ShieldOS – Linux Hardening Audit Tool

Author: Suyash Pathade
Institute: Pune Institute of Computer Technology (PICT)

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 Misconfigurations, outdated services, and exposed system parameters often become entry points for attackers.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 modular, Python-based Linux hardening audit tool that performs security analysis across key domains including system configuration, file permissions, firewall status, service behavior, user account safety, and potential rootkit infections. It generates reports in multiple formats (`.txt`, `.html`, `.json`) and includes a scorecard summary and best practice recommendations. It is fast, flexible, and customizable using CLI flags, and provides users with a practical way to improve the security posture of their systems.

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. **Planning**: Identified audit sections to cover the essentials of system security (firewall, services, users, permissions, rootkits).

2. **Modular Codebase**: Implemented separate functions for each category to ensure code readability, scalability, and testability.

3. **CLI Integration**: Added user-friendly command-line flags like --fast, --section, --json, and --output using argparse.

4. **Reporting System**: Designed and exported results in HTML (print-ready and theme-switchable), plaintext, and JSON formats.

5. **Audit Logic**: Each audit checks for real-world vulnerabilities like UID 0 clones, world-writable files, empty passwords, and passwordless sudoers.

6. **Bash Wrapper**: Crafted a vibrant CLI experience with a cyber-themed banner, motivational security tips, and dynamic help menus.

7. **Project Hardening**: Created .gitignore, .gitkeep, LICENSE (MIT), and README with badges to prepare the tool for GitHub release.

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.