AUG - SEPT 2025

COMPREHENSIVE PENETRATION TEST REPORT

Metasploitable2 Assessment

BY

Hibullahi AbdulAzeez (CYB3RLEO)

DOCUMENT CONTROL

REPORT VERSION	1.0
TARGET SYSTEM	Metasploitable2 (Ubuntu 8.04)
ASSESSMENT TYPE	Internal Penetration Testing
TESTER	CYB3RLEO
ASSESSMENT TIME FRAME	4-weeks (20 days)
CLASSIFICATION	Confidential

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Overview

A comprehensive penetration test was conducted against the Metasploitable2 vulnerable virtual machine in a controlled lab environment. The assessment revealed multiple critical vulnerabilities across various services, resulting in complete system compromise through multiple attack vectors. The target exhibited an extremely weak security posture with numerous services vulnerable to remote code execution, authentication bypass, and privilege escalation.

Risk Rating

Overall Risk: CRITICAL 🔴

- Confidentiality Impact: Complete
- Integrity Impact: Complete
- Availability Impact: Complete
- Exploitability: Trivial

Key Findings

- 15+ critical vulnerabilities identified
- Multiple remote code execution vectors
- Complete authentication bypass across multiple services
- Root-level access achieved through 8 different methods
- Extensive data exfiltration capabilities demonstrated

Recommendations Priority

1. Immediate Action Required: Disable unnecessary services
2. High Priority: Implement proper authentication mechanisms
3. Medium Priority: Apply security hardening configurations
4. Long-term: Establish ongoing security monitoring

INTRODUCTION

Target Description

Metasploitable2 is an intentionally vulnerable Ubuntu-based virtual machine designed for security training and penetration testing practice. The system runs outdated software with numerous known vulnerabilities across multiple services.

Assessment Objectives

- Identify security vulnerabilities in a controlled environment
- Demonstrate real-world attack techniques and methodologies
- Develop comprehensive security assessment skills
- Practice documentation and reporting procedures

Testing Methodology

The assessment followed a structured approach:

1. Reconnaissance: Network scanning and service enumeration
2. Vulnerability Assessment: Identifying security weaknesses
3. Exploitation: Gaining unauthorized access
4. Post-Exploitation: Maintaining access and lateral movement
5. Reporting: Documenting findings and recommendations

SCOPE OF WORK

In-Scope Systems

- Primary Target: Metasploitable2 (192.168.56.101)
- Services: All running network services
- Applications: Web applications and database systems
- Testing Types: Network, web application, and database penetration testing

Out-of-Scope

- Social engineering attacks
- Physical security assessment
- Denial of service testing
- Third-party systems or networks

Testing Limitations

- Conducted in isolated lab environment
- Limited to technical vulnerabilities only
- No production data or systems affected

FINDINGS & VULNERABILITIES

CRITICAL VULNERABILITIES

Remote Code Execution Vulnerabilities

Service	Port	Vulnerability	Impact
vsftpd	21	Backdoor (CVE-2011-2523)	Root Access
UnrealIRCd	6667	Backdoor (CVE-2010-2075)	Root Access
Samba	139/445	Usermap Script (CVE-2007-2447)	Root Access
DistCC	3632	Command Injection (CVE-2004-2687)	Root Access
Java RMI	1099	Deserialization	Root Access

Authentication Bypass Vulnerabilities

Service	Port	Vulnerability	Impact
MySQL	3306	Blank Root Password	DB Compromise
PostgreSQL	5432	Default Credential	DB Compromise
NFS	2049	no_root_squash Misconfiguration	Root Access

FINDINGS & VULNERABILITIES II

Web Application Vulnerabilities

Service	Vulnerability Type	Impact
DVWA	SQL Injection	DB Compromise
DVWA	Cross site scripting	Session Hijacking
DVWA	CSRF	Account Takeover
DVWA	Command Injection	System Access
TomCat	Unauthenticated Manager	RCE via WAR Deployment

Attack Chain Analysis

Initial Compromise Vectors

1. Network Service Exploitation: Direct RCE through vulnerable services
2. Web Application Attacks: SQL injection and command injection
3. Authentication Bypass: Default credentials and misconfigurations

Privilege Escalation

- SUID Misconfigurations: Nmap and other SUID binaries
- Service Privileges: Services running as root
- Kernel Exploits: Potential outdated kernel vulnerabilities

Persistence Mechanisms

- SSH key implantation
- User account creation
- Web shell deployment
- Cron job manipulation

Data Exposure Assessment

Sensitive Data Accessed

- Password hashes (/etc/shadow)
- User credentials (database contents)
- System configuration files
- Application source code

