**Practical Vulnerability Assessment and Report**

Name: A.D. Sanjeewa Dilhan

Date : 5th of May 2025

# Executive Summary

This vulnerability assessment report provides an overview of the evaluation performed on a simulated network environment. The scope included identifying system weaknesses, assessing their impact, and providing actionable recommendations for mitigation. The assessment was conducted using OpenSCAP on CentOS 9 virtual machines configured via VMware Workstation.

Key findings include SSH configuration issues and adherence to strong cryptographic protocols. Recommendations prioritize addressing high-risk vulnerabilities, including misconfigurations in SSH policies, to enhance security without significant resource impact. The report also outlines estimated timeframes and budgetary considerations for implementation.

These vulnerabilities were analyzed against CVSS metrics, underscoring their potential exploitability and impact. To address these findings, the report recommends implementing a patch management strategy, reconfiguring insecure services, and enforcing stricter access controls, supported by automated updates and regular compliance checks. Additionally, adopting a continuous monitoring framework will help proactively identify and mitigate new risks. These measures will collectively enhance the system's security posture, reduce the likelihood of breaches, minimize downtime, and ensure alignment with industry standards and best practices, thereby safeguarding critical assets against evolving threats.

# Vulnerability Assessment

## 2.1 Introduction

The assessment was carried out in a controlled environment with two CentOS 9 VMs acting as the master and client, respectively. VMware Workstation was utilized to set up the virtualized infrastructure. OpenSCAP was chosen for its compliance with SCAP standards and capability to perform automated vulnerability assessments.

* **Vulnerability assessment tool** – OpenSCAP
* **Operating system** – CentOS stream 9
* **Design architecture** - Using the VMware Virtual environment Mater and Client VMs are created on the same subnet. Client VM scanned over Master VM perspective to the security tool.

A diagram of a software work station

AI-generated content may be incorrect.

## *Figure 1: Lab Infrastructure on VMware Workstation*

## 2.2 Vulnerability Assessment Report

## This assessment was conducted in a controlled lab environment using VMware Workstation to simulate a realistic system setup. The setup included two CentOS 9 VMs, configured as "master" and "client." The assessment aimed to evaluate system vulnerabilities related to SSH configurations, cryptographic practices, and overall compliance with recognized security benchmarks. OpenSCAP was selected for its robust capabilities in scanning, benchmarking, and generating actionable reports. The profile xccdf\_org.ssgproject.content\_profile\_cis was used as the baseline due to its comprehensive criteria for ensuring secure server configurations.

## 2.2.1 Steps followed for Executing the Vulnerability Assessment

The assessment spanned two virtual machines (VMs): a "Master" system responsible for performing scanning activities and a "Client" system representing the target. The primary focus was on assessing SSH configurations and ensuring adherence to security benchmarks.

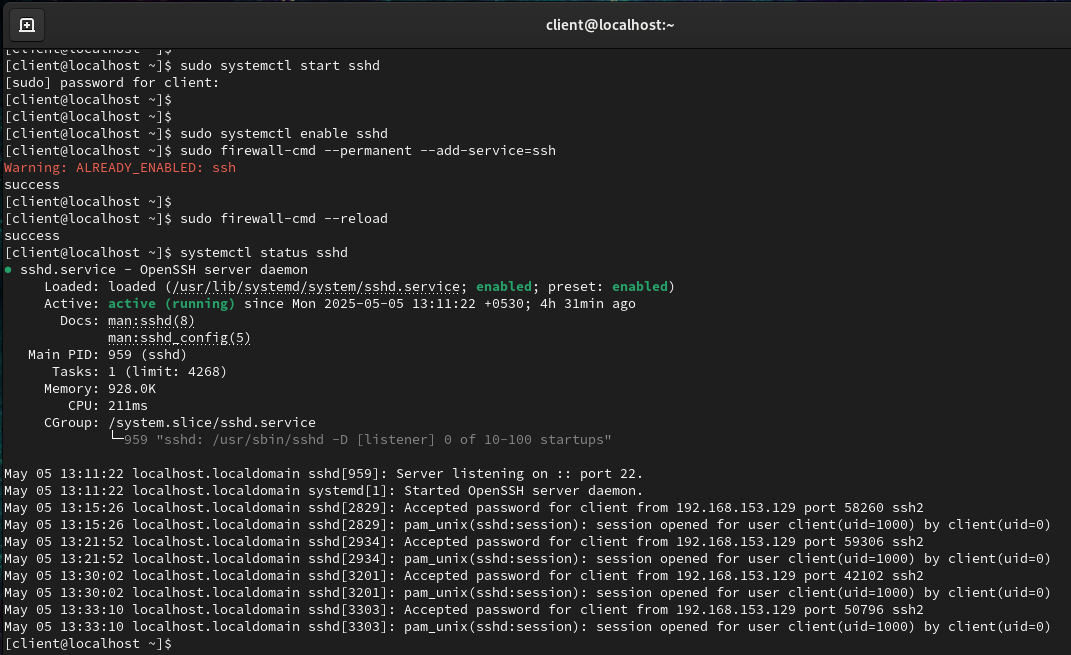
1. **VM Preparation and Implementing Environment Setup**  
   Both the Master and Client VMs were created and updated to the latest software versions:
2. **OpenSCAP Installation preparation -** This ensured the system was prepared for OpenSCAP installation and scanning. On both VMs, the necessary tools were installed:

