📄 Vulnerability Assessment and Penetration Testing (VAPT) Report

Title

Vulnerability Assessment and Penetration Testing (VAPT) of Metasploitable Using Open-Source Tools

Prepared By

Atharva Dave

Tools Used

- Kali Linux
- Nmap
- OpenVAS (Greenbone Vulnerability Manager)
- Nikto
- Google Sheets (Risk Tracking)
- VMware Workstation

1. Executive Summary

This report presents the results of a Vulnerability Assessment and Penetration Testing (VAPT) exercise performed on an intentionally vulnerable system (Metasploitable). The objective was to identify security vulnerabilities using free and open-source tools, analyze their risks, and recommend remediation steps.

The assessment identified multiple **Critical and High severity vulnerabilities**, including outdated services, exposed network services, weak configurations, and web application vulnerabilities. Successful exploitation of these vulnerabilities could lead to **remote code execution, unauthorized access, credential theft, and full system compromise**.

2. Scope and Objectives

2.1 Scope

- **Target System:** Metasploitable Virtual Machine
- **Target IP Address:** `192.168.227.129`
- **Assessment Type:** Vulnerability Assessment and Limited Penetration Testing

- **Out of Scope:** Denial of Service (DoS) and Social Engineering attacks

2.2 Objectives

- Identify vulnerabilities without using paid tools
- Perform network and web vulnerability scanning
- Assess risks using CVSS scoring
- Document findings and remediation steps

---

3. Methodology (VAPT Approach)

The assessment followed a structured VAPT methodology aligned with **NIST**, **OWASP**, and industry best practices.

3.1 Planning

- Defined scope and rules of engagement
- Selected open-source tools
- Configured an isolated lab environment

3.2 Discovery

- Network and service discovery using **Nmap**
- Identification of exposed ports and running services

3.3 Vulnerability Assessment

- Automated vulnerability scanning using **OpenVAS**
- Web server scanning using **Nikto**

3.4 Risk Assessment

- CVSS-based risk scoring
- Risk prioritization using a 3×3 risk matrix

3.5 Reporting

- Documentation of findings
- Remediation recommendations
- Evidence-based reporting

---

4. Lab Environment and Network Setup

4.1 Environment Details

Machine	Role	IP Address
Kali Linux	Attacker	192.168.227.128
Metasploitable	Target	192.168.227.129
OpenVAS	Vulnerability Scanner	192.168.227.131

4.2 Network Configuration

- Hypervisor: VMware Workstation
- Network Type: Host-Only (Isolated Testing Environment)

---

5. Connectivity Verification

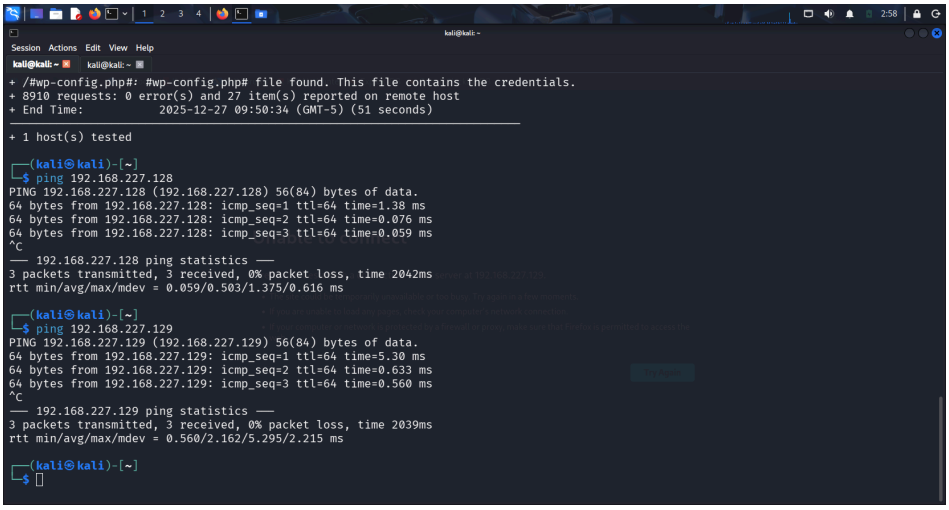
To verify network connectivity between the attacker and target machines, ICMP ping tests were performed.

Ping Test Results

```
ping 192.168.227.128
ping 192.168.227.129
```

Result:

- 0% packet loss
- Low latency observed



- Ping results from Kali to Metasploitable

---

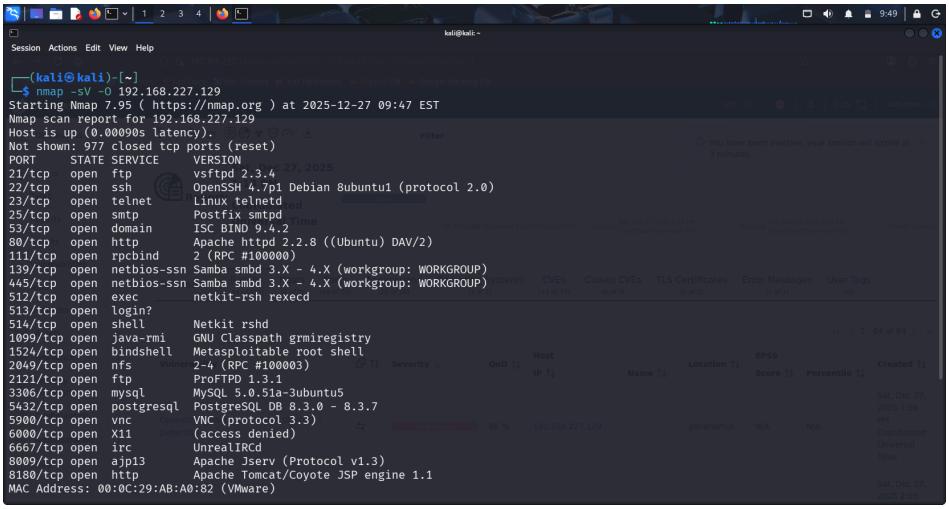
6. Discovery Phase – Nmap Scan

6.1 Nmap Command Used

```
nmap -sV -O 192.168.227.129
```

6.2 Key Findings

- Multiple open ports detected (FTP, SSH, HTTP, SMB, MySQL, Tomcat, IRC)
- Several outdated and vulnerable services running
- Presence of a root bind shell on port 1524



- Nmap scan output

---

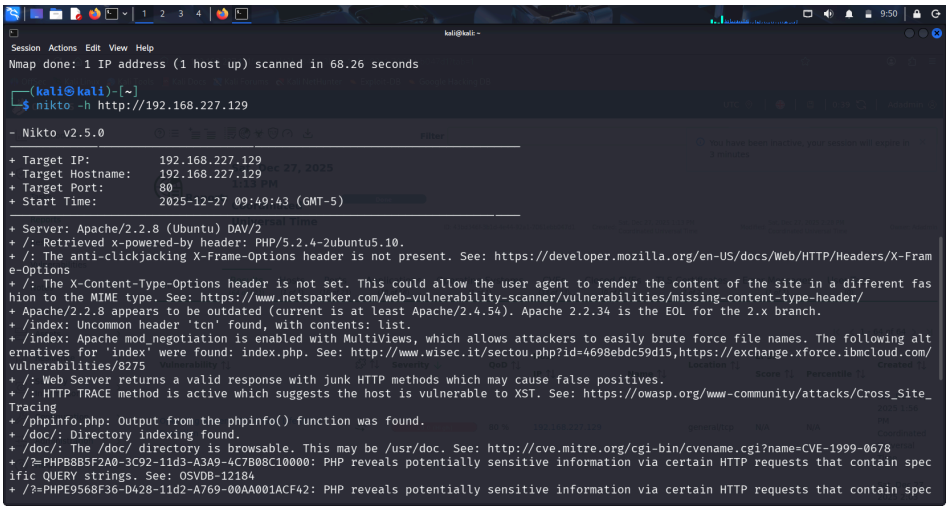
7. Web Vulnerability Scanning – Nikto

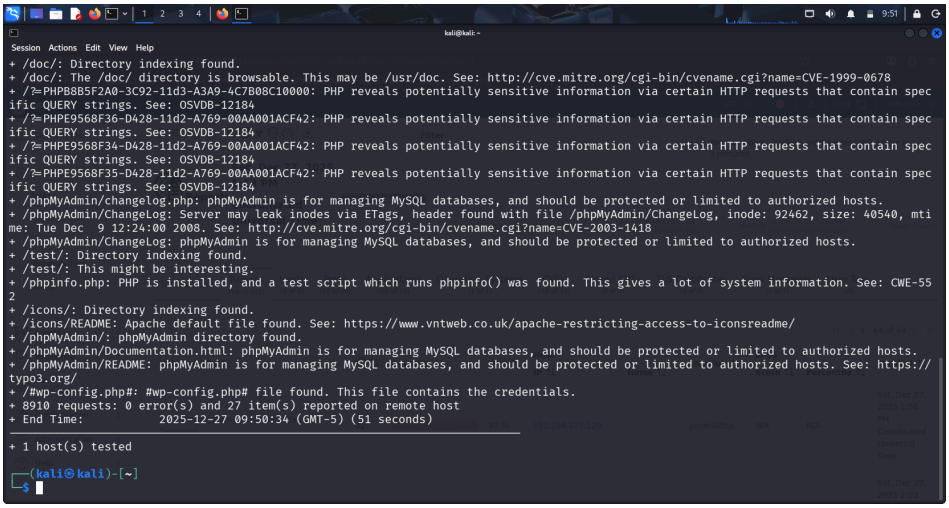
7.1 Nikto Command Used

```
nikto -h http://192.168.227.129
```

7.2 Key Findings

- Outdated Apache web server
- Missing security headers
- Directory listing enabled
- Exposed phpinfo() page
- phpMyAdmin publicly accessible





- Nikto scan output

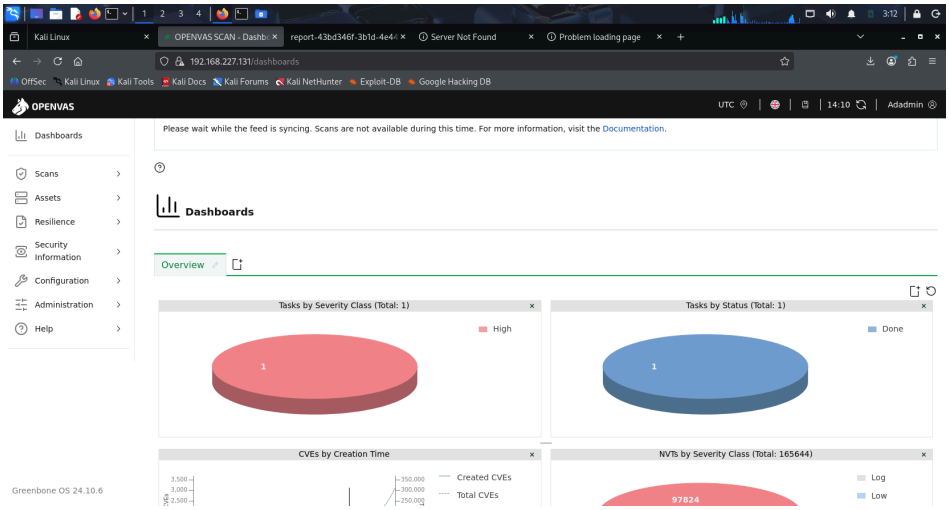
---

8. Vulnerability Assessment – OpenVAS

8.1 Scan Overview

- Scan Type: Full and Fast
- Tool: OpenVAS (Greenbone)
- Target: Metasploitable

The OpenVAS scan identified multiple vulnerabilities across network services and web applications, including several **Critical** vulnerabilities.



- OpenVAS dashboard showing scan summary

---

9. Detailed Vulnerability Analysis (Sample)

TWiki Cross-Site Scripting and Command Execution Vulnerability

Vulnerability Name:

TWiki XSS and Command Execution Vulnerabilities

OID:

1.3.6.1.4.1.25623.1.0.800320

Installed Version:

01.Feb.2003

Fixed Version:

4.2.4

CVE IDs:

- CVE-2008-5304
- CVE-2008-5305

Description

The vulnerability exists due to improper input sanitization of `%URLPARAM{}%` and `%SEARCH{}%` variables. The `%SEARCH{}%` variable is directly evaluated using Perl `eval()`, allowing attackers to inject and execute arbitrary code.

Impact

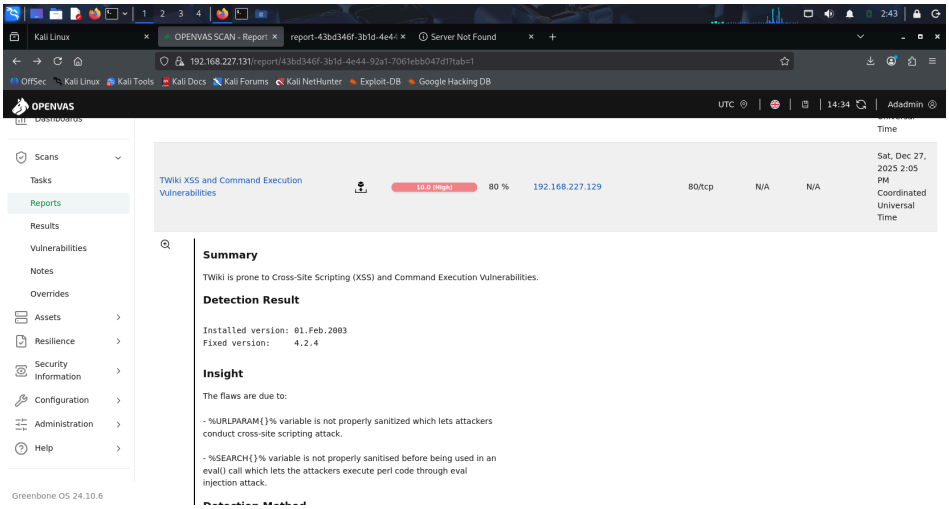
Successful exploitation could allow:

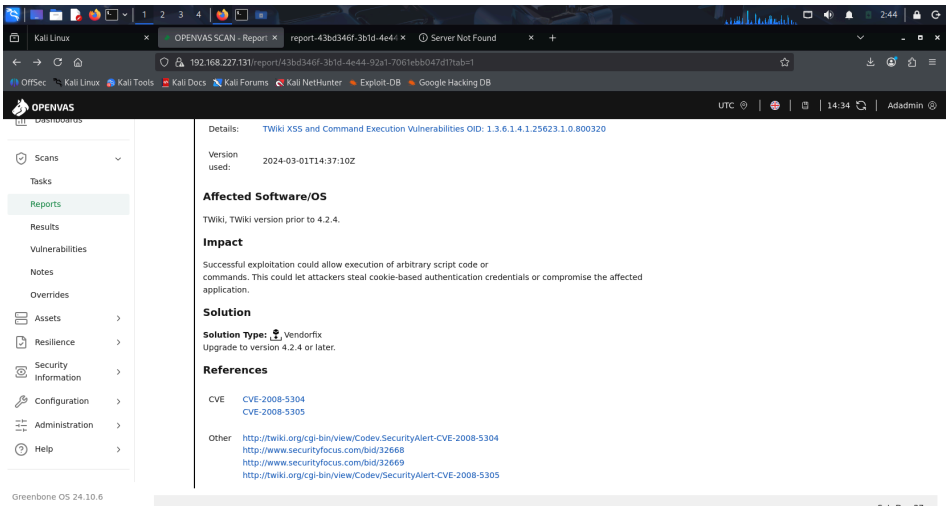
- Cross-Site Scripting (XSS)

- Remote command execution
- Theft of authentication cookies
- Complete application compromise

Remediation

Upgrade TWiki to version **4.2.4 or later**.





- OpenVAS detailed vulnerability page

---

10. Risk Assessment

10.1 CVSS Severity Classification

Severity	CVSS Score
Critical	9.0 – 10.0

Severity	CVSS Score
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9

10.2 Risk Matrix (3×3)

Likelihood	Impact	Risk
High	High	Critical
Medium	High	High
Low	Medium	Medium

10.3 Google Sheet Link:

https://docs.google.com/spreadsheets/d/1MBNVd9gAjG6ezBX_6rh664ZK7_1TcjPSRBkHvrHPZ8M/edit?usp=sharing

---

11. Remediation Recommendations

- Disable unused and insecure services (FTP, Telnet, Bind Shell)
- Upgrade outdated software and services
- Apply CIS Benchmarks for system hardening
- Restrict access to administrative interfaces
- Implement proper input validation for web applications
- Conduct regular vulnerability scans

---

12. Conclusion

The VAPT exercise demonstrated that the target system is highly vulnerable due to outdated software, insecure configurations, and exposed services. Immediate remediation is required to prevent exploitation. Regular vulnerability assessments, patch management, and secure configuration practices are essential to maintaining a secure environment.

---

13. References

- NIST SP 800-115
- OWASP Top 10
- Greenbone OpenVAS Documentation
- NVD CVSS Calculator
- CIS Benchmarks