# Linux Security Hardening Audit Tool Report

## Abstract

This work implemented a full Linux Security Hardening Audit Tool for automated assessment of security measures against CIS benchmarks and wide spread standards. The utility checks firewall settings, SSH hardening options, file permissions, service verification, as well as presence of rootkits, among others against Linux distributions. It is implemented in both Python and Bash, and provides comprehensive scorecards for grading an environment's compliance status along with recommendations. The solution was designed to solve the pressing need to standardize security auditing in the enterprise, to save manual audit time, to improve accuracy, and to maintain consistency.

## Introduction

## Manual security audits take time, are prone to errors and not consistent. This work presents an automatic security audit tool that performs a structural check of Linux systems against known security standards. Organizations using the Linux Hardening Audit Tool as a common security audit mechanism can consistently audit distributed systems. By utilizing checks defined from CIS(Center for Internet Security) benchmarks, the tool also covers a broad area for security hardening and provides readable output in-order for improving the security.

## Tools Used

1. **Python 3**: Core implementation with advanced data structures, subprocess management, and JSON reporting
2. **Bash Shell**: Lightweight version optimized for minimal dependencies and maximum portability

**System Assessment Utilities:**

1. **systemctl**: Analysis on the management of services and Unwanted services
2. **iptables/ufw**: Firewall configuration assessment and rule analysis
3. **ss/netstat**: Network connection monitoring and port scanning
4. **stat**: File Permission Check and Ownership Authentication

## Steps Involved in Building the Project

## **Phase 1: Study of CIS benchmarks and security frameworks to narrow down on target areas.**

## **Stage 2: Specialty modules were created for each security discipline**

## **Stage 3: Adopted smart technologies for detection.**

## **Phase 4: Created an integrated reporting framework.**

## **Phase 5: Tested the whole thing on multiple Linux destros (Ubuntu, CentOS, Arch)**

## Conclusion

The LSHAT (Linux Security Hardening Audit Tool) fills an enormous gap in the landscape today for Linux systems, where no pre-existing solution focus on providing high level security checklists/experts specifically tailored to testing one local system. This is a strong work, bridging advanced security analysis and pragmatic usability in a versatile approach.

This software enables continuous security monitoring and compliance, enhancing security posture in Linux-based infrastructures.