

# ELEVATE LABS CYBER SECURITY INTERNSHIP

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

### 1) 1.Install Nmap from ocial website.

Already i have nmap on my machine

### 2.Find your local IP range

```
kishan_22064@kali on [192.168.51.37] $  
/home/kishan_22064  
ifconfig  
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 112 bytes 8528 (8.3 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 112 bytes 8528 (8.3 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.51.37 netmask 255.255.255.0 broadcast 192.168.51.255  
    inet6 2401:4900:627d:d158:a27a:4da:9352:efb8 prefixlen 64 scopeid 0x0<global>  
    inet6 fe80::709a:6168:4fcb:1987 prefixlen 64 scopeid 0x20<link>  
    ether 14:13:33:b8:d0:43 txqueuelen 1000 (Ethernet)  
    RX packets 64 bytes 8843 (8.6 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 67 bytes 5420 (5.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
kishan_22064@kali on [192.168.51.37] $  
/home/kishan_22064  
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: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000  
    link/ether 14:13:33:b8:d0:43 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.51.37/24 brd 192.168.51.255 scope global dynamic noprefixroute wlan0  
        valid_lft 2663sec preferred_lft 2663sec  
    inet6 2401:4900:627d:d158:a27a:4da:9352:efb8/64 scope global dynamic noprefixroute  
        valid_lft 6912sec preferred_lft 6912sec  
    inet6 2409:40f4:215a:6ece:13a2:bc79:feab:8f4c/64 scope global deprecated dynamic noprefixroute  
        valid_lft 6891sec preferred_lft 0sec  
    inet6 fe80::709a:6168:4fcb:1987/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

### 3.Run: nmap -sS 10.0.2.5/24 to perform TCP SYN scan

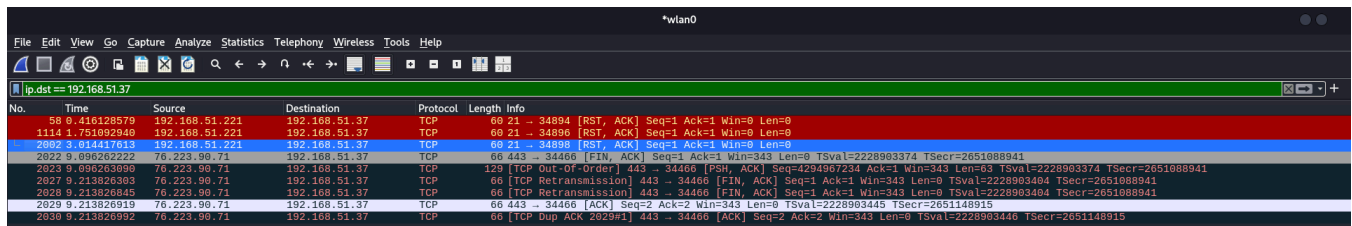
```
kishan_22064@kali on [192.168.51.37] $  
/home/kishan_22064  
nmap -sS 192.168.51.0/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 21:00 IST  
Nmap scan report for 192.168.51.41  
Host is up (0.026s latency).  
All 1000 scanned ports on 192.168.51.41 are in ignored states.  
Not shown: 1000 filtered tcp ports (no-response)  
MAC Address: A0:C5:89:A3:7A:1E (Intel Corporate)  
  
Nmap scan report for 192.168.51.74  
Host is up (0.0048s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
53/tcp    open  domain  
MAC Address: 46:0D:C6:DA:73:C1 (Unknown)  
  
Nmap scan report for 192.168.51.221  
Host is up (0.0072s latency).  
All 1000 scanned ports on 192.168.51.221 are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
MAC Address: A0:C5:89:A3:7A:1E (Intel Corporate)  
  
Nmap scan report for 192.168.51.37  
Host is up (0.0000040s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
  
