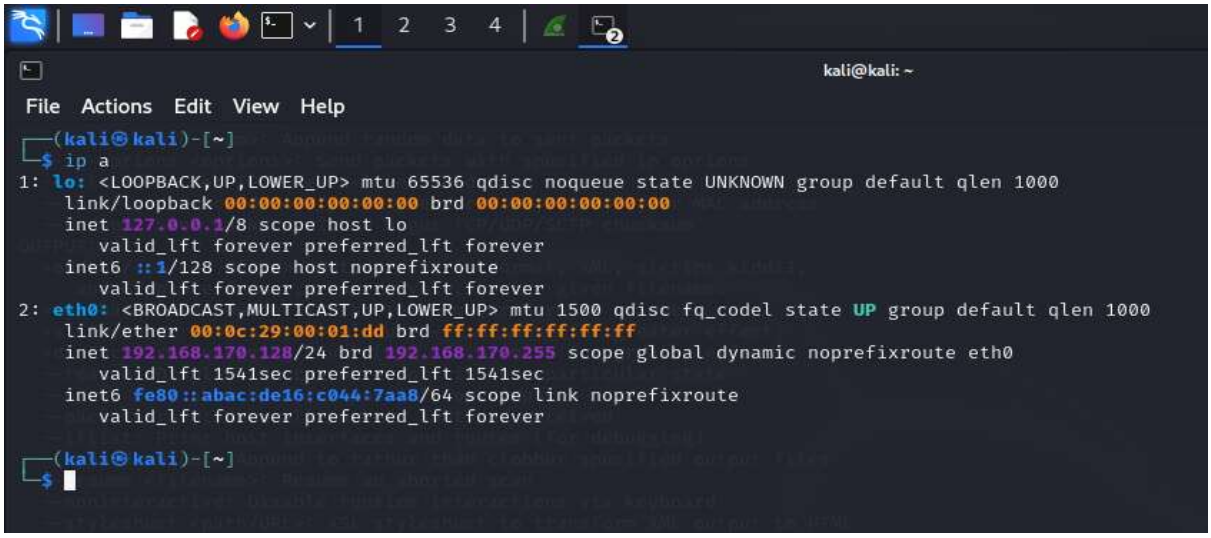
CYBER SECURITY INTERNSHIP

Day 1

Date : 23/06/2025

Task 1: Scan Your Local Network for Open Ports:



OPEN PORTS (80,135,139,445,3306):

This task was a valuable hands-on experience that helped me understand how network scanning works in real-world environments. By using Nmap, I was able to identify active devices in my local network and examine which ports were open, what services were running on those ports, and what risks those services might pose.

My Opinion that includes **details about the open ports (80, 135, 139, 445, 3306)** you discovered during the scan — making it more personal and relevant to your task:

Port 80 (HTTP):
This port is used to show websites. In my scan, it showed that a website is running. But the problem is — it is using **HTTP without encryption**, which means if someone logs in or sends data, **a hacker can see that information easily**. This is not safe. It is better to use **HTTPS (secure version)** instead.

Port 135 (MSRPC):
This port is used by Windows to allow programs to talk to each other remotely. But it is **often targeted by attackers** to run harmful code from far away (called remote code execution). So, **keeping this port open is risky**, especially if the computer is connected to the internet.

Port 139 (NetBIOS) and **Port 445 (SMB):**
These ports are used for **file sharing in Windows**. If they are open, an attacker can find out **what folders are shared**, **usernames**, or even access files without permission. Port 445 is very dangerous — it was used in a real attack called **WannaCry ransomware**. These ports should be closed unless we really need file sharing in a private network.

Port 3306 (MySQL):
This port is used by the **MySQL database**. It helps websites or apps store and use data. If this port is open to the internet, someone could try to **guess the password** or **steal the data** using attacks like **SQL injection**. It is better to keep this port open only inside the system (not public) and use a strong password.