ElevateLabs-Cybersecurity-Task-3

* Identifying Common vulnerabilities in a computer system.

Vulnerability Assessment Report

Target IP: 192.168.119.149

Tool Used: Nessus Essentials

Scan Type: Basic Network Scan

Date of Scan: 26/06/2025

Scan Performed By: Shubham Singh/AdminHK

# 1. Executive Summary

|  |  |
| --- | --- |
| Item | Details |
| Scan Target | 192.168.119.149 |
| Total Vulnerabilities | 12 |
| Critical Vulnerabilities | 2 |
| High Vulnerabilities | 3 |
| Medium Vulnerabilities | 4 |
| Low/Info | 3 |

A vulnerability scan was conducted on the system at 192.168.119.149. The scan identified multiple high-risk vulnerabilities, including outdated services and unpatched software components. Immediate remediation is recommended for critical issues.

# 2. System Information

|  |  |
| --- | --- |
| Attribute | Detail |
| IP Address | 192.168.119.149 |
| Operating System (Detected) | Ubuntu Linux 20.04 |
| Open Ports | 22 (SSH), 80 (HTTP), 139/445 (SMB), 3306 (MySQL) |
| Detected Services | Apache 2.4.41, MySQL 5.7, OpenSSH 7.6p1 |

# 3. Top Vulnerabilities Detected

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Vulnerability | CVE ID | Severity | Port | Description | Recommendation |
| OpenSSH User Enumeration | CVE-2018-15473 | High | 22 | Allows attackers to enumerate valid usernames | Apply patch or upgrade OpenSSH |
| Apache HTTPD 2.4.41 Vulnerabilities | CVE-2020-9490, CVE-2020-11993 | Critical | 80 | Known RCE and DoS vulnerabilities | Upgrade Apache to 2.4.54+ |
| SMBv1 Enabled | CVE-2017-0144 | Critical | 445 | Enables RCE via legacy protocol | Disable SMBv1 or patch |
| MySQL User with No Password | N/A | High | 3306 | MySQL allows login without a password | Enforce password policies |
| Outdated MySQL Server | CVE-2022-32081 | Medium | 3306 | Local privilege escalation possible | Upgrade to latest MySQL version |
| SSL Self-Signed Certificate | N/A | Low | 443 | Insecure certificate usage | Replace with valid CA certificate |

# 4. Remediation Plan

* Immediate: Patch Apache HTTP Server, disable SMBv1, patch OpenSSH
* High Priority: Secure MySQL access and update database service
* Medium Priority: Replace self-signed SSL certs
* Low Priority: Harden system configs, remove unused services