Linux Hardening Audit Tool - Project Report

1. Introduction

This project report describes the design and implementation of a Linux Hardening Audit Tool developed using Python. The tool audits a Linux system for basic security configurations and generates a text-based report highlighting current status and recommendations for improvement.

2. Objectives

- Check basic Linux security settings.
- Identify misconfigurations in SSH and file permissions.
- Verify if the system is protected by a firewall.
- Detect potential rootkits using chkrootkit (if available).
- Provide hardening recommendations based on the audit.
- Generate a summary report and security score.

3. Tools and Technologies Used

- Python 3.x
- Kali Linux (or any Debian-based distro)
- UFW (Uncomplicated Firewall)
- chkrootkit (optional)

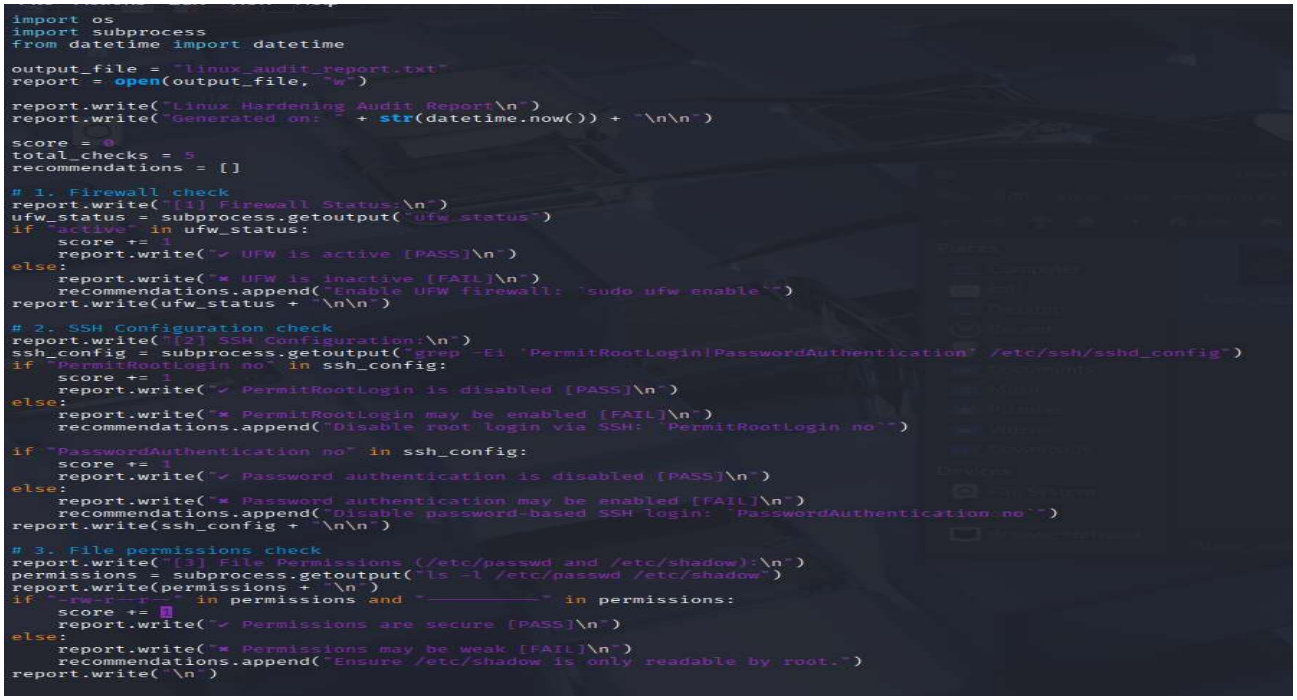
4. Features of the Tool

- ✓ Checks UFW firewall status
- ✓ Verifies SSH hardening settings
- ✓ Checks file permissions of critical files (/etc/passwd, /etc/shadow)
- ✓ Detects rootkits (if chkrootkit is available)
- ✓ Lists disabled/unused system services
- ✓ Generates a detailed audit report with a security score and hardening suggestions

