Network Vulnerability Assessment Report

Extion Infotech Cybersecurity Internship Project

Executive Summary

This report presents the findings of a comprehensive network vulnerability assessment conducted on the target IP address 192.168.137.1. The assessment was performed using Tenable Nessus Essentials on May 28, 2025, and identified multiple security vulnerabilities that require immediate attention.

Key Findings:

- **Total Vulnerabilities Found:** 47
- **Critical:** 0
- **High:** 0
- **Medium:** 4
- **Low:** 0
- **Informational:** 43

Target Information

- **IP Address:** 192.168.137.1
- **Scan Date:** May 28, 2025, 10:47:24 IST
- **Assessment Tool:** Tenable Nessus Essentials
- **Assessment Duration:** Full network scan
- **Operating System:** Microsoft Windows (detected)

Critical Vulnerability Analysis

1. SSL Certificate Cannot Be Trusted (Plugin ID: 51192)

- **Severity:** MEDIUM
- **CVSS Score:** 6.5
- **Description:** The SSL certificate presented by the remote host cannot be trusted due to certificate chain issues
- **Risk:** Man-in-the-middle attacks, data interception

- **Impact:** Medium - Could compromise encrypted communications

2. SSL Self-Signed Certificate (Plugin ID: 57582)

- **Severity:** MEDIUM
- **CVSS Score:** 6.5
- **Description:** The remote host is using a self-signed SSL certificate
- **Risk:** Authentication bypass, impersonation attacks
- **Impact:** Medium - Users cannot verify server authenticity

3. SMB Signing Not Required (Plugin ID: 57608)

- **Severity:** MEDIUM
- **CVSS Score:** 5.3
- **Description:** SMB signing is not required, allowing potential man-in-the-middle attacks
- **Risk:** Session hijacking, data tampering
- **Impact:** Medium - SMB communications can be intercepted and modified

4. SSL Certificate with Wrong Hostname (Plugin ID: 45411)

- **Severity:** MEDIUM
- **CVSS Score:** 5.3
- **Description:** SSL certificate hostname does not match the server hostname
- **Risk:** Certificate validation bypass
- **Impact:** Medium - SSL/TLS protection may be ineffective

5. Additional Security Concerns (Informational)

- **MySQL Server Detection:** Database service exposed
- **Multiple SSL/TLS Configuration Issues:** Cipher suite weaknesses
- **Windows SMB Service Exposure:** Network file sharing protocols accessible

---

Detailed Mitigation Plan

Priority 1: SSL/TLS Certificate Issues

Vulnerabilities Addressed:

- SSL Certificate Cannot Be Trusted

- SSL Self-Signed Certificate
- SSL Certificate with Wrong Hostname

Mitigation Steps:

1. **Obtain Valid SSL Certificate**
   - Purchase or obtain a certificate from a trusted Certificate Authority (CA)
   - Ensure certificate covers all required hostnames/domains
   - **Timeline:** 1-2 business days
   - **Resources Required:** SSL certificate, server administrator access
2. **Install and Configure Certificate**
   - Remove existing self-signed certificate
   - Install new CA-signed certificate
   - Update certificate chain and intermediate certificates
   - **Timeline:** 2-4 hours
   - **Resources Required:** Server downtime window, SSL certificate files
3. **Verify Certificate Installation**
   - Test SSL configuration using SSL Labs or similar tools
   - Verify hostname matching
   - Confirm certificate chain validity
   - **Timeline:** 30 minutes
   - **Resources Required:** Online SSL testing tools

Priority 2: SMB Security Hardening

Vulnerability Addressed:

- SMB Signing Not Required

Mitigation Steps:

1. **Enable SMB Signing**
   - Configure Group Policy: "Microsoft network client: Digitally sign communications (always)"
   - Set "Microsoft network server: Digitally sign communications (always)"
   - **Timeline:** 30 minutes + reboot
   - **Resources Required:** Administrative privileges, system restart

2. **SMB Protocol Updates**
    - Disable SMBv1 protocol if not required
    - Ensure SMBv2/SMBv3 with encryption is enabled
    - **Timeline:** 1 hour
    - **Resources Required:** Network configuration access

Priority 3: Service Hardening

Services to Secure:

- MySQL Database Server
- Windows SMB Services

Mitigation Steps:

1. **Database Security**
    - Review MySQL configuration for unnecessary exposure
    - Implement database firewall rules
    - Enable SSL/TLS for database connections
    - **Timeline:** 2-3 hours
    - **Resources Required:** Database administrator access
2. **Network Segmentation**
    - Implement firewall rules to restrict SMB access
    - Use VPN for remote file sharing access
    - **Timeline:** 1-2 hours
    - **Resources Required:** Network administrator access

Implementation Timeline

Priority	Task	Duration	Dependencies
1	SSL Certificate Procurement	1-2 days	Budget approval, domain verification
1	SSL Certificate Installation	2-4 hours	Maintenance window
2	SMB Signing Configuration	1 hour	System restart approval
3	Database Hardening	2-3 hours	Database maintenance window
3	Network Segmentation	1-2 hours	Network change approval

Total Estimated Time: 3-5 business days

Risk Assessment

Current Risk Level: **MEDIUM**

Risk Factors:

- SSL/TLS vulnerabilities expose encrypted communications
- SMB signing issues allow network-level attacks
- Database service exposure increases attack surface
- Multiple informational findings indicate potential security gaps

Post-Mitigation Risk Level: **LOW**

Residual Risks:

- Ongoing certificate management required
- Regular security assessments needed
- Continuous monitoring of exposed services

Recommendations for Security Improvement

Immediate Actions (0-30 days)

1. Implement all critical vulnerability fixes
2. Establish SSL certificate management process
3. Review and harden all network services
4. Implement network monitoring solutions

Medium-term Actions (30-90 days)

1. Deploy comprehensive vulnerability management program
2. Implement regular security assessments
3. Establish incident response procedures
4. Conduct security awareness training

Long-term Actions (90+ days)

1. Develop security metrics and KPIs

2. Implement advanced threat detection
3. Regular penetration testing
4. Security architecture review

Conclusion

The network vulnerability assessment revealed several medium-severity vulnerabilities primarily related to SSL/TLS configuration and SMB security settings. While no critical vulnerabilities were identified, the discovered issues require prompt attention to maintain adequate security posture.

The proposed mitigation plan addresses all identified vulnerabilities and provides a structured approach to improving overall network security. Implementation of these recommendations will significantly reduce the organization's security risk profile.

Next Steps:

1. Approve and schedule implementation of mitigation plan
2. Assign responsible personnel for each remediation task
3. Establish timeline for follow-up security assessment
4. Document all changes for compliance and audit purposes

Report Prepared By: Yug Moradiya
Date: May 30, 2025
Assessment Tool: Tenable Nessus Essentials