Log Monitoring & Analysis Report

February 6, 2026

1 Objective

The objective of this task is to monitor and analyze system logs in order to identify authentication issues, detect anomalies, correlate events, and understand the fundamentals of Security Information and Event Management (SIEM).

2 Tools Used

- Linux System Logs
- journalctl
- grep
- last command
- Windows Event Viewer (conceptual understanding)

3 Log Sources Examined

- `/var/log/auth.log`
- `/var/log/syslog`
- System journal logs accessed using `journalctl`

4 Commands Used

4.1 Viewing Logs

```
ls /var/log
less /var/log/syslog
```

4.2 Authentication Log Analysis

```
cat /var/log/auth.log
sudo journalctl | grep ssh
```

4.3 Finding Failed Logins

```
grep "Failed password" /var/log/auth.log
sudo journalctl | grep Failed
```

4.4 Checking Login History

```
last
lastb
who
```

5 Findings

5.1 Failed Login Attempts

Multiple failed SSH login attempts were observed.

Example log entry:

```
Failed password for invalid user admin
```

Risk Level: Medium

Reason: This may indicate brute-force login attempts.

5.2 Successful Login Tracking

User login history was verified using:

```
last
```

No suspicious sessions were identified.

5.3 Anomaly Detection

Analysis revealed:

- No unusual login hours
- No unauthorized sudo usage
- Normal system activity

6 Event Correlation

Logs were examined for sequences such as:

- Failed login followed by successful breach
- Privilege escalation attempts

No correlated malicious activity was found.

7 Recommendations

- Enable log rotation
- Configure automated alerts
- Implement SIEM monitoring
- Disable root SSH login
- Deploy Fail2Ban

8 Conclusion

System logs were successfully monitored and analyzed. No critical threats were detected during this assessment. Continuous monitoring and improved alert mechanisms are recommended for enhanced security posture.