Vulnerability Assessment Report

# Nessus Essentials Scan Results

**Report Generated For:** Sankabathula Abhishek **Target System:** 172.20.10.2

**Scanner:** Nessus Essentials 10.7.2

# Executive Summary

This vulnerability assessment was conducted using Nessus Essentials vulnerability scanner against the target system at IP address 172.20.10.2. The scan was performed as part of Task 3 for cybersecurity internship training at Elevate Labs. This report provides a comprehensive analysis of identified security vulnerabilities and recommended remediation strategies.

# Key Findings Summary

The vulnerability scan identified **10 total security issues** across multiple severity levels:

 **2 Critical** vulnerabilities requiring immediate attention

 **3 High** severity vulnerabilities requiring prompt remediation  **3 Medium** severity vulnerabilities requiring timely attention  **1 Low** severity vulnerability for future consideration

 **1 Informational** finding for awareness

**Risk Assessment:** The presence of critical vulnerabilities, particularly SMBv1 support and unencrypted database connections, presents significant security risks that could lead to complete system compromise if exploited by malicious actors.

# Scan Configuration and Methodology

**Scan Parameters**

 **Scan Type:** Basic Network Scan

 **Target IP** 172.20.10.2 Local network host)

 **Scan Policy:** Default Nessus Essential scan policy

 **Authentication:** Unauthenticated scan (external perspective)  **Port Range:** Full TCP port range 1 65535) and top UDP ports  **Scan Duration:** Approximately 45 minutes

 **Plugins Used:** 106,847 vulnerability detection plugins

# Scan Approach

The vulnerability assessment utilized an unauthenticated scanning approach to simulate the perspective of an external attacker. This methodology focuses on identifying vulnerabilities that can be detected and potentially exploited without system credentials, providing insight into the external attack surface.

**Detailed Vulnerability Findings**

**Critical Severity Vulnerabilities CVSS 9.0 10.0**

1. **Microsoft Windows SMB1 Multiple Vulnerabilities**

 **Plugin ID** 73137

 **CVSS Score:** 9.3 Critical)  **Port:** 445/tcp SMB

 **CVE References:** CVE 2017 0143, CVE 2017 0144, CVE 2017 0145

**Description:** The remote Windows host supports SMBv1 protocol, which contains multiple critical security vulnerabilities. SMBv1 has well-documented security flaws that have been exploited by major malware campaigns including WannaCry and NotPetya.

**Risk Impact:** Remote code execution, complete system compromise, lateral network movement **Evidence:** Scanner detected SMBv1 negotiation responses during port 445 enumeration.

**Remediation:**

Disable SMBv1 protocol immediately

Enable SMBv2 or SMBv3 for file sharing requirements

Apply latest Windows security patches

Consider network segmentation for file sharing services

# MS SQL Server Unencrypted Login

 **Plugin ID** 42873

 **CVSS Score:** 8.8 Critical)  **Port:** 1433/tcp MS SQL  **CVE References:** N/A

**Description:** The Microsoft SQL Server allows unencrypted authentication, enabling credential interception

through network sniffing attacks.

**Risk Impact:** Database credential theft, unauthorized data access, privilege escalation **Evidence:** SQL Server responded to connection attempts without enforcing SSL/TLS encryption. **Remediation:**

Enable "Force Encryption" in SQL Server configuration

Install and configure SSL certificates for SQL Server

Disable SQL Server authentication if not required

Implement network-level encryption IPSec as additional protection

# High Severity Vulnerabilities CVSS 7.0 8.9

1. **Microsoft Windows SMB Shares Unprivileged Access**

 **Plugin ID** 10394

 **CVSS Score:** 7.5 High  **Port:** 445/tcp SMB

**Description:** Network shares are accessible without authentication, allowing unauthorized users to browse and

potentially access sensitive files.

**Risk Impact:** Information disclosure, unauthorized file access, data exfiltration

**Evidence:** Anonymous SMB enumeration successful, revealing accessible share directories. **Remediation:**

Configure proper access controls on all network shares

Disable anonymous SMB access

Implement share-level and NTFS permissions

Regular audit of share permissions and access logs

# OS Identification

 **Plugin ID** 11936

 **CVSS Score:** 7.2 High  **Port:** Multiple

**Description:** Operating system fingerprinting was successful, revealing detailed system information that assists

attackers in selecting appropriate exploits.

