Penetration Testing Report – Metasploitable2

# 1. Executive Summary

This report details the findings of an internal penetration test conducted against the Metasploitable2 virtual machine. The goal was to simulate a real-world attack scenario and identify exploitable vulnerabilities in a safe, controlled environment. Multiple high-severity vulnerabilities were successfully exploited, including FTP backdoor access, web application injection flaws, and privilege escalation using local kernel vulnerabilities. Remediation strategies are provided for each issue.

# 2. Scope

Target System: Metasploitable2  
Attacking Machine: Kali Linux  
Testing Type: Black-box/Internal  
Tools Used: Nmap, Gobuster, WhatWeb, Burp Suite, Metasploit, searchsploit, Linux Exploit Suggester

# 3. Methodology

The following phases were followed:  
1. Reconnaissance  
2. Enumeration  
3. Exploitation  
4. Privilege Escalation  
5. Reporting

# 4. Vulnerability Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Vulnerability | Severity (CVSS) | CVE/Exploit | Affected Component | Recommendation |
| vsFTPd Backdoor | 9.8 (Critical) | CVE-2011-2523 | FTP Service | Update to a secure FTP version |
| Tomcat Manager WAR Upload | 8.1 (High) | Exploit via Metasploit | Tomcat Web Server | Restrict access and use strong credentials |
| SQL Injection (DVWA) | 7.5 (High) | Manual Exploit | Web Application | Sanitize inputs and use prepared statements |
| Command Injection (Mutillidae) | 8.8 (High) | Manual Exploit | Web Application | Validate and sanitize all user inputs |
| Kernel Privilege Escalation | 7.8 (High) | Linux Kernel Exploit (searchsploit) | OS Kernel | Apply latest kernel patches |

# 5. Technical Details

Detailed exploitation steps for each vulnerability identified are as follows:

## 5.1 vsFTPd Backdoor Exploit

Used Metasploit's exploit for vsFTPd v2.3.4 to gain a shell on port 21.

## 5.2 Tomcat WAR Upload

Brute-forced Tomcat credentials, then uploaded a WAR shell via the manager panel using Metasploit.

## 5.3 SQL Injection on DVWA

Injected SQL payloads into login form to bypass authentication and dump data.

## 5.4 Command Injection (Mutillidae)

Injected OS commands into vulnerable parameter to gain a reverse shell.

## 5.5 Privilege Escalation

Enumerated the system and exploited a kernel vulnerability using a local privilege escalation script from searchsploit.

# 6. Recommendations

All identified vulnerabilities should be addressed in order of severity. Services such as FTP and Tomcat should be updated or replaced with secure alternatives. Input validation and output sanitization must be enforced across all web applications. Kernel-level patches should be applied regularly to minimize privilege escalation risks.