LOG ANALYZER PROJECT REPORT

Abstract

The Log Analyzer project is designed to automate the process of detecting and classifying suspicious log activities from various sources like Windows logs, Web logs, and Network logs. The system uses pattern matching and regular expressions to identify common attack types such as SQL Injection, Cross-Site Scripting (XSS), and Brute Force attempts. This automation provides an efficient method for real-time security analysis and alert generation.

Introduction

In modern cybersecurity infrastructure, analyzing system and network logs is crucial to identify potential threats and vulnerabilities. Manual log inspection is inefficient, hence the development of this Python-based automated Log Analyzer. The project integrates data from multiple log sources, processes them, and identifies malicious or abnormal activities using regex-based detection and classification.

Tools Used

- Python 3
- Pandas for data manipulation
- Matplotlib and Seaborn for visualization
- Regular Expressions (re module) for pattern-based detection
- Jupyter Notebook / VS Code for implementation
- CSV for data storage and analysis

Steps Involved in Building the Project

1. Data Collection – Imported Windows, Web, and Network logs in CSV format.
2. Data Cleaning – Removed missing or irrelevant data and standardized column names.
3. Suspicious Log Detection – Applied conditions and regex rules to detect anomalies.
4. Classification – Classified attacks into SQL Injection, XSS, Brute Force, etc.
5. Visualization – Displayed log distribution using Seaborn charts.
6. Report Generation – Generated summary reports and exported suspicious logs to CSV.

Conclusion

The Log Analyzer project successfully automates the detection and classification of suspicious log entries across multiple systems. It provides an effective, scalable, and lightweight solution for early-stage security monitoring and forensic analysis. Future improvements may include integration with SIEM tools and the addition of machine learning-based anomaly detection for better precision.