Vulnerability Assessment Report

Name: Meena Saxena
Date: October 26, 2025

This report summarizes the results of a vulnerability assessment performed on my local system using Nessus Essentials. The goal of this task was to identify potential security vulnerabilities, understand their severity, and learn the basics of vulnerability scanning as part of the Cybersecurity Internship Task 3.

Objective:
To perform a full vulnerability scan on my local machine using Nessus Essentials and analyze the findings to understand potential security risks and mitigation steps.

Environment Details:
- Scanner Used: Nessus Essentials (Version 10.10.0)
- Operating System: Kali Linux (Kernel 6.16.8)
- Host IP: 192.168.29.186
- Scan Type: Credentialed Localhost Scan
- Scan Duration: ~7 minutes

Methodology:
1. Installed and configured Nessus Essentials.
2. Added localhost as the target and enabled credentialed checks.
3. Started a full vulnerability scan using the Advanced Scan policy.
4. Waited for scan completion and exported results in HTML format.
5. Reviewed identified vulnerabilities and analyzed them based on severity and impact.

Severity	Vulnerability	Description	Recommended Action
High	Ruby REXML 3.3.3 < 3.4.2 DoS vulnerability	Denial of Service vulnerability due to parsing issue	Update REXML gem to version 3.4.2
Info	Apache HTTP Server Installed	Detected Apache HTTP Server 2.4.65 installed	Ensure latest version and disable if u
Info	Node.js Installed	Detected Node.js version 20.19.5 installed	Keep it updated regularly.
Info	OpenSSL Installed	Multiple OpenSSL versions detected	Remove older or unused versions.
Info	Reachable IPv6 Address	Host may be reachable via global IPv6 address	Disable unused IPv6 interfaces.

Recommendations:
- Regularly update system packages and libraries.
- Patch Ruby REXML library to latest version (≥ 3.4.2).
- Disable or secure unused services like Apache and Nginx.
- Review IPv6 settings and disable global access if not required.
- Conduct periodic vulnerability scans (monthly or after major updates).

Conclusion:
The vulnerability scan was successfully completed using Nessus Essentials. The overall system appears secure with only one high-severity issue (Ruby REXML DoS). Most findings were informational. Applying timely updates and maintaining good patch management practices will ensure continued system security.