OpenVAS Vulnerability Report

Date: 29-10-2025

Target System: Metasploitable2 VM (Test Environment)

Scanner Used: Greenbone Vulnerability Management (GVM/OpenVAS)

1. Scan Overview:

- Scan Type: Full and fast vulnerability scan
- Target IP: 192.168.56.101
- Scan Duration: ~45 minutes
- Total Vulnerabilities Detected: 87
  - Critical: 12
  - High: 24
  - Medium: 31
  - Low: 20

2. Key Findings Summary

Severity	Example Vulnerabilities	Affected Services
Critical	Remote Code Execution (RCE), Unauthenticated Access	FTPd,Samba,Apache
High	SQL Injection, Weak SSH Keys	MySQL, SSH
Medium	Outdated Packages, Directory Listing Enabled	Apache, PHP
Low	Missing Security Headers, Open Ports	HTTP, Telnet

3. Notable Vulnerabilities

Remote Code Execution via vsFTPd v2.3.4

- Description: Backdoor vulnerability allowing shell access.
- CVSS Score: 10.0 (Critical)
- Recommendation: Disable vsFTPd or upgrade to a secure version.

Samba Usermap Script Exploit:

- Description: Allows privilege escalation via crafted usermap script.

- CVSS Score: 9.8 (High)
- Recommendation: Apply latest Samba patches and restrict anonymous access.

Apache Directory Listing:

- Description: Directory contents exposed due to misconfiguration.
- CVSS Score: 5.3 (Medium)
- Recommendation: Disable directory listing in Apache config.

4. Tools & Methodology

- Scanner: OpenVAS via GVM interface on Kali Linux
- Target: Metasploitable2 VM (VirtualBox NAT network)
- Pre-Scan Checks: Nmap used to identify open ports and services
- Post-Scan Analysis: Vulnerabilities categorized by severity and mapped to CVEs

5. Suggested Fixes & Mitigation

Vulnerability	Fix Recommendation	Priority
vsFTPd RCE	Remove or upgrade service	Critical
Samba Exploit	Patch and restrict access	High
SQL Injection	Sanitize inputs, update DB	High
Apache Issues	Reconfigure server settings	Medium

6.Conclusion

This vulnerability assessment highlights critical exposures in the test environment, simulating real-world attack surfaces. The findings demonstrate proficiency in using OpenVAS, interpreting results, and recommending actionable fixes. This report aligns with GRC principles and supports risk-based remediation planning.