Elevate_Labs_Task1

Rudra Srilakshmi

Task 1: Scan Your Local Network for Open Ports

Tools & Technologies :

Nmap: Open-source network scanning tool

Operating Systems: Ubuntu (Linux Terminal), Kali Linux

Wireshark for packet analysis(here, i used only for kali)

Method 1: Ubuntu (Linux Terminal)

Step 1: Install Nmap

I used these commands to install:

- sudo apt update
- sudo apt install nmap

```
rudra99@DESKTOP-L2T7O1I:~$ sudo apt install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  htop libestr0 libfastjson4
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  liblinear4 lua-lpeg nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat ndiff zenmap
The following NEW packages will be installed:
  liblinear4 lua-lpeg nmap nmap-common
0 upgraded, 4 newly installed, 0 to remove and 128 not upgraded.
Need to get 5744 kB of archives.
After this operation, 25.6 MB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 liblinear4 amd64 2.3.0+dfsg-5 [41.4 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy/universe amd64 lua-lpeg amd64 1.0.2-1 [31.4 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 nmap-common all 7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1 [3940 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 nmap amd64 7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1 [1731 kB]
Fetched 5744 kB in 7s (767 kB/s)
Selecting previously unselected package liblinear4:amd64.
(Reading database ... 160287 files and directories currently installed.)
Preparing to unpack .../liblinear4_2.3.0+dfsg-5_amd64.deb ...
Unpacking liblinear4:amd64 (2.3.0+dfsg-5) ...
Selecting previously unselected package lua-lpeg:amd64.
Preparing to unpack .../lua-lpeg_1.0.2-1_amd64.deb ...
Unpacking lua-lpeg:amd64 (1.0.2-1) ...
Selecting previously unselected package nmap-common.
Preparing to unpack .../nmap-common_7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1_all.deb ...
Unpacking nmap-common (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
Selecting previously unselected package nmap.
Preparing to unpack .../nmap_7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1_amd64.deb ...
Unpacking nmap (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
Setting up lua-lpeg:amd64 (1.0.2-1) ...
Setting up liblinear4:amd64 (2.3.0+dfsg-5) ...
Setting up nmap-common (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1) ...
```

Step 2: Finding local IP range

I used the command – “ip a” and It shows the Network Info as

- Scanned Range: 172.21.96.0/20

- Local Machine IP: 172.21.108.213

```
rudra99@DESKTOP-L2T7O1I:~$ 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
    inet 10.255.255.254/32 brd 10.255.255.254 scope global lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1492 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:c8:95:07 brd ff:ff:ff:ff:ff:ff
    inet 172.21.108.213/20 brd 172.21.111.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fec8:9507/64 scope link
       valid_lft forever preferred_lft forever
```

Step 3: To perform TCP-SYN-scan and saving results as a text file

I used this command – "sudo nmap -sS 172.21.96.0/20 -oN TCP-SYN-scan-results.txt"

```
rudra99@DESKTOP-L2T7O1I:~$ nmap -sS 172.21.96.0/20
You requested a scan type which requires root privileges.
QUITTING!
rudra99@DESKTOP-L2T7O1I:~$ sudo nmap -sS 172.21.96.0/20
Starting Nmap 7.80 ( https://nmap.org ) at 2025-06-23 12:53 IST
Nmap scan report for DESKTOP-L2T7O1I.mshome.net (172.21.96.1)
Host is up (0.00068s latency).
All 1000 scanned ports on DESKTOP-L2T7O1I.mshome.net (172.21.96.1) are filtered
MAC Address: 00:15:5D:C8:95:1E (Microsoft)

Nmap scan report for 172.21.108.213
Host is up (0.0000020s latency).
All 1000 scanned ports on 172.21.108.213 are closed

Nmap done: 4096 IP addresses (2 hosts up) scanned in 33.01 seconds
```

Here, in this we can see that all ports are filtered, it means the host is reachable, but a firewall is blocking all port responses. so, I tried with kali, the same scan to see any open ports.

Step 6: Research Common Services

In this scan, no open ports were found on the active devices. One host (172.21.96.1) had all ports filtered, which likely means a firewall is blocking scan attempts. The other host (172.21.108.213) had all ports closed, meaning no services are currently listening.

Step 7: Identify Potential Security Risks

Since no ports were open, there were no immediate exposed services found on the scanned hosts. The filtered status on one device is a good sign of firewall protection, and closed ports indicate that the device isn't running unnecessary services. Overall, the network appears to be secure with minimal exposure.

