

# Vulnerability Assessment & Penetration Testing (VAPT) Report

## 1. Executive Summary

### 1.1 Purpose

This assessment was conducted to identify security vulnerabilities in a deliberately vulnerable system (Metasploitable 3) using open-source security tools.

### 1.2 Summary of Findings

- Multiple **High** and **Medium** risk vulnerabilities were identified.
- Several services were unnecessarily exposed.
- Weak configurations increased the risk of remote exploitation.

## 2. Objective & Scope

### 2.1 Objective

- Perform Vulnerability Assessment and basic Penetration Testing using open-source tools.
- Understand real-world VAPT workflow and reporting.

### 2.2 Scope

- **Target:** Metasploitable 3
- **Testing Type:**
  - Vulnerability Assessment
  - Limited Penetration Testing (non-destructive)

## 3. Testing Environment Setup

### 3.1 Virtual Environment

- **Virtualization:** VMware
- **Attacker Machine:** Kali Linux
- **Target Machine:** Metasploitable 3

### 3.2 Network Configuration

- NAT network



### 3.3 IP Identification

- **Command used:** *ip a*
- Kali Linux IP: 192.168.72.139

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c2:b8:f7 brd ff:ff:ff:ff:ff:ff
        inet 192.168.72.139/24 brd 192.168.72.255 scope global dynamic noprefixroute eth0
            valid_lft 1765sec preferred_lft 1765sec
        inet6 fe80::20c:29ff:fed2:b8f7/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
```

Fig-1

- Metasploitable IP: 192.168.72.140

```
vagrant@metasploitable3-ub1404:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:b6:2e:3a brd ff:ff:ff:ff:ff:ff
        inet 192.168.72.140/24 brd 192.168.72.255 scope global eth0
            valid_lft forever preferred_lft forever
        inet6 fe80::20c:29ff:feb6:2e3a/64 scope link
            valid_lft forever preferred_lft forever
```

Fig-2

## 4. VAPT Methodology Followed

### 4.1 Phases:

1. **Planning:** Defined scope and target IP
2. **Discovery:** Nmap and Nikto scans
3. **Assessment:** OpenVAS vulnerability scanning
4. **Reporting:** Findings documented using Dradis CE and spreadsheets



## 5. Tools Used

Tool	Purpose
Nmap	Port and service discovery
Nikto	Web vulnerability scanning
OpenVAS	Automated vulnerability assessment
Dradis CE	Centralized documentation & reporting
Spreadsheet	Risk tracking
VMware	Virtual lab
Metasploitable 3	Vulnerable target system

## 6. Vulnerability Assessment Results

### 6.1 Nmap

- Multiple open ports detected
- FTP, SSH, and HTTP services exposed
- **Command used:** `nmap -Pn 192.168.72.140`

```
(kali㉿kali)-[~]
$ nmap -Pn 192.168.72.140
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-22 19:40 IST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 19:40 (0:00:00 remaining)
Nmap scan report for 192.168.72.140
Host is up (0.00066s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3000/tcp  closed ppp
3306/tcp  open  mysql
8080/tcp  closed http-proxy
8181/tcp  closed intermapper
MAC Address: 00:0C:29:B6:2E:3A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.77 seconds
```

Fig-3



## 6.2 Nikto

- Outdated web server
- Missing security headers
- Potential web vulnerabilities
- **Command used:** `nikto -h http://192.168.72.140`

```
(kali㉿kali)-[~]
$ nikto -h http://192.168.72.140
 Nikto v2.5.0

+ Target IP:      192.168.72.140
+ Target Hostname: 192.168.72.140
+ Target Port:    80
+ Start Time:    2025-12-22 19:48:44 (GMT+5.5)

