Vulnerability Scan Report

Eleyate Cyber Security Internship - Task 3

Prepared by: Sujay Vegi

Date: May 29, 2025

1. Introduction

This report documents the process and findings of a basic vulnerability scan performed on a personal computer as part of Task 3 for the Eleyate Cyber Security Internship. The objective was to use a free vulnerability scanning tool to identify common vulnerabilities, assess their severity, and propose mitigations. The scan was conducted using OpenVAS Community Edition, and this report includes the scan results, critical vulnerabilities, and recommended remediation steps.

2. Methodology

The vulnerability scan was performed following these steps:

1. Tool Installation: OpenVAS Community Edition was installed from https://www.openvas.org.
2. Scan Configuration: The scan target was set to the local machine (IP: 127.0.0.1). A full vulnerability scan profile was selected.
3. Scan Execution: The scan was initiated and ran for approximately 45 minutes, scanning for known vulnerabilities.
4. Result Analysis: The report was reviewed to identify vulnerabilities and assess their severity.
5. Mitigation Research: Fixes were researched using online resources and vendor advisories.

3. Scan Results

The vulnerability scan identified 28 vulnerabilities:

- Critical: 2

- High: 5
- Medium: 10
- Low: 11

4. Critical Vulnerabilities

1. Outdated OpenSSL Version:

   - Description: OpenSSL 1.1.1 is outdated and vulnerable to known exploits.
   - CVSS Score: 9.8
   - Impact: Remote code execution possible.
   - Mitigation: Upgrade to the latest OpenSSL version.

2. Open Port 445 (SMBv1):

   - Description: SMBv1 is enabled and susceptible to EternalBlue exploit.
   - CVSS Score: 9.3
   - Impact: Can lead to system compromise.
   - Mitigation: Disable SMBv1 and close port 445.

5. Recommendations

- Keep operating systems and software up to date.
- Configure the firewall to block unnecessary ports.
- Perform monthly vulnerability scans.
- Educate users to avoid untrusted downloads and enable auto-updates.

6. Conclusion

The scan provided crucial insights into the security of the system. It highlighted the importance of regular vulnerability assessments and proactive remediation. Tools like OpenVAS are essential in maintaining a secure computing environment.

7. References

- OpenVAS: https://www.openvas.org

- CVSS: https://www.first.org/cvss

- Nessus Essentials: https://www.tenable.com/products/nessus/nessus-essentials