Task 12: Log Monitoring & Analysis Report

Name: Mohammed Fadil PK **Date:** February 3, 2026

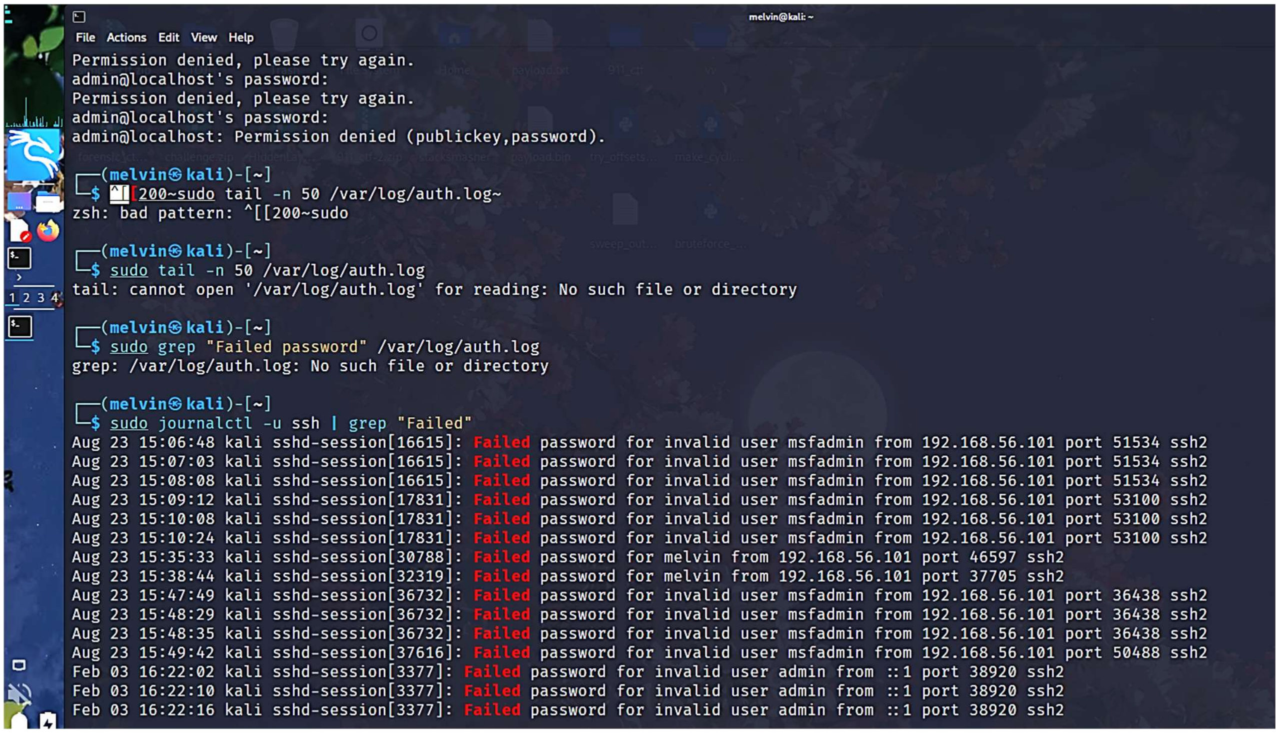
1. Introduction

Logs are the digital footprints of every action taken on a system. In this task, I performed log analysis on both Linux and Windows environments to detect simulated security events. The goal was to understand how to identify "Brute Force" attacks and monitor system authentication.

2. Linux Log Analysis (Simulated Attack)

I simulated a "Brute Force" attack on my Kali Linux machine by attempting to SSH into the localhost with incorrect passwords multiple times.

- **Command Used:** ssh admin@localhost
- **Analysis Tool:** I used the journalctl command to filter the system logs for failed attempts. sudo journalctl -u ssh | grep "Failed"
- **Observation:** The logs successfully captured every failed login attempt, showing the timestamp, invalid user, and source IP (::1 for localhost).