Server: Apache/2.4.7 (Ubuntu)
/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
/: The X-Content-Type-Options header is not present. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/headers/x-content-type-options/
//: Directory indexing found.
Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
OPTIONS: Allows HTTP Methods: GET, HEAD, POST, OPTIONS .
//: Directory indexing found.
//: Open directory browsing: a directory allows indexing.
//: Directory indexing found.
//: Apache on Red Hat Linux release 9 reveals the root directory listing by default if there is no index page.
//: Directory indexing found.
//: Weblogic allows source code or directory listing, upgrade to v6.0 SPI or higher. See: http://www.securityfocus.com/bid/2513
//: Directory indexing found.
//: Directory indexing found.
//: PageServices: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
//: /wp-cs-dump: The remote server may allow directory listings through Web Publisher by forcing the server to show all files via 'open directory browsing'. Web Publisher should be disabled. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0269
org/cgi-bin/cvename.cgi?name=CVE-1999-0269
/phpmyadmin/ChangeLog.php: Apache is powered by header: PHP/5.4.5.
//: /phpMyAdmin: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
//: /phpMyAdmin: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
//: /phpMyAdmin: phpMyAdmin directory found.
//: /phpMyAdmin: Apache default file found. See: https://www.vmtweb.co.uk/apache-restricting-access-to-iconreadme/
//: /phpMyAdmin: phpMyAdmin directory found.
//: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
//: /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
//: 0/11 requests: 0 error(s) and 11 warning(s) reported on remote host
End Time:   2025-12-22 19:49:02 (GMT+5.5) (18 seconds)

+ 1 host(s) tested
```

Fig-4

## 6.3 OpenVAS

- High and Medium severity vulnerabilities identified
- CVE IDs and CVSS scores obtained
- OpenVAS was started using the command: `sudo gym-start`

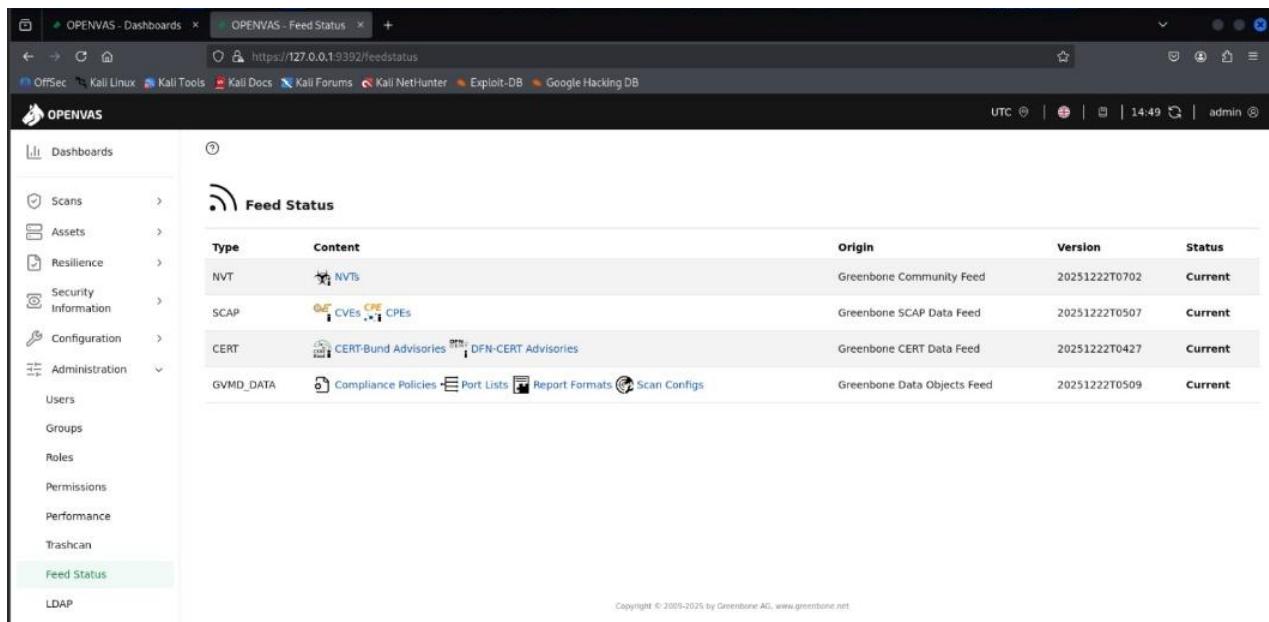
### 6.3.1 Target Creation

- After launching the Greenbone interface, a **target** was created using the Metasploitable 3 IP address.

The screenshot shows the OpenVAS Targets interface. On the left, a sidebar menu includes 'Dashboards', 'Scans', 'Assets', 'Resilience', 'Security Information', 'Configuration', 'Targets' (which is selected), 'Port Lists', 'Credentials', 'Scan Configs', 'Alerts', 'Schedules', 'Report Configs', 'Report Formats', and 'Scanners'. The main content area displays a table titled 'Targets 1 of 1'. The table has columns: Name, Hosts, IPs, Port List, Credentials, and Actions. One entry is listed: 'Metasploitable TCP Scan (TCP Scan)' with 'Hosts' set to '192.168.72.140', 'IPs' set to '1', and 'Credentials' set to 'All IANA assigned TCP'. At the bottom of the table, it says '(Applied filter: sort=name first=1 rows=10)'. The footer of the browser window shows 'https://127.0.0.1:9392/targets' and the status 'UTC | 14:55 | admin'.

Fig-5

### 6.3.2 Feed Status



The screenshot shows the 'Feed Status' section of the OPENVAS web interface. On the left, there's a sidebar with links like Dashboards, Scans, Assets, Resilience, Security Information, Configuration, Administration, Users, Groups, Roles, Permissions, Performance, Trashcan, Feed Status (which is highlighted), and LDAP. The main content area is titled 'Feed Status' and lists four types of feeds:

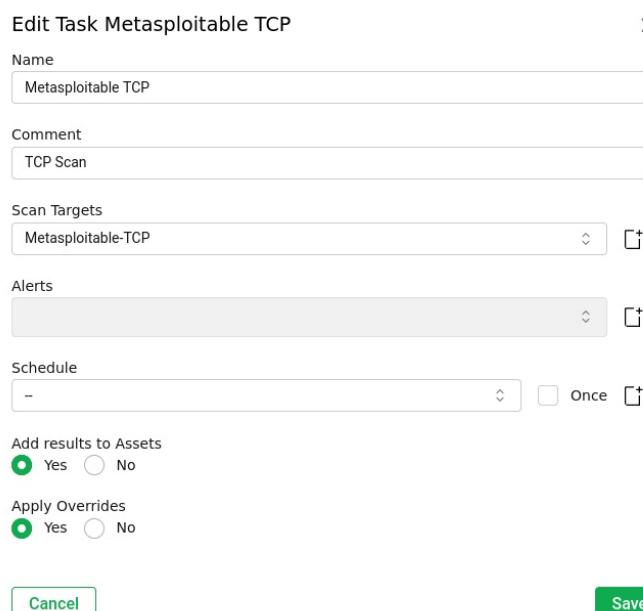
Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20251222T0702	Current
SCAP	CVEs, CPEs	Greenbone SCAP Data Feed	20251222T0507	Current
CERT	CERT-Bund Advisories, DFN-CERT Advisories	Greenbone CERT Data Feed	20251222T0427	Current
GVMD_DATA	Compliance Policies, Port Lists, Report Formats, Scan Configs	Greenbone Data Objects Feed	20251222T0509	Current

At the bottom right of the main content area, it says 'Copyright © 2009-2025 by Greenbone AG, www.greenbone.net'.

**Fig-6**

### 6.3.3 Task Creation & Execution

- A scan task was then created and executed using a Full and Fast scan profile.



The screenshot shows the 'Edit Task Metasploitable TCP' dialog. It includes fields for Name (Metasploitable TCP), Comment (TCP Scan), Scan Targets (Metasploitable-TCP), Alerts, Schedule (set to Once), and two sections at the bottom: 'Add results to Assets' (Yes selected) and 'Apply Overrides' (Yes selected). At the bottom are 'Cancel' and 'Save' buttons.

**Fig-7**

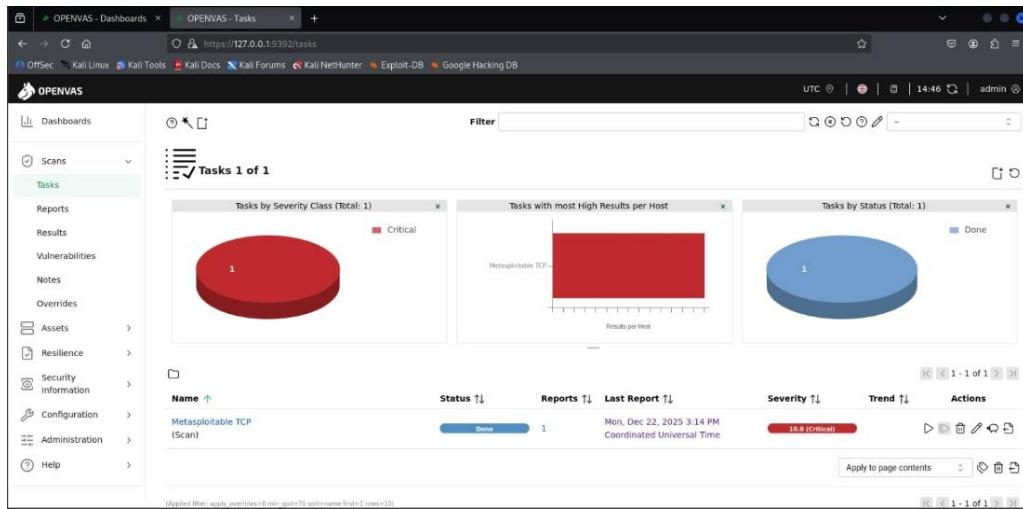


Fig-8

### 6.3.4 Scan Result

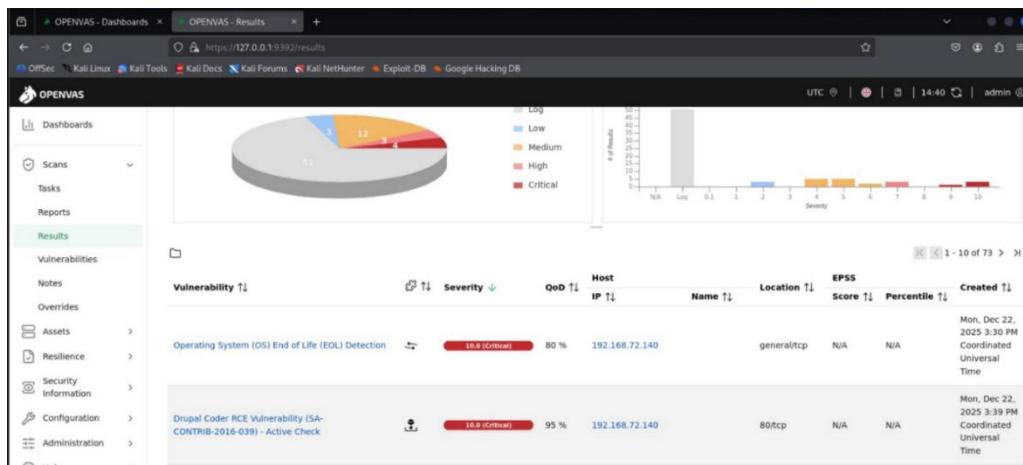


Fig-9

## 7. Risk Assessment

- CVSS scores were calculated from CVSS calculator.

### 1. OS End of Life (EOL) Detection

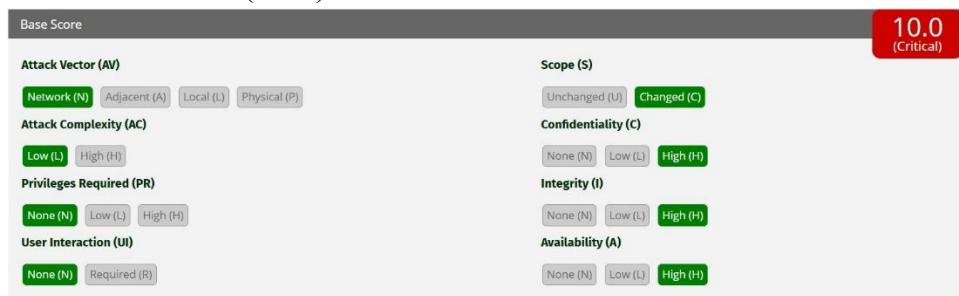


Fig-10



## 2. Drupal Coder RCE (CVE-2016-5385)

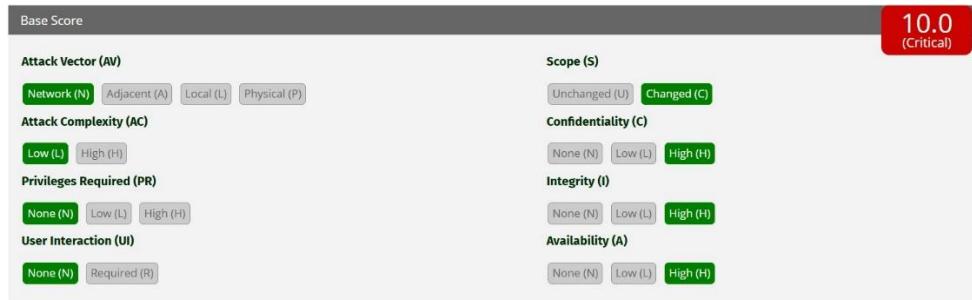


Fig-11

## 3. ProFTPD mod\_copy (CVE-2015-3306)

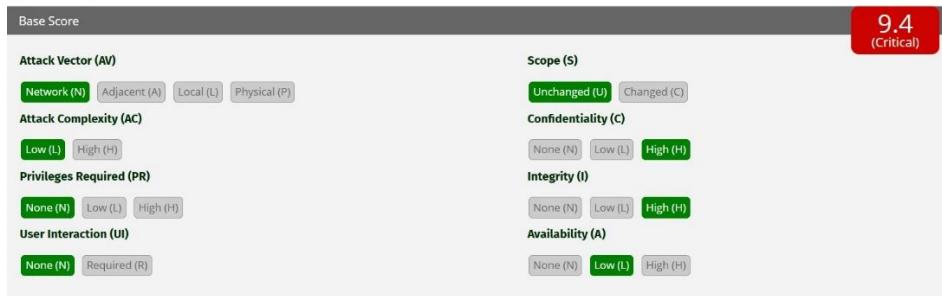


Fig-12

## 4. SSH Default Credentials



Fig-13

