Task 3

Vulnerability Assessment Report

Tool Used: Greenbone Vulnerability Manager (OpenVAS)

Prepared For: Internal Security Review

1. Executive Summary

A vulnerability assessment was conducted against host 192.168.36.147 using Greenbone/OpenVAS.
The scan identified 22 confirmed vulnerabilities (out of 370 checks performed).

- Critical Findings (Severity 10.0): 2
- High Findings (Severity 7.0 – 9.9): 4
- Medium Findings (Severity 4.0 – 6.9): 12
- Low/Informational: Not detailed in this report

The vulnerabilities discovered include Remote Code Execution (RCE), SQL Injection, unauthenticated file access, weak cryptography, and use of deprecated libraries. Immediate remediation is required, especially for the ProFTPD mod_copy and Drupal RCE vulnerabilities, both rated Critical (10.0).

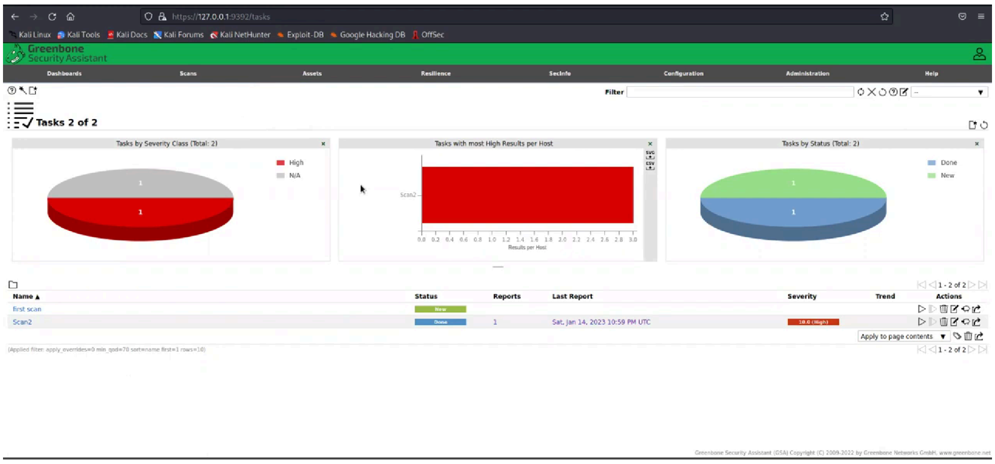
2. Methodology

1. **Tool: Greenbone Vulnerability Manager (OpenVAS)**

2. **Target: `192.168.36.147`**

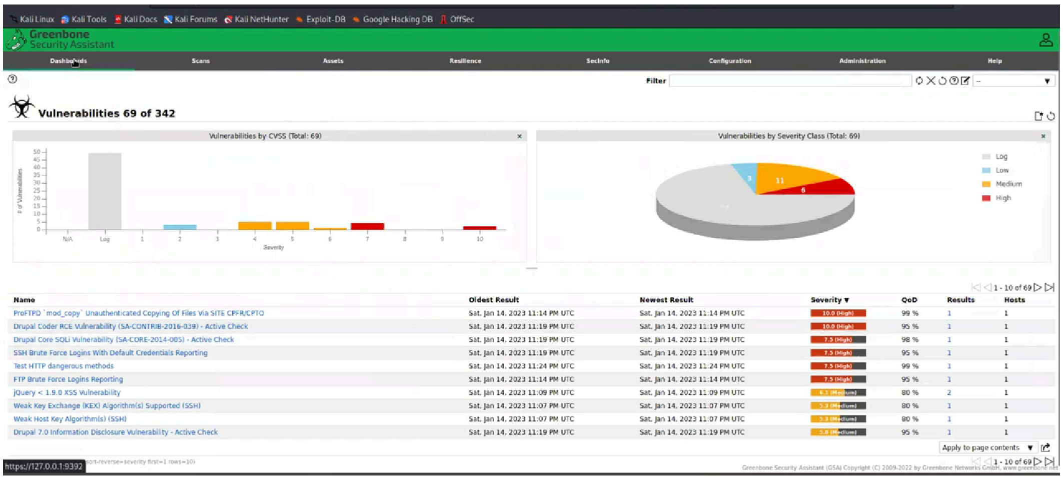
3. **Scope:**
   - **Open ports: 21 (FTP), 22 (SSH), 80 (HTTP), 631 (IPP/HTTP printing)**
   - **Applications detected: Drupal CMS, ProFTPD, jQuery, SSH services**

4. **Approach:**
   - **Full port and service enumeration**
   - **Active checks for known CVEs and misconfigurations**
   - **Verification of encryption and authentication mechanisms**



Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
first scan	New					
Scan2	Done	1	Sat, Jan 14, 2023 10:59 PM UTC	10.0 (High)		

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)



