
VULNERABILITY REMEDIATION PLAN

Analyst: Alexander T. Ramos
Date: October 5, 2025
Target: Metasploitable 2 (192.168.56.101)
Scanner Tools: Nmap + Nikto (Kali Linux)

---

1. EXECUTIVE SUMMARY

This remediation plan addresses vulnerabilities identified during a simulated vulnerability assessment of the Metasploitable 2 virtual machine using Nmap and Nikto. The goal is to outline corrective actions, mitigation priorities, and verification steps to strengthen the system’s security posture.

---

2. ASSESSMENT OVERVIEW

Environment: Local virtual environment (VirtualBox)
Scanning Tools: Nmap 7.93, Nikto 2.1.6
Scan Type: SYN Scan (-sS), Service/Version Detection (-sV), Default Scripts (-sC), Web Enumeration
Target System: Linux (Ubuntu 8.04) – Metasploitable 2
Total Findings: 5 (1 Critical, 2 High, 1 Medium, 1 Low)

---

3. VULNERABILITY SUMMARY

Critical - vsftpd Backdoor (FTP/21): Vulnerable vsftpd 2.3.4 contains a malicious backdoor allowing remote shell access. CVE-2011-2523
High - Apache Path Traversal (HTTP/80): Apache 2.2.8 path traversal vulnerability allowing potential RCE. CVE-2011-3192
High - Samba RCE (SMB/139,445): Samba 3.X allows unauthenticated RCE via crafted packets. CVE-2007-2447
Medium - Weak MySQL Credentials (3306): Default credentials detected; possible unauthorized access.
Low - Missing Security Headers: HTTP response missing X-Frame-Options and related security headers.

---

4. RECOMMENDED ACTIONS

[CRITICAL] vsftpd Backdoor: Disable vsftpd service; patch or remove. Validate with `nmap -p 21 192.168.56.101`.
[HIGH] Apache Path Traversal: Upgrade Apache; restrict HTTP methods to GET/POST; re-scan using Nikto.
[HIGH] Samba RCE: Apply patches or upgrade; restrict SMB to trusted hosts via smb.conf.
[MEDIUM] MySQL Credentials: Enforce strong passwords; disable remote root access; remove test DBs.
[LOW] Missing Security Headers: Add headers via .htaccess or Apache config. Validate with `curl -I http://192.168.56.101`.

---

5. VERIFICATION STEPS

Re-run:
nmap -sS -sV -sC 192.168.56.101
nikto -h http://192.168.56.101
Confirm critical/high vulnerabilities resolved. Review Splunk logs for anomalies. Document verification in Vuln_Scan_Report.md.

---

6. CONCLUSION

All identified vulnerabilities were remediated through patching, configuration hardening, and service restrictions. Future scans will be conducted quarterly to ensure continuous risk reduction.

NOTE: This is a simulated remediation plan created for cybersecurity training and portfolio demonstration purposes only.