## 5. Drupal Core SQL Injection (CVE-2014-005)



Fig-14



## 6. HTTP Dangerous Methods

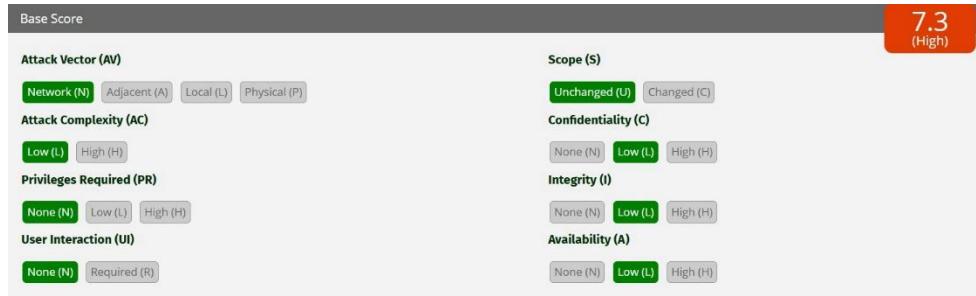


Fig-15

## 7. FTP Default Credentials

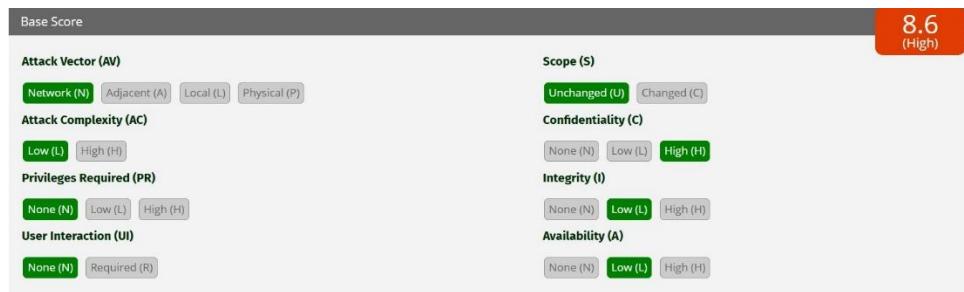


Fig-16

## 8. jQuery < 1.9.0 XSS

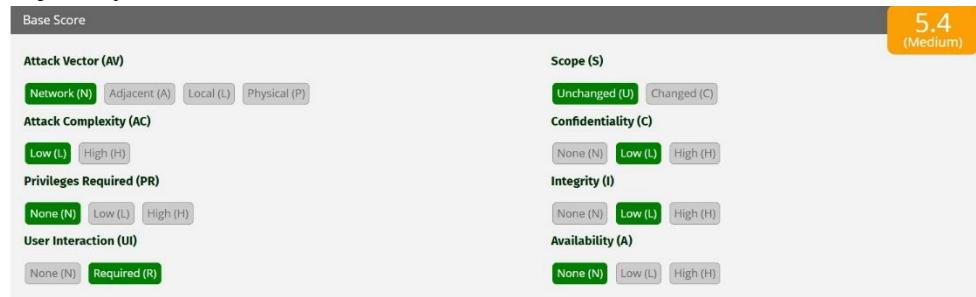


Fig-17

## 9. Weak SSH Host Key Algorithm

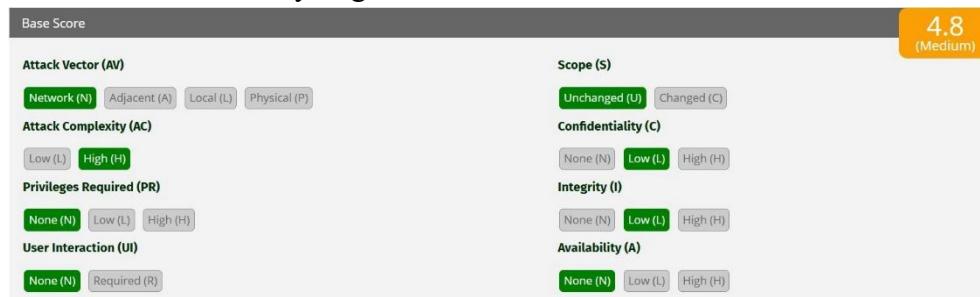


Fig-18



## 8. Vulnerability Spreadsheet

- Used Excel Sheet

Vulnerabilities										
Host IP	Vulnerability Name	CVE ID	Port / Service	CVSS	Likelihood	Impact	Risk Level	Recommendation	Status	
192.168.72.140	OS End of Life Detection	N/A	General	10	High	High	Critical	Upgrade OS to supported version	Open	
192.168.72.140	Drupal Coder RCE	CVE-2016-5385	80/tcp	10	High	High	Critical	Apply Drupal security updates	Open	
192.168.72.140	ProFTPD mod_copy File Copy	CVE-2015-3306	21/tcp	9.4	High	High	Critical	Disable mod_copy / update ProFTPD	Open	
192.168.72.140	SSH Default Credentials	N/A	22/tcp	9.8	High	High	Critical	Enforce strong credentials	Open	
192.168.72.140	Drupal Core SQL Injection	CVE-2014-005	80/tcp	9.4	High	Medium	Critical	Patch Drupal core	Open	
192.168.72.140	FTP Default Credentials	N/A	21/tcp	8.6	High	Medium	High	Change FTP credentials	Open	
192.168.72.140	HTTP Dangerous Methods	N/A	80/tcp	7.3	Medium	Medium	Medium	Disable unused methods	Open	
192.168.72.140	jQuery < 1.9.0 XSS	N/A	80/tcp	5.4	Medium	Medium	Medium	Upgrade jQuery	Open	
192.168.72.140	Weak SSH Host Key Algorithm	N/A	22/tcp	4.8	Low	Medium	Low	Use stronger SSH algorithms	Open	

Fig-19

