

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

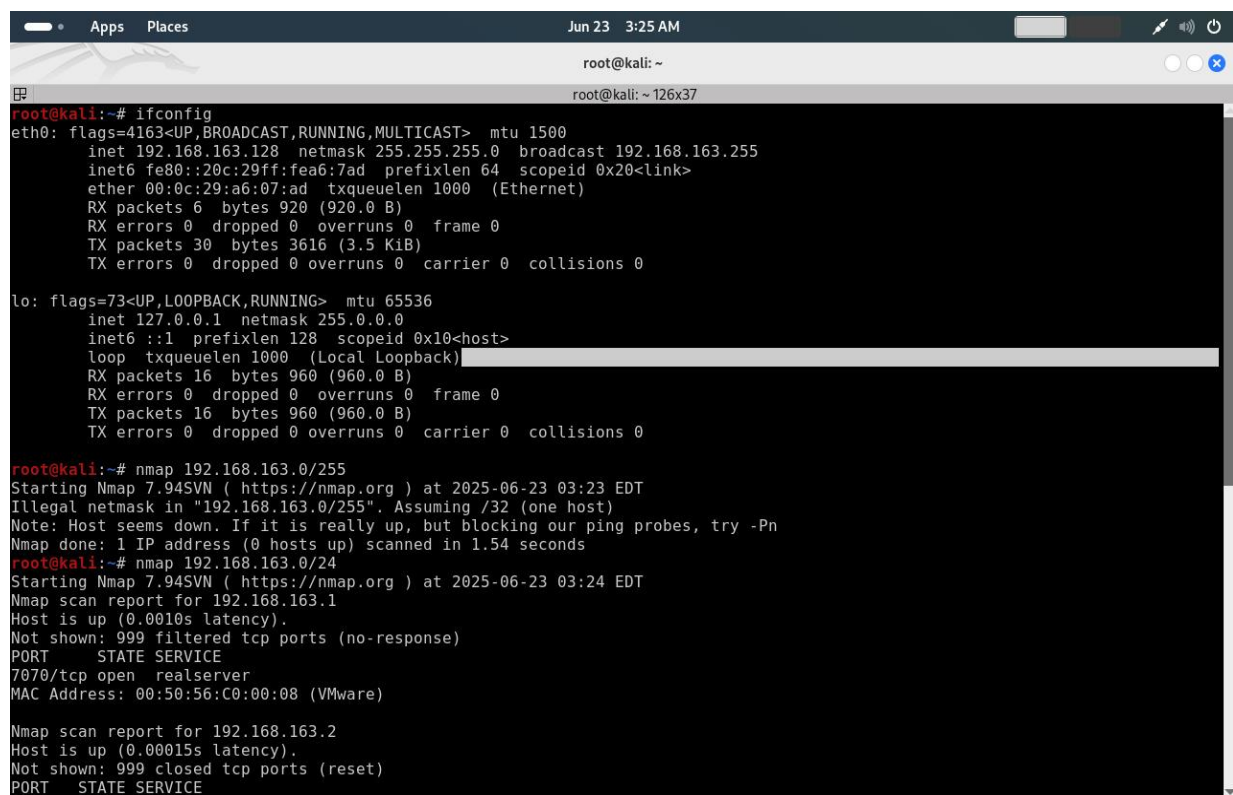
**Objective:** Learn to discover open ports on devices in your local network to understand network exposure.

**Required Tools:** Nmap, Wireshark

**Outcome:** Basic network reconnaissance skills; understanding network service exposure

For scanning the nmap before we need to know the ip address of the machine, for that we use the command to find the ipaddress of the machine is

Command: **ifconfig**



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.163.128 netmask 255.255.255.0 broadcast 192.168.163.255
    inet6 fe80::20c:29ff:fea6:7ad prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:a6:07:ad txqueuelen 1000 (Ethernet)
    RX packets 6 bytes 920 (920.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 30 bytes 3616 (3.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 16 bytes 960 (960.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 960 (960.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# nmap 192.168.163.0/255
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-23 03:23 EDT
Illegal netmask in "192.168.163.0/255". Assuming /32 (one host)
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.54 seconds
root@kali:~# nmap 192.168.163.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-23 03:24 EDT
Nmap scan report for 192.168.163.1
Host is up (0.0010s 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 192.168.163.2
Host is up (0.00015s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
```

Ipaddress is :192.168.163.128

After that we have to start scanning with founded ip address using the command

Command: **nmap**

For scanning the network here is the syntax:

**nmap <ip address> → nmap 192.168.163.0/24**

or

**nmap -sn 192.168.163.0/24**