Nmap done: 256 IP addresses (4 hosts up) scanned in 10.15 seconds
```

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

The IP addresses of the open ports found are 192.168.51.41 and 192.168.51.37

### 5.Optionally analyze packet capture with Wireshark

Captured the live trac through wireshark



No.	Time	Source	Destination	Protocol	Length	Info
58	0.416128579	192.168.51.221	192.168.51.37	TCP	60	21 → 34894 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1114	1.751892940	192.168.51.221	192.168.51.37	TCP	60	21 → 34896 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2802	3.614417615	192.168.51.221	192.168.51.37	TCP	60	21 → 34898 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2822	9.096262222	76.223.90.71	192.168.51.37	TCP	66	443 → 34466 [FIN, ACK] Seq=1 Ack=1 Win=343 Len=0 TSval=2228903374 TSecr=2651088941
2823	9.096263990	76.223.90.71	192.168.51.37	TCP	128	[TCP Out-Of-Order] 443 → 34466 [PSH, ACK] Seq=4294967234 Ack=1 Win=343 Len=63 TSval=2228903374 TSecr=2651088941
2827	9.213828303	76.223.90.71	192.168.51.37	TCP	66	[TCP Retransmission] 443 → 34466 [FIN, ACK] Seq=1 Ack=1 Win=343 Len=0 TSval=2228903404 TSecr=2651088941
2828	9.213828845	76.223.90.71	192.168.51.37	TCP	66	[TCP Retransmission] 443 → 34466 [FIN, ACK] Seq=1 Ack=1 Win=343 Len=0 TSval=2228903404 TSecr=2651088941
2829	9.213826919	76.223.90.71	192.168.51.37	TCP	66	443 → 34466 [ACK] Seq=2 Ack=2 Win=343 Len=0 TSval=2228903445 TSecr=2651148915
2830	9.213826992	76.223.90.71	192.168.51.37	TCP	66	[TCP Dup ACK 2829#1] 443 → 34466 [ACK] Seq=2 Ack=2 Win=343 Len=0 TSval=2228903446 TSecr=2651148915

Time	192.168.51.221	192.168.51.37	76.223.90.71	Comment
0.416128579	21 → 34894 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0	34894		TCP: 21 → 34894 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
1.751092940	21 → 34896 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0	34896		TCP: 21 → 34896 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
3.014417613	21 → 34898 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0	34898		TCP: 21 → 34898 (RST, ACK) Seq=1 Ack=1 Win=0 Len=0
9.096262222		34466 → 443 (FIN, ACK) Seq=1 Ack=1 Win=343 Len=0	443	TCP: 443 → 34466 (FIN, ACK) Seq=1 Ack=1 Win=343 Len=0
9.096263090		[TCP Out-Of-Order] 443 → 34466 (PSH, ACK) Seq=...	443	TCP: [TCP Out-Of-Order] 443 → 34466 (PSH, ACK) Seq=...
9.213826303		[TCP Retransmission] 443 → 34466 (FIN, ACK) Seq=...	443	TCP: [TCP Retransmission] 443 → 34466 (FIN, ACK) Seq=...
9.213826845		[TCP Retransmission] 443 → 34466 (FIN, ACK) Seq=...	443	TCP: [TCP Retransmission] 443 → 34466 (FIN, ACK) Seq=...
9.213826919		443 → 34466 (ACK) Seq=2 Ack=2 Win=343 Len=0 T...	443	TCP: 443 → 34466 (ACK) Seq=2 Ack=2 Win=343 Len=0 T...
9.213826992		[TCP Dup ACK 2029H] 443 → 34466 (ACK) Seq=2...	443	TCP: [TCP Dup ACK 2029H] 443 → 34466 (ACK) Seq=2 A...

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

Port - 22

Service - ssh

Purpose - Securely access remote computers or servers over a network.

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

Port 22 runs the SSH service, which is used to securely access remote systems. However, if left open, it can be a target for brute-force attacks, especially if weak passwords or root login are allowed. Hackers or bots may try to exploit vulnerabilities in outdated SSH versions. To reduce risks, it's best to use SSH keys, disable root login, limit access with firewalls, change the default port, and keep the system updated. Tools like fail2ban can also help block repeated login attempts.

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

```
kishan_22064@kali on [192.168.51.37] $
/home/kishan_22064
nmap -sS 192.168.51.0/24 -oN SCAN_FILES.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 21:37 IST
Nmap scan report for 192.168.51.41
Host is up (0.023s 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 192.168.51.74
Host is up (0.0062s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 46:0D:C6:DA:73:C1 (Unknown)

Nmap scan report for 192.168.51.37
Host is up (0.0000040s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 7.40 seconds
```

Here this result is saved as scan\_files.txt file