Linux & macOS Hardening Audit Project

Introduction

This project focused on auditing and hardening two systems: Kali Linux and macOS. The objective was to identify misconfigurations and vulnerabilities, apply fixes, and validate improvements with compliance scoring.

Abstract

The baseline audit revealed serious security gaps. Kali Linux scored 49.5% compliance, failing SSH hardening, password policies, updates, audit logging, and brute-force protection. macOS scored 30.5%, failing firewall, SSH, password policies, and audit logging. After remediation — applying updates, enforcing password policies, hardening SSH, enabling audit logging and brute-force defenses — both systems showed improved security posture, demonstrating the effectiveness of OS hardening.

Tools Used

- Python (linux_audit.py) – custom audit tool for Linux
- Bash (mac_audit.sh) – macOS audit checks
- Linux Security Tools – ufw, auditd, fail2ban
- macOS Security Tools – socketfilterfw (firewall), fdesetup (FileVault), softwareupdate

Steps Involved

- Baseline Audit: Kali Linux compliance score 49.5%; macOS compliance score 30.5%.
- Identified Issues: Kali – weak SSH config, weak password policy, 449 outdated packages, auditd and Fail2ban disabled. macOS – firewall undetected, weak SSH settings, no password policy, audit logging disabled.
- Remediation Actions: Kali – applied updates, hardened SSH, enabled auditd and Fail2ban, enforced password policy. macOS – enabled firewall and FileVault, disabled Remote Login, applied updates.
- Re-Audit: Confirmed improved compliance with critical risks resolved.

Conclusion

Hardening improved both systems significantly, reducing exposure to brute-force attacks, unpatched vulnerabilities, and weak authentication. This project highlights the importance of continuous auditing, timely updates, and layered defenses across different platforms.