Name	Oldest Result	Newest Result	Severity ▼	QoD	Results	Hosts
ProFTPD `mod_copy` Unauthenticated Copying Of Files Via SITE CPFR/CPTO	Sat, Jan 14, 2023 11:14 PM UTC	Sat, Jan 14, 2023 11:14 PM UTC	10.0 (High)	99 %	1	1
Drupal Coder RCE Vulnerability (SA-CONTRIB-2016-039) - Active Check	Sat, Jan 14, 2023 11:19 PM UTC	Sat, Jan 14, 2023 11:19 PM UTC	10.0 (High)	95 %	1	1
Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check	Sat, Jan 14, 2023 11:19 PM UTC	Sat, Jan 14, 2023 11:19 PM UTC	7.5 (High)	98 %	1	1
SSH Brute Force Logins With Default Credentials Reporting	Sat, Jan 14, 2023 11:19 PM UTC	Sat, Jan 14, 2023 11:19 PM UTC	7.5 (High)	95 %	1	1
Test HTTP dangerous methods	Sat, Jan 14, 2023 11:24 PM UTC	Sat, Jan 14, 2023 11:24 PM UTC	7.5 (High)	99 %	1	1
FTP Brute Force Logins Reporting	Sat, Jan 14, 2023 11:14 PM UTC	Sat, Jan 14, 2023 11:14 PM UTC	7.5 (High)	95 %	1	1
jQuery < 1.9.0 XSS Vulnerability	Sat, Jan 14, 2023 11:09 PM UTC	Sat, Jan 14, 2023 11:09 PM UTC	6.1 (Medium)	80 %	2	1
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	Sat, Jan 14, 2023 11:07 PM UTC	Sat, Jan 14, 2023 11:07 PM UTC	5.3 (Medium)	80 %	1	1
Weak Host Key Algorithm(s) (SSH)	Sat, Jan 14, 2023 11:07 PM UTC	Sat, Jan 14, 2023 11:07 PM UTC	5.3 (Medium)	80 %	1	1
Drupal 7.0 Information Disclosure Vulnerability - Active Check	Sat, Jan 14, 2023 11:19 PM UTC	Sat, Jan 14, 2023 11:19 PM UTC	5.0 (Medium)	95 %	1	1

sort-reverse=severity first=1 rows=10)

3. Key Findings

Critical Vulnerabilities

Vulnerability	Severity	Affected Service/Port	Description
ProFTPD mod_copy – Unauthenticated File Copying (CVE-2015-3306)	10.0 (Critical)	FTP (21/tcp)	Allows attackers to copy files to arbitrary locations without authentication. Can lead to privilege escalation or service compromise.
Drupal Coder Module RCE (SA-CONTRIB-2016-039)	10.0 (Critical)	HTTP (80/tcp)	Remote Code Execution vulnerability in Drupal contributed module. Exploitation allows full takeover of the CMS.

High Vulnerabilities

Vulnerability	Severiy	Affected Service/Port	Description
HTTP Dangerous Methods Enabled	7.5 (High)	HTTP (80/tcp)	Methods like PUT/DELETE are enabled, allowing attackers to upload or modify files.
SSH Default/Weak Credentials (Brute Force Possible)	7.5 (High)	SSH (22/tcp)	Scanner detected possibility of brute force with default usernames/passwords.
Drupal Core SQL Injection (SA-CORE-2014-005)	7.5 (High)	HTTP (80/tcp)	SQL injection flaw in Drupal, allowing attackers to extract or manipulate database data.
FTP Brute Force / Weak Credentials	7.5 (High)	FTP (21/tcp)	FTP service susceptible to brute force attacks due to weak or default credentials.

Medium Vulnerabilities

- **jQuery < 1.9.0 – XSS Vulnerabilities → Outdated JavaScript library exposes site to DOM-based XSS.**
- **Weak Host Keys & Key Exchange Algorithms in SSH → Reduces confidentiality of sessions.**
- **Sensitive File Disclosure (HTTP) → Webserver exposes sensitive files.**
- **Cleartext Transmission of Credentials (FTP/HTTP) → Usernames & passwords transmitted without encryption.**
- **SSL/TLS Deprecated Versions (TLSv1.0, TLSv1.1) → Enables downgrade attacks and weak encryption.**

---

4. Risk Analysis

- Business Impact: Successful exploitation of RCE vulnerabilities can lead to complete system compromise, data exfiltration, and lateral movement inside the network.
- Likelihood: High, as services are accessible and misconfigured.
- Overall Risk Rating: Critical (requires urgent remediation).

---

5. Recommendations

Immediate Actions (0–3 Days)

- Disable FTP (ProFTPD) or patch/remove `mod_copy` module. Replace with secure alternatives (SFTP/FTPS).

- Patch/Upgrade Drupal core and all modules. If module is deprecated, remove it.

- Disable HTTP dangerous methods (PUT/DELETE/TRACE). Restrict to GET/POST only.

- Reset and enforce strong credentials. Remove default logins, enforce key-based SSH authentication.
  .

---

6. Conclusion

The scan results show that the system is highly vulnerable, with multiple critical and high-risk issues.
If left unpatched, attackers can gain unauthorized access, execute arbitrary code, steal data, or pivot further into the network.

Urgent remediation is mandatory.
The security team should address critical issues first, then proceed with medium risks, and finally perform a full re-scan for verification.

OpenVAS (GVM) Installation Guide

Step 1: Install Greenbone Vulnerability Manager

```
sudo apt update && sudo apt upgrade -y
sudo apt install -y gvm
```

Step 2: Initialize and Setup

```
sudo gvm-setup
sudo gvm-start
```

- This creates the default admin account and downloads the vulnerability feeds.

Step 3: Verify Installation

```
sudo gvm-check-setup
```

Step 4: Access Web Interface

- Open browser → `https://127.0.0.1:9392`
- Login with the admin credentials created during setup.

Step 5: (Optional) Sync Feeds Manually

```
sudo greenbone-nvt-sync
sudo greenbone-scapdata-sync
sudo greenbone-certdata-sync
```
