Network Vulnerability Assessment Report

Metasploitable2 Security Analysis and Mitigation Plan

Prepared by: Jay Uchagonkar
Date: January 2, 2025
Organization: Extion Infotech
Position: Cyber Security Intern

Executive Summary

This comprehensive report presents the findings and analysis from a network vulnerability assessment conducted on Metasploitable2, a purposely vulnerable Linux virtual machine. The assessment utilized multiple security tools including Nessus Essentials as the primary scanner, along with Nmap, Enum4linux, and Nikto for detailed analysis. Multiple critical and high-severity vulnerabilities were identified that require immediate attention.

Testing Environment Details

- **Attack Platform:** Kali Linux 2023.4
- **Target System:** Metasploitable2
- **Primary Scanner:** Nessus Essentials
- **Additional Tools:** Nmap, Enum4linux, Nikto
- **Network:** Isolated testing environment
- **Assessment Date:** January 2, 2025

Assessment Methodology

1. Initial Reconnaissance

Tool Used: Nmap

```
nmap -aV -sC -O -p- [target_ip]
```

Key open ports discovered:

- Port 21 (FTP)
- Port 22 (SSH)
- Port 23 (Telnet)
- Port 80 (HTTP)
- Port 445 (SMB)

2. SMB Enumeration

Tool Used: Enum4linux

```
enum4linux -a [target_ip]
```

Key findings:

- Discovered shared folders
- Identified user accounts
- Found system information
- Detected security misconfigurations

3. Web Server Assessment

Tool Used: Nikto

```
nikto -h [target_ip]
```

Key findings:

- Identified outdated server software
- Discovered vulnerable scripts
- Found potential exploit vectors
- Detected misconfigured security headers

Critical Vulnerabilities and Mitigation Strategies

1. Outdated Software and Missing Security Patches

Severity Level: Critical
Initial Detection: Nessus Essentials scan

Mitigation Steps:

- Create inventory of all systems requiring updates
- Test patches in isolated environment
- Schedule maintenance window for updates
- Implement automated patch management system
- Verify successful patch installation

Timeline: 1-2 weeks
Resources: Patch management software, system admin access, testing environment

2. Weak Authentication Mechanisms

Severity Level: Critical
Initial Detection: Default credentials and weak password policies identified

Mitigation Steps:

- Implement multi-factor authentication (MFA)
- Enforce strong password policies
- Remove default credentials
- Implement account lockout policies
- Regular password audits

Timeline: 1 week
Resources: MFA solution, password policy management tools

3. Misconfigured Firewall Rules

Severity Level: High
Initial Detection: Multiple unnecessarily open ports

Mitigation Steps:

- Audit existing firewall rules
- Remove redundant/obsolete rules
- Implement least-privilege access
- Document all rule changes
- Test network connectivity post-changes

Timeline: 3-4 days
Resources: Firewall management console, network documentation

4. Unencrypted Data Transmission

Severity Level: High
Initial Detection: Services using unencrypted communications

Mitigation Steps:

- Identify all unencrypted communications
- Implement TLS 1.3 for all data transmission
- Configure proper certificate management
- Disable older SSL/TLS versions
- Verify encryption implementation

Timeline: 1 week
Resources: SSL/TLS certificates, encryption tools

5. Exposed Network Services

Severity Level: Critical
Initial Detection: Multiple exposed services discovered

Mitigation Steps:

- Conduct port scanning to identify exposed services
- Close unnecessary ports
- Implement network segmentation
- Configure proper access controls
- Regular monitoring of network traffic

Timeline: 2-3 days
Resources: Network scanning tools, firewall access

Implementation Schedule

Week 1:

- Days 1-2: Address exposed network services
- Days 3-5: Implement firewall configurations
- Days 6-7: Begin software updates

Week 2:

- Days 8-10: Complete software updates
- Days 11-12: Implement authentication changes
- Days 13-14: Deploy encryption solutions

Conclusion

This vulnerability assessment of Metasploitable2 revealed several critical security issues requiring immediate attention. The proposed mitigation plan provides a structured approach to addressing these vulnerabilities while ensuring minimal disruption to system operations. Regular reassessment using the outlined tools will help verify the effectiveness of implemented solutions.

Submitted by:
Jay Uchagonkar
Cyber Security Intern
Extion Infotech