

# ELEVATE LABS CYBER SECURITY INTERNSHIP

## Task-1:

### 1. Install Nmap from official website.

Used the linux command `sudo apt install nmap` in my kali linux and downloaded nmap.

```
(kali@kali)-[~]
$ sudo apt install nmap
[sudo] password for kali:
nmap is already the newest version (7.95+dfsg-3kali1).
nmap set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 32
```

### 2. Find your local IP range

```
(kali@kali)-[~]
$ 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 00:0c:29:d7:8a:47 brd ff:ff:ff:ff:ff:ff
   inet 192.168.51.222/24 brd 192.168.51.255 scope global dynamic noprefixroute eth0
       valid_lft 3259sec preferred_lft 3259sec
   inet6 2401:4900:627d:d158:8cf:6f23:409e:d85b/64 scope global dynamic noprefixroute
       valid_lft 7098sec preferred_lft 7098sec
   inet6 fe80::f62c:97c4:1981:2b03/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: bridge0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
   link/ether 2a:91:6e:5c:3b:31 brd ff:ff:ff:ff:ff:ff
```

Here I can find my ip address as `192.168.51.222` with the subnet `/24`. Now I am scanning this in the nmap using the command `sudo nmap -sn 192.168.51.222/24` to perform ping scan without a port scan.

### 3. Run: `nmap -sS 192.168.51.222/24` to perform TCP SYN scan

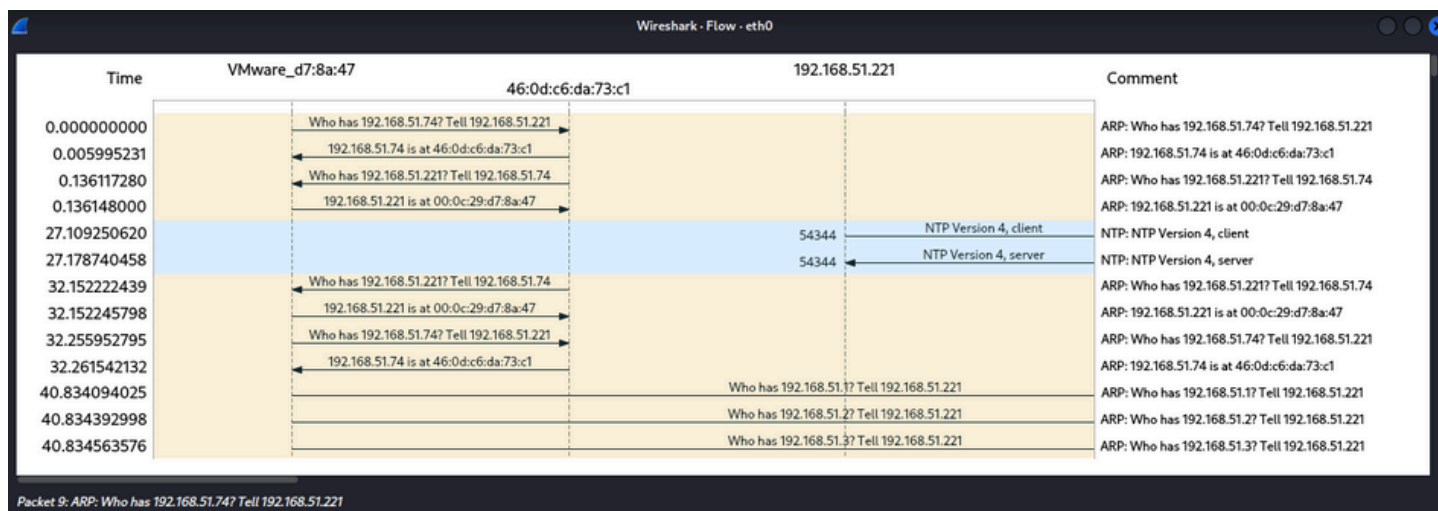
```
(kali㉿kali)-[~]  
$ nmap -sS 192.168.51.221/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 20:53 IST  
Nmap scan report for 192.168.51.37  
Host is up (0.029s latency).  
All 1000 scanned ports on 192.168.51.37 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: 14:13:33:B8:D0:43 (AzureWave Technology)  
  
Nmap scan report for 192.168.51.41  
Host is up (0.00098s latency).  
All 1000 scanned ports on 192.168.51.41 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: A0:C5:89:A3:7A:1E (Intel Corporate)  
  
Nmap scan report for 192.168.51.136  
Host is up (0.00070s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
MAC Address: 00:0C:29:75:DC:02 (VMware)  
  
Nmap scan report for 192.168.51.221  
Host is up (0.0000050s latency).  
All 1000 scanned ports on 192.168.51.221 are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
  
Nmap done: 256 IP addresses (4 hosts up) scanned in 9.95 seconds
```

#### 4. Note down IP addresses and open ports found.

The IP addresses of the open ports found are 192.168.51.136 ( 2 open ports).

#### 5. Optionally analyze packet capture with Wireshark.

Captured the live trac through wireshark



## 6. Research common services running on those ports.

Port	Service	Purpose
22/tcp	ssh	Provides secure command-line access and remote login over an encrypted connection.
80/tcp	http	Facilitates the transfer of web pages and resources over the internet.

## 7. Identify potential security risks from open ports.

Port	Service	Potential Security Risks
22/tcp	SSH	<ul style="list-style-type: none"> <li>Brute-force attacks on login credentials.</li> <li>If weak or default passwords are used, attackers may gain remote access.</li> <li>Unpatched SSH versions can have vulnerabilities.</li> </ul>
80/tcp	HTTP	<ul style="list-style-type: none"> <li>Unencrypted data transmission, making it vulnerable to eavesdropping or Man-in-the-Middle (MitM) attacks.</li> <li>May expose web server software to exploits if outdated.</li> <li>Susceptible to web attacks like XSS, SQL injection, etc. if web apps are misconfigured.</li> </ul>

## 8. Save scan results as a text or HTML file.

```
(kali㉿kali)-[~]  
$ nmap -sS 192.168.51.221/24 -oN results.txt  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 21:12 IST  
Nmap scan report for 192.168.51.37  
Host is up (0.011s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
MAC Address: 14:13:33:B8:D0:43 (AzureWave Technology)  
  
Nmap scan report for 192.168.51.41  
Host is up (0.00026s latency).  
All 1000 scanned ports on 192.168.51.41 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: A0:C5:89:A3:7A:1E (Intel Corporate)  
  
Nmap scan report for 192.168.51.221  
Host is up (0.0000040s latency).  
All 1000 scanned ports on 192.168.51.221 are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
  
Nmap done: 256 IP addresses (3 hosts up) scanned in 10.18 seconds  
  
(kali㉿kali)-[~]  
$ sudo apt install nmap  
[sudo] password for kali:  
nmap is already the newest version (7.95+dfsg-3kali1).  
nmap set to manually installed.  
Summary:  
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 32
```