Internship Final Report

Project Title: Windows Event Log Analyzer for Suspicious Activity Detection

Name: Sujay

Internship Duration: 1 Month

Project Duration: 2 Weeks

Internship Organization: Elevate Labs

GitHub Repository: https://github.com/Sujayskp/windows-log-analyzer

Abstract

The Windows Event Log Analyzer is a Python-based tool that simulates the responsibilities of a SOC (Security Operations Center) Analyst by collecting and analyzing Windows Security Event Logs. It identifies suspicious activities such as failed logins, unauthorized user creations, or privilege misuse. The analyzer reads logs, filters specific Event IDs, and generates a report, helping organizations monitor critical security events locally without a SIEM.

Tools & Technologies Used

- Python 3.10
- pywin32 - for accessing Windows Event Logs
- pandas - for structuring and filtering data
- colorama - for color-coded terminal output
- Windows 10/11 (Administrator access required)

Steps Involved

1. Set Up Log Connection: Used win32evtlog from pywin32 to connect to the Security Event Log.
2. Read and Parse Logs: Retrieved entries and extracted details like Event ID, timestamp, and source.
3. Filter Suspicious Events: Focused on Event IDs 4625, 4648, 4688, 4720, 4726.
4. Highlight Suspicious Entries: Used pandas for filtering and colorama for terminal alerts.
5. Export Final Report: Saved filtered events to report.txt file.

Sample Output

Terminal Output:

Suspicious Events Found:

Time EventID Source

Fri Jun 13 20:45:39 4625 Microsoft-Windows-Security-Auditing

Fri Jun 13 20:45:41 4648 Microsoft-Windows-Security-Auditing

File Output (report.txt):

A structured list of logs containing timestamp, event ID, source, and full event message.

Conclusion

This project provided practical exposure to Windows log analysis, a core SOC skill. The tool effectively simulates how analysts identify threats like brute-force attacks and unauthorized access attempts using built-in logs. It highlights the importance of log monitoring in detecting early-stage intrusions and forms a strong base for advanced SIEM tools.

Key Takeaways

- Learned real-world SOC responsibilities
- Understood common Event IDs used in threat detection
- Practiced log filtering, report generation, and automation
- Successfully completed a project aligned with entry-level cybersecurity jobs