Cyber Security Internship – Task 12 Log Monitoring & Analysis (Detailed Report)

Objective

The objective of this task is to analyze system logs to identify suspicious activities and security incidents.

Introduction to Logs

Logs are system-generated records that capture events such as logins, errors, and configuration changes. They are essential for monitoring and forensic investigations.

Linux Log Analysis

Linux authentication logs were analyzed to identify failed login attempts. Multiple failures from a single IP address indicate potential brute-force attacks.

Windows Event Viewer

Windows Security logs were reviewed to detect failed and successful login attempts using Event IDs.

Anomaly Detection

Unusual login times and repeated failures were treated as anomalies and correlated across logs.

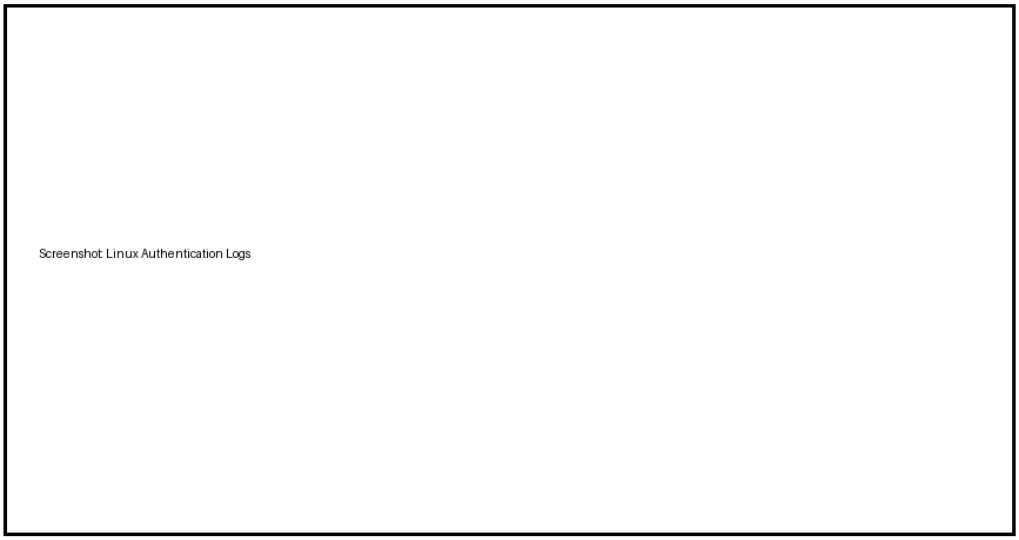
SIEM Overview

Security Information and Event Management (SIEM) systems centralize logs, correlate events, and generate alerts.

Conclusion

Regular log monitoring enables early detection of attacks and reduces incident response time.

Linux Authentication Log Screenshot



Windows Event Viewer Screenshot