

OUTPUT

1. To identify the network configuration

—(Arun@kali)-[~/Desktop]

└─\$ ifconfig

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10<host>

loop txqueuelen 1000 (Local Loopback)

RX packets 88 bytes 6960 (6.7 KiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 88 bytes 6960 (6.7 KiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.1.35 netmask 255.255.255.0 broadcast 192.168.1.255

inet6 fe80::2763:c693:d46c:5a3a prefixlen 64 scopeid 0x20<link>

inet6 2406:8800:82:906d:fb18:201e:e70e:e724 prefixlen 64 scopeid 0x0<global>

ether 60:ff:9e:1d:4b:1a txqueuelen 1000 (Ethernet)

RX packets 5368 bytes 4651321 (4.4 MiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 3338 bytes 3087463 (2.9 MiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

—(Arun@kali)-[~/Desktop]

└─\$ 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: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
group default qlen 1000
```

```
link/ether 60:ff:9e:1d:4b:1a brd ff:ff:ff:ff:ff:ff
inet 192.168.1.35/24 brd 192.168.1.255 scope global dynamic noprefixroute wlan0
valid_lft 86346sec preferred_lft 86346sec
inet6 2406:8800:82:906d:fb18:201e:e70e:e724/64 scope global dynamic
noprefixroute
valid_lft 1468370sec preferred_lft 604370sec
inet6 fe80::2763:c693:d46c:5a3a/64 scope link noprefixroute
valid_lft forever preferred_lft forever
```

```
└──(Arun@kali)-[~/Desktop]
```

```
└─$ ip addr
```

```
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: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
group default qlen 1000
```

```
link/ether 60:ff:9e:1d:4b:1a brd ff:ff:ff:ff:ff:ff
inet 192.168.1.35/24 brd 192.168.1.255 scope global dynamic noprefixroute wlan0
valid_lft 86333sec preferred_lft 86333sec
```

```
inet6 2406:8800:82:906d:fb18:201e:e70e:e724/64 scope global dynamic
noprofixroute

valid_lft 1468358sec preferred_lft 604358sec

inet6 fe80::2763:c693:d46c:5a3a/64 scope link noprofixroute

valid_lft forever preferred_lft forever
```

2. To test your network connectivity

