Log Monitoring & Analysis Report

Task 12 – Cyber Security Internship

Objective

The objective of this task is to understand basic log monitoring and analysis, identify failed login attempts, and learn how logs help in detecting security incidents.

Tools Used

- Linux system logs (auth.log – conceptual)
- Windows Event Viewer (Security logs)
- SIEM (basic theoretical understanding)

What Are Logs?

Logs are records of events generated by systems and applications. They help track user activity, errors, and security-related events.

Log Analysis Performed

- Studied authentication logs
- Identified failed and successful login attempts
- Observed repeated login failures
- Noted unusual login patterns (time/IP based)

Findings

- Multiple failed login attempts can indicate brute-force attacks
- Logs are essential for monitoring suspicious activity
- Event correlation helps in better incident detection

Conclusion

This task helped me understand the importance of logs in cyber security and improved my basic incident detection and analysis skills.

Final Outcome

✔️ Basic understanding of log monitoring ✔️ Improved security analysis skills