```
root@kali: ~  
root@kali: ~ 126x37  
root@kali:~# nmap 192.168.163.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-23 03:24 EDT  
Nmap scan report for 192.168.163.1  
Host is up (0.0010s 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 192.168.163.2  
Host is up (0.00015s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
53/tcp open  domain  
MAC Address: 00:50:56:E8:19:FE (VMware)  
  
Nmap scan report for 192.168.163.254  
Host is up (0.00046s latency).  
All 1000 scanned ports on 192.168.163.254 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 00:50:56:EE:BA:7C (VMware)  
  
Nmap scan report for 192.168.163.128  
Host is up (0.000010s latency).  
All 1000 scanned ports on 192.168.163.128 are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
  
Nmap done: 256 IP addresses (4 hosts up) scanned in 8.92 seconds  
root@kali:~# nmap -sn 192.168.163.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-23 03:25 EDT  
Nmap scan report for 192.168.163.1  
Host is up (0.00034s latency).  
MAC Address: 00:50:56:C0:00:08 (VMware)  
Nmap scan report for 192.168.163.2  
Host is up (0.00035s latency).  
MAC Address: 00:50:56:E8:19:FE (VMware)  
Nmap scan report for 192.168.163.254
```

After that we can see the open port what are open in that network.

After completing that we have to start scanning the tcp scan .

In this tcp scanning they are two : 1.TCP CONNECTION SCAN

2.TCP SYN SCAN

For TCP CONNECTION SCAN we use the syntax:

```
nmap -sC 192.168.163.0/24
```

```
root@kali: ~  
root@kali: ~ 126x37  
Nmap done: 256 IP addresses (4 hosts up) scanned in 14.03 seconds  
root@kali:~# nmap -sC 192.168.163.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-23 03:28 EDT  
Nmap scan report for 192.168.163.1  
Host is up (0.00052s latency).  
Not shown: 999 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
7070/tcp open  realserver  
|_ ssl-date: TLS randomness does not represent time  
|_ ssl-cert: Subject: commonName=AnyDesk Client  
|_ Not valid before: 2023-11-28T12:58:43  
|_ Not valid after: 2073-11-15T12:58:43  
MAC Address: 00:50:56:C0:00:08 (VMware)  
  
Nmap scan report for 192.168.163.2  
Host is up (0.00032s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
53/tcp open  domain  
|_ dns-nsid:  
|_ bind.version: dnsmasq-2.51  
MAC Address: 00:50:56:E8:19:FE (VMware)  
  
Nmap scan report for 192.168.163.254  
Host is up (0.00032s latency).  
All 1000 scanned ports on 192.168.163.254 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 00:50:56:EE:BA:7C (VMware)  
  
Nmap scan report for 192.168.163.128  
Host is up (0.000080s latency).  
All 1000 scanned ports on 192.168.163.128 are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
  
Nmap done: 256 IP addresses (4 hosts up) scanned in 23.07 seconds  
root@kali:~# nmap -sC 192.168.163.0/24
```

For TCP SYN SCAN we use the syntax:

```
nmap -sS 192.168.163.0/24
```

```
root@kali: ~  
root@kali: ~ 126x37  
Host is up (0.00035s latency).  
MAC Address: 00:50:56:E8:19:FE (VMware)  
Nmap scan report for 192.168.163.254  
Host is up (0.00025s latency).  
MAC Address: 00:50:56:EE:BA:7C (VMware)  
Nmap scan report for 192.168.163.128  
Host is up.  
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.10 seconds  
root@kali:~# nmap -sS 192.168.163.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-23 03:27 EDT  
Nmap scan report for 192.168.163.1  
Host is up (0.00040s 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 192.168.163.2  
Host is up (0.00032s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
53/tcp    open  domain  
MAC Address: 00:50:56:E8:19:FE (VMware)  
  
Nmap scan report for 192.168.163.254  
Host is up (0.00031s latency).  
All 1000 scanned ports on 192.168.163.254 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 00:50:56:EE:BA:7C (VMware)  
  
Nmap scan report for 192.168.163.128  
Host is up (0.000010s latency).  
All 1000 scanned ports on 192.168.163.128 are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
  
Nmap done: 256 IP addresses (4 hosts up) scanned in 10.62 seconds  
root@kali:~#
```

In another way also we can find the open port that is using the tool wireshark

apt-install wireshark