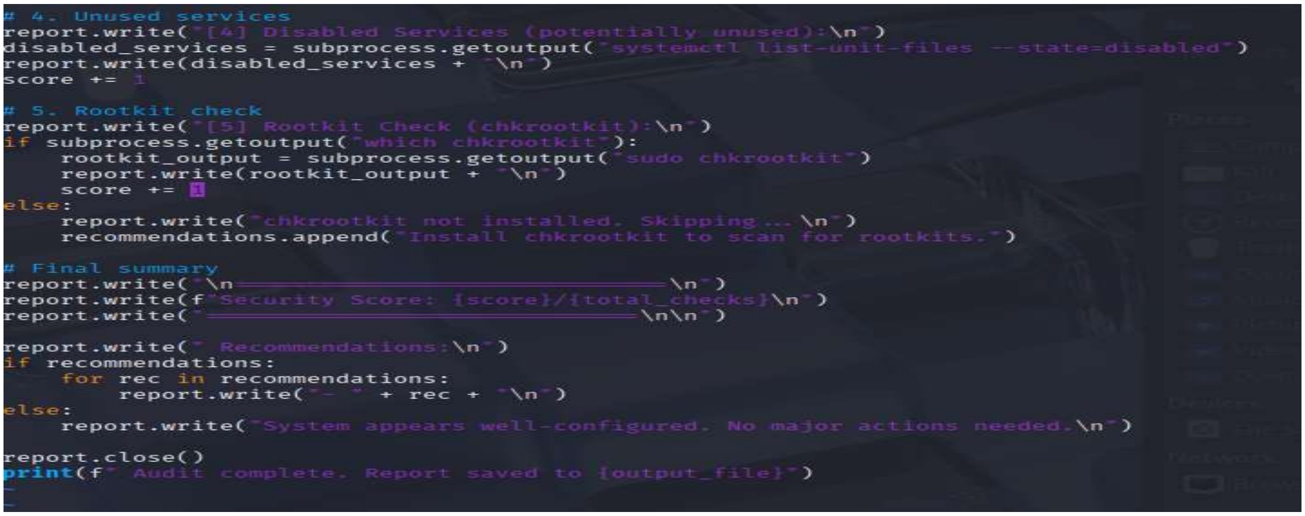
5. How It Works

The tool uses built-in shell commands and Python subprocess module to gather system data and writes the output to a formatted report file.
It checks for active firewall rules, SSH configuration values, sensitive file permissions, unused services, and the presence of rootkits.
Each check is scored and summarized.

Python Code Used to develop this code:



```python
import os
import subprocess
from datetime import datetime

output_file = "linux_audit_report.txt"
report = open(output_file, "w")

report.write("Linux Hardening Audit Report\n")
report.write("Generated on: " + str(datetime.now()) + "\n\n")

score = 0
total_checks = 5
recommendations = []

# 1. Firewall check
report.write("[1] Firewall Status:\n")
ufw_status = subprocess.getoutput("ufw status")
if "active" in ufw_status:
    score += 1
    report.write("✓ UFW is active [PASS]\n")
else:
    report.write("✗ UFW is inactive [FAIL]\n")
    recommendations.append("Enable UFW firewall: `sudo ufw enable`")
report.write(ufw_status + "\n\n")

# 2. SSH Configuration check
report.write("[2] SSH Configuration:\n")
ssh_config = subprocess.getoutput("grep -Ei 'PermitRootLogin|PasswordAuthentication' /etc/ssh/sshd_config")
if "PermitRootLogin no" in ssh_config:
    score += 1
    report.write("✓ PermitRootLogin is disabled [PASS]\n")
else:
    report.write("✗ PermitRootLogin may be enabled [FAIL]\n")
    recommendations.append("Disable root login via SSH: `PermitRootLogin no`")

if "PasswordAuthentication no" in ssh_config:
    score += 1
    report.write("✓ Password authentication is disabled [PASS]\n")
else:
    report.write("✗ Password authentication may be enabled [FAIL]\n")
    recommendations.append("Disable password-based SSH login: `PasswordAuthentication no`")
report.write(ssh_config + "\n\n")

# 3. File permissions check
report.write("[3] File Permissions (/etc/passwd and /etc/shadow):\n")
permissions = subprocess.getoutput("ls -l /etc/passwd /etc/shadow")
report.write(permissions + "\n")
if "-rw-r--r--" in permissions and "----------" in permissions:
    score += 1
    report.write("✓ Permissions are secure [PASS]\n")
else:
    report.write("✗ Permissions may be weak [FAIL]\n")
    recommendations.append("Ensure /etc/shadow is only readable by root.")
report.write("\n")
```



```python
# 4. Unused services
report.write("[4] Disabled Services (potentially unused):\n")
disabled_services = subprocess.getoutput("systemctl list-unit-files --state=disabled")
report.write(disabled_services + "\n")
score += 1

# 5. Rootkit check
report.write("[5] Rootkit Check (chkrootkit):\n")
if subprocess.getoutput("which chkrootkit"):
    rootkit_output = subprocess.getoutput("sudo chkrootkit")
    report.write(rootkit_output + "\n")
    score += 1
else:
    report.write("chkrootkit not installed. Skipping...\n")
    recommendations.append("Install chkrootkit to scan for rootkits.")

# Final summary
report.write("\n══════════════════════════════════════\n")
report.write(f"Security Score: {score}/{total_checks}\n")
report.write("══════════════════════════════════════\n\n")

report.write(" Recommendations:\n")
if recommendations:
    for rec in recommendations:
        report.write("- " + rec + "\n")
else:
    report.write("System appears well-configured. No major actions needed.\n")

report.close()
print(f" Audit complete. Report saved to {output_file}")
```

