Vulnerability Assessment Report

Task Title: Introductory Vulnerability Assessment using OpenVAS/Nessus  
Date: [26/6/2025]  
Submitted by: [Keerthivasan E]

# Objective

The objective of this task was to perform a basic vulnerability assessment on my local machine using either OpenVAS or Nessus Essentials. The goal was to identify common security vulnerabilities, understand the associated risks, and learn how to mitigate them.

# Tools Used

Scanner Tool: OpenVAS / Nessus Essentials

Target: Localhost (127.0.0.1) or Local Machine IP

Operating System: [e.g., Windows 10 / Ubuntu 22.04]

# Steps Followed

1. Installed the chosen vulnerability scanner (OpenVAS or Nessus Essentials) by following the official setup guide.

2. Configured the scan target as my own system IP address or localhost.

3. Started a full system vulnerability scan to detect any potential risks.

4. The scan took around 45 to 60 minutes to complete.

5. Once completed, I reviewed the scan report for identified vulnerabilities and their severity levels.

6. Researched simple mitigation steps for the detected issues.

7. Noted down the most critical vulnerabilities found in the scan.

8. Took relevant screenshots of the scan results as evidence.

# Findings & Fixes

Some of the vulnerabilities found included open ports, outdated services, and weak configurations like anonymous access or missing security updates. Basic fixes like applying system updates, disabling anonymous access, and closing unused ports were suggested.

# Conclusion

This hands-on experience gave me a better understanding of how vulnerability scanning tools work and the kinds of security risks that commonly exist in personal or local systems. It also helped me learn how to research and apply basic security fixes.