ShieldOS – Linux Hardening Audit Tool

Author: Suyash Pathade  
Institute: Pune Institute of Computer Technology (PICT)  
Domain: Cybersecurity, Linux Security Auditing

# Introduction

In today's rapidly evolving cyber landscape, securing Linux systems has become paramount for organizations and individual users alike. Misconfigurations, outdated services, and exposed system parameters often become entry points for attackers. ShieldOS is a lightweight, modular Linux auditing tool built to identify such weaknesses and recommend hardening actions. The project emphasizes security hygiene, automation, and clear reporting to empower users at all levels of technical proficiency.

# Abstract

ShieldOS is a command-line tool designed to perform a comprehensive security audit of Linux-based operating systems. It performs checks across several key areas including OS configuration, firewall settings, file permissions, rootkit detection, service hardening, user account safety, and more. Reports are generated in multiple formats such as .txt, .html, and .json, and include a summarized scorecard and actionable recommendations. The tool is interactive, extensible, and provides a security tip of the day with every run.

# Tools Used

- Python 3.8+: Core programming language

- Jinja2: HTML report generation via templating

- Bash: Shell script wrapper for Python CLI

- subprocess module: To run system-level Linux commands

- systemctl, ufw: System and firewall interaction

- chkrootkit: Rootkit detection utility

# Steps Involved in Building the Project

1. Requirement Analysis:

- Identified key hardening and auditing areas (users, SSH, firewall, services, file permissions).

- Outlined modular design to keep code extensible.

2. CLI Design:

- Used argparse to provide customizable flags like --section, --fast, --json, --output.

3. Audit Modules:

- Developed Python functions for each check category: System Info, Firewall & SSH Status, File Permissions, Rootkit Detection (automated + manual), User Account and Sudo Policy, Service Risk Analysis, Advanced Hardening (audit logs, login banner, etc.)

4. Report Generation:

- Wrote functions to export audits to .txt, .html, and .json.

- HTML report styled with dark/light themes, print-ready layout, and Jinja2 templates.

5. Automation & Polish:

- Wrapped the tool in a colorful Bash launcher with ASCII art and randomized cybersecurity tips.

- Introduced .gitignore, LICENSE, and a proper folder structure for GitHub publishing.

# Conclusion

ShieldOS delivers a complete Linux hardening audit experience with clarity, usability, and extensibility at its core. It combines best practices from cybersecurity operations and Linux internals into an accessible tool usable by students, sysadmins, and professionals alike. ShieldOS has laid the foundation for future features like live dashboards, integration with cron jobs, and real-time notifications. Through this project, deep insights into system security and Python-based tooling were achieved, making it a significant milestone in my cybersecurity learning journey.