```
└─(Arun@kali)-[~/Desktop]
```

```
└─$ ping -4 google.com
```

PING google.com (142.250.205.142) 56(84) bytes of data.

64 bytes from pnmaaa-aw-in-f14.1e100.net (142.250.205.142): icmp_seq=1 ttl=114
time=105 ms

64 bytes from pnmaaa-aw-in-f14.1e100.net (142.250.205.142): icmp_seq=2 ttl=114
time=126 ms

64 bytes from pnmaaa-aw-in-f14.1e100.net (142.250.205.142): icmp_seq=3 ttl=114
time=44.7 ms

64 bytes from pnmaaa-aw-in-f14.1e100.net (142.250.205.142): icmp_seq=4 ttl=114
time=66.6 ms

64 bytes from pnmaaa-aw-in-f14.1e100.net (142.250.205.142): icmp_seq=5 ttl=114
time=88.8 ms

64 bytes from pnmaaa-aw-in-f14.1e100.net (142.250.205.142): icmp_seq=6 ttl=114 time=111
ms

64 bytes from pnmaaa-aw-in-f14.1e100.net (142.250.205.142): icmp_seq=7 ttl=114
time=84.9 ms

64 bytes from pnmaaa-aw-in-f14.1e100.net (142.250.205.142): icmp_seq=8 ttl=114
time=52.1 ms

64 bytes from pnmaaa-aw-in-f14.1e100.net (142.250.205.142): icmp_seq=9 ttl=114
time=74.1 ms

64 bytes from pnmaaa-aw-in-f14.1e100.net (142.250.205.142): icmp_seq=10 ttl=114
time=96.8 ms

64 bytes from pnmaaa-aw-in-f14.1e100.net (142.250.205.142): icmp_seq=11 ttl=114 time=79.0 ms

64 bytes from pnmaaa-aw-in-f14.1e100.net (142.250.205.142): icmp_seq=12 ttl=114 time=24.0 ms

64 bytes from pnmaaa-aw-in-f14.1e100.net (142.250.205.142): icmp_seq=13 ttl=114 time=61.7 ms

64 bytes from pnmaaa-aw-in-f14.1e100.net (142.250.205.142): icmp_seq=14 ttl=114 time=82.6 ms

64 bytes from pnmaaa-aw-in-f14.1e100.net (142.250.205.142): icmp_seq=15 ttl=114 time=21.1 ms

64 bytes from pnmaaa-aw-in-f14.1e100.net (142.250.205.142): icmp_seq=16 ttl=114 time=93.7 ms

64 bytes from pnmaaa-aw-in-f14.1e100.net (142.250.205.142): icmp_seq=17 ttl=114 time=46.6 ms

^C

--- google.com ping statistics ---

17 packets transmitted, 17 received, 0% packet loss, time 16032ms

rtt min/avg/max/mdev = 21.082/74.016/125.588/28.618 ms

└─(Arun@kali)-[~/Desktop]

└─\$ ping localhost

PING localhost (::1) 56 data bytes

64 bytes from localhost (::1): icmp_seq=1 ttl=64 time=0.036 ms

64 bytes from localhost (::1): icmp_seq=2 ttl=64 time=0.078 ms

64 bytes from localhost (::1): icmp_seq=3 ttl=64 time=0.070 ms

64 bytes from localhost (::1): icmp_seq=4 ttl=64 time=0.095 ms

64 bytes from localhost (::1): icmp_seq=5 ttl=64 time=0.078 ms

64 bytes from localhost (::1): icmp_seq=6 ttl=64 time=0.047 ms

64 bytes from localhost (::1): icmp_seq=7 ttl=64 time=0.082 ms

64 bytes from localhost (::1): icmp_seq=8 ttl=64 time=0.096 ms

64 bytes from localhost (::1): icmp_seq=9 ttl=64 time=0.073 ms