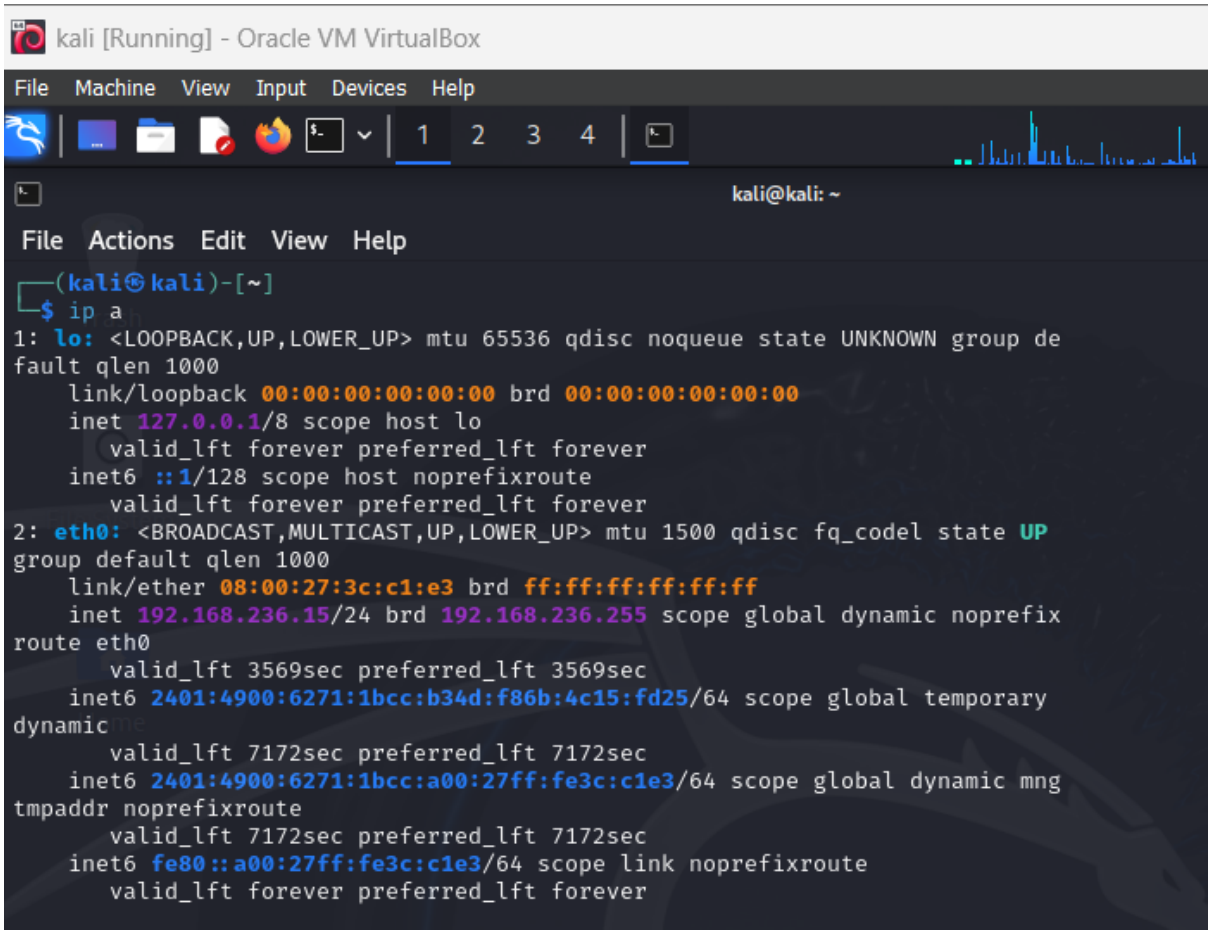
Method 2: kali version

Step 1 and 2: Install Nmap and finding ip

I followed the step 1 and step2 same to find the local ip range using "ip a" command

The Network Info

- Scanned Range: 192.168.236.0/24
- Local IP: 192.168.236.15 the result is as follows for this kali version:



Step 3:To perform TCP-SYN-scan and saving results as a text file(kali)

Verification: for this, i used cat kali-scan-results.txt command to verify the text file content

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.236.0/24 -oN kali-scan-results.txt
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-23 19:41 IST
Nmap scan report for 192.168.236.138
Host is up (0.0053s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 82:82:59:B1:44:AD (Unknown)

Nmap scan report for 192.168.236.223
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.236.223 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 4C:D5:77:5B:EF:FD (Chongqing Fugui Electronics)

Nmap scan report for 192.168.236.15
Host is up (0.0000080s latency).
All 1000 scanned ports on 192.168.236.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 16.94 seconds

