Cyber Security Internship Task 1 - Port Scanning Using Nmap

❖ Tools Used

- Nmap: For scanning open ports and performing TCP SYN scan

❖ Objective

To perform basic network reconnaissance by scanning the local network for open ports using Nmap and understand the potential risks associated with exposed network services.

❖ Steps Performed

1. Identified Local IP Range

Used the command

- On Linux: `ifconfig` or `ip a`

Found my local IP: `192.168.18.108`, so the range is: `192.168.18.108/24`

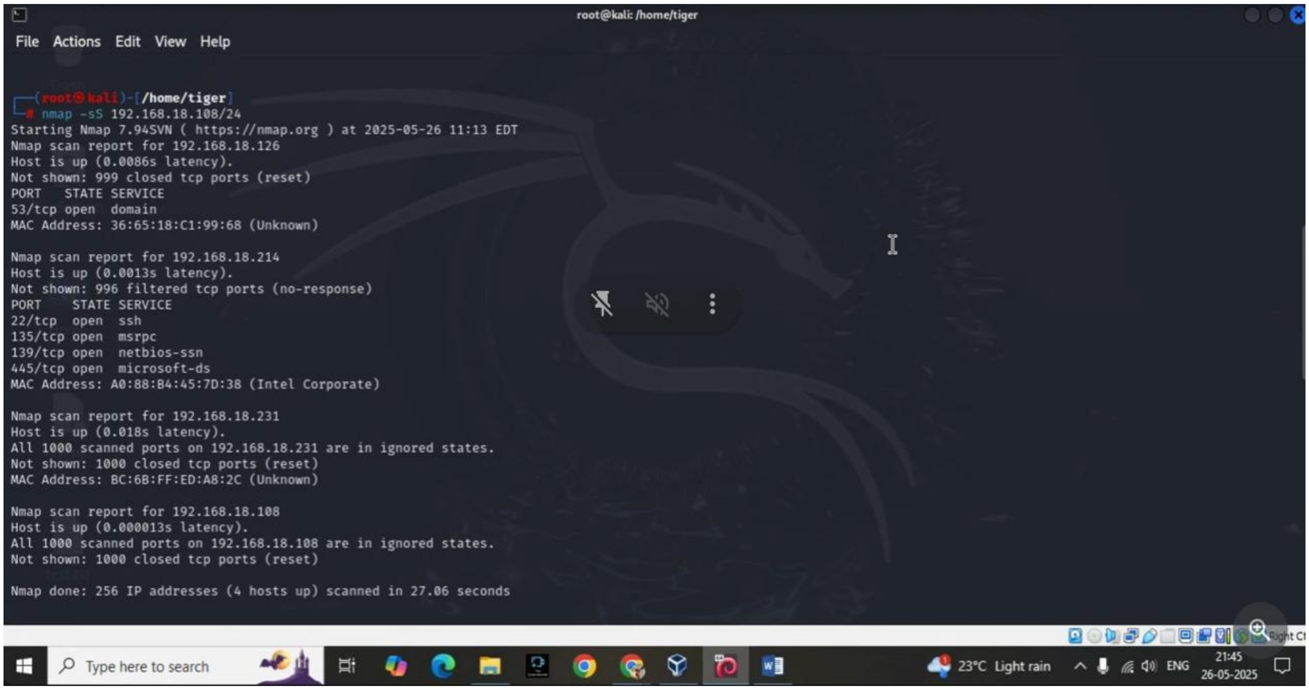
2. Ran TCP SYN Scan

Command:

(nmap -sS 192.168.18.108/24)

❖ Open Port

PORT	STATE	SERVICE
22/tcp	open	ssh
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds



```
┌──(root㉿kali)-[/home/tiger]
└─# nmap -sS 192.168.18.108/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-26 11:13 EDT
Nmap scan report for 192.168.18.126
Host is up (0.0086s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 36:65:18:C1:99:68 (Unknown)

Nmap scan report for 192.168.18.214
Host is up (0.0013s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: A0:88:B4:45:7D:38 (Intel Corporate)

Nmap scan report for 192.168.18.231
Host is up (0.018s latency).
All 1000 scanned ports on 192.168.18.231 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: BC:6B:FF:ED:A8:2C (Unknown)

Nmap scan report for 192.168.18.108
Host is up (0.000013s latency).
All 1000 scanned ports on 192.168.18.108 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 27.06 seconds
```