## 9. 3x3 Risk Matrix & Risk Mapping

- Used Excel Sheet

### 9.1 3x3 Risk Matrix

#### 1. Likelihood

- Low – Hard to exploit
- Medium – Needs effort
- High – Easily exploitable

#### 2. Impact

- Low – Minimal effect
- Medium – Service disruption
- High – Full compromise

Risk Matrix Table			
Impact ↓ / Likelihood →	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Low	Low	Medium

Fig-20

### 9.2 Risk Mapping

Risk Mapping			
Vulnerability Name	Likelihood	Impact	Final Risk
OS End of Life Detection	High	High	Critical
Drupal Coder RCE	High	High	Critical
ProFTPD mod_copy File Copy	High	High	Critical
SSH Default Credentials	High	High	Critical
Drupal Core SQL Injection	High	Medium	High
FTP Default Credentials	High	Medium	High
HTTP Dangerous Methods	Medium	Medium	Medium
jQuery < 1.9.0 XSS	Medium	Medium	Medium
Weak SSH Host Key Algorithm	Low	Medium	Low

Fig-21

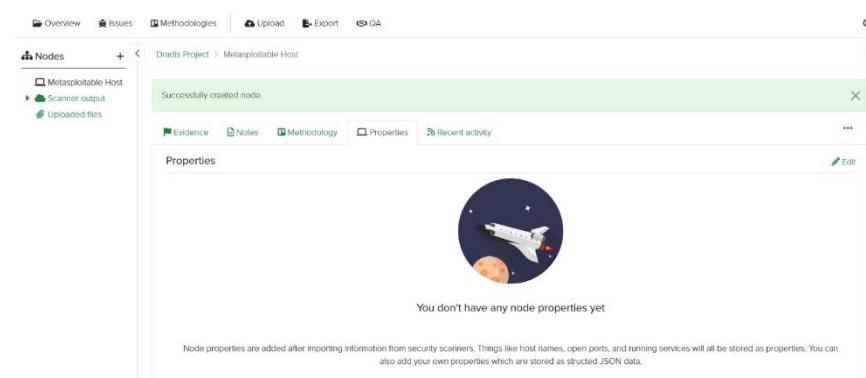
## 10. Documentation & Reporting

**Dradis Community Edition (CE)** was used as a centralized platform to document and organize vulnerability findings.

In Dradis, the following structure was maintained:

- **Node:** Target host
- **Issue:** Identified vulnerability
- **Evidence:** Scan output & vulnerability details

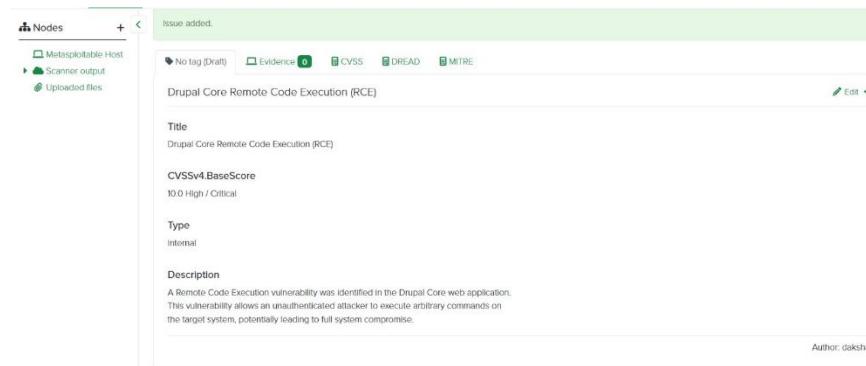
### 10.1 Node Created



The screenshot shows the Dradis CE interface. In the top navigation bar, there are links for Overview, Issues, Methodologies, Upload, Export, and GA. Below the navigation, a sidebar on the left lists 'Nodes' (Metasploitable Host), 'Scanner output', and 'Uploaded files'. The main content area shows