Linux Hardening Audit Report

Author: Mohammed Nihal
Platform: Kali Linux (VirtualBox – Oracle VM)
Kernel Version: 6.18.9-kali
Audit Date: 21 Feb 2026

1. Objective

The objective of this project was to design and implement a Linux Hardening Audit Tool to evaluate system security configuration against CIS-style best practices. The tool audits firewall status, SSH hardening, file permissions, rootkit presence, running services, and system updates, generating a compliance score and risk classification.

2. Firewall Configuration

UFW firewall was enabled and confirmed active. Port 22 (SSH) was allowed, Port 80 denied, and additional deny rules configured.

3. SSH Security Assessment

Current SSH configuration detected 'PermitRootLogin yes' and 'PasswordAuthentication yes', which pose security risks such as brute-force attacks and unauthorized root access.

4. Rootkit & Malware Scan

chkrootkit and rkhunter were executed. No rootkits or malicious indicators were detected.

5. Lynis Audit

Lynis 3.1.6 was used to perform a full system audit. Standard hardening recommendations were identified, mainly focused on SSH security and authentication mechanisms.

6. Custom Audit Tool Results

Check	Status
Firewall	PASS
Root Login	FAIL
Password Authentication	WARN
/etc/shadow Permissions	PASS
Insecure Services	PASS
Rootkit Detection	PASS
System Updates	WARN

Security Score: 57.14%
Risk Level: MEDIUM

7. Recommendations

- Disable SSH root login - Disable password authentication (use SSH keys) - Apply pending system updates - Configure Fail2Ban for brute-force protection - Restrict SSH access to trusted IP addresses