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

```
neon-white@kali-linux: ~
┌──(neon-white㉿kali-linux)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.13  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 2401:4900:8fc8:b09d:359d:db1e:89a8:ba61  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a00:27ff:fe6a:225d  prefixlen 64  scopeid 0x20<link>
        inet6 2401:4900:8fc8:b09d:a00:27ff:fe6a:225d  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:6a:22:5d  txqueuelen 1000  (Ethernet)
        RX packets 6828  bytes 2163239 (2.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 21702  bytes 1348695 (1.2 MiB)
        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 4105  bytes 175180 (171.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4105  bytes 175180 (171.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(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     [illegible]            3     180  Nokia Solutions and Networks GmbH & Co. KG
192.168.1.7     [illegible]            1      60  Cloud Network Technology (Samoa) Limited
192.168.1.4     [illegible]            1      60  GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP.,LTD
192.168.1.3     [illegible]            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     [illegible]            3     180  Nokia Solutions and Networks GmbH & Co. KG
192.168.1.7     [illegible]            1      60  Cloud Network Technology (Samoa) Limited
192.168.1.4     [illegible]            1      60  GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP.,LTD
192.168.1.3     [illegible]            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_tryno 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_tryno 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 wsdapi

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: