# Metasploitable2 Penetration Test Report

**Prepared for:** Client / Lab Environment
**Prepared by: Valdrs**
**Date:** 2025-10-22

## Table of Contents

1. Executive Summary
2. Scope & Methodology
3. Findings Summary
4. Detailed Findings
   4.1 Exposed Login Interface
   4.2 Directory Enumeration
   4.3 Remote Code Execution
   4.4 SMB Misconfiguration
   4.5 SQL Injection
   4.6 Reflected XSS
   4.7 Stored XSS
5. Appendix A — Commands
6. Legal Notice
7. Version History

# 1. Executive Summary

A penetration test was performed against the Metasploitable2 virtual machine located at `192.168.1.40`. The assessment identified several high-risk vulnerabilities including remote code execution, SQL injection, and multiple cross-site scripting flaws.

Additionally, several administrative interfaces and outdated services were exposed without access controls, significantly increasing the attack surface.

While Metasploitable2 is intentionally insecure for training purposes, the vulnerabilities identified represent **critical security risks** in real-world production environments.

---

# 2. Scope & Methodology

## Scope

- **Target System:** Metasploitable2
- **IP Address:** `192.168.1.40`
- **Testing Type:** Authorized penetration test
- **Engagement Duration:** One controlled session

## Authorized Testing Activities

- Network and service discovery
- Web application testing
- Vulnerability exploitation (proof-of-concept only)

## Methodology Framework

1. **Reconnaissance**
2. **Enumeration**

3. **Exploitation & Validation**
4. **Reporting & Documentation**

---

## 3. Findings Summary

| ID | Vulnerability | Severity | Affected System |
|---|---|---|---|
| F-01 | Exposed Login Interface (DVWA) | High | Web Server |
| F-02 | Sensitive Directory Exposure | High | Web Server |
| F-03 | vsftpd 2.3.4 Backdoor (Remote Code Execution) | **Critical** | FTP Service |
| F-04 | SMB Information Disclosure | Medium | Samba |
| F-05 | SQL Injection | High | DVWA |
| F-06 | Reflected Cross-Site Scripting | High | DVWA |
| F-07 | Stored Cross-Site Scripting | High | DVWA |

---

## 4. Detailed Findings

### F-01 — Exposed Login Interface (DVWA)

A publicly accessible login portal was identified. Applications such as DVWA frequently rely on weak authentication and may facilitate credential brute forcing and further access escalation.

---

### F-02 — Directory Enumeration Findings

Directory enumeration revealed sensitive endpoints including `/phpinfo`, `/phpMyAdmin`, and wiki installations. These interfaces expose configuration information and may allow unauthorized administrative access.

---

### F-03 — vsftpd 2.3.4 Remote Code Execution

An exploit was executed against the vsftpd service resulting in a remote root shell. This vulnerability grants full compromise without authentication.

---

### F-04 — SMB Information Disclosure

SMB scanning revealed OS details, NetBIOS naming, domain information, and indicated message signing was disabled. This increases exposure to NTLM-relay-style attacks.

---

### F-05 — SQL Injection

sqlmap successfully executed an automated SQL injection attack against DVWA, extracting the application’s user database.

---

### F-06 — Reflected XSS

Reflected XSS was confirmed through unsanitized user input being executed in the browser context.

---

### F-07 — Stored XSS

Stored XSS was confirmed within DVWA’s guestbook feature. Payloads were retained server-side and executed when viewed, enabling persistence and potential session hijacking.

---

## 5. Appendix A — Commands Used

```
nmap -sV -sC -O 192.168.1.40
gobuster dir -u http://192.168.1.40 -w directory-list-2.3-medium.txt
-t 10
msfconsole > exploit/unix/ftp/vsftpd_234_backdoor
sqlmap -u "http://192.168.1.40/dvwa/vulnerabilities/sqli/?id=1" --dump
```

---

## 6. Legal Notice

This report was produced as part of an authorized lab-based penetration test. Testing or exploiting systems **without explicit permission is illegal**.