Network Vulnerability Assessment Report

Target Environment: Internal Lab Network

Tool Used: Nessus Essentials

Assessor: Sayada Mehnaaz

Date: August 22, 2025

1. Executive Summary

A vulnerability assessment was conducted using Nessus Essentials on the target environment. The scan identified multiple vulnerabilities across different severity levels, including critical issues such as outdated web servers and insecure SSL configurations. Exploitation of these vulnerabilities could lead to unauthorized access, data leakage, and service disruptions.

2. Scope of Assessment

- **Target:** Internal Lab Network (Windows & Linux hosts)
- **Tool:** Nessus Essentials vulnerability scanner
- **Scan Type:** Basic Network Scan
- **Goal:** Identify vulnerabilities by severity and provide remediation steps

3. Findings Summary

Severity	Count	Examples	Status
Critical	2	Apache 2.4.49 RCE, SMBv1 Enabled	Open
High	3	SSL/TLS Weak Cipher, OpenSSH outdated, MySQL default creds	Open
Medium	4	Outdated Windows Patch, Information Disclosure	Open
Low	5	ICMP Timestamp, Missing Security Headers	Open

4. Detailed Findings

4.1 Apache 2.4.49 Path Traversal / RCE (Critical)

Description: The host is running Apache 2.4.49, which is vulnerable to a path traversal and remote code execution vulnerability (CVE-2021-41773).

Impact: An attacker can read arbitrary files and potentially execute code on the server.

Recommendation: Upgrade Apache to the latest patched version (>= 2.4.51).

4.2 SMBv1 Enabled (Critical)

Description: The server supports SMBv1, an outdated protocol vulnerable to EternalBlue (CVE-2017-0144).

Impact: Could allow ransomware (e.g., WannaCry) to propagate and compromise systems.

Recommendation: Disable SMBv1 protocol and use SMBv2/SMBv3.

4.3 SSL/TLS Weak Cipher Suites (High)

Description: The server supports weak ciphers (RC4, 3DES) that can be broken by modern attacks.

Impact: Could allow attackers to decrypt sensitive traffic.

Recommendation: Reconfigure SSL/TLS settings to only allow strong ciphers (AES, TLS 1.2+).

4.4 MySQL Default Credentials (High)

Description: The MySQL database is accessible with default root credentials.

Impact: Leads to full compromise of the database.

Recommendation: Change default credentials and enforce strong authentication.

4.5 Outdated Windows Patch (Medium)

Description: Windows host missing several security updates.

Impact: Leaves system exposed to privilege escalation and malware.

Recommendation: Apply the latest Microsoft security updates.

---

5. Conclusion

The Nessus vulnerability assessment revealed multiple critical and high-severity vulnerabilities. Immediate remediation should focus on upgrading vulnerable services (Apache, SMB, MySQL) and implementing secure configurations. Regular patching and vulnerability scanning should be integrated into the organization's security operations lifecycle.