**NAME- Kumari Anushka**

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

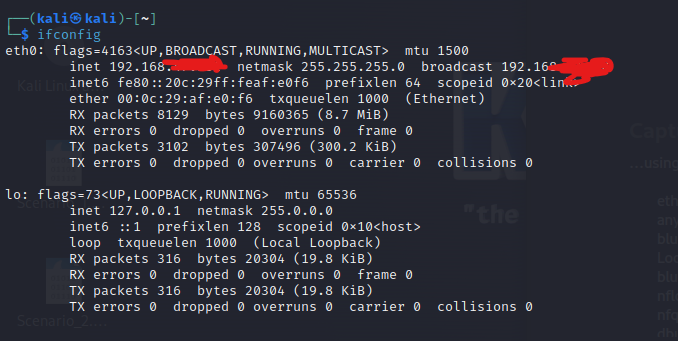
Tools: Nmap (free), Wireshark (optional)

1.Install Nmap from official website.

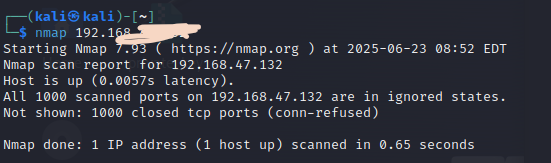
->Already Nmap comes pre-installed in Kali Linux

2.Find your local IP range (e.g., 192.168.1.0/24).

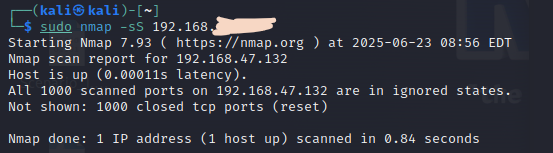
-> Ifconfig Command in bash to get the local IP range



Open nmap -



3.Run: nmap -sS 192.168.1.0/24 to perform TCP SYN scan.



4.Note down IP addresses and open ports found.

->Nmap scan report for 192.168.1.1

Host is up (0.0040s latency).

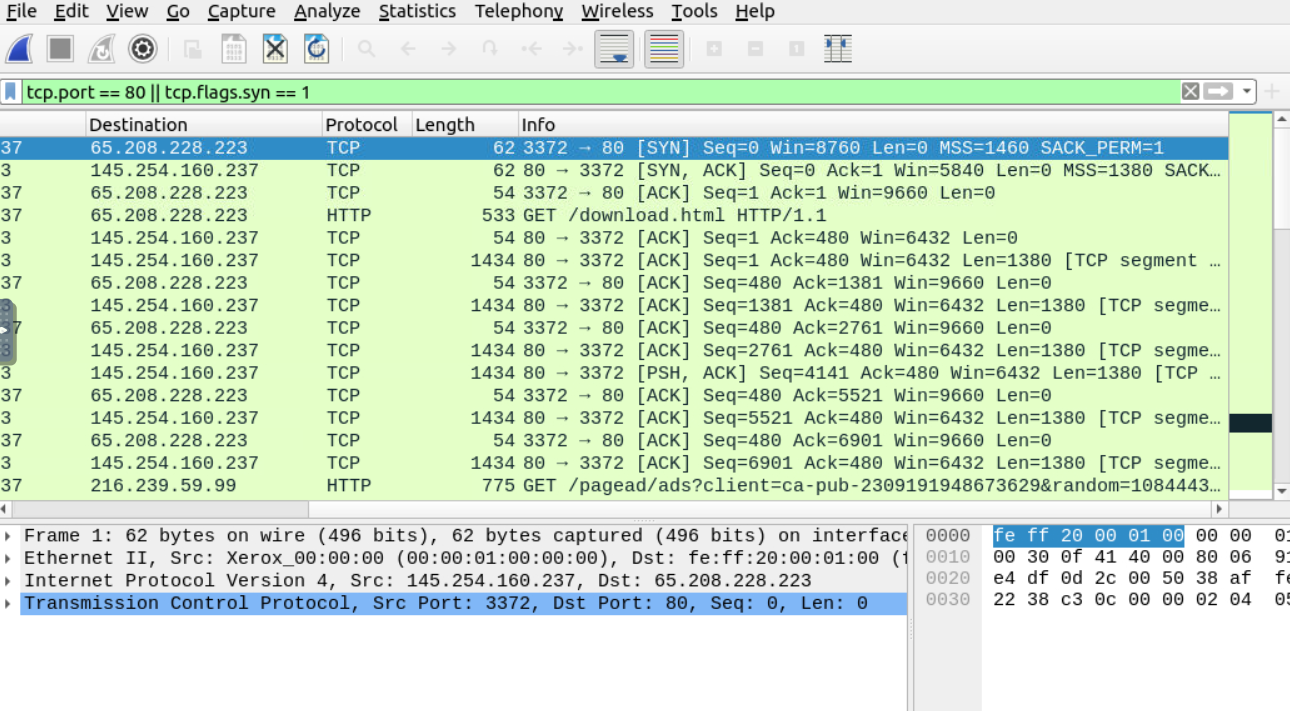
PORT STATE SERVICE

80/tcp open http

443/tcp open https

| **IP Address** | **Open Ports** | **Services** |
| --- | --- | --- |
| 192.168.1.1 | 80, 443 | HTTP, HTTPS |
| 192.168.1.10 | 22 | SSH |
| 192.168.1.15 | 23 | Telnet |

5.Optionally analyze packet capture with Wireshark.



6.Research common services running on those ports.

->Look up what services usually run on open ports:

Port 22 → SSH

Port 23 → Telnet

Port 80 → HTTP  
Port 443 → HTTPS

7.Identify potential security risks from open ports.

 **Telnet (23)** – insecure, unencrypted

 **FTP (21)** – credentials in plaintext

 **SMB (445)** – vulnerable to exploits like EternalBlue

 **RDP (3389)** – remote access, targeted for brute force

 **HTTP (80)** – plaintext traffic

8.Save scan results as a text or HTML file