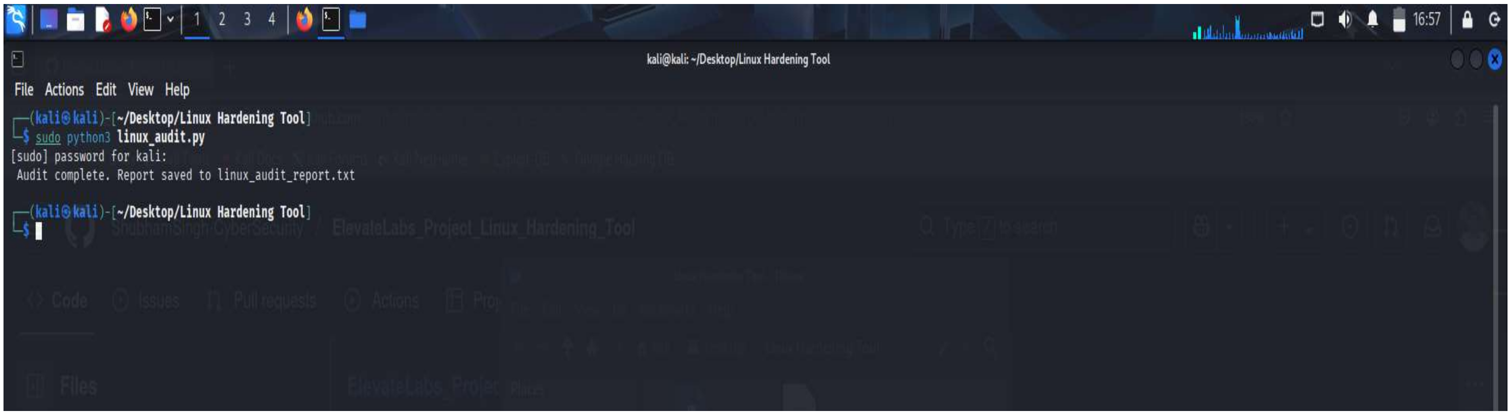
6. How to Run the Tool

1. Make the script executable using `chmod +x linux_audit.py`

2. Run with sudo: `sudo ./linux_audit.py`

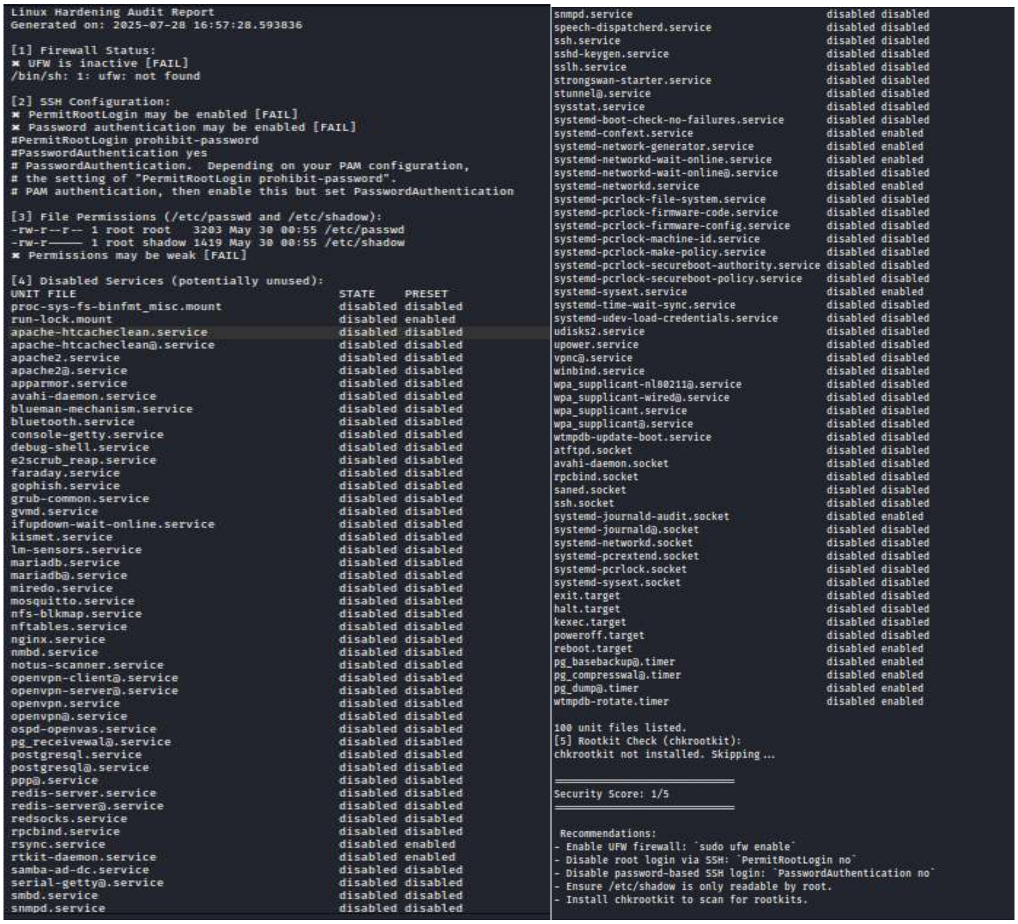
3. Output will be saved in `linux_audit_report.txt`

*Sample Image to demonstrate the execution:



```
┌──(kali㉿kali)-[~/Desktop/Linux Hardening Tool]
└─$ sudo python3 linux_audit.py
[sudo] password for kali:
 Audit complete. Report saved to linux_audit_report.txt

┌──(kali㉿kali)-[~/Desktop/Linux Hardening Tool]
└─$ 
```

