OpenVAS Vulnerability Scanning Lab – Cybersecurity Home Lab Project

# Overview

In this lab, I performed a clean installation and configuration of Greenbone’s OpenVAS Community Edition on Kali Linux. The goal was to simulate a real-world vulnerability scanning workflow using a dedicated vulnerability scanner in a virtualized lab environment. This setup serves as a foundational exercise in vulnerability management and network security assessment.

# Objectives

• Reinstall and configure OpenVAS (GVM) Community Edition  
• Troubleshoot service, socket, and database issues  
• Perform full vulnerability scans against a test subnet  
• Analyze scan results for detection coverage and accuracy

# Lab Setup

## Environment

• Host Machine: VirtualBox  
• OS: Kali Linux (latest updates applied)  
• Targets: Metasploitable 2, Kali Linux, and other local VMs  
• Network Setup:  
 - NAT Adapter (for initial setup and package updates)  
 - Internal Network (`intnet`) for isolated scanning

# Configuration Steps

• Performed `sudo apt update && sudo apt upgrade -y` to resolve potential missing dependencies  
• Cleanly reinstalled OpenVAS and GVM packages  
• Ran `sudo gvm-setup` to initialize GVM components  
• Used `gvm-check-setup` to validate installation and identify missing data  
• Synced missing feeds using:  
 - `sudo greenbone-feed-sync --type scap`  
• Verified services were running properly:  
 - `gvmd`  
 - `ospd-openvas`  
• Confirmed socket file permissions and GMP compatibility  
• Created and launched a full vulnerability scan against the internal lab subnet  
• Validated scan config availability (e.g., Full and Fast)

# Challenges Faced

• PID file and socket access issues with `gvmd`  
• Broken GMP compatibility and missing scanner version errors  
• Failed XML command execution due to outdated `gvm-cli` usage  
• Incomplete scan config population due to failed feed sync  
• \_gvm user permissions and limited sudo access caused operational delays

# Outcome

• Successfully completed a full scan using "Full and Fast" profile  
• Discovered and confirmed partial vulnerabilities on Metasploitable 2  
• Learned how OpenVAS integrates with `ospd-openvas`, Redis, and PostgreSQL  
• Gained experience with systemd, socket permissions, and scan tuning

# Future Enhancements

• Explore creating custom scan configurations  
• Integrate email alerting and scan scheduling  
• Expand target variety to include Windows hosts and web apps  
• Consider pairing OpenVAS with a SIEM like Wazuh for correlation

Author

Luis C. – Cybersecurity Student | Home Lab Enthusiast