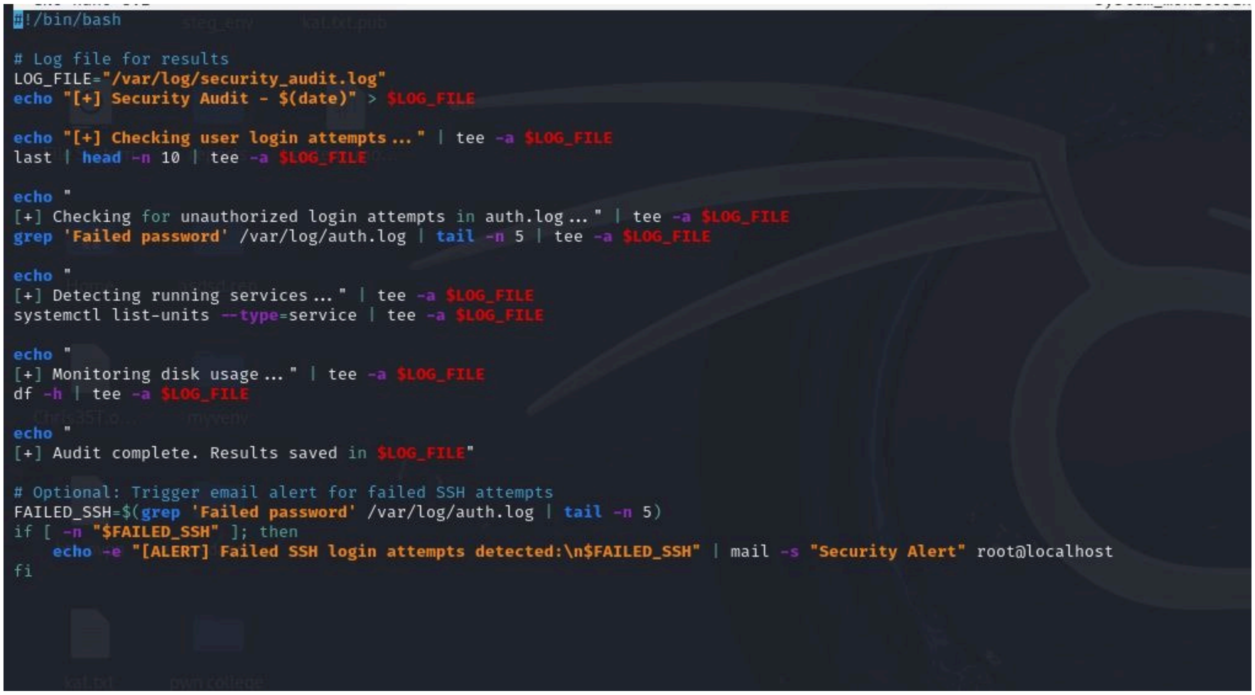
Task 5

Automated Security Auditing & Scripting

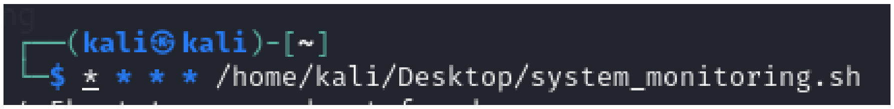
Exploit



```
#!/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 generate a script as an example exploitation scenario which may involve identifying weak accounts from the previous output, such as old or inactive accounts. Additionally, detecting unused or vulnerable services through `systemctl` can reveal potential entry points for attackers. Lastly, noticing excessive storage usage could indicate a risk of Denial of Service DoS attacks exploiting resource exhaustion.

Mitigation

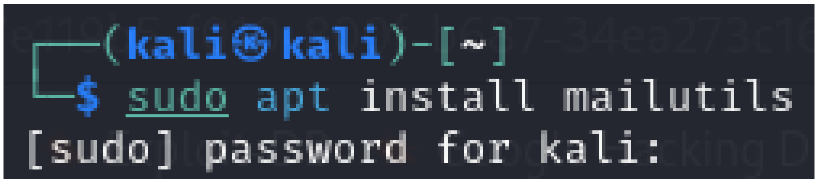


```
┌──(kali㉿kali)-[~]
└─$ * * * * /home/kali/Desktop/system_monitoring.sh
```

To automate proactive monitoring with cron, add the following line to your cron jobs:

```
0 * * * * /path/to/system_monitoring.sh
```

This configuration schedules the script to run hourly, ensuring consistent system monitoring.



```
┌──(kali㉿kali)-[~]
└─$ sudo apt install mailutils
[sudo] password for kali:
```

For enhanced security, implement email alerts for unauthorized SSH attempts. First, ensure `mailutils` is installed using the command:

```
sudo apt install mailutils
```

This solution improves your system's security posture by providing timely notifications and valuable insights into potential attack vectors.