7. Sample Output



```
Linux Hardening Audit Report
Generated on: 2025-07-28 16:57:28.593836

[1] Firewall Status:
✖ UFW is inactive [FAIL]
/bin/sh: 1: ufw: not found

[2] SSH Configuration:
✖ PermitRootLogin may be enabled [FAIL]
✖ Password authentication may be enabled [FAIL]
#PermitRootLogin prohibit-password
#PasswordAuthentication yes
# PasswordAuthentication.  Depending on your PAM configuration,
# the setting of "PermitRootLogin prohibit-password".
# PAM authentication, then enable this but set PasswordAuthentication

[3] File Permissions (/etc/passwd and /etc/shadow):
-rw-r--r-- 1 root root   3203 May 30 00:55 /etc/passwd
-rw-r----- 1 root shadow 1419 May 30 00:55 /etc/shadow
✖ Permissions may be weak [FAIL]

[4] Disabled Services (potentially unused):
UNIT FILE                                    STATE    PRESET
proc-sys-fs-binfmt_misc.mount                disabled disabled
run-lock.mount                               disabled enabled
apache-htcacheclean.service                  disabled disabled
apache-htcacheclean@.service                 disabled disabled
apache2.service                              disabled disabled
apache2@.service                             disabled disabled
apparmor.service                             disabled disabled
avahi-daemon.service                         disabled disabled
blueman-mechanism.service                    disabled disabled
bluetooth.service                            disabled disabled
console-getty.service                        disabled disabled
debug-shell.service                          disabled disabled
e2scrub_reap.service                         disabled disabled
faraday.service                              disabled disabled
gophish.service                              disabled disabled
grub-common.service                          disabled disabled
gvmd.service                                 disabled disabled
ifupdown-wait-online.service                 disabled disabled
kismet.service                               disabled disabled
lm-sensors.service                           disabled disabled
mariadb.service                              disabled disabled
mariadb@.service                             disabled disabled
miredo.service                               disabled disabled
mosquitto.service                            disabled disabled
nfs-blkmap.service                           disabled disabled
nftables.service                             disabled disabled
nginx.service                                disabled disabled
nmbd.service                                 disabled disabled
notus-scanner.service                        disabled disabled
openvpn-client@.service                      disabled disabled
openvpn-server@.service                      disabled disabled
openvpn.service                              disabled disabled
openvpn@.service                             disabled disabled
ospd-openvas.service                         disabled disabled
pg_receivewal@.service                       disabled disabled
postgresql.service                           disabled disabled
postgresql@.service                          disabled disabled
ppp@.service                                 disabled disabled
redis-server.service                         disabled disabled
redis-server@.service                        disabled disabled
redsocks.service                             disabled disabled
rpcbind.service                              disabled disabled
rsync.service                                disabled enabled
rtkit-daemon.service                         disabled enabled
samba-ad-dc.service                          disabled disabled
serial-getty@.service                        disabled disabled
smbd.service                                 disabled disabled
snmpd.service                                disabled disabled
```

```
snmpd.service                                disabled disabled
