Technical Report: OpenVAS Vulnerability Scanning

1. Introduction

The objective of this task is to perform a basic vulnerability assessment using **Nessus**, a widely used commercial vulnerability scanner. This task introduces the fundamentals of vulnerability scanning by identifying security flaws in a target system, evaluating risk levels, and generating a detailed report. It helps students understand how attackers exploit weaknesses and how to mitigate them to enhance cybersecurity.

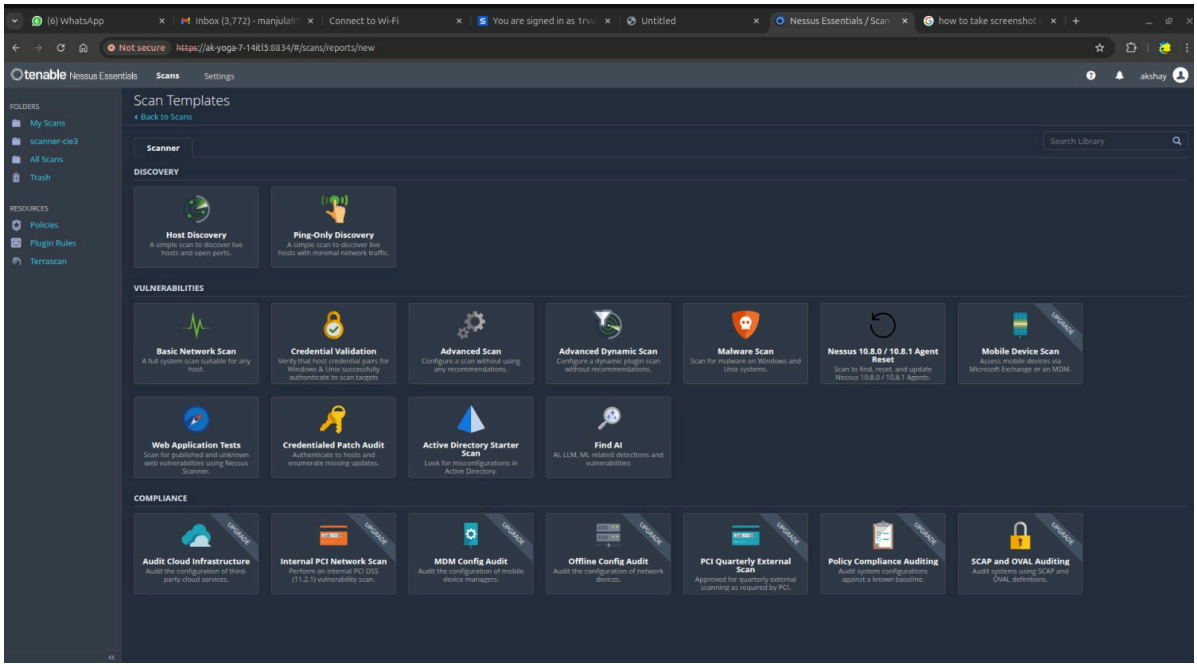
2. Tools Used

- **Nessus Vulnerability Scanner**: A powerful tool developed by Tenable, used to scan systems for known vulnerabilities, misconfigurations, and compliance issues. It provides detailed risk ratings, CVE references, and remediation suggestions.
- **Kali Linux** : Used to access the Nessus web-based dashboard to configure and run scans.

