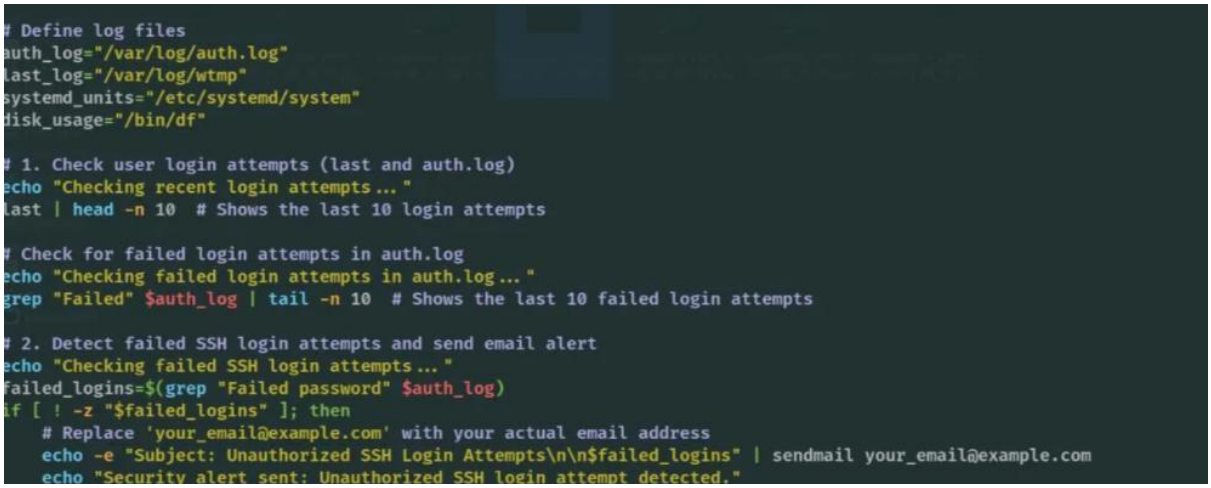
POC TASK 5

Automated Security :



```
# Define log files
auth_log="/var/log/auth.log"
last_log="/var/log/wtmp"
systemd_units="/etc/systemd/system"
disk_usage="/bin/df"

# 1. Check user login attempts (last and auth.log)
echo "Checking recent login attempts..."
last | head -n 10  # Shows the last 10 login attempts

# Check for failed login attempts in auth.log
echo "Checking failed login attempts in auth.log..."
grep "Failed" $auth_log | tail -n 10  # Shows the last 10 failed login attempts

# 2. Detect failed SSH login attempts and send email alert
echo "Checking failed SSH login attempts..."
failed_logins=$(grep "Failed password" $auth_log)
if [ ! -z "$failed_logins" ]; then
    # Replace 'your_email@example.com' with your actual email address
    echo -e "Subject: Unauthorized SSH Login Attempts\n\n$failed_logins" | sendmail your_email@example.com
    echo "Security alert sent: Unauthorized SSH login attempt detected."
```

- It develop and run basic configure systems
- It includes automating the script by scheduled task.

Here we use

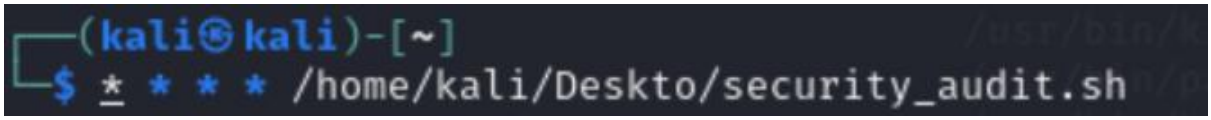
- Login attempts
- Running services
- Disk usage
- Inactive users

Mitigration - Automating monitoring with cron:

1)

Acessing the "crontab" configuration to check security

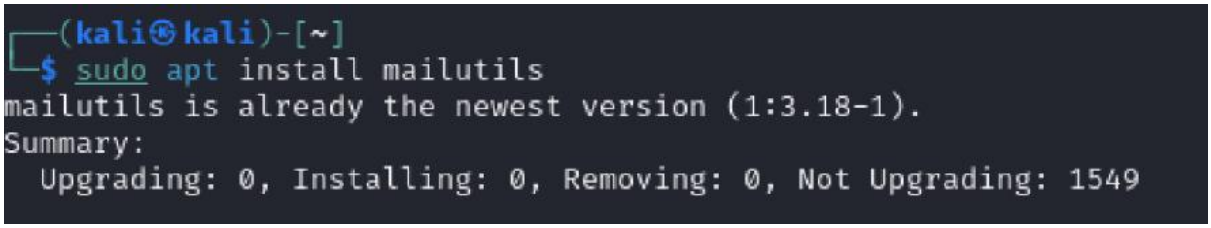
2)



* we use **** /home/kali/Deskto/security_audit.sh to automate monitoring with cron

*It scehdules the script to run Hourly ensuring consistent monitoring.

3)



We should ensure to install "email service" to unaurthorized SSH