

# Elevate Labs (Cyber-Security Internship):

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

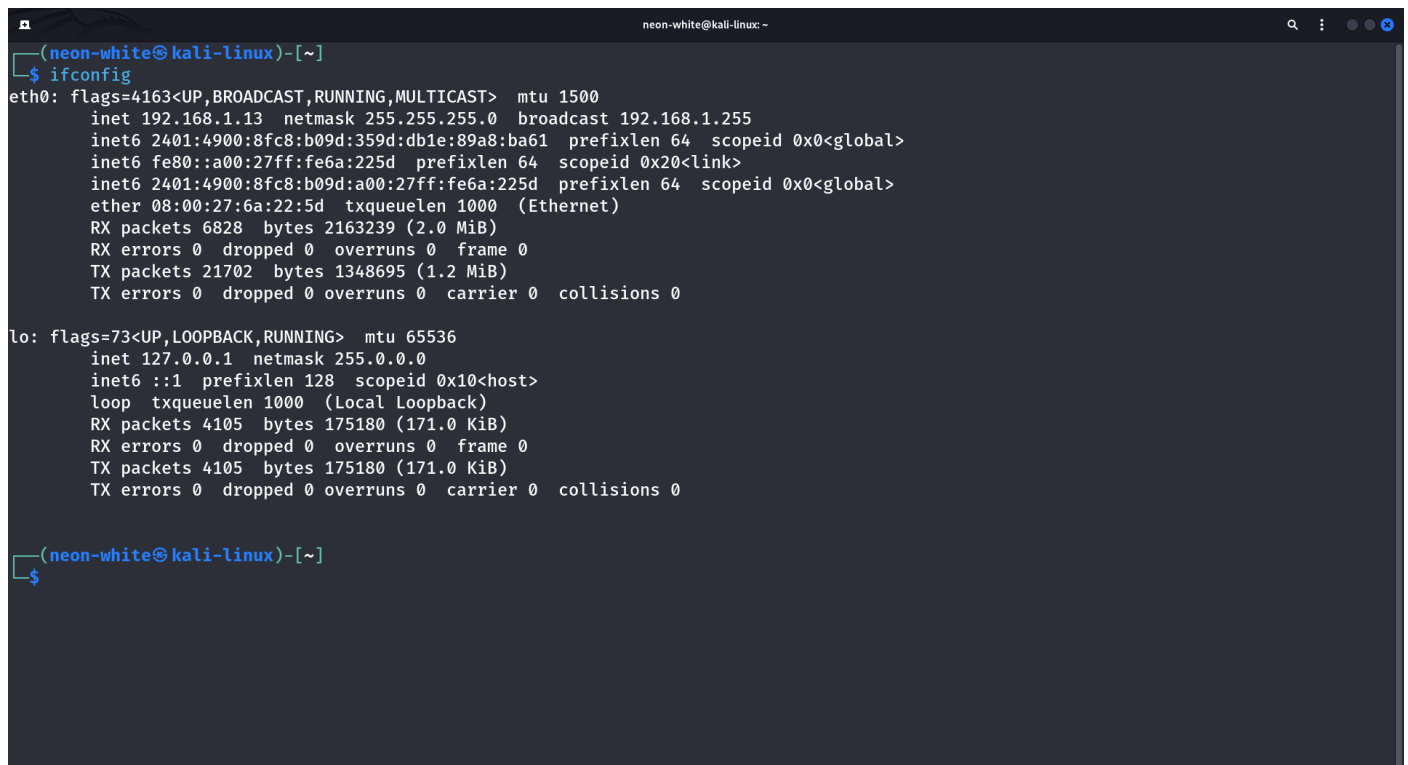
**Objective:** Learn to discover OPEN ports on devices in your Local Network to understand Network Exposure.

**Tools:** NMAP (Network-Map), Wire-Shark & Kali-Linux

**Outcome:**

### Step One: First, Check your Local IP-Address

**Command:** ifconfig

A screenshot of a terminal window titled 'neon-white@kali-linux -'. The prompt is '(neon-white@kali-linux)-[~]'. The user has entered the command '\$ ifconfig'. The output shows details for two network interfaces: 'eth0' and 'lo'. For 'eth0', it lists flags, MTU, IP address (192.168.1.13), netmask (255.255.255.0), broadcast address (192.168.1.255), MAC address (08:00:27:6a:22:5d), and various statistics. For 'lo', it lists flags, MTU, IP address (127.0.0.1), netmask (255.0.0.0), and statistics. The prompt returns to '(neon-white@kali-linux)-[~] \$'.

