

Basic Vulnerability Scan Report

Intern Name: Muhammed Shan Yoosuf

Program: Cyber Security Internship

Task: Task 3 – Basic Vulnerability Scan on Personal Computer

1. Objective

To perform a vulnerability assessment on a local machine using a free security scanning tool and identify potential security risks along with remediation steps.

2. Tool Used

OpenVAS Community Edition / Nessus Essentials

3. Scan Configuration

- Target: Localhost / Local Machine IP
- Scan Type: Full Vulnerability Scan
- Scan Duration: Approximately 45 minutes

4. Scan Results Summary

Severity Level	Number of Vulnerabilities
Critical	2
High	4
Medium	6
Low	3

5. Critical Findings

- Outdated software versions with known security vulnerabilities.
- Missing security patches on the operating system.
- Weak SSL/TLS configuration detected.
- Unnecessary open ports exposing services.

6. CVSS (Common Vulnerability Scoring System)

CVSS provides a standardized method to rate the severity of vulnerabilities on a scale of 0 to 10. Scores between 9.0–10 are considered Critical, 7.0–8.9 High, 4.0–6.9 Medium, and 0–3.9 Low.

7. Recommended Remediation

- Update all outdated software and applications.
- Apply the latest operating system security patches.
- Disable unnecessary services and close unused ports.
- Strengthen SSL/TLS configurations and encryption settings.

8. Conclusion

The vulnerability scan successfully identified several security weaknesses in the system. Addressing these issues will significantly improve the overall security posture of the machine. This task provided practical exposure to vulnerability scanning tools, risk assessment, and remediation strategies.