Divyanshu Sharma
Divyanshu08.92Sharma@gmail.com

Cybersecurity Project

Log Analysis For Security Events

—

Notes

Objective:

Build a log analyzer that detects security events from system logs.

Foundational Understanding

Logs & their importance in Cybersecurity

Logs are records of system, network, or application activities that provide a trail of events happening within a system.
They are crucial in cybersecurity because they help with

- Threat Detection & Investigation: Identifying suspicious activities and tracing cyberattacks.
- Compliance & Auditing: Meeting security standards.
- Incident Response: Understanding security breaches and taking corrective actions.
- System Performance Monitoring: Ensuring systems run smoothly and troubleshooting issues.

Types of Logs & Examples in Major OS

Windows Logs

Stored in Event Viewer (eventvwr.msc), categorized as:

- Security Logs: User logins, failed login attempts (Security.evtx).
- System Logs: System startup, shutdown, hardware failures (System.evtx).
- Application Logs: Errors from software like browsers, security tools (Application.evtx)

macOS Logs

Stored in /var/log/ and can be accessed via Console.app

- System Logs: System crashes, kernel logs (system.log).
- Application Logs: Errors and status of applications (/Library/Logs/)
- Console App: More System Logs in Console App

Linux Logs

Stored in /var/log/.

- Authentication Logs: Login attempts (/var/log/auth.log or /var/log/secure).
- System Logs: Kernel, boot, system events (/var/log/syslog or /var/log/messages).
- Application Logs: Errors from web servers, security tools (/var/log/httpd/access.log).