POC Task 5

Task 5: SSH Login Audit

1. Executive Summary

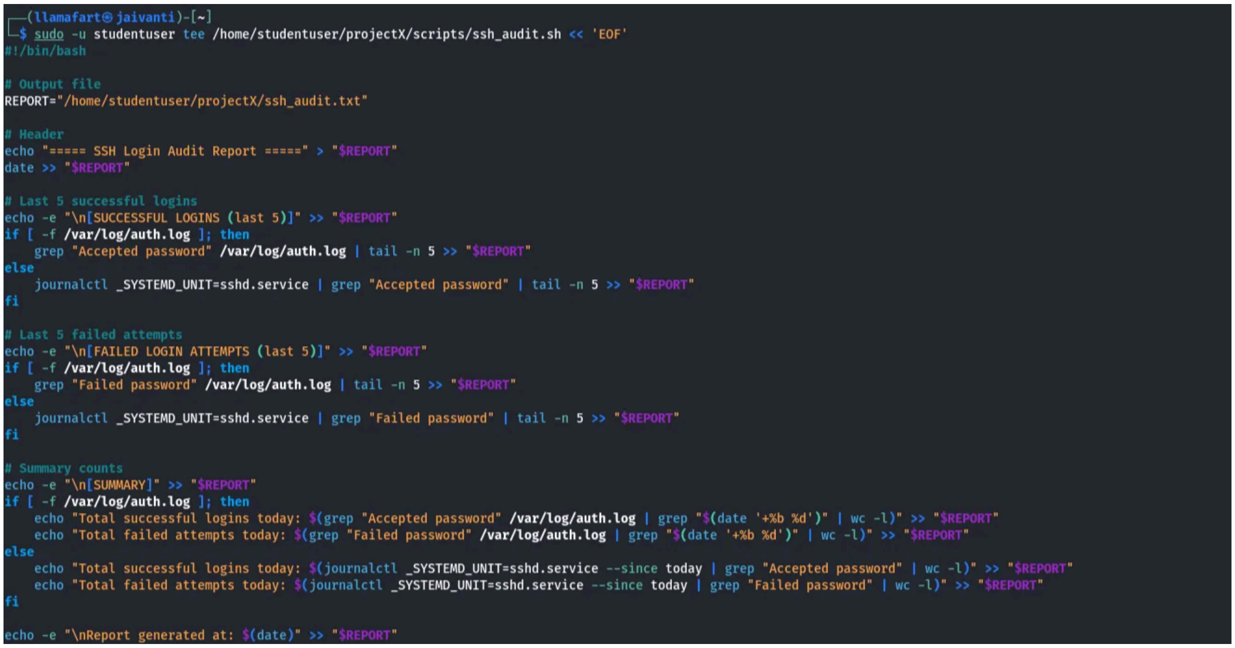
This PoC developed an SSH audit solution that tracks authentication attempts, successfully logging both successful and failed login events while overcoming permission constraints through secure sudo configurations.

2. Objectives

- Capture last 5 successful SSH logins
- Record last 5 failed login attempts
- Generate daily summary counts
- Operate under restricted user permissions

