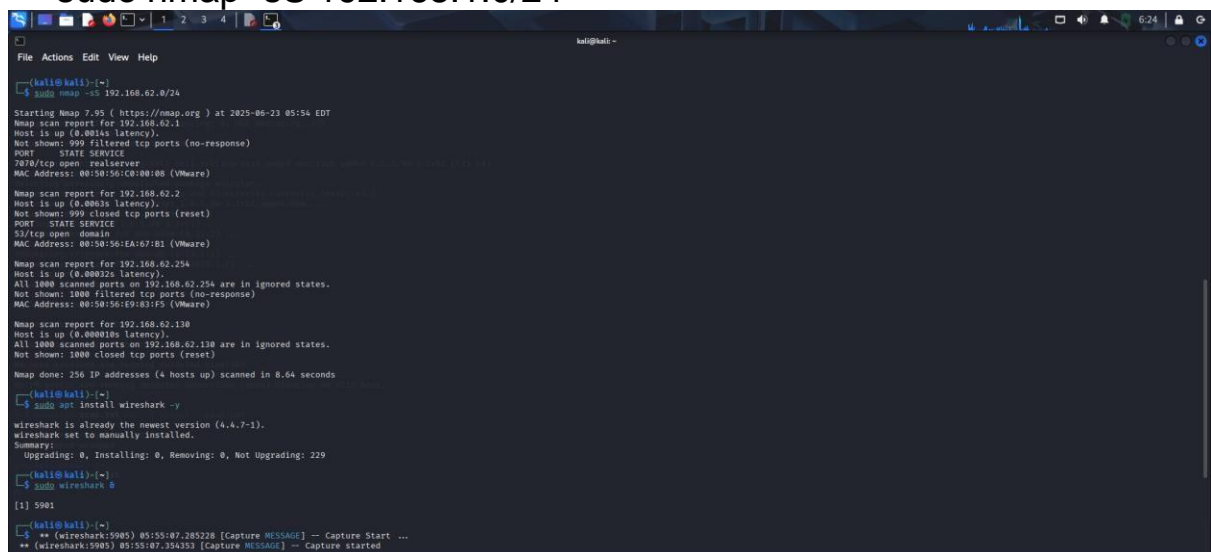
```
(kali@kali)~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        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:35ef:f008:62dc/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
    valid_lft forever preferred_lft forever
4: br-d942c81cfd15: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:41:58:02:6d 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 (0.0014s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
7070/tcp  open  realserver
MAC Address: 00:15:56:C8:00:08 (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
33/tcp    open  domain
MAC Address: 00:15:56:E4:67:B1 (VMware)

Nmap scan report for 192.168.62.254
Host is up (0.00032s latency).
All 1000 scanned ports on 192.168.62.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:15:56:E9:83:F5 (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 MESSAGE] -- Capture Start ...
** (wireshark:5905) 05:55:07.354353 [Capture MESSAGE] -- 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.

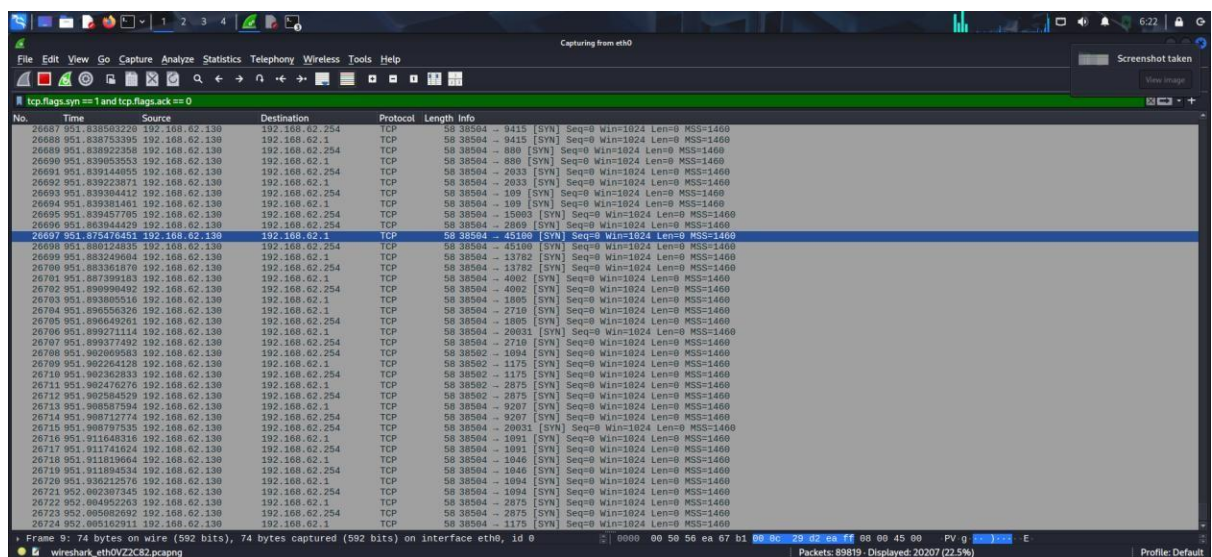
5. Analyze packet capture with Wireshark.