3. Step-by-Step Execution

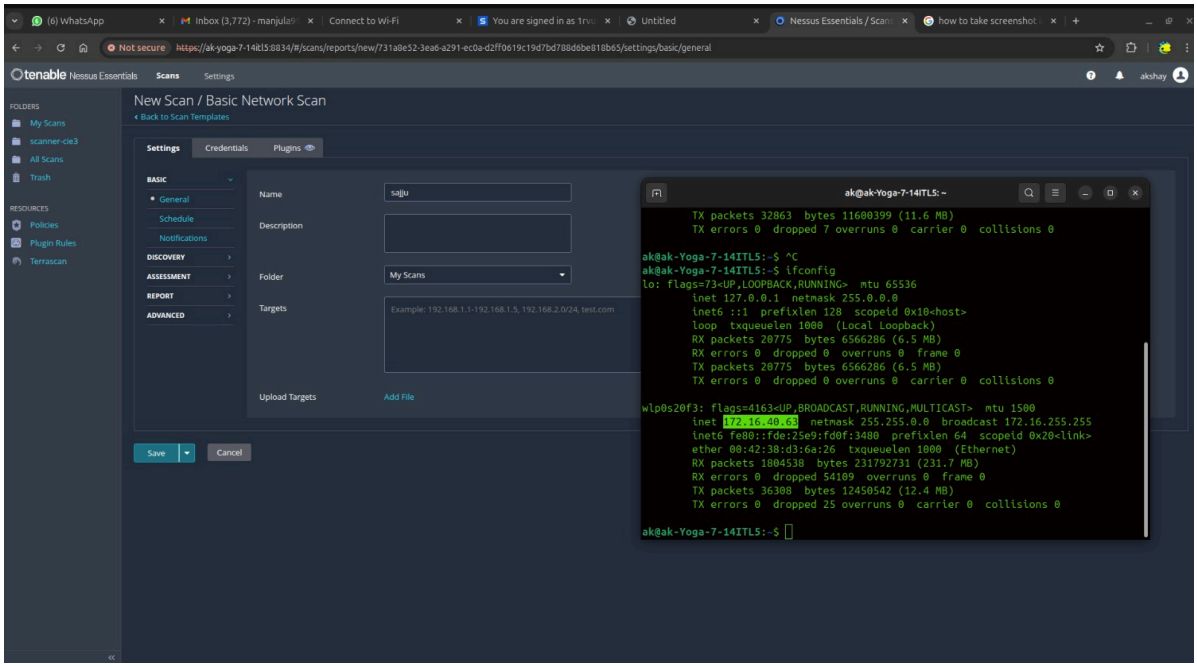
Accessing the Nessus Dashboard

- Opened a browser and accessed https://localhost:8834.
- Logged in using administrator credentials.