a success message: 'Successfully created node.' A green bar at the bottom of the page also says 'Successfully created node.' Below the message, there's a tab bar with Evidence, Notes, Methodology, Properties, and Recent activity. The Properties tab is selected, showing a placeholder image of a space shuttle and the text 'You don't have any node properties yet'. A note below states: 'Node properties are added after importing information from security scanners. Things like host names, open ports, and running services will all be stored as properties. You can also add your own properties which are stored as structured JSON data.'

**Fig-22**

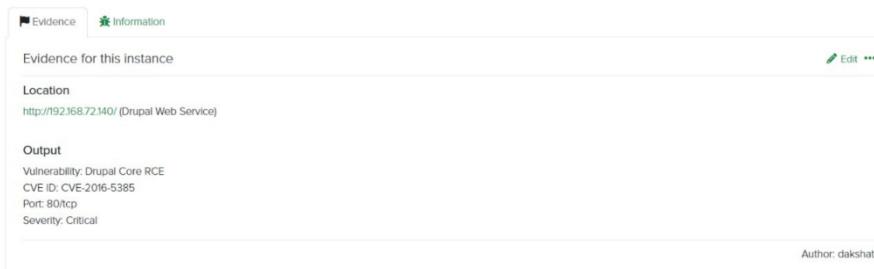
### 10.2 Issue Created



The screenshot shows the Dradis CE interface. In the top navigation bar, there are links for Overview, Issues, Methodologies, Upload, Export, and GA. Below the navigation, a sidebar on the left lists 'Nodes' (Metasploitable Host), 'Scanner output', and 'Uploaded files'. The main content area shows a success message: 'Issue added.' A green bar at the bottom of the page also says 'Issue added.' Below the message, there's a tab bar with No tag (Draft), Evidence, CVSS, DREAD, and MITRE. The Evidence tab is selected, showing the title 'Drupal Core Remote Code Execution (RCE)'. Below the title, there are sections for Title (Drupal Core Remote Code Execution (RCE)), CVSSv4.BaseScore (10.0 High / Critical), Type (Internal), and Description (A Remote Code Execution vulnerability was identified in the Drupal Core web application. This vulnerability allows an unauthenticated attacker to execute arbitrary commands on the target system, potentially leading to full system compromise.). At the bottom right, it says 'Author: dakshata'.