```
(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.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

6:23

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

No.	Time	Source	Destination	Protocol	Length	Info
89640	125.14424087	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 37835 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465330392 TSecr=0 WS=128
89652	125.14248624	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 37835 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465321174 TSecr=0 WS=128
89655	132.18735768	192.168.62.130	192.168.1.100	TCP	74	37205 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465273245 TSecr=0 WS=128
89686	132.18270656	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 37205 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465374254 TSecr=0 WS=128
89687	132.18071144	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 37205 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465374779 TSecr=0 WS=128
89688	132.18306538	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 37205 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465276302 TSecr=0 WS=128
89689	132.18541333	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 37205 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465376304 TSecr=0 WS=128
89691	132.19944973	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 37205 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465283866 TSecr=0 WS=128
89693	133.2592318	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 37205 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465284822 TSecr=0 WS=128
89693	134.1421951	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 37205 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465292214 TSecr=0 WS=128
89703	134.03353131	192.168.62.130	192.168.1.100	TCP	74	37205 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465335381 TSecr=0 WS=128
89730	1404.1153950	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 33287 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465344562 TSecr=0 WS=128
89737	1406.7398771	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 33287 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465350886 TSecr=0 WS=128
89739	1410.0634960	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 33287 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465345910 TSecr=0 WS=128
89739	1407.7872856	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 33287 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465357074 TSecr=0 WS=128
89742	1406.8115349	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 33287 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465358958 TSecr=0 WS=128
89743	1410.8270214	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 33287 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465366974 TSecr=0 WS=128
89744	1414.8590881	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 33287 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465365906 TSecr=0 WS=128
89747	1423.6348434	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 33287 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465373139 TSecr=0 WS=128
89742	1430.152558	192.168.62.130	192.168.1.100	TCP	74	35555 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465351410 TSecr=0 WS=128
89780	1487.1740253	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 43995 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465345562 TSecr=0 WS=128
89784	1488.1985573	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 43995 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465346526 TSecr=0 WS=128
89786	1490.2221739	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 43995 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465378758 TSecr=0 WS=128
89789	1490.2462798	192.168.62.130	192.168.1.100	TCP	74	TCP Retransmission(1) 43995 - 1515 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3465348374 TSecr=0 WS=128
89792	1491.2704459	192.168.62.130	192.168.1.100	TCP	74	TCP Ret

- A TCP SYN scan was performed on the local subnet 192.168.62.0/24 using the command `sudo nmap -sS -oN /home/kali/scan.txt 192.168.62.0/24`.
- The scan successfully detected 4 active hosts out of 256 IP addresses in the range and completed in 9.31 seconds.
- The system at IP 192.168.62.1 was found with port 7070/tcp open, running the realservice service, which may indicate streaming or proxy functionalities.
- Another host, 192.168.62.2, had port 53/tcp open, indicating it might be running a DNS service. Two additional hosts.

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
```