Linux Hardening Audit Tool

Introduction

In today's digital environment, securing Linux systems is crucial to protect sensitive data and ensure system integrity. This project aims to develop a Linux Hardening Audit Tool that automates security audits by checking system configurations and identifying vulnerabilities. The tool provides recommendations based on industry standards to improve system security.

Abstract

The Linux Hardening Audit Tool is a shell script designed to audit and analyze key security parameters of a Linux system. It performs multiple checks including firewall status, SSH configurations, file permissions, unwanted services, rootkit scans, kernel version, and world-writable directories. The results are summarized with compliance scores and recommended actions for improving system hardening, helping administrators proactively secure their systems.

Tools Used

- Bash (Shell Scripting Language)
- Linux Operating System (Ubuntu/Kali)
- chkrootkit (Rootkit scanner)
- ufw (Firewall utility)
- netstat (Network utility)
- grep, awk, stat, find (Linux built-in commands)

Steps Involved in Building the Project

1. Installed Linux system (Kali Linux used in this project).
2. Created a project directory using mkdir and navigated into it.
3. Developed the audit script using Bash scripting language.
4. Implemented different checks: Firewall, SSH, file permissions, unwanted services, rootkits, kernel version, world-writable files.

5. Installed chkrootkit using apt install chkrootkit.
6. Executed the script using sudo ./linux_audit.sh to perform system audit.
7. Captured audit outputs, analyzed compliance score, and recorded recommendations.
8. Prepared project documentation with code and results for submission.

Conclusion

The Linux Hardening Audit Tool successfully automates the basic security audit of Linux systems. By identifying weak configurations and providing actionable recommendations, the tool simplifies the system hardening process and enhances overall system security. This project demonstrates the importance of automation in cybersecurity and serves as a practical solution for Linux system administrators.