┌──(kali㉿kali)-[~]
└─$
```

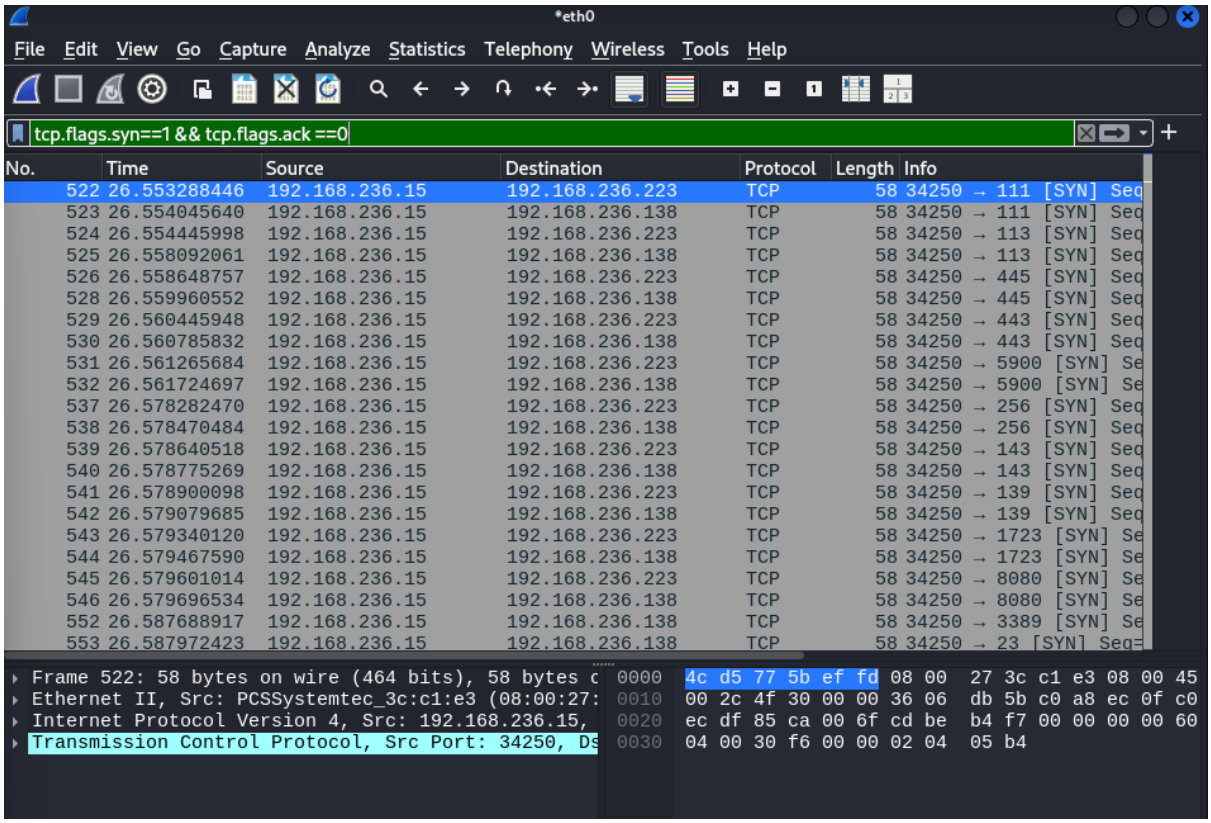
```
┌──(kali㉿kali)-[~]
└─$ cat kali-scan-results.txt
# Nmap 7.94SVN scan initiated Mon Jun 23 19:41:13 2025 as: /usr/lib/nmap/nmap -sS -oN kali-scan-results.txt 192.168.
236.0/24
Nmap scan report for 192.168.236.138
Host is up (0.0053s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 82:82:59:B1:44:AD (Unknown)

Nmap scan report for 192.168.236.223
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.236.223 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 4C:D5:77:5B:EF:FD (Chongqing Fugui Electronics)

Nmap scan report for 192.168.236.15
Host is up (0.0000080s latency).
All 1000 scanned ports on 192.168.236.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

# Nmap done at Mon Jun 23 19:41:30 2025 -- 256 IP addresses (3 hosts up) scanned in 16.94 seconds

┌──(kali㉿kali)-[~]
└─$
```

Step 4: Note IP Addresses and Open Ports

After running the scan, I reviewed the results from step 3 figure, to identify which IP addresses were active and whether any ports were open. Out of the scanned range, three devices were found to be active. Among them, only one device had an open port (53/tcp), while the others had all ports either closed or filtered. This helps in understanding which devices are visible on the network and what services they might be exposing.

Step 5: Wireshark analysis(kali)

Here, in kali, followed same procedure as ubuntu till the third step then, open Wireshark and started packet capturing while running nmap command in the terminal and filtered the TCP SYN responses in real time using filter "tcp.flags.syn==1 && tcp.flags.ack==0" and saved the pcap file.



Step 6: Research Common Services

The scan found only one open port: 53/tcp, which is used for DNS (Domain Name System). This service is usually found on routers or servers to resolve domain names. In this case, it was found on 192.168.236.138, which may be a router or a device running DNS. If it's not meant to run DNS, this could be a misconfiguration.

Step 7: Identify Potential Security Risks

An open DNS port on a normal device can be risky if not needed — it may allow misuse like DNS tunneling. The other devices had all ports closed or filtered, which is good because it means no unnecessary services are exposed and firewalls may be protecting them.