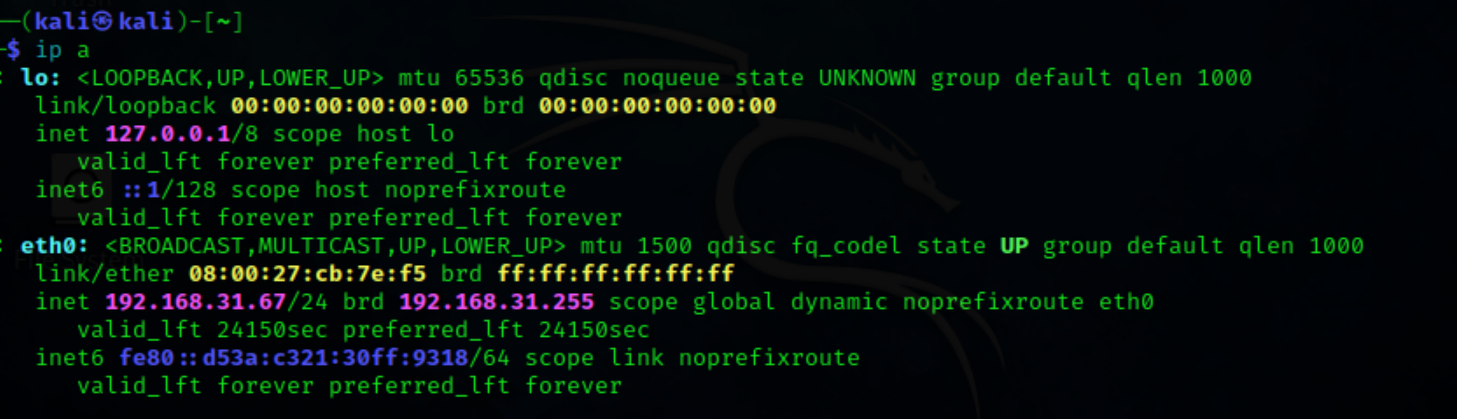


|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |
|  | | Cyber Security | | |  | |
|  |  | | | | |  |
|  | | |  |  | | |
|  | | | Tejaswini Sardar |  | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | MAY 26 2025—CYBER SECURITY— |  | |
|  |  | | |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | |  |  | | |  |
|  | INTRODUCTION | | | | | | |  |
|  |  | | |  |  | | |  |
|  |  | |  | | |  | |  |
|  |  |  | Task 1:  Scan Your Local Network for Open Ports.  The objective of this task is to explore and identify open ports on devices within the local network to assess potential network exposure and associated security risks. | | |  |  |  |
| Decorative | | | | |
|  |  |  |  |
|  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Decorative | |  |  | | |  |  | |
|  | | THE PROCESS | | | | |  | |
|  | |  |  | | |  |  | |
|  | TOOLS :-  * Nmap (Network Mapper): A free and open-source network scanning tool used for network discovery and security auditing. * Metasploit (Metasploit is a framework for security testing and vulnerability management Tool) * Wireshark (A network protocol analyzer used to inspect network traffic.)   These Are The Tools Used While Doing The Task For  Scanning Ports . | | | | | | |  |
|  | ProcedureStep 1: Install Nmap | | |  | **Step 2 :- Find Your Local IP Range**  Step 1: Open Terminal | | |  |
|  | Nmap was downloaded and installed from the official website: <https://nmap.org>. The installation was performed on a Windows/Linux system.  **Step 2: Identify Your IP Address**  Run the following command to view your network configuration:  ip a | | |  |  | | |  |

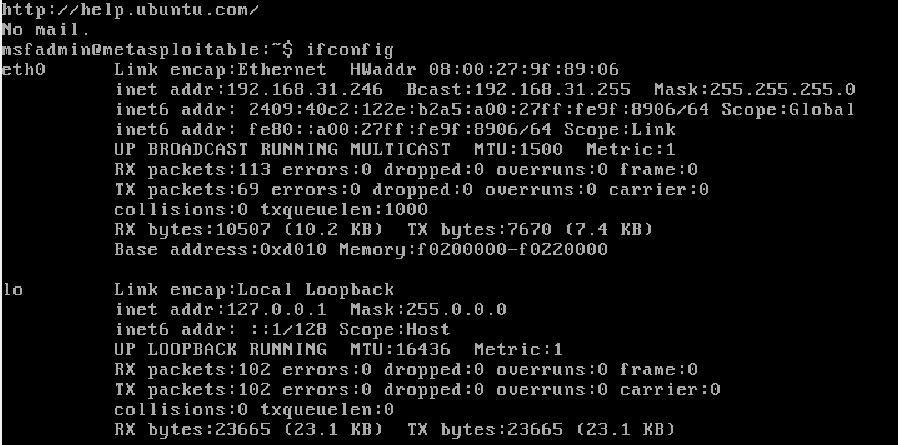


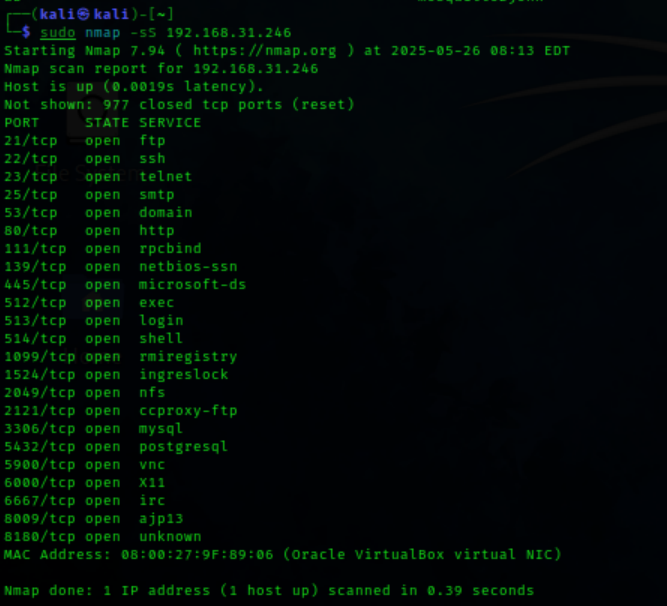
|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

**Step 3: Perform TCP SYN Scan**

A SYN scan was performed using the following Nmap command:

$ Sudo nmap -sS 192.168





**Conclusion**

The network scan revealed multiple devices with open ports, many running common services. Some of these services (e.g., SMB, HTTP) may expose the network to known vulnerabilities. It is recommended to:

* Disable unnecessary services.
* Secure remote access protocols.
* Keep firmware and software up to date.
* Implement firewall rules to restrict exposure.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | |
|  |  | |  |
|  |  |  | |