1. Introduction

Log monitoring is the process of analyzing system log files to identify suspicious activities, errors, and security threats. Logs provide important evidence about system behaviour, login attempts, and system events. In this task, log monitoring and analysis were performed on a Kali Linux system to observe login activity and detect possible anomalies.

---

2. Objectives

- To monitor system logs
- To analyze login activities
- To detect failed authentication attempts
- To identify security anomalies

---

3. Tools Used

- Kali Linux
- Linux Terminal
- journalctl
- last command
- Apache Log Files

---

4. Commands Used

```
cd /var/log
ls
sudo journalctl -n 20
sudo journalctl | grep -i failed
last
```

```
sudo lastb
sudo journalctl -p err -n 10
cd /var/log/apache2
sudo tail access.log
```

---

5. Log Analysis Process

1. Navigated to the `/var/log` directory to view available system logs.
2. Since `auth.log` was not present, system logs were analyzed using `journalctl`.
3. Recent system activities were checked using `journalctl -n 20`.
4. Login history was monitored using the `last` command.
5. Failed login attempts were checked using `lastb` and journal logs.
6. Apache web server logs were reviewed to observe web activity.

---

6. Observations

- Login history shows only local GUI sessions (tty7).
- No remote IP-based login activity was detected.
- Kernel messages related to VirtualBox drag-and-drop were observed, which is normal system behaviour.
- No failed authentication attempts were found.
- No critical system errors were detected.

---

7. Findings

The system logs indicate normal operating behaviour. All login activities were legitimate local user sessions. There were no signs of brute-force attacks, unauthorized access, or suspicious anomalies during the monitoring period.

8. Conclusion

Log monitoring helps in identifying potential threats and understanding system behaviour. In this task, logs were successfully analyzed using journalctl and login monitoring commands. The analysis confirmed that the system is operating securely with no suspicious activities detected.