Task 1 Cybersecurity Intern

Objective: Learn to discover open ports on devices in your local network to understand network exposure.
Tools: Nmap (free), Wireshark (optional).

Solution:

Nmap Tool

Nmap, short for Network Mapper, is an open-source and free tool used for network exploration and security auditing. It discovers hosts and services on a network by sending specially crafted packets and analyzing the responses to gather information like open ports, running services, operating systems, and even potential vulnerabilities. Network administrators and security professionals use Nmap for tasks such as network inventory, monitoring service uptime, performing vulnerability assessments, and conducting penetration testing.

1. Install Nmap

- Go to https://nmap.org/download.html
- Download and install Nmap for your operating system (Windows, macOS, Linux).

2. Find Your Local IP & Network Range

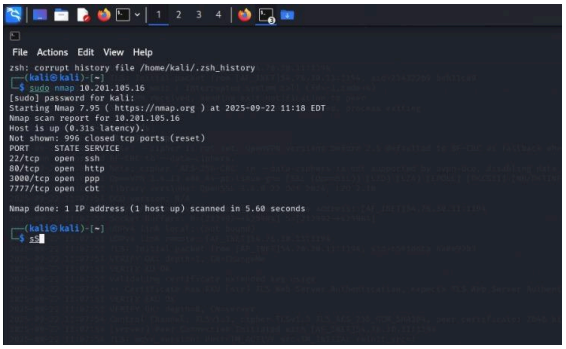
- **Open Command Prompt/Terminal and check your IP:**

  After checking ip address , Using Nmap Tool check which port is open

  - Command For Nmap
    Sudo nmap –open <IP address>

3**. Save Scan Results**

To save output as text



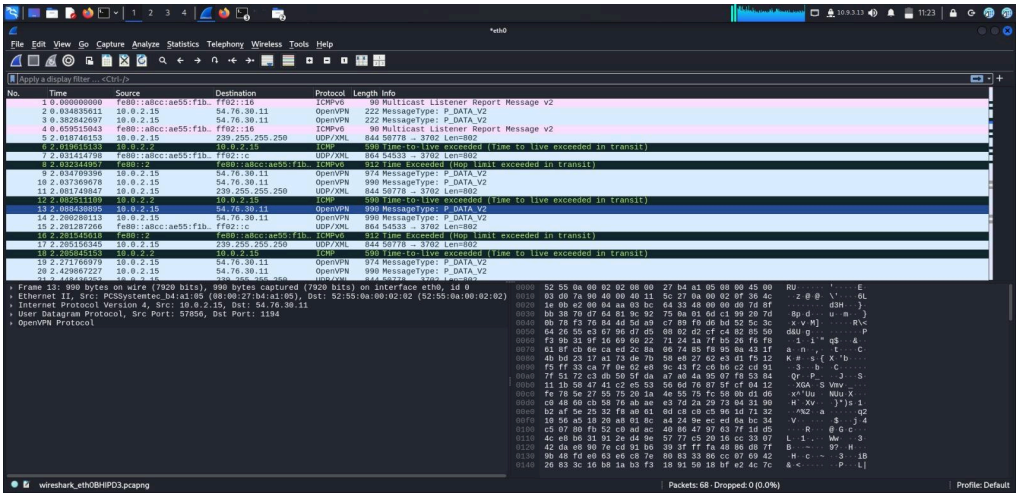
After Using Nmap tool , We found Four ports open

Port No.	State	Service
22/tcp	**open**	**ssh**
80/tcp	**open**	**http**
3000/tcp	**open**	**ppp**
7777/tcp	**open**	**cbt**

5. Open Wireshark Tool analyze the packets

Wireshark

Wireshark is a free, open-source, and widely used network protocol analyzer that captures, inspects, and analyzes network traffic in real-time. It acts as a "packet sniffer," allowing users to view the contents of data packets as they travel across a network.



After analyzing the packet , we found multiple packet on basis of our Ip Address and also with the help of openVPN.

Conclusion:

Through this task, I successfully learned how to perform basic network reconnaissance using **Nmap** and optionally analyze traffic with **Wireshark**. By scanning my local network, I identified four open ports (22/SSH, 80/HTTP, 3000/PPP, 7777/CBT) and understood the services associated with them.

This exercise helped me gain hands-on experience with:

- Discovering active hosts and open ports on a network
- Understanding potential attack surfaces created by open ports
- Observing real network traffic to see how devices communicate

Overall, this task improved my knowledge of **network exposure** and **security auditing**. It highlighted the importance of closing unnecessary ports, using firewalls, and regularly monitoring network activity to reduce risk. This practical exposure is essential for any cybersecurity professional aiming to protect systems from unauthorized access and network-based attack