Data Exfiltration Capabilities

- Direct file access through compromised services
- Database extraction via SQL queries
- Network transfer capabilities established

TECHNICAL ANALYSIS

SECURITY POSTURE ASSESSMENT

Network Security

- Firewall: No host-based firewall configured
- Service Exposure: All services exposed to network
- Network Segmentation: No segmentation implemented

System Security

- Patch Level: Extremely outdated (no security updates)
- User Accounts: Weak password policies
- File Permissions: Multiple misconfigurations
- Logging: Minimal security logging configured

Application Security

- Input Validation: Lacking across all applications
- Authentication: Weak or missing authentication mechanisms
- Configuration: Default configurations with known vulnerabilities

ATTACK SURFACE ANALYSIS

External Attack Surface

- 20+ network services exposed
- Multiple web applications accessible
- Database services network-accessible

Internal Attack Surface

- Inter-service communication vulnerabilities
- Local privilege escalation vectors
- Credential storage weaknesses

HARDENING RECOMMENDATION

Immediate Actions (Critical)

Service Management

- Disable unnecessary services (FTP, IRC, RPC, etc.)
- Implement firewall rules restricting service access
- Move critical services to non-standard ports

Authentication Security

- Change all default credentials
- Implement strong password policies
- Disable root remote login for SSH

Access Controls

- Implement proper file permissions
- Remove unnecessary SUID/SGID binaries
- Configure service accounts with least privilege

Medium-term Improvements

System Hardening

- Implement regular patch management process
- Configure host-based firewall (iptables)
- Enable and monitor system logging
- Install and configure intrusion detection system

Network Security

- Implement network segmentation
- Configure VLANs for service isolation
- Deploy network monitoring solutions

Application Security

- Implement input validation across all applications
- Configure proper error handling
- Enable security headers for web applications
- Conduct regular code reviews

HARDENING RECOMMENDATION II

Long-term Security Strategy

Security Governance

- Establish security policies and procedures
- Implement regular security assessments
- Develop incident response plan
- Conduct security awareness training

Technical Controls

- Deploy Web Application Firewall (WAF)
- Implement file integrity monitoring
- Configure centralized logging and monitoring
- Establish backup and recovery procedures

Continuous Improvement

- Regular vulnerability scanning
- Periodic penetration testing
- Security configuration reviews
- Compliance monitoring and reporting

CONCLUSION

Summary of Findings

The Metasploitable2 system exhibited an extremely vulnerable security posture with multiple critical vulnerabilities leading to complete system compromise. The assessment demonstrated how outdated software, misconfigurations, and poor security practices can lead to significant security breaches.

Final Recommendations

- Immediate Remediation: Address critical vulnerabilities identified
- Security Hardening: Implement comprehensive security controls
- Ongoing Monitoring: Establish continuous security monitoring
- Regular Assessment: Conduct periodic security testing

Risk Assessment

The overall risk rating for the system is CRITICAL due to:

- Multiple remote code execution vulnerabilities
- Complete authentication bypass capabilities
- Lack of security controls and monitoring
- Extensive attack surface exposure

Lessons Learned

This assessment highlighted the importance of:

- Regular patch management
- Proper service configuration
- Strong authentication mechanisms
- Defense-in-depth strategies
- Comprehensive security monitoring

APPENDICES

Appendix A: Testing Tools Used

- Nmap - Network scanning and enumeration
- Metasploit - Exploitation framework
- SQLMap - SQL injection testing
- BeEF - Browser exploitation framework
- Custom scripts and manual testing techniques

Appendix C: References

- OWASP Testing Guide
- NIST Cybersecurity Framework
- CIS Security Benchmarks
- Vendor security advisories

Appendix B: Vulnerability Details

Detailed vulnerability information available in individual assessment reports for each service and application tested on my GITHUB and MEDIUM

Appendix D: Terminology

- RCE: Remote Code Execution
- XSS: Cross-Site Scripting
- CSRF: Cross-Site Request Forgery
- SQLi: SQL Injection
- CVSS: Common Vulnerability Scoring System
- DB: DataBase

DISCLAIMER:

THIS PENETRATION TEST WAS CONDUCTED IN A CONTROLLED LAB ENVIRONMENT FOR EDUCATIONAL PURPOSES ONLY. THE TECHNIQUES AND FINDINGS DOCUMENTED IN THIS REPORT SHOULD ONLY BE USED FOR LEGITIMATE SECURITY TESTING WITH PROPER AUTHORIZATION. UNAUTHORIZED TESTING AGAINST SYSTEMS IS ILLEGAL AND UNETHICAL.

CYB3RLEO

abdulazeezhibullahikolade@gmail.com
+234-810-435-6114