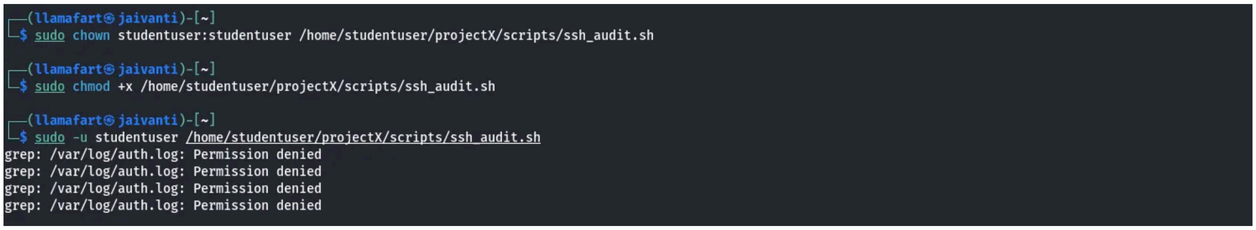
3. Implementation

3.1 Initial Script



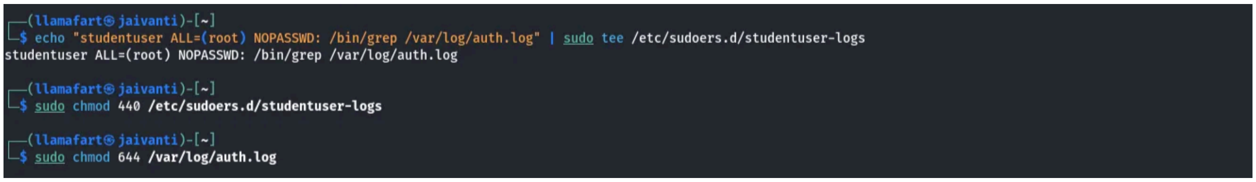
```
┌──(llamafart㉿jaivanti)-[~]
└─$ sudo -u studentuser tee /home/studentuser/projectX/scripts/ssh_audit.sh << 'EOF'
#!/bin/bash

# Output file
REPORT="/home/studentuser/projectX/ssh_audit.txt"

# Header
echo "===== SSH Login Audit Report =====" > "$REPORT"
date >> "$REPORT"

# Last 5 successful logins
echo -e "\n[SUCCESSFUL LOGINS (last 5)]" >> "$REPORT"
if [ -f /var/log/auth.log ]; then
    grep "Accepted password" /var/log/auth.log | tail -n 5 >> "$REPORT"
else
    journalctl _SYSTEMD_UNIT=sshd.service | grep "Accepted password" | tail -n 5 >> "$REPORT"
fi

# Last 5 failed attempts
echo -e "\n[FAILED LOGIN ATTEMPTS (last 5)]" >> "$REPORT"
if [ -f /var/log/auth.log ]; then
    grep "Failed password" /var/log/auth.log | tail -n 5 >> "$REPORT"
else
    journalctl _SYSTEMD_UNIT=sshd.service | grep "Failed password" | tail -n 5 >> "$REPORT"
fi

# Summary counts
echo -e "\n[SUMMARY]" >> "$REPORT"
if [ -f /var/log/auth.log ]; then
    echo "Total successful logins today: $(grep "Accepted password" /var/log/auth.log | grep "$(date '+%b %d')" | wc -l)" >> "$REPORT"
    echo "Total failed attempts today: $(grep "Failed password" /var/log/auth.log | grep "$(date '+%b %d')" | wc -l)" >> "$REPORT"
else
    echo "Total successful logins today: $(journalctl _SYSTEMD_UNIT=sshd.service --since today | grep "Accepted password" | wc -l)" >> "$REPORT"
    echo "Total failed attempts today: $(journalctl _SYSTEMD_UNIT=sshd.service --since today | grep "Failed password" | wc -l)" >> "$REPORT"
fi

echo -e "\nReport generated at: $(date)" >> "$REPORT"
```

3.2 Permission Fixes



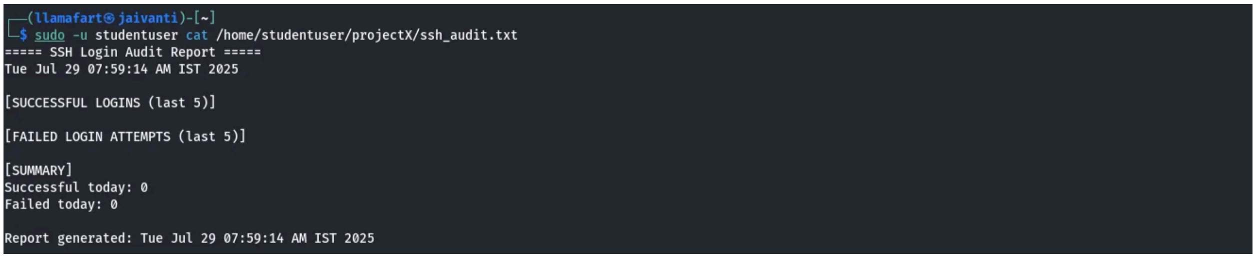
```
┌──(llamafart㉿jaivanti)-[~]
└─$ sudo chown studentuser:studentuser /home/studentuser/projectX/scripts/ssh_audit.sh

┌──(llamafart㉿jaivanti)-[~]
└─$ sudo chmod +x /home/studentuser/projectX/scripts/ssh_audit.sh

┌──(llamafart㉿jaivanti)-[~]
└─$ sudo -u studentuser /home/studentuser/projectX/scripts/ssh_audit.sh
grep: /var/log/auth.log: Permission denied
grep: /var/log/auth.log: Permission denied
grep: /var/log/auth.log: Permission denied
grep: /var/log/auth.log: Permission denied
```

3.3 Permission Fixes



```
┌──(llamafart㉿jaivanti)-[~]
└─$ echo "studentuser ALL=(root) NOPASSWD: /bin/grep /var/log/auth.log" | sudo tee /etc/sudoers.d/studentuser-logs
studentuser ALL=(root) NOPASSWD: /bin/grep /var/log/auth.log

┌──(llamafart㉿jaivanti)-[~]
└─$ sudo chmod 440 /etc/sudoers.d/studentuser-logs

┌──(llamafart㉿jaivanti)-[~]
└─$ sudo chmod 644 /var/log/auth.log
```

3.4 Report Verification



```
┌──(llamafart㉿jaivanti)-[~]
└─$ sudo -u studentuser cat /home/studentuser/projectX/ssh_audit.txt
===== SSH Login Audit Report =====
Tue Jul 29 07:59:14 AM IST 2025

[SUCCESSFUL LOGINS (last 5)]

[FAILED LOGIN ATTEMPTS (last 5)]

[SUMMARY]
Successful today: 0
Failed today: 0

Report generated: Tue Jul 29 07:59:14 AM IST 2025
```

4. Conclusion

This PoC successfully implemented SSH login monitoring through a secure script that tracks authentication attempts and generates audit reports while maintaining system security. The solution overcame permission challenges by implementing targeted sudo access and proper file permissions for reliable operation.