speech-dispatcherd.service                   disabled disabled
ssh.service                                  disabled disabled
sshd-keygen.service                          disabled disabled
sslh.service                                 disabled disabled
strongswan-starter.service                   disabled disabled
stunnel@.service                             disabled disabled
sysstat.service                              disabled disabled
systemd-boot-check-no-failures.service       disabled disabled
systemd-confext.service                      disabled enabled
systemd-network-generator.service            disabled enabled
systemd-networkd-wait-online.service         disabled enabled
systemd-networkd-wait-online@.service        disabled disabled
systemd-networkd.service                     disabled enabled
systemd-pcrlock-file-system.service          disabled disabled
systemd-pcrlock-firmware-code.service        disabled disabled
systemd-pcrlock-firmware-config.service      disabled disabled
systemd-pcrlock-machine-id.service           disabled disabled
systemd-pcrlock-make-policy.service          disabled disabled
systemd-pcrlock-secureboot-authority.service disabled disabled
systemd-pcrlock-secureboot-policy.service    disabled disabled
systemd-sysext.service                       disabled enabled
systemd-time-wait-sync.service               disabled disabled
systemd-udev-load-credentials.service        disabled disabled
udisks2.service                              disabled disabled
upower.service                               disabled disabled
vpnc@.service                                disabled disabled
winbind.service                              disabled disabled
wpa_supplicant-nl80211@.service              disabled disabled
wpa_supplicant-wired@.service                disabled disabled
wpa_supplicant.service                       disabled disabled
wpa_supplicant@.service                      disabled disabled
wtmpdb-update-boot.service                   disabled disabled
atftpd.socket                                disabled disabled
avahi-daemon.socket                          disabled disabled
rpcbind.socket                               disabled disabled
saned.socket                                 disabled disabled
ssh.socket                                   disabled disabled
systemd-journald-audit.socket                disabled enabled
systemd-journald@.socket                     disabled disabled
systemd-networkd.socket                      disabled disabled
systemd-pcrextend.socket                     disabled disabled
systemd-pcrlock.socket                       disabled disabled
systemd-sysext.socket                        disabled disabled
exit.target                                  disabled disabled
halt.target                                  disabled disabled
kexec.target                                 disabled disabled
poweroff.target                              disabled disabled
reboot.target                                disabled enabled
pg_basebackup@.timer                         disabled enabled
pg_compresswal@.timer                        disabled enabled
pg_dump@.timer                               disabled enabled
wtmpdb-rotate.timer                          disabled enabled

100 unit files listed.
[5] Rootkit Check (chkrootkit):
chkrootkit not installed. Skipping...

══════════════════════════════
Security Score: 1/5
══════════════════════════════

 Recommendations:
- Enable UFW firewall: `sudo ufw enable`
- Disable root login via SSH: `PermitRootLogin no`
- Disable password-based SSH login: `PasswordAuthentication no`
- Ensure /etc/shadow is only readable by root.
- Install chkrootkit to scan for rootkits.
```

8. Conclusion

This Linux Hardening Audit Tool provides an easy and effective way to assess the security posture of a Linux system.
It is lightweight, beginner-friendly, and useful for students, system administrators, or anyone seeking to improve system hardening.