Linux Hardening Audit Tool

- **Dharunya mahalakshmi B**

Introduction

Securing Linux servers requires systematic auditing to identify configuration weaknesses and compliance gaps. The Linux Hardening Audit Tool is an open-source Python utility designed to help users efficiently assess and enhance the security posture of Linux systems by automating core hardening and audit checks based on recognized industry standards.

Abstract

The project aims to provide a lightweight, easily deployable solution for Linux security auditing. By simulating critical checks (firewall status, service hygiene, SSH hardening, file permissions, and rootkit traces), it produces actionable reports that guide system administrators in remediating vulnerabilities. This hands-on tool supplements official compliance benchmarks and enables rapid security assessments, contributing to stronger system defense.

Tools Used

- **Python 3**: Main programming language for the audit script.
- **Standard OS utilities**: The tool calls system binaries such as `ufw`, `firewalld`, `iptables`, `ss`, `systemctl`, and `lsmod` to gather evidence from the host.
- **Linux system files**: Audits configurations and permissions on `/etc/passwd`, `/etc/group`, `/etc/shadow`, and `/etc/ssh/sshd_config`.
- **Optional JSON output**: Enables integration with other security tools or workflows.

Steps Involved in Building the Project

1. **Requirement Analysis**: Identified the common security benchmarks (CIS, industry best practices) required for baseline hardening.
2. **Tool Selection**: Chose essential OS commands and configuration files for auditing; implemented checks using Python's `subprocess` and OS modules.
3. **Script Design**: Built modular functions to verify firewall operation, disabled risky services, SSH settings, file permissions, and rootkit indicators.
4. **Reporting Logic**: Designed the output as a readable console summary and optional structured JSON for further processing.
5. **Testing and Validation**: Ran tests across diverse virtual Linux environments to ensure reliability and accuracy. Documentation and error handling were added to accommodate differences in Linux distributions.
6. **Remediation Guidance**: Embedded step-by-step recommendations for each failed control to help administrators address issues directly from the report.

Conclusion

The Linux Hardening Audit Tool serves as a practical solution for security-conscious administrators and developers seeking to improve system resiliency. By automating crucial checks and offering clear remediation advice, the tool streamlines the process of detecting and addressing vulnerabilities, complementing official security frameworks and reducing risk on Linux deployments.

Output