Cyber Security Project Report

Linux Auditing & System Hardening

Submitted by:
Pusarla Vinay

Date of Submission:
12th September 2025

Internship Duration:
15th Aug – 15th Sept 2025

Institution/Organization:
Cyber Security Intern

About this Project

This project focuses on auditing and hardening a Linux system using firewall checks, SSH configuration analysis, file permission verification, process monitoring, and rootkit scanning. The goal is to identify weaknesses, strengthen defenses, and improve overall system security.

Index

Introduction:

This project focused on learning and applying Linux auditing and system hardening techniques using practical tools. The aim was to check firewall status, verify SSH configuration, monitor file permissions, detect suspicious processes, and scan for rootkits. These steps improve the security posture of a Linux machine and help prevent malicious exploitation.

Abstract:

The project involved executing security auditing tasks on Kali Linux. The process included creating and running a custom **audit.sh** script for automated system checks and using **chkrootkit** to detect possible rootkits. The report summarizes the tools used, the commands executed, and the key findings.

Tools Used:

- Bash scripting (for automation)
- UFW (Uncomplicated Firewall) – firewall management tool
- chkrootkit – rootkit detection tool
- System utilities: **ps**, **ls**, **cat**, **nano**, **chmod**

Steps Involved

Step 1 – Creating the Audit Script

nano audit.sh chmod
+x audit.sh sudo
./audit.sh
This script performed firewall checks, SSH config checks, file permission audits, process monitoring, and checked for rootkits.

Step 2 – Checking Firewall (UFW)

sudo ufw status
Result: Firewall was active. Rules showed SSH (port 22) was allowed.

Step 3 – Checking SSH Config

- Verified that root login was disabled.
- Password authentication was still enabled (recommendation: use SSH keys).

Step 4 – File Permissions

ls -l /etc/passwd ls -l
/etc/shadow
/etc/passwd □ permissions secure (644)
/etc/shadow □ permissions secure (640)

Step 5 – Checking Suspicious Processes

ps aux --sort=-%cpu | head -10
No major anomalies, but high CPU usage processes flagged.

Step 6 – Installing and Running chkrootkit

sudo apt install chkrootkit -y sudo
chkrootkit
Findings: Most binaries reported clean. Some suspicious warnings flagged but no active rootkits
detected

```
┌──(root㉿kali)-[/home/kali]
└─# nano audit.sh

┌──(root㉿kali)-[/home/kali]
└─# chmod +x audit.sh

┌──(root㉿kali)-[/home/kali]
└─# ./audit.sh

┌──(root㉿kali)-[/home/kali]
└─# cat system_audit_report.txt

Linux Hardening Audit Report - Mon Aug 18 11:27:37 AM EDT 2025
-----------------------------------------------------------
[+] Checking Firewall ...
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)
```

```
┌──(root㉿kali)-[/home/kali]
└─# sudo apt install chkrootkit -y
sudo chkrootkit

Installing:
  chkrootkit

Installing dependencies:
  bsd-mailx  exim4-base  exim4-config  exim4-daemon-light  liblockfile1

Suggested packages:
  exim4-doc-html | exim4-doc-info  eximon4  spf-tools-perl

Summary:
  Upgrading: 0, Installing: 6, Removing: 0, Not Upgrading: 495
  Download size: 2,434 kB
  Space needed: 5,550 kB / 54.9 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 exim4-config all 4.98.2-1 [249 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 exim4-base amd64 4.98.2-1 [1,141 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 exim4-daemon-light amd64 4.98.2-1 [629 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 liblockfile1 amd64 1.17-2 [11.9 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 bsd-mailx amd64 8.1.2-0.20220412cvs-1.1 [82.2 kB]
Get:6 http://http.kali.org/kali kali-rolling/main amd64 chkrootkit amd64 0.58b-5+b2 [321 kB]
Fetched 2,434 kB in 2s (1,167 kB/s)
Preconfiguring packages ...
Selecting previously unselected package exim4-config.
(Reading database ... 413763 files and directories currently installed.)
Preparing to unpack .../0-exim4-config_4.98.2-1_all.deb ...
Unpacking exim4-config (4.98.2-1) ...
Selecting previously unselected package exim4-base.
Preparing to unpack .../1-exim4-base_4.98.2-1_amd64.deb ...
Unpacking exim4-base (4.98.2-1) ...
Selecting previously unselected package exim4-daemon-light.
Preparing to unpack .../2-exim4-daemon-light_4.98.2-1_amd64.deb ...
Unpacking exim4-daemon-light (4.98.2-1) ...
Selecting previously unselected package liblockfile1:amd64.
Preparing to unpack .../3-liblockfile1_1.17-2_amd64.deb ...
Unpacking liblockfile1:amd64 (1.17-2) ...
Selecting previously unselected package bsd-mailx.
Preparing to unpack .../4-bsd-mailx_8.1.2-0.20220412cvs-1.1_amd64.deb ...
Unpacking bsd-mailx (8.1.2-0.20220412cvs-1.1) ...
Selecting previously unselected package chkrootkit.
Preparing to unpack .../5-chkrootkit_0.58b-5+b2_amd64.deb ...
Unpacking chkrootkit (0.58b-5+b2) ...
Setting up chkrootkit (0.58b-5+b2) ...
Created symlink '/etc/systemd/system/timers.target.wants/chkrootkit.timer' → '/usr/lib/systemd/system/chkrootkit.timer'.
Setting up exim4-config (4.98.2-1) ...
Adding system-user for exim (v4)
Setting up liblockfile1:amd64 (1.17-2) ...
Setting up exim4-base (4.98.2-1) ...
exim: DB upgrade, deleting hints-db
update-rc.d: As per Kali policy, exim4 init script is left disabled.
Created symlink '/etc/systemd/system/timers.target.wants/exim4-base.timer' → '/usr/lib/systemd/system/exim4-base.timer'.
exim4-base.service is a disabled or a static unit, not starting it.
Setting up exim4-daemon-light (4.98.2-1) ...
exim4.service is a disabled or a static unit, not starting it.
Setting up bsd-mailx (8.1.2-0.20220412cvs-1.1) ...
update-alternatives: using /usr/bin/bsd-mailx to provide /usr/bin/mailx (mailx) in auto mode
Processing triggers for doc-base (0.11.2) ...
Processing 41 changed doc-base files, 3 added doc-base files...
Processing triggers for libc-bin (2.41-6) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.2.7) ...
ROOTDIR is '/'
Checking 'amd' ...                                  not found
Checking 'basename' ...                             not infected
```

```
Checking 'chfn' ...                                 not infected
Checking 'chsh' ...                                 not infected
Checking 'cron' ...                                 not infected
Checking 'crontab' ...                              not infected
Checking 'date' ...                                 not infected
Checking 'du' ...                                   not infected
Checking 'dirname' ...                              not infected
Checking 'echo' ...                                 not infected
Checking 'egrep' ...                                not infected
Checking 'env' ...                                  not infected
Checking 'find' ...                                 not infected
Checking 'fingerd' ...                              not found
Checking 'gpm' ...                                  not found
Checking 'grep' ...                                 not infected
Checking 'hdparm' ...                               not infected
Checking 'su' ...                                   not infected
Checking 'ifconfig' ...                             not infected
Checking 'inetd' ...                                not tested
Checking 'inetdconf' ...                            not found
Checking 'identd' ...                               not found
Checking 'init' ...                                 not infected
Checking 'killall' ...                              not infected
Checking 'ldsopreload' ...                          not infected
Checking 'login' ...                                not infected
Checking 'ls' ...                                   not infected
Checking 'lsof' ...                                 not infected
Checking 'mail' ...                                 not infected
Checking 'mingetty' ...                             not found
Checking 'netstat' ...                              not infected
Checking 'named' ...                                not found
Checking 'passwd' ...                               not infected
Checking 'pidof' ...                                not infected
Checking 'pop2' ...                                 not found
Checking 'pop3' ...                                 not found
Checking 'ps' ...                                   not infected
Checking 'pstree' ...                               not infected
Checking 'rpcinfo' ...                              not infected
Checking 'rlogind' ...                              not found
Checking 'rshd' ...                                 not found
Checking 'slogin' ...                               not found
Checking 'sendmail' ...                             not infected
Checking 'sshd' ...                                 not infected
Checking 'syslogd' ...                              not found
Checking 'tar' ...                                  not infected
Checking 'tcpd' ...                                 not found
Checking 'tcpdump' ...                              not infected
Checking 'top' ...                                  not infected
Checking 'telnetd' ...                              not found
Checking 'timed' ...                                not found
Checking 'traceroute' ...                           not infected
Checking 'vdir' ...                                 not infected
Checking 'w' ...                                    not infected
Checking 'write' ...                                not found
Checking 'aliens' ...                               started
Searching for suspicious files in /dev ...          not found
Searching for known suspicious directories ...      not found
Searching for known suspicious files ...            not found
Searching for sniffer's logs ...                    not found
Searching for HiDrootkit rootkit ...                not found
Searching for t0rn rootkit ...                      not found
Searching for t0rn v8 (or variation) ...            not found
Searching for Lion rootkit ...                      not found
Searching for RSHA rootkit ...                      not found
Searching for RH-Sharpe rootkit ...                 not found
Searching for Ambient (ark) rootkit ...             not found
Searching for suspicious files and dirs ...         WARNING

WARNING: The following suspicious files and directories were found:
/usr/lib/python3/dist-packages/aiohttp/_websocket/.hash [From Debian package: python3-aiohttp]
/usr/lib/python3/dist-packages/numpy/f2py/tests/src/f2cmap/.f2py_f2cmap [From Debian package: python3-numpy]
/usr/lib/python3/dist-packages/numpy/f2py/tests/src/assumed_shape/.f2py_f2cmap [From Debian package: python3-numpy]
```

Conclusion:

This cybersecurity project demonstrated the importance of systematic Linux auditing and hardening by performing firewall verification, SSH configuration checks, file permission analysis, process monitoring, and rootkit detection. The system was found to be moderately secure, with strengths in areas such as file permissions and disabled root login, but with improvement opportunities in SSH authentication, firewall restrictions, and regular rootkit monitoring.

The project not only validated the effectiveness of Linux security tools and automation scripts but also enhanced practical skills in identifying, interpreting, and mitigating security issues. With a current security score of 80/100, the system is reasonably protected; however, by implementing the recommended improvements, this score can be significantly increased, ensuring stronger resilience against real-world cyber threats.