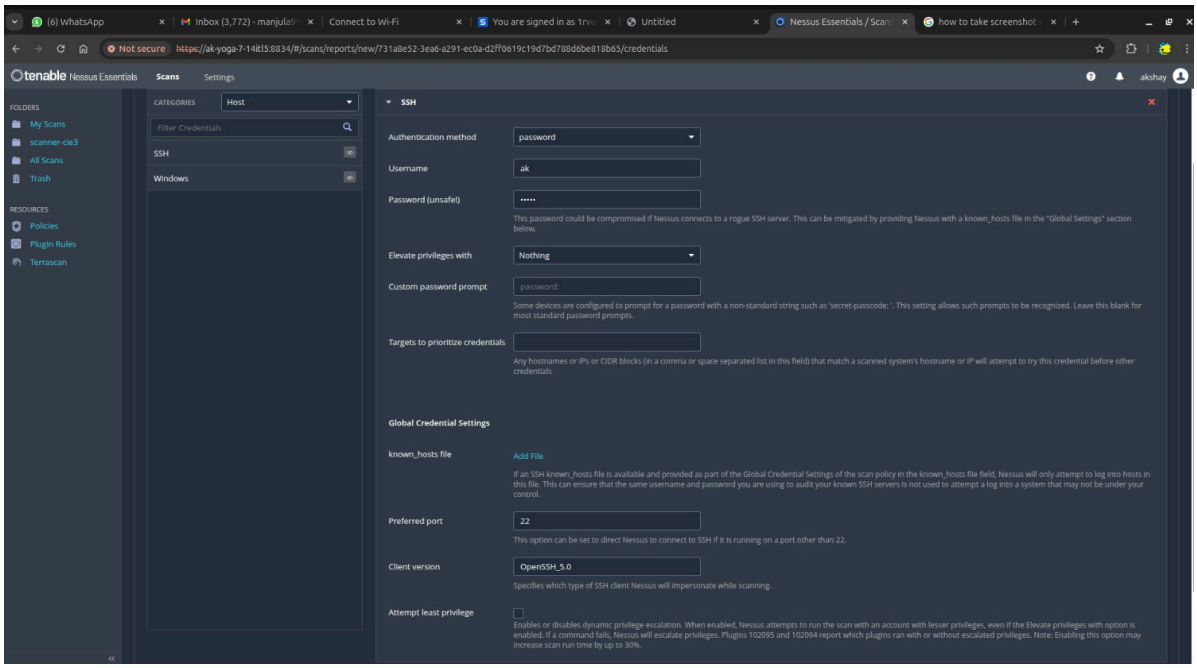
Creating a New Scan

- Selected the option “New Scan” from the dashboard.
- Chose a scan template (e.g., **Basic Network Scan**).
- Provided a scan name and the target IP address to be scanned.



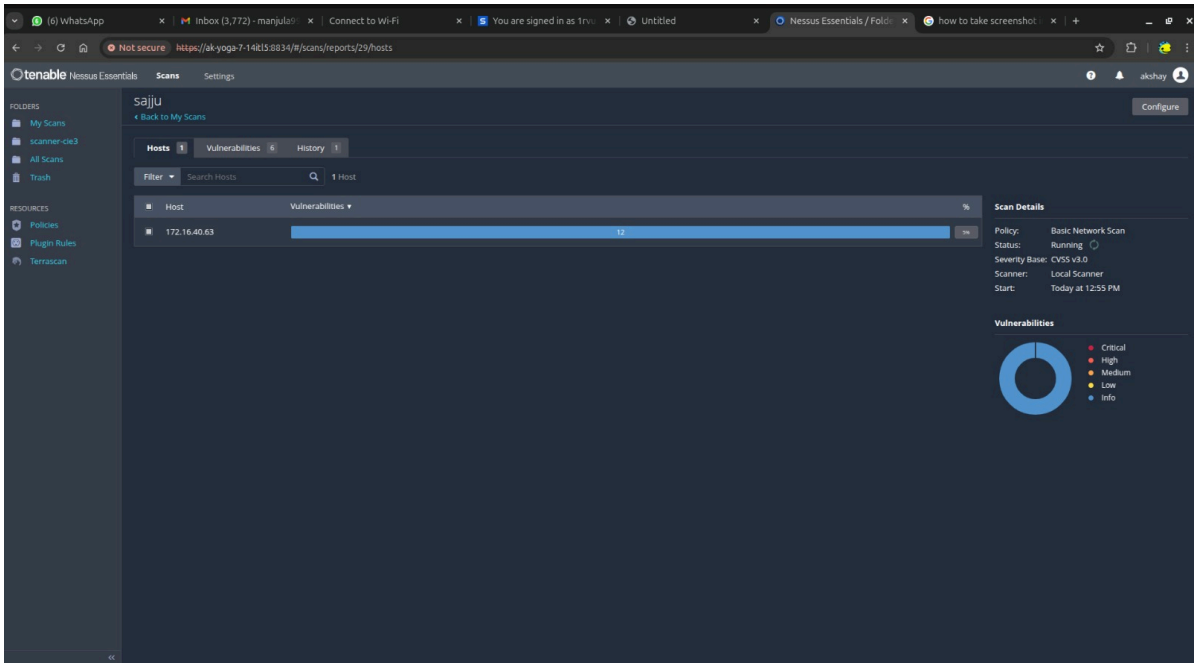
Launching the Scan

- After configuring the scan, clicked on “Save” and then “Launch” to initiate the scan.
- Waited for the scan to complete while Nessus analyzed the system.



