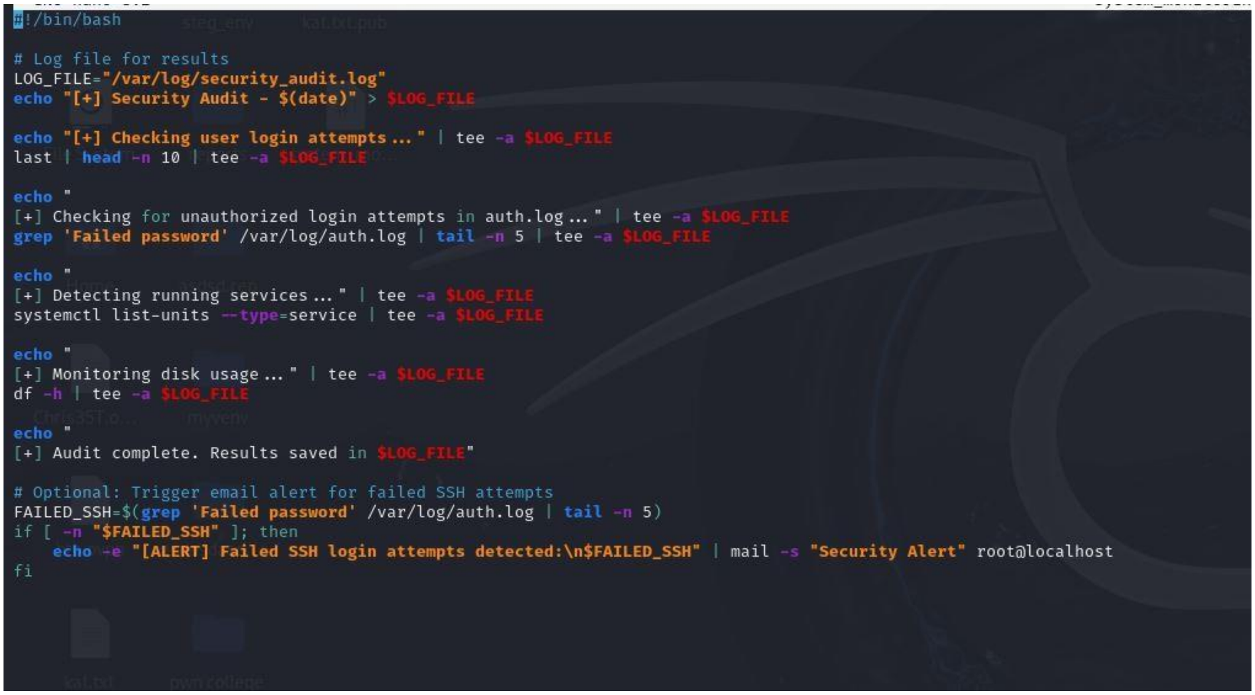
Task 5 :

Automated Security Auditing & Scripting

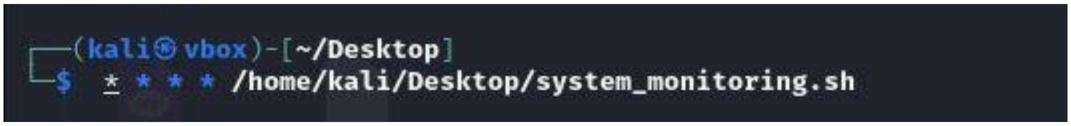
Exploit



```
#!/bin/bash

# Log file for results
LOG_FILE="/var/log/security_audit.log"
echo "[+] Security Audit - $(date)" > $LOG_FILE

echo "[+] Checking user login attempts ... " | tee -a $LOG_FILE
last | head -n 10 | tee -a $LOG_FILE

echo "
[+] Checking for unauthorized login attempts in auth.log ... " | tee -a $LOG_FILE
grep 'Failed password' /var/log/auth.log | tail -n 5 | tee -a $LOG_FILE

echo "
[+] Detecting running services ... " | tee -a $LOG_FILE
systemctl list-units --type=service | tee -a $LOG_FILE

echo "
[+] Monitoring disk usage ... " | tee -a $LOG_FILE
df -h | tee -a $LOG_FILE

echo "
[+] Audit complete. Results saved in $LOG_FILE"

# Optional: Trigger email alert for failed SSH attempts
FAILED_SSH=$(grep 'Failed password' /var/log/auth.log | tail -n 5)
if [ -n "$FAILED_SSH" ]; then
    echo -e "[ALERT] Failed SSH login attempts detected:\n$FAILED_SSH" | mail -s "Security Alert" root@localhost
fi
```

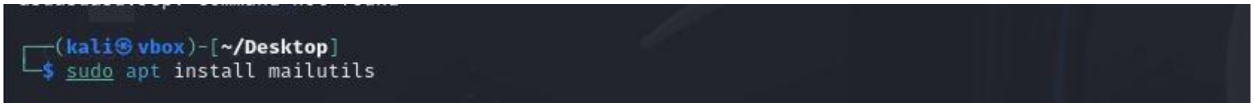
We create a script to simulate an exploitation scenario by identifying weak accounts, unused services, or excessive storage use. These issues can be entry points for attackers or risks for DoS attacks.

Mitigation



```
┌──(kali㉿vbox)-[~/Desktop]
└─$  * * * * /home/kali/Desktop/system_monitoring.sh
```

To automate monitoring, add the script to cron with the following line:
This schedules it to run hourly for continuous system monitoring.



```
┌──(kali㉿vbox)-[~/Desktop]
└─$ sudo apt install mailutils
```

To improve security, set up email alerts for unauthorized SSH attempts.
First, install the required package using:
This helps monitor attacks by sending timely notifications.