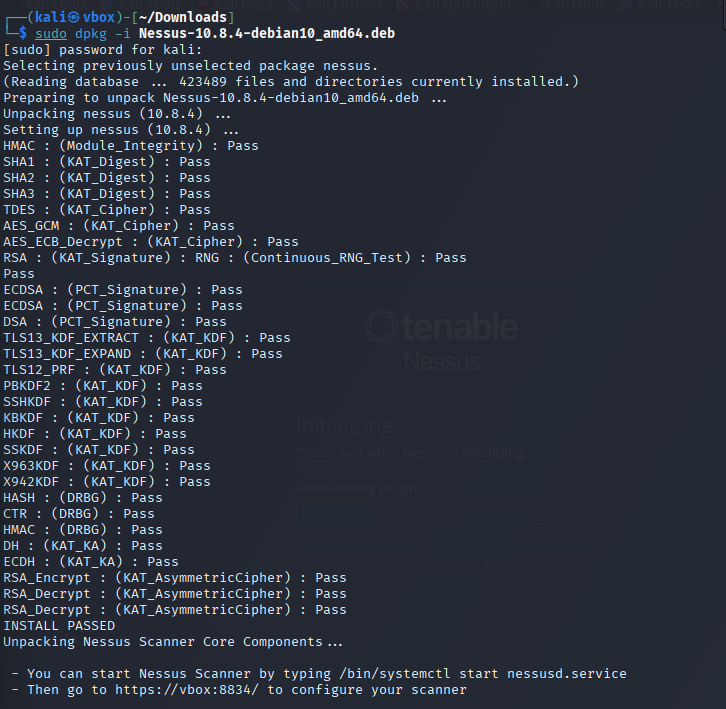
Task 3 : Perform a Basic Vulnerability Scan on Your PC

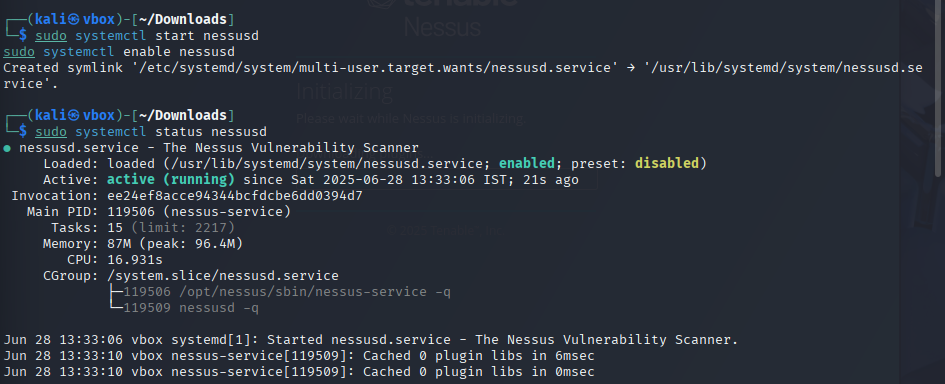
Tool used: Nessus

1. Terminal commands for installation

* After installing Nessus for Linux OS



This screenshot shows the successful installation of Nessus 10.8.4 on Kali Linux using the .deb package. The terminal output confirms that all cryptographic self-tests passed, indicating a valid and secure setup. At the end, it instructs the user to start the Nessus service and access the web UI at https://localhost:8834.



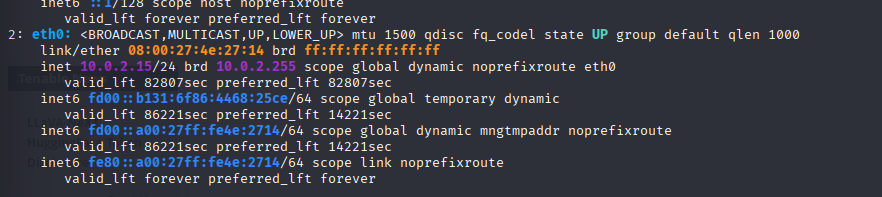
This shows the successful start and the Nessus service is enabled using systemctl command. The service status confirms that Nessus is **active (running)** and ready to serve the web interface at <https://localhost:8834>

3.In the GUI of Nessus tool Running a network scan to indentify vulnerabilities

Step-1: accessing it in local host with this url [Nessus / Initializing](https://localhost:8834/#/) and Wait for Plugin Update