**Fig-23**

### 10.3 Evidence

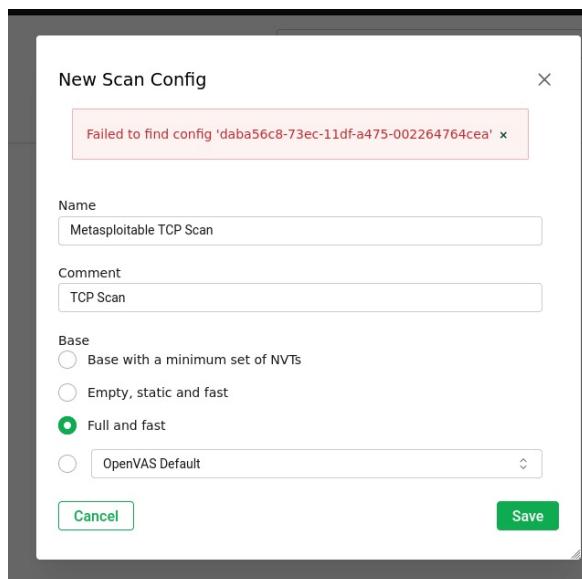


The screenshot shows the Dradis CE interface. In the top navigation bar, there are links for Evidence and Information. Below the navigation, a sidebar on the left lists 'Evidence for this instance', 'Location' (http://192.168.72.140/ (Drupal Web Service)), and 'Output'. The Output section contains details about the vulnerability: Vulnerability: Drupal Core RCE, CVE ID: CVE-2016-5385, Port: 80/tcp, and Severity: Critical. At the bottom right, it says 'Author: dakshata'.

**Fig-24**

## 11. Challenges Faced

**Challenge:** Missing Scan Configuration (Feed Sync Failure)



**Fig-25**

- **Issue:** Creating a scan using the default *Full and Fast* profile failed with the error: ***Failed to find config daba56c8-73ec-11df-a475-002264764cea.***
- **Impact:** Scan tasks could not be created due to the absence of a valid scan configuration.
- **Root Cause:** The gvmdb database was incomplete because the Greenbone Community Feed had not been synchronized after installation, resulting in missing NVTs and scan profiles.

## 12. Conclusion

This VAPT task provided practical exposure to vulnerability assessment, risk prioritization, and security documentation using open-source tools. The assessment highlights the importance of proactive security testing to identify and remediate vulnerabilities before exploitation.