REPORT

Log File Analyzer for Intrusion Detection

Author: Dhanush Reddy Email: dhanushdyasani@gmail.com

Abstract :

This project focuses on developing a Python-based tool to analyze server log files (Apache and SSH) to detect potential intrusion attempts. The system identifies patterns such as brute-force attacks, port scanning, and DoS activity using log parsing, data analysis, and visualization techniques. The results are summarized and exported into structured CSV reports for further review.

Introduction :

Cybersecurity threats are increasing rapidly, and early detection plays a crucial role in minimizing damage. Server log files contain valuable information about user activities and network access. The Log File Analyzer automates the process of identifying suspicious activities in these logs by detecting repeated failed login attempts, unusual access frequencies, and known malicious IP addresses. This project demonstrates how data driven log analysis can help improve system security monitoring.

Tools Used :

1. Python – Core programming language used.
2. Pandas – For data manipulation and filtering.
3. Regex – For parsing and pattern matching in log entries.
4. Matplotlib – For visualizing access and attack trends.
5. CSV – For structured export of detected incidents.

-

Steps Involved in Building the Project :

1. Data Collection: Sample Apache and SSH logs were gathered for analysis.

2. Log Parsing: Regular expressions were used to extract IP addresses, timestamps, and event types.

3. Pattern Detection: The system identified brute-force and DoS attempts based on frequency thresholds.

4. Visualization: Matplotlib graphs highlighted access patterns and peak activity hours. 5. Reporting: All flagged