Task 12 – System Log Monitoring and Analysis

Internship: Cyber Security Internship
Name: Adil
Date: 29 January 2026
Operating System: Ubuntu Linux
Tools Used: Linux Terminal, auth.log, syslog

Objective

The objective of this task was to analyze Linux system logs in order to understand user authentication activities, detect failed and successful login attempts, and monitor system-level events. This task helps in identifying potential security issues such as unauthorized access attempts and system changes.

Steps Performed

Step 1: Listing System Log Files

The /var/log directory was explored to identify important system log files.

Command used:

ls /var/log

Observation:
Key log files such as auth.log, syslog, kern.log, and rotated log files (.gz) were present.

Screenshot: List of log files in /var/log

Step 2: Viewing Authentication Logs

The authentication log was examined to review login activity.

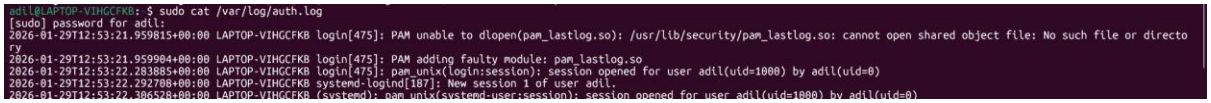
Command used:

sudo cat /var/log/auth.log

Observation:

- Successful login sessions for user **adil**
- PAM authentication messages
- Session open events logged by systemd

Screenshot: auth.log showing login activity



Step 3: Checking Failed Login Attempts

The authentication log was searched for failed password attempts.

Command used:

sudo grep "Failed password" /var/log/auth.log

Observation:
No failed SSH login attempts were detected, indicating no brute-force or unauthorized access attempts during the observed period.

Screenshot: Failed password search output

Step 4: Checking Successful Login Attempts

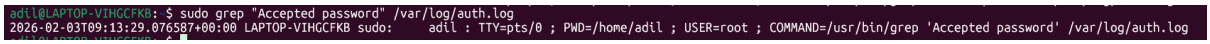
The log was searched for successful authentication events.

Command used:

sudo grep "Accepted password" /var/log/auth.log

Observation:
Successful authentication entries were found, confirming legitimate user access.

Screenshot: Accepted password log entries



Step 5: Extracting Usernames from Failed Attempts

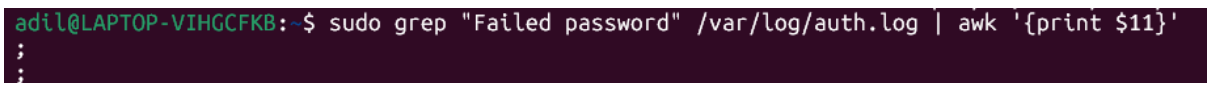
An additional command was executed to extract usernames from failed login attempts.

Command used:

sudo grep "Failed password" /var/log/auth.log | awk '{print $11}'

Observation:
No output was returned, confirming there were no failed login attempts recorded.

Screenshot: Username extraction command output



Step 6: Reviewing System Logs

The system log was reviewed to analyze system services and background activity.

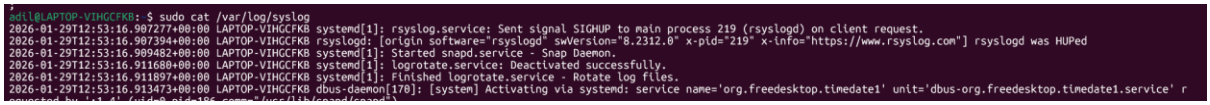
Command used:

sudo cat /var/log/syslog

Observation:

- Log rotation events
- System services restarting
- Time and service synchronization logs

Screenshot: syslog entries



Results and Analysis

- The system logs show **normal and healthy activity**
- No failed or suspicious login attempts were detected
- User authentication was successful and legitimate
- System services were running as expected with proper logging
- **Conclusion**
- This task successfully demonstrated how Linux system logs can be monitored and analyzed to detect authentication events and system activities. Log analysis is a critical part of system security monitoring, helping administrators identify unauthorized access attempts and maintain system integrity.

Learning Outcome

- Learned how to navigate and analyze Linux log files
- Understood the importance of auth.log and syslog in security monitoring
- Gained hands-on experience with log filtering using grep and awk