**Result:** Local IP-Address: 192.168.1.13 & Local IP-Range: 192.168.1.0

## Step Two: Now, we will Discover various HOST, connected in Local-Network

**Command:** netdiscover -r 192.168.1.0/24

**Result:**

```
neon-white@kali-linux: -
Currently scanning: Finished! | Screen View: Unique Hosts

6 Captured ARP Req/Rep packets, from 4 hosts. Total size: 360

-----
IP            At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.1.1    26:8e:8a:3d:8f:91    3      180  Nokia Solutions and Networks GmbH & Co. KG
192.168.1.7    a8:57:99:4a:3a:62    1       60  Cloud Network Technology (Samoa) Limited
192.168.1.4    86:3a:3f:7a:4b:83    1       60  GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP.,LTD
192.168.1.3    58:3c:4a:85:3a:9a    1       60  GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP.,LTD
```

## Step Three: Now, we will Check whether the HOST are LIVE or NOT

**Command:** ping -4 192.168.1.4

**Result:**

```
neon-white@kali-linux: -
Currently scanning: Finished! | Screen View: Unique Hosts

6 Captured ARP Req/Rep packets, from 4 hosts. Total size: 360

-----
IP            At MAC Address      Count  Len  MAC Vendor / Hostname
-----
192.168.1.1    26:8e:8a:3d:8f:91    3      180  Nokia Solutions and Networks GmbH & Co. KG
192.168.1.7    a8:57:99:4a:3a:62    1       60  Cloud Network Technology (Samoa) Limited
192.168.1.4    86:3a:3f:7a:4b:83    1       60  GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP.,LTD
192.168.1.3    58:3c:4a:85:3a:9a    1       60  GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP.,LTD

(neon-white@kali-linux)-[~]
$ ping -4 192.168.1.4
PING 192.168.1.4 (192.168.1.4) 56(84) bytes of data.
64 bytes from 192.168.1.4: icmp_seq=5 ttl=64 time=165 ms
64 bytes from 192.168.1.4: icmp_seq=6 ttl=64 time=87.5 ms
64 bytes from 192.168.1.4: icmp_seq=7 ttl=64 time=5.08 ms
64 bytes from 192.168.1.4: icmp_seq=8 ttl=64 time=5.63 ms
64 bytes from 192.168.1.4: icmp_seq=9 ttl=64 time=48.5 ms
^C
--- 192.168.1.4 ping statistics ---
9 packets transmitted, 5 received, 44.4444% packet loss, time 8103ms
rtt min/avg/max/mdev = 5.084/62.417/165.329/59.879 ms

(neon-white@kali-linux)-[~]
$
```

#### Step Four: Now, we will Perform SYN Scan, & Discover OPEN Ports

**Command:** nmap -v -sS 192.168.1.0/24

#### **Result:**

Starting Nmap 7.95 ( <https://nmap.org> ) at 2025-08-04 13:08 IST

Initiating ARP Ping Scan at 13:08

Scanning 255 hosts [1 port/host]

Completed ARP Ping Scan at 13:08, 1.94s elapsed (255 total hosts)

Initiating Parallel DNS resolution of 3 hosts. at 13:08

Completed Parallel DNS resolution of 3 hosts. at 13:08, 0.08s elapsed

Initiating Parallel DNS resolution of 1 host. at 13:08

Completed Parallel DNS resolution of 1 host. at 13:08, 0.06s elapsed

Initiating SYN Stealth Scan at 13:08

Scanning 3 hosts [1000 ports/host]

Discovered open port 443/tcp on 192.168.1.1

Completed SYN Stealth Scan against 192.168.1.3 in 3.33s (2 hosts left)

Increasing send delay for 192.168.1.1 from 0 to 5 due to max\_successful\_ryno increase to 4

Discovered open port 5357/tcp on 192.168.1.7

Completed SYN Stealth Scan against 192.168.1.7 in 34.62s (1 host left)

Increasing send delay for 192.168.1.1 from 5 to 10 due to max\_successful\_ryno increase to 5

Completed SYN Stealth Scan at 13:09, 71.74s elapsed (3000 total ports)

Nmap scan report for Unit (192.168.1.1)

Host is up (0.0037s latency).

Not shown: 983 filtered tcp ports (no-response), 2 filtered tcp ports (port-unreach)

PORT	STATE	SERVICE
------	-------	---------

22/tcp	closed	ssh
--------	--------	-----

443/tcp	open	https
---------	------	-------

445/tcp	closed	microsoft-ds
---------	--------	--------------

631/tcp	closed	ipp
---------	--------	-----

8099/tcp	closed	unknown
----------	--------	---------

49153/tcp	closed	unknown
-----------	--------	---------

49154/tcp closed unknown

49155/tcp closed unknown

49156/tcp closed unknown

49157/tcp closed unknown

49158/tcp closed unknown

49159/tcp closed unknown

49160/tcp closed unknown

49161/tcp closed unknown

49163/tcp closed unknown

MAC Address: 00:00:00:00:00:00 (Unknown)

Nmap scan report for 192.168.1.3

Host is up (0.0053s latency).

