Task 3: Vulnerability Assessment Using OpenVAS

Task Objective:

To set up and demonstrate a basic vulnerability scan on a local system using OpenVAS (Greenbone Vulnerability Manager). The scan process should include installation, configuration of the scanner, creation of scan target and task, and ideally execution of a scan to identify security vulnerabilities in the system.

Tool Used:

- OpenVAS / GVM (Greenbone Vulnerability Management)
- System: Kali Linux (Dual Boot)
- GVM Version: 25.x (2024+)
- Scanner Version: OpenVAS 23.20.1
- Database: PostgreSQL 17.5
- Interface: Web GUI at https://127.0.0.1:9392

What is OpenVAS?

OpenVAS is a powerful open-source vulnerability scanner used to assess system and network security. It detects vulnerabilities in services, ports, and applications by using regularly updated vulnerability feeds and scan configurations.

Steps Performed

1. Installation & Setup

Installed OpenVAS via Kali's default packages using **gvm-setup**. Fixed PostgreSQL collation issues by recreating the gvmd database and refreshing system collations.

2. Feed Synchronization

Successfully synced GVMD_DATA, SCAP, and CERT feeds using **greenbone-feed-sync** commands.

3. User Creation & Access

Logged into OpenVAS Web UI with admin user created during setup.

4. Scanner Setup & Verification

Verified OpenVAS scanner is alive using **gvmd --verify-scanner** and confirmed socket path.

5. Target and Task Creation

Created target 127.0.0.1 and scan task with Full and Fast / Base config and linked scanner.

Problem Faced: Scan Button Disabled

Despite valid configuration, the green 'Start' () button remained disabled. Tried multiple fixes including service restarts, XML scan config import, and gvmd rebuild. Issue matches a known UI-desync bug in GVM 25.x on Kali Linux.

Summary of Actions Taken

Task	Status
OpenVAS Installation	✓Done
PostgreSQL Fix & Recreation	✓Done
Feed Synchronization	✓Done
Admin Login	✓Done
Scanner Verification	✓Done
Target Creation	✓Done
Scan Task Creation	✓Done
Scan Execution	✗Failed (UI bug in GVM 25.x)

Learning Outcome

Understood GVM architecture, resolved real-world setup issues, and performed scanner validation and scan task creation. Learned feed management and how to troubleshoot common GVM bugs even though scan execution did not succeed.

Suggested GitHub Structure:

task-3-vulnerability-scan/

```
├── screenshots/
│   ├── target_created.png
│   ├── task_created.png
│   ├── scanner_verified.png
│   └── gvmd_get_scanners.png
│   └──so on…..
├── report.pdf ← (this file)
```

Commands Summary (for Review)

```
# Setup and Install
sudo apt update && sudo apt install openvas -y
sudo gvm-setup

# PostgreSQL Fix
sudo runuser -u postgres -- dropdb gvmd
sudo -u postgres psql -c "ALTER DATABASE template1 REFRESH COLLATION VERSION;"
sudo -u postgres psql -c "ALTER DATABASE postgres REFRESH COLLATION VERSION;"
sudo runuser -u postgres -- /usr/share/gvm/create-postgresql-database

# Feed Sync
sudo runuser -u _gvm -- greenbone-feed-sync --type GVMD_DATA
sudo runuser -u _gvm -- greenbone-feed-sync --type SCAP
sudo runuser -u _gvm -- greenbone-feed-sync --type CERT

# Restart Services
sudo gvm-stop
sudo pkill ospd-openvas
sudo gvm-start

# Scanner Check
sudo runuser -u _gvm -- gvmd --get-scanners
sudo runuser -u _gvm -- gvmd --verify-scanner=<UUID>



# Rebuild and Config Import
sudo runuser -u _gvm -- gvmd --rebuild
sudo runuser -u _gvm -- gvmd --create-config=/var/lib/gvm/data-
objects/gvmd/202*/configs/full-and-fast.xml
```

```
# Clean Feed Sync Flags
sudo rm -f /var/lib/gvm/gvmd/*_sync.status
```