# Linux Hardening Audit Tool – Project Report

## Introduction

The Linux operating system is widely used in enterprise environments. Securing these systems is crucial to prevent unauthorized access, misconfigurations, and exploitation. This project aims to automate basic Linux security checks using a Python-based audit tool.

---

## Abstract

This project involved building an automated Linux Hardening Audit Tool using Python to perform essential security audits. The script checks firewall status, SSH configurations, file permissions, unused services, rootkit indicators, user accounts, world writable files, password expiry policies, active ports, and the sudoers file. It generates a detailed report with a security score and recommendations to help system administrators strengthen their system security posture efficiently.

---

## Tools Used

- **Python 3** – Programming language to build the audit tool
- **Linux Terminal Commands** – ufw, chkrootkit, netstat, systemctl, find, chage, etc.
- **VS Code / Sublime** – For writing and editing Python scripts
- **Operating System** – Kali Linux for testing and demonstration

---

## Steps Involved in Building the Project

1. **Project Planning**
   Decided core audit features required in the tool for basic hardening checks.
2. **Setting Up Environment**
   Installed necessary packages like chkrootkit and ensured ufw was configured.
3. **Script Development**
   - **Day 1-3:** Wrote functions to check firewall, SSH settings, file permissions, running services, rootkit indicators, and user accounts.
   - **Day 4:** Added world writable file checks and password expiry policy checks.
   - **Day 5:** Implemented scoring logic and security recommendations section.
   - **Day 6 (Final Polish):** Added active ports and connections scan, sudoers file check, and cleaned the code with comments for clarity.

4. **Testing**
   Ran the tool on the Kali Linux environment to verify output accuracy and validated that it generated audit_report.txt successfully with an appropriate security score.

5. **Documentation**
   Prepared final code comments, project summary, and demonstration screenshots for submission and interview readiness.

---

**Conclusion**

The Linux Hardening Audit Tool project strengthened understanding of practical cybersecurity auditing by automating essential system checks. It demonstrates real-world skills in writing audit scripts, interpreting Linux command outputs, and recommending security improvements. This tool can be further expanded to include vulnerability scanning integrations in future projects for advanced system audits.