Vulnerability Assessment Report

# Task Overview

This report documents the execution of a full vulnerability scan using OpenVAS on a local Kali Linux virtual machine.   
The task was conducted to fulfill the following requirements:

1. Install OpenVAS or Nessus Essentials.  
2. Set up scan target as your local machine IP or localhost.  
3. Start a full vulnerability scan.  
4. Wait for scan to complete (may take 30–60 mins).  
5. Review the report for vulnerabilities and severity.  
6. Research simple fixes or mitigations for found vulnerabilities.  
7. Document the most critical vulnerabilities.  
8. Take screenshots of the scan results.

# Scan Summary

Scan Tool Used: OpenVAS (Greenbone Vulnerability Manager)

Scan Configuration: Full and Fast

Scan Target: 127.0.0.1 (localhost)

Scanner: OpenVAS Default

Scan Status: Completed

Scan Start Time: 2025-05-31 08:59:37

Scan End Time: 2025-05-31 09:06:08

Total Scan Duration: 0:06:31

# Vulnerability Summary

Total Results: 23

High Severity: 0

Medium Severity: 1

Low Severity: 0

Warnings/Logs: 24 (1 warning, 23 log-level messages)

Overall Severity Score: 5.9

# Most Critical Vulnerabilities

Based on the scan results, the most notable finding was a medium-severity vulnerability.

Since the scan did not detect any high or critical severity vulnerabilities, only one medium issue is considered significant.

Example Vulnerability:  
- Name: TLS Version 1.0 Protocol Detection  
- Severity: Medium  
- Description: The TLS 1.0 protocol was detected on this host. TLS 1.0 is considered insecure and has been deprecated.  
- Fix: Disable TLS 1.0 in server configuration and enforce usage of TLS 1.2 or higher.

# Screenshots

Screenshots of the GVM web interface, scan task, and report should be included here.