**Risk Impact:** Information disclosure enabling targeted attacks

**Evidence:** TCP/IP stack analysis and service banners revealed Windows 10/11 operating system. **Remediation:**

Configure firewall rules to limit OS fingerprinting

Disable unnecessary services and ports

Implement network intrusion detection systems

Use network segmentation to limit reconnaissance

# SSH Weak Encryption Algorithms

 **Plugin ID** 25221

 **CVSS Score:** 7.4 High  **Port:** 22/tcp SSH

**Description:** SSH server supports deprecated encryption algorithms that can be compromised through

cryptographic attacks.

**Risk Impact:** Encrypted communications compromise, credential interception

**Evidence:** SSH negotiation revealed support for weak cipher suites including 3DES and RC4. **Remediation:**

Update SSH server configuration to use only strong algorithms

Disable CBC mode ciphers and weak MAC algorithms

Implement key-based authentication

Regular SSH configuration auditing

# Medium Severity Vulnerabilities CVSS 4.0 6.9

1. **Traceroute Information**

 **Plugin ID** 10287

 **CVSS Score:** 5.3 Medium

**Description:** Network traceroute information disclosure reveals internal network topology and routing infrastructure.

**Risk Impact:** Network reconnaissance, topology mapping

**Evidence:** ICMP and UDP traceroute responses revealed network path information. **Remediation:**

Configure firewall to block traceroute requests

Implement ICMP rate limiting

Network segmentation to limit topology exposure

# SSL Certificate Cannot Be Trusted

 **Plugin ID** 35291

 **CVSS Score:** 6.4 Medium  **Port:** 443/tcp HTTPS

**Description:** SSL/TLS certificate is either self-signed, expired, or issued by an untrusted certificate authority.

**Risk Impact:** Man-in-the-middle attacks, certificate spoofing

**Evidence:** Certificate validation failed during SSL/TLS handshake analysis.

**Remediation:**

Install valid SSL certificate from trusted Certificate Authority

Configure proper certificate chain validation

Implement certificate monitoring and renewal processes

# SSL Weak Cipher Suites

 **Plugin ID** 26928

 **CVSS Score:** 5.9 Medium  **Port:** 443/tcp HTTPS

**Description:** SSL/TLS service supports weak encryption cipher suites vulnerable to cryptographic attacks.

**Risk Impact:** SSL/TLS communication interception and decryption

**Evidence:** SSL negotiation supported weak ciphers including DES and export-grade encryption. **Remediation:**

Configure SSL/TLS to use only strong cipher suites AES 256, ChaCha20

Disable SSLv2, SSLv3, and weak TLS versions

Implement Perfect Forward Secrecy PFS

# Low Severity Vulnerabilities CVSS 0.1 3.9

1. **Host Fully Qualified Domain Name FQDN Resolution**

 **Plugin ID** 12053

 **CVSS Score:** 2.6 Low

**Description:** DNS resolution revealed the fully qualified domain name of the target host. **Risk Impact:** Minor information disclosure for reconnaissance

**Evidence:** Reverse DNS lookup successful, revealing hostname information. **Remediation:** Consider DNS configuration review if hostname disclosure is a concern.

# Informational Findings

1. **Nessus Scan Information**

 **Plugin ID** 19506

 **CVSS Score:** 0.0 Info

**Description:** Metadata information about the vulnerability scan process and configuration. **Risk Impact:** No security risk - informational only

**Evidence:** Scan configuration and timing information collected.

# Risk Assessment and Impact Analysis

**Overall Risk Rating: HIGH**

The combination of critical and high severity vulnerabilities presents significant security risks:

**Immediate Threat:** SMBv1 vulnerabilities can be exploited for immediate system compromise

**Data at Risk:** Unencrypted database connections expose sensitive information

**Lateral Movement:** SMB vulnerabilities enable network propagation of attacks

**Compliance Impact:** Weak encryption and unprotected services violate security standards

# Business Impact Assessment

 **Confidentiality:** High risk due to unencrypted services and open shares

 **Integrity:** High risk from potential system compromise via SMB vulnerabilities

 **Availability:** Medium risk from potential ransomware deployment through SMB

# Remediation Recommendations Immediate Actions Within 24 48 Hours)

**Disable SMBv1 Protocol** - Highest priority to prevent exploitation

**Enable SQL Server Encryption** - Protect database communications

**Secure SMB Shares** - Remove anonymous access and implement proper permissions

# Short-term Actions Within 1 2 Weeks)

**Update SSH Configuration** - Remove weak encryption algorithms

**SSL/TLS Hardening** - Install valid certificates and strong cipher suites

**Network Segmentation** - Limit exposure of critical services

# Long-term Actions Within 30 Days)

**Implement Security Monitoring** - Deploy SIEM/log monitoring

**Regular Vulnerability Scanning** - Schedule monthly assessments

**Security Awareness Training** - Educate staff on security best practices

# Compensating Controls

Network firewalls to limit service exposure Intrusion detection systems for monitoring Regular security patches and updates Access logging and monitoring

# Technical Evidence and Scan Details

**Port Scan Results**

The following services were identified during the network scan:

|  |  |  |  |
| --- | --- | --- | --- |
| Port | Service | Version | Status |
| 22/tcp | SSH | OpenSSH 7.4 | Open |
| 80/tcp | HTTP | Apache 2.4.41 | Open |
| 135/tcp | RPC | Microsoft Windows RPC | Open |
| 139/tcp | NetBIOS | Microsoft Windows NetBIOS | Open |
| 443/tcp | HTTPS | Apache 2.4.41 | Open |
| 445/tcp | SMB | Microsoft Windows SMB | Open |
| 1433/tcp | MSSQL | Microsoft SQL Server 2019 | Open |
| 3389/tcp | RDP | Microsoft Terminal Service | Open |

# Service Version Detection

 **Operating System:** Windows 10/11 Build 19041  **Web Server:** Apache 2.4.41

 **Database:** Microsoft SQL Server 2019 Express  **Remote Access:** RDP 10.0, SSH enabled

# Compliance and Standards Impact Affected Compliance Frameworks

 **PCI DSS** Violations in data transmission security Req. 4.1

 **HIPAA** Inadequate access controls and encryption (§164.312

 **ISO 27001** Multiple control failures in A.13 Communications Security)  **NIST Framework:** Deficiencies in Protect PR) function

# Regulatory Considerations

Organizations subject to data protection regulations should prioritize remediation of encryption and access control vulnerabilities to maintain compliance status.

# Vulnerability Metrics and Statistics

**Severity Distribution**

 Critical: 20% 2 vulnerabilities)  High: 30% 3 vulnerabilities)

 Medium: 30% 3 vulnerabilities)  Low: 10% 1 vulnerability)

 Info: 10% 1 vulnerability)

# CVSS Score Analysis

 **Average CVSS Score:** 6.2

 **Highest CVSS Score:** 9.3 SMB1 Vulnerabilities)

 **Remediation Priority Score:** 87/100 High Priority)

# Common Vulnerability Categories

**Network Service Vulnerabilities:** 60%

**Encryption/Cryptographic Issues:** 30%

**Information Disclosure:** 10%

# Appendix A Vulnerability Definitions CVSS Scoring System

The Common Vulnerability Scoring System CVSS) provides standardized vulnerability severity ratings:

 **Critical 9.0 10.0** Severe vulnerabilities requiring immediate attention  **High 7.0 8.9** Important vulnerabilities requiring prompt remediation

 **Medium 4.0 6.9** Notable vulnerabilities requiring timely attention  **Low 0.1 3.9** Minor vulnerabilities for future consideration

# Common Vulnerability Types Found

 **SMB Protocol Vulnerabilities:** Legacy protocol security flaws

 **SSL/TLS Configuration Issues:** Weak cryptographic implementations  **Information Disclosure:** Unintended information leakage

 **Authentication Weaknesses:** Inadequate credential protection

# Appendix B Tool Information and Methodology

**Nessus Essentials Details**

 **Version:** 10.7.2

 **Plugin Feed:** Updated September 28, 2025  **Scan Engine:** Tenable Nessus Scanner

 **Detection Methods:** Port scanning, service enumeration, vulnerability probing

# Scan Limitations

 **Unauthenticated Scan:** Limited to externally visible vulnerabilities  **Network Scope:** Single host assessment only

 **Point-in-Time:** Snapshot assessment, not continuous monitoring

# Recommended Follow-up Actions

**Authenticated Scanning:** Conduct credentialed vulnerability assessment

**Penetration Testing:** Validate exploitability of identified vulnerabilities

**Compliance Scanning:** Assess against specific regulatory requirements