A screenshot of a computer

AI-generated content may be incorrect.

*Figure 2: OPenSCAP Installation*

1. **SSH Configuration for Remote Scanning**  
   On the Client VM, the SSH service was configured to facilitate remote access:
   1. Started and enabled the SSH service
   2. Configured the firewall to allow SSH traffic
   3. Verified SSH service status
   4. On the Master VM, SSH connectivity to the Client VM was tested:



*Figure 3: Getting Inter VM communication over SSH*

1. Execute the scan : on both Master and Client VMs agents were installed as below sequence

A screenshot of a computer

AI-generated content may be incorrect.

*Figure 4: Execution commands from OpenSCAP on the Master VM*

## 2.3 Evaluation

The vulnerability assessment identified issues in SSH configurations and cryptographic policies on the client VM. Misconfigured parameters like MaxSessions and MaxStartups could lead to resource exhaustion, while weak cryptographic algorithms posed risks to data confidentiality. These findings highlight gaps in compliance with security benchmarks and underscore the importance of addressing configuration weaknesses to improve the network's security posture.

# 3.Results and Mitigation Recommendations

**3.1 Result of the Vulnerability Scan**

The OpenSCAP vulnerability scan produced an HTML report summarizing the security assessment. As illustrated in the accompanying image, 145 test cases were successfully passed, 96 tests failed, and 26 were categorized as "other." The overall compliance score achieved was 70.41%, reflecting areas of improvement required to meet the defined security benchmarks. Here are more deep level security test cases as showing in below figure

A screenshot of a computer

AI-generated content may be incorrect.

*Figure 5: Compliance and scoring section*

The report provides detailed insights into individual security checks, highlighting failed test cases related to SSH configurations and cryptographic policies.

**3.2 Vulnerability Severity and Impact Assessment**

The scan categorized vulnerabilities based on their severity: critical, high, medium, and low. The critical vulnerabilities pose an immediate threat to the system's security and require urgent attention. High and medium vulnerabilities, while less severe, also demand prompt resolution to prevent potential exploitation. Low-severity issues should be addressed as part of routine maintenance.

**A screenshot of a computer

AI-generated content may be incorrect.**

*Figure 6: Periodizing the severity of the Results*

**3.2 Mitigation Recommendations**

1. Apply Security Patches: Ensure all software and systems are updated with the latest patches.  
2. Configure System Settings: Implement recommended configurations to mitigate misconfigurations.  
3. Use Monitoring Tools: Deploy monitoring tools to detect and respond to potential threats.  
4. Conduct Regular Audits: Periodically evaluate the system's security posture to identify new vulnerabilities.  
5. Enhance Access Controls: Implement strict access controls to minimize unauthorized access.

# 4. References

**[1]** Red Hat Security Content Automation Protocol (SCAP) Guide. Available at: https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/ (Accessed: 5 May 2025).

**[2]** National Institute of Standards and Technology (NIST). Security Content Automation Protocol (SCAP). Available at: <https://csrc.nist.gov/projects/security-content-automation-protocol> (Accessed: 5 May 2025).

**[3]** Center for Internet Security (CIS). CIS Benchmarks. Available at: https://www.cisecurity.org/cis-benchmarks (Accessed: 5 May 2025).

**[4]** SCAP Security Guide for OpenSCAP. Available at: <https://github.com/ComplianceAsCode/content> (Accessed: 5 May 2025).