Linux Hardening Audit Tool

By- Dhruv Bhatia

Introduction

Linux systems are widely deployed in enterprise and cloud environments due to their stability, performance, and flexibility. However, improper configurations or lack of updates can expose them to critical vulnerabilities. System hardening refers to the process of securing a system by reducing its attack surface—disabling unnecessary services, enforcing secure configurations, and auditing system policies. To assist in this process, we developed a Linux Hardening Audit Tool that performs automated security checks and generates a report outlining compliance and risks.

Objectives

- Perform a basic security audit of a Linux system.
- Identify misconfigurations and weaknesses.
- Provide scores and actionable remediation suggestions.
- Generate a simple, readable report for system administrators.

Methodology

The tool was implemented in **Python** and designed to run on systems with administrative privileges. It performs a series of checks in the following categories:

Firewall Configuration: Checks whether a firewall is enabled and if restrictive rules are in place (using ufw, iptables, or firewalld).

User and Group Auditing: Detects unnecessary or privileged user accounts, empty passwords, and sudoers file configurations.

SSH Configuration: Scans /etc/ssh/sshd_config to verify settings like:

- Root login disabled
- Protocol version 2
- Strong cipher usage

File and Directory Permissions: Checks for world-writable files and sensitive files (e.g., /etc/passwd, /etc/shadow) with improper permissions.

Installed Packages and Updates: Checks for outdated or vulnerable packages using apt or yum.

Service and Daemon Auditing: Identifies unnecessary or insecure services running (e.g., Telnet, FTP).

Sample Output Snippet:

```
›[-] Firewall is not active. Enable ufw for better security.
[+] No suspicious services enabled.
[-] Insecure SSH settings detected. Ensure 'PermitRootLogin no' and 'Protocol 2'.
[+] File permissions are correct on /etc/passwd and /etc/shadow.
[+] No basic rootkit indicators found.

--- Recommendations ---
- Enable UFW firewall if disabled: `sudo ufw enable`
- Disable unused services: `systemctl disable <service>`
- Harden SSH: Disable root login and use Protocol 2
- Set correct permissions:
  `chmod 644 /etc/passwd`

- Use chkrootkit or rkhunter for deep rootkit scans

[*] Compliance Score: 60.0% (3/5)
```

Conclusion

The Linux Hardening Audit Tool provides a lightweight yet effective way to assess a system's security posture. While it is not a substitute for professional security assessments or industry frameworks like CIS Benchmarks, it offers a fast and informative snapshot of common misconfigurations. With continuous updates and additional modules (e.g., SELinux/AppArmor, auditd), it can evolve into a robust open-source compliance scanner for small to medium Linux deployments.