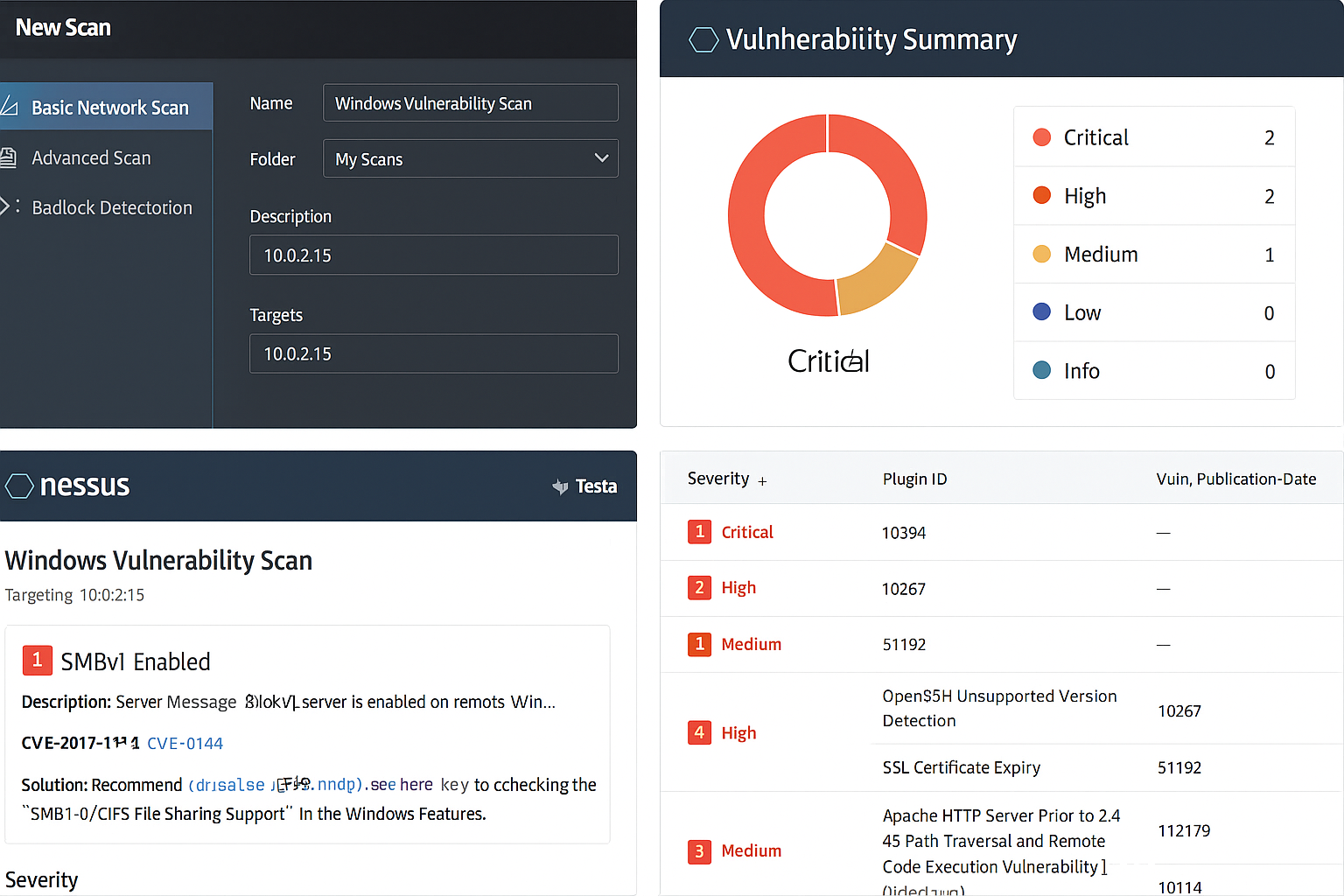
Step-2 Create and run a scan

Scanning my local internal ip that is found using ip a command



Step-3

Running a scan in Nessus



Mitigation

OpenSSH Information Leak (CVE-2016-0777)

Mitigation:

Update OpenSSH to the latest version:

sudo apt update

sudo apt upgrade openssh-server