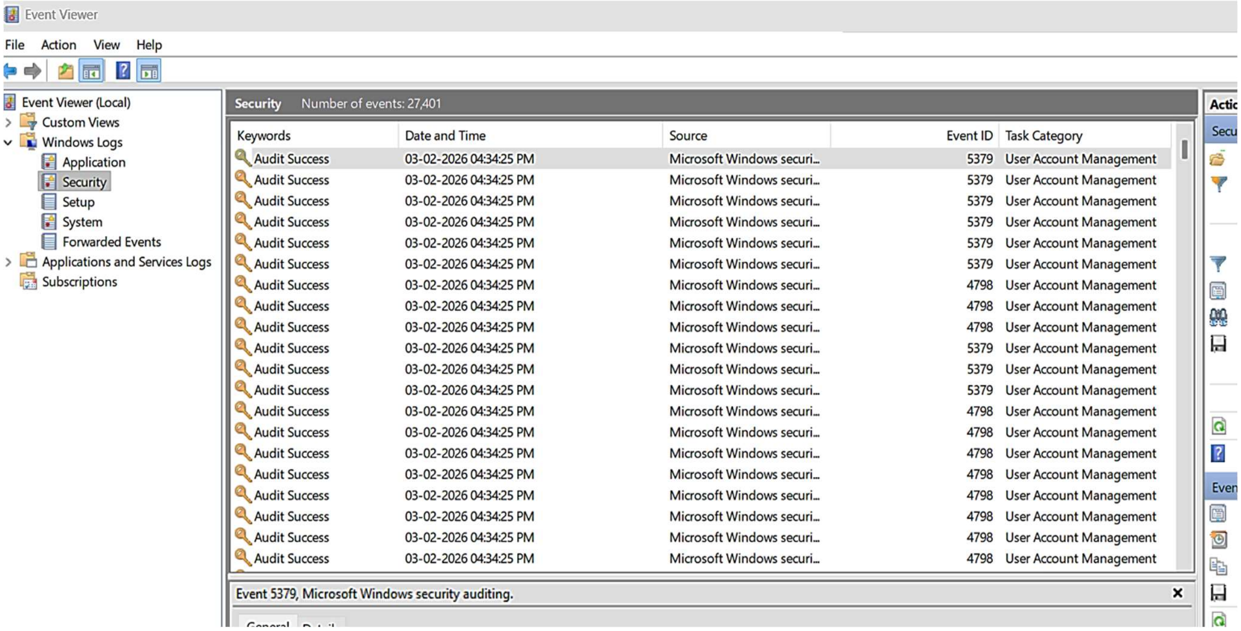
```
Permission denied, please try again.
admin@localhost's password:
Permission denied, please try again.
admin@localhost's password:
admin@localhost: Permission denied (publickey,password).

┌──(melvin㉿kali)-[~]
└─$ ^[[200~sudo tail -n 50 /var/log/auth.log~
zsh: bad pattern: ^[[200~sudo

┌──(melvin㉿kali)-[~]
└─$ sudo tail -n 50 /var/log/auth.log
tail: cannot open '/var/log/auth.log' for reading: No such file or directory

┌──(melvin㉿kali)-[~]
└─$ sudo grep "Failed password" /var/log/auth.log
grep: /var/log/auth.log: No such file or directory

┌──(melvin㉿kali)-[~]
└─$ sudo journalctl -u ssh | grep "Failed"
Aug 23 15:06:48 kali sshd-session[16615]: Failed password for invalid user msfadmin from 192.168.56.101 port 51534 ssh2
Aug 23 15:07:03 kali sshd-session[16615]: Failed password for invalid user msfadmin from 192.168.56.101 port 51534 ssh2
Aug 23 15:08:08 kali sshd-session[16615]: Failed password for invalid user msfadmin from 192.168.56.101 port 51534 ssh2
Aug 23 15:09:12 kali sshd-session[17831]: Failed password for invalid user msfadmin from 192.168.56.101 port 53100 ssh2
Aug 23 15:10:08 kali sshd-session[17831]: Failed password for invalid user msfadmin from 192.168.56.101 port 53100 ssh2
Aug 23 15:10:24 kali sshd-session[17831]: Failed password for invalid user msfadmin from 192.168.56.101 port 53100 ssh2
Aug 23 15:35:33 kali sshd-session[30788]: Failed password for melvin from 192.168.56.101 port 46597 ssh2
Aug 23 15:38:44 kali sshd-session[32319]: Failed password for melvin from 192.168.56.101 port 37705 ssh2
Aug 23 15:47:49 kali sshd-session[36732]: Failed password for invalid user msfadmin from 192.168.56.101 port 36438 ssh2
Aug 23 15:48:29 kali sshd-session[36732]: Failed password for invalid user msfadmin from 192.168.56.101 port 36438 ssh2
Aug 23 15:48:35 kali sshd-session[36732]: Failed password for invalid user msfadmin from 192.168.56.101 port 36438 ssh2
Aug 23 15:49:42 kali sshd-session[37616]: Failed password for invalid user msfadmin from 192.168.56.101 port 50488 ssh2
Feb 03 16:22:02 kali sshd-session[3377]: Failed password for invalid user admin from ::1 port 38920 ssh2
Feb 03 16:22:10 kali sshd-session[3377]: Failed password for invalid user admin from ::1 port 38920 ssh2
Feb 03 16:22:16 kali sshd-session[3377]: Failed password for invalid user admin from ::1 port 38920 ssh2
```

Fig 1: Linux Terminal showing "Failed password" logs

3. Windows Log Analysis

I also audited the security logs on a Windows host using the **Event Viewer**.

- **Tool Used:** Windows Event Viewer (eventvwr).
- **Log Source:** Windows Logs -> Security.
- **Observation:** I inspected the log stream for **Event ID 4624 (Logon Success)** and **Event ID 4625 (Logon Failure)** to monitor user activity.



Security Number of events: 27,401

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	5379	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	5379	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	5379	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	5379	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	5379	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	5379	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	4798	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	4798	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	4798	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	5379	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	5379	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	5379	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	4798	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	4798	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	4798	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	4798	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	4798	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	4798	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	4798	User Account Management
Audit Success	03-02-2026 04:34:25 PM	Microsoft Windows securi...	4798	User Account Management

Event 5379, Microsoft Windows security auditing.

Fig 2: Windows Event Viewer

4. Interview Questions & Answers

- **What is a Log?** A log is a record of events that happen within a computer system, such as errors, user logins, or file accesses.
- **What is SIEM?** SIEM (Security Information and Event Management) is a tool that collects logs from many different sources (firewalls, PCs, servers) into one central place to analyse them for threats automatically (e.g., Splunk).
- **Why are logs important?** They are the primary source of evidence for troubleshooting errors, detecting cyberattacks, and performing forensic investigations after a hack.
- **What is Anomaly Detection?** It is the process of finding patterns that do not match "normal" behaviour. For example, a user logging in at 3:00 AM from a different country is an anomaly.

5. Conclusion

This task demonstrated that logs are essential for security. By manually inspecting auth.log (via journalctl) and Windows Event Viewer, I learned how to differentiate between normal user activity and potential security threats.