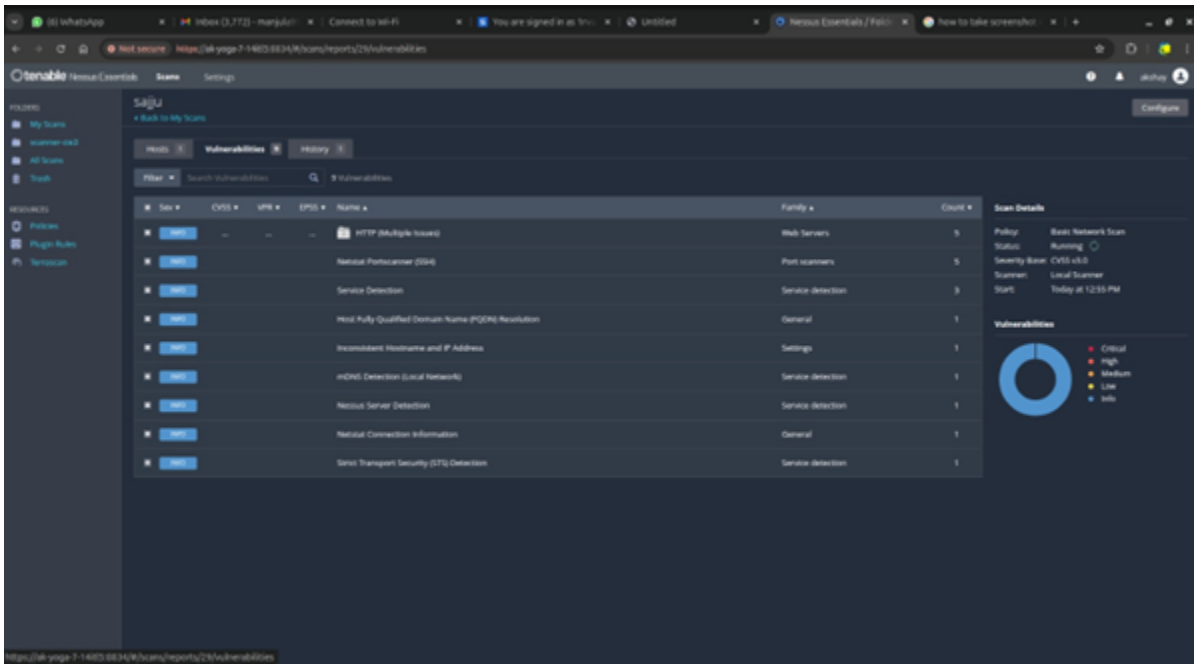
Viewing Results

- Navigated to the “Completed Scans” section.
- Opened the scan report to review identified vulnerabilities.
- Vulnerabilities were categorized into severity levels: **Critical, High, Medium, Low, and Info**.



4. Findings & Analysis

The Nessus Essentials scan identified a total of 12 informational vulnerabilities on the target host. While no critical, high, medium, or low-risk vulnerabilities were found, the following informational issues were detected:



Key Observations:

- **HTTP Server Information Disclosure and Allowed Methods can reveal sensitive server configuration data.**
- **Netstat Portscanner (SSH) and SYN Scanner indicate that open ports and services are exposed and were successfully detected.**
- **HSTS Not Enabled means the web server does not enforce secure HTTPS connections, potentially exposing users to downgrade attacks.**
- **Inconsistent Hostname and IP Address may reflect misconfigured network settings or DNS entries.**

5. Recommendations

- **Apply Software Updates**: Immediately patch known vulnerabilities listed in the report.
- **Secure Network Services**: Disable or harden vulnerable services (e.g., SMB, Telnet).
- **Use Strong Encryption**: Upgrade SSL/TLS configurations to use strong cipher suites.
- **Implement Access Control**: Limit user privileges and segment networks appropriately.
- **Continuous Monitoring**: Perform vulnerability scans regularly and after each major system update.

6. Conclusion

Using Nessus for vulnerability scanning gave practical insight into real-world cybersecurity issues. The task emphasized the importance of identifying and patching weaknesses before attackers can exploit them. This experience helps build foundational skills for system auditing, vulnerability assessment, and maintaining robust system security.