All 1000 scanned ports on 192.168.1.3 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

MAC Address: 00:00:00:00:00:00 (Guangdong Oppo Mobile Telecommunications)

Nmap scan report for 192.168.1.4

Host is up (0.0056s latency).

All 1000 scanned ports on 192.168.1.4 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

MAC Address: 00:00:00:00:00:00 (Guangdong Oppo Mobile Telecommunications)

Nmap scan report for 192.168.1.7

Host is up (0.0012s latency).

Not shown: 999 filtered tcp ports (no-response)

PORT STATE SERVICE

5357/tcp open wsddapi

MAC Address: 00:00:00:00:00:00 (Cloud Network Technology (Samoa) Limited)

## Step Five (Optional): Now, we can Perform SYN Scan & Check on Wire-Shark (Tool)

So, firstly we have Open Wire-Shark, and then perform following command :

**Command:** `nmap -v -sS 192.168.1.0/24`

Then, Open Wire-Shark and Apply Filter: `tcp.flags.syn == 1 && tcp.flags.ack == 0`

**Result:**

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main display area is divided into three panes. The top pane shows the packet list with a filter `tcp.flags.syn == 1 && tcp.flags.ack == 0` applied. It lists 20 captured packets, all of which are TCP SYN packets from 192.168.1.13 to 192.168.1.4. The middle pane shows the details of the selected packet (No. 20), including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII. The status bar at the bottom indicates that 8931 packets were captured and 6027 (67.5%) are displayed.

No.	Time	Source	Destination	Protocol	Length	Info
577	31.967003931	192.168.1.13	192.168.1.3	TCP	58	59578 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
578	31.967589253	192.168.1.13	192.168.1.4	TCP	58	59578 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
579	31.967822381	192.168.1.13	192.168.1.7	TCP	58	59578 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
580	31.968044966	192.168.1.13	192.168.1.1	TCP	58	59578 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
581	31.968569450	192.168.1.13	192.168.1.3	TCP	58	59578 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
582	31.968730788	192.168.1.13	192.168.1.4	TCP	58	59578 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
583	31.968960854	192.168.1.13	192.168.1.7	TCP	58	59578 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
584	31.969307660	192.168.1.13	192.168.1.1	TCP	58	59578 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
585	31.969515469	192.168.1.13	192.168.1.3	TCP	58	59578 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
586	31.969896654	192.168.1.13	192.168.1.4	TCP	58	59578 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
587	32.069719660	192.168.1.13	192.168.1.3	TCP	58	59578 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
588	32.070202297	192.168.1.13	192.168.1.4	TCP	58	59578 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
589	32.073082693	192.168.1.13	192.168.1.3	TCP	58	59578 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
590	32.073759667	192.168.1.13	192.168.1.4	TCP	58	59578 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
600	32.175288636	192.168.1.13	192.168.1.3	TCP	58	59578 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
601	32.175534594	192.168.1.13	192.168.1.4	TCP	58	59578 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
602	32.175754445	192.168.1.13	192.168.1.3	TCP	58	59578 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
603	32.175872476	192.168.1.13	192.168.1.4	TCP	58	59578 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
604	32.176249610	192.168.1.13	192.168.1.3	TCP	58	59578 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
605	32.176366675	192.168.1.13	192.168.1.4	TCP	58	59578 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
606	32.176529979	192.168.1.13	192.168.1.3	TCP	58	59578 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
607	32.176814169	192.168.1.13	192.168.1.4	TCP	58	59578 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
608	32.177020823	192.168.1.13	192.168.1.3	TCP	58	59578 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
609	32.177174766	192.168.1.13	192.168.1.4	TCP	58	59578 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
610	32.177387866	192.168.1.13	192.168.1.4	TCP	58	59578 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Frame 8649: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0  
Ethernet II, Src: PCSSystemtec\_6a:22:5d (08:00:27:6a:22:5d), Dst: NokiaSolutio\_3d:8f:91 (24:de:8a:3d:8f:91)  
Internet Protocol Version 4, Src: 192.168.1.13, Dst: 192.168.1.1  
Transmission Control Protocol, Src Port: 59588, Dst Port: 555, Seq: 0, Len: 0

0000 24 de 8a 3d 8f 91 08 00 27 6a 22 5d 08 00 45 00 \$ = ... "j" E  
0010 00 2c 85 b4 00 00 38 06 79 b9 c0 a8 01 0d c0 a8 , ... 8 y ...  
0020 01 01 c5 94 02 2b 0b 36 7e ef 00 00 00 00 00 02 ... + 6 ...  
0030 04 00 be e2 00 00 02 04 05 b4 ...