```

64 bytes from localhost (::1): icmp_seq=10 ttl=64 time=0.083 ms
64 bytes from localhost (::1): icmp_seq=11 ttl=64 time=0.097 ms
64 bytes from localhost (::1): icmp_seq=12 ttl=64 time=0.073 ms
64 bytes from localhost (::1): icmp_seq=13 ttl=64 time=0.058 ms
64 bytes from localhost (::1): icmp_seq=14 ttl=64 time=0.074 ms
64 bytes from localhost (::1): icmp_seq=15 ttl=64 time=0.033 ms
64 bytes from localhost (::1): icmp_seq=16 ttl=64 time=0.036 ms
64 bytes from localhost (::1): icmp_seq=17 ttl=64 time=0.076 ms
64 bytes from localhost (::1): icmp_seq=18 ttl=64 time=0.098 ms
64 bytes from localhost (::1): icmp_seq=19 ttl=64 time=0.076 ms

```

^C

--- localhost ping statistics ---

19 packets transmitted, 19 received, 0% packet loss, time 18418ms

rtt min/avg/max/mdev = 0.033/0.071/0.098/0.020 ms

3. To view active ports

—(Arun@kali)-[~/Desktop]

└─\$ netstat -a

Active Internet connections (servers and established)

| Proto | Recv-Q | Send-Q | Local Address | Foreign Address | State |
|-------|--------|--------|-------------------------|-------------------------|-------------|
| tcp | 0 | 0 | 192.168.1.35:48228 | 93.243.107.34.bc.:https | ESTABLISHED |
| tcp6 | 0 | 0 | 2406:8800:82:906d:50772 | sa-in-x54.1e100.n:https | ESTABLISHED |
| tcp6 | 0 | 0 | 2406:8800:82:906d:38808 | maa03s39-in-x04.1:https | ESTABLISHED |
| tcp6 | 0 | 0 | 2406:8800:82:906d:54762 | maa05s12-in-x0a.1:https | ESTABLISHED |
| tcp6 | 0 | 0 | 2406:8800:82:906d:56818 | pnmaaa-an-in-x03.1:http | ESTABLISHED |
| tcp6 | 0 | 0 | 2406:8800:82:906d:40868 | lcmaaa-au-in-x05.:https | ESTABLISHED |
| tcp6 | 0 | 0 | 2406:8800:82:906d:40628 | lcmaaa-au-in-x03.:https | ESTABLISHED |
| tcp6 | 0 | 0 | 2406:8800:82:906d:55768 | pnmaaa-an-in-x03.1:http | ESTABLISHED |
| tcp6 | 0 | 0 | 2406:8800:82:906d:40292 | maa03s43-in-x0e.1:https | ESTABLISHED |

| | | | | | |
|------|---|---|--------------------------|-------------------------|-------------|
| tcp6 | 0 | 0 | 2406:8800:82:906d:34850 | maa03s41-in-x03.1:https | TIME_WAIT |
| udp | 0 | 0 | 192.168.1.35:bootpc | 192.168.1.1:bootps | ESTABLISHED |
| udp6 | 0 | 0 | :::40492 | :::* | |
| udp6 | 0 | 0 | :::49252 | :::* | |
| udp6 | 0 | 0 | fe80::276:dhcprv6-client | :::* | |
| udp6 | 0 | 0 | :::41611 | :::* | |
| raw6 | 0 | 0 | :::ipv6-icmp | :::* | 7 |

Active UNIX domain sockets (servers and established)

| Proto | RefCnt | Flags | Type | State | I-Node | Path |
|-------|--------|---------|--------|-----------|--------|--------------------------------------|
| unix | 3 | [] | STREAM | CONNECTED | | 2708 /run/dbus/system_bus_socket |
| unix | 3 | [] | STREAM | CONNECTED | | 2632 |
| unix | 2 | [ACC] | STREAM | LISTENING | 11665 | /tmp/.ICE-unix/1083 |
| unix | 3 | [] | DGRAM | CONNECTED | | 12607 |
| unix | 3 | [] | STREAM | CONNECTED | | 10957 |
| unix | 3 | [] | STREAM | CONNECTED | | 2707 /run/dbus/system_bus_socket |
| unix | 3 | [] | STREAM | CONNECTED | | 319 |
| unix | 3 | [] | DGRAM | CONNECTED | | 7571 |
| unix | 3 | [] | STREAM | CONNECTED | | 11617 /run/systemd/journal/stdout |
| unix | 2 | [ACC] | STREAM | LISTENING | 750 | /tmp/ssh-skiEi4olHZVm/agent.1180 |
| unix | 3 | [] | DGRAM | CONNECTED | | 12606 |
| unix | 3 | [] | STREAM | CONNECTED | | 2602 /run/user/1000/bus |
| unix | 2 | [ACC] | STREAM | LISTENING | 15878 | /run/user/1000/gcr/ssh |
| unix | 3 | [] | STREAM | CONNECTED | | 20673 |
| unix | 3 | [] | STREAM | CONNECTED | | 3978 /run/user/1000/bus |
| unix | 3 | [] | STREAM | CONNECTED | | 10805 |

| | | | | | |
|--|---------|-----------|-----------|-------|--------------------|
| unix 3 | [] | STREAM | CONNECTED | 847 | /run/user/1000/at- |
| spi/bus_0 | | | | | |
| unix 3 | [] | STREAM | CONNECTED | 6883 | |
| unix 3 | [] | STREAM | CONNECTED | 16040 | |
| unix 2 | [ACC] | STREAM | LISTENING | 15880 | |
| /run/user/1000/keyring/control | | | | | |
| unix 2 | [ACC] | STREAM | LISTENING | 15881 | |
| /run/user/1000/gnupg/S.gpg-agent.browser | | | | | |
| unix 3 | [] | SEQPACKET | CONNECTED | 25163 | |
| unix 3 | [] | STREAM | CONNECTED | 10808 | |
| unix 3 | [] | STREAM | CONNECTED | 9663 | @/tmp/.X11-unix/X0 |
| unix 3 | [] | STREAM | CONNECTED | 748 | /run/user/1000/bus |
| unix 3 | [] | STREAM | CONNECTED | 13776 | |
| unix 3 | [] | STREAM | CONNECTED | 665 | |
| unix 3 | [] | STREAM | CONNECTED | 12847 | /run/user/1000/bus |
| unix 3 | [] | STREAM | CONNECTED | 13807 | |
| unix 2 | [ACC] | STREAM | LISTENING | 739 | /run/user/1000/at- |
| spi/bus_0 | | | | | |
| unix 3 | [] | STREAM | CONNECTED | 12675 | |
| /run/systemd/journal/stdout | | | | | |
| unix 3 | [] | STREAM | CONNECTED | 12555 | |
| unix 3 | [] | STREAM | CONNECTED | 10906 | |
| unix 3 | [] | STREAM | CONNECTED | 16039 | |
| unix 3 | [] | STREAM | CONNECTED | 10917 | |
| unix 3 | [] | DGRAM | CONNECTED | 7575 | |
| unix 3 | [] | STREAM | CONNECTED | 6955 | |
| unix 3 | [] | STREAM | CONNECTED | 11671 | @/tmp/.X11-unix/X0 |
| unix 3 | [] | STREAM | CONNECTED | 822 | |
| /run/systemd/journal/stdout | | | | | |
| unix 3 | [] | STREAM | CONNECTED | 12709 | |
| unix 3 | [] | STREAM | CONNECTED | 24691 | |

```
unix 3      [ ]    STREAM  CONNECTED      2717  /run/user/1000/bus
unix 3      [ ]    STREAM  CONNECTED      741
```

```
└─(Arun@kali)-[~/Desktop]
```

```
└─$ netstat -at
```

Active Internet connections (servers and established)

| Proto | Recv-Q | Send-Q | Local Address | Foreign Address | State |
|-------|--------|--------|-------------------------|-------------------------|-------------|
| tcp | 0 | 0 | 192.168.1.35:48228 | 93.243.107.34.bc.:https | ESTABLISHED |
| tcp6 | 0 | 0 | 2406:8800:82:906d:49224 | pnmaaa-as-in-x03.:https | ESTABLISHED |
| tcp6 | 0 | 0 | 2406:8800:82:906d:55526 | maa05s20-in-x0a.1:https | ESTABLISHED |
| tcp6 | 0 | 0 | 2406:8800:82:906d:38898 | maa05s05-in-x03.1:https | TIME_WAIT |
| tcp6 | 0 | 0 | 2406:8800:82:906d:37824 | pnmaaa-aq-in-x0e.:https | ESTABLISHED |

```
└─(Arun@kali)-[~/Desktop]
```

```
└─$ netstat -au
```

Active Internet connections (servers and established)

| Proto | Recv-Q | Send-Q | Local Address | Foreign Address | State |
|-------|--------|--------|--------------------------|--------------------|-------------|
| udp | 0 | 0 | 192.168.1.35:bootpc | 192.168.1.1:bootps | ESTABLISHED |
| udp6 | 0 | 0 | :::40492 | :::* | |
| udp6 | 0 | 0 | :::49252 | :::* | |
| udp6 | 0 | 0 | fe80::276:dhcpcv6-client | :::* | |
| udp6 | 0 | 0 | :::50027 | :::* | |

```
└─(Arun@kali)-[~/Desktop]
```

```
└─$ netstat -l
```

Active Internet connections (only servers)

| Proto | Recv-Q | Send-Q | Local Address | Foreign Address | State |
|-------|--------|--------|---------------|-----------------|-------|
| udp6 | 0 | 0 | :::48209 | :::* | |
| udp6 | 0 | 0 | :::40492 | :::* | |


```

udp6  0      0 [::]:49252      [::]:*
udp6  0      0 fe80::276:dhcpgv6-client [::]:*
raw6   0      0 [::]:ipv6-icmp  [::]:*      7

```

Active UNIX domain sockets (only servers)

| Proto | RefCnt | Flags | Type | State | I-Node | Path |
|-------|--------|---------|-----------|-----------|--------|--|
| unix | 2 | [ACC] | STREAM | LISTENING | 485 | /tmp/.X11-unix/X0 |
| unix | 2 | [ACC] | STREAM | LISTENING | 11665 | /tmp/.ICE-unix/1083 |
| unix | 2 | [ACC] | STREAM | LISTENING | 750 | /tmp/ssh-skiEi4olHZVm/agent.1180 |
| unix | 2 | [ACC] | STREAM | LISTENING | 7576 | /run/systemd/private |
| unix | 2 | [ACC] | STREAM | LISTENING | 7577 | /run/systemd/userdb/io.systemd.DynamicUser |
| unix | 2 | [ACC] | STREAM | LISTENING | 7578 | /run/systemd/io.systemd.ManagedOOM |
| unix | 2 | [ACC] | STREAM | LISTENING | 7592 | /run/systemd/io.systemd.Credentials |
| unix | 2 | [ACC] | STREAM | LISTENING | 7595 | /run/systemd/journal/stdout |
| unix | 2 | [ACC] | SEQPACKET | LISTENING | 7596 | /run/udev/control |
| unix | 2 | [ACC] | STREAM | LISTENING | 10746 | /run/user/1000/systemd/private |
| unix | 2 | [ACC] | STREAM | LISTENING | 10757 | /run/user/1000/bus |
| unix | 2 | [ACC] | STREAM | LISTENING | 15877 | /run/user/1000/gnupg/S.dirmngr |
| unix | 2 | [ACC] | STREAM | LISTENING | 15878 | /run/user/1000/gcr/ssh |
| unix | 2 | [ACC] | STREAM | LISTENING | 15880 | /run/user/1000/keyring/control |
| unix | 2 | [ACC] | STREAM | LISTENING | 15881 | /run/user/1000/gnupg/S.gpg-agent.browser |
| unix | 2 | [ACC] | STREAM | LISTENING | 15882 | /run/user/1000/gnupg/S.gpg-agent.extra |

```
└─(Arun@kali)-[~/Desktop]
```

```
└─$ netstat -lt
```

Active Internet connections (only servers)

| Proto | Recv-Q | Send-Q | Local Address | Foreign Address | State |
|-------|--------|--------|---------------|-----------------|-------|
|-------|--------|--------|---------------|-----------------|-------|

```
└─(Arun@kali)-[~/Desktop]
```

```
└─$ netstat -lu
```

Active Internet connections (only servers)

| Proto | Recv-Q | Send-Q | Local Address | Foreign Address | State |
|-------|--------|--------|---------------|-----------------|-------|
|-------|--------|--------|---------------|-----------------|-------|

| | | | | | |
|------|---|---|----------|------|--|
| udp6 | 0 | 0 | :::40492 | :::* | |
|------|---|---|----------|------|--|

| | | | | | |
|------|---|---|----------|------|--|
| udp6 | 0 | 0 | :::49252 | :::* | |
|------|---|---|----------|------|--|

| | | | | | |
|------|---|---|--------------------------|------|--|
| udp6 | 0 | 0 | fe80::276:dhcprv6-client | :::* | |
|------|---|---|--------------------------|------|--|

| | | | | | |
|------|---|---|----------|------|--|
| udp6 | 0 | 0 | :::50027 | :::* | |
|------|---|---|----------|------|--|

4. To find hardware/MAC address

```
└─(Arun@kali)-[~/Desktop]
```

```
└─$ arp
```

| Address | HWtype | HWaddress | Flags | Mask | Iface |
|-------------|--------|-------------------|-------|------|-------|
| 192.168.1.1 | ether | 20:0c:86:56:49:20 | C | | wlan0 |

5. View network configuration file

```
└─(Arun@kali)-[~/Desktop]
```

```
└─$ ls -a
```

```
. .. a chrome network 'New Folder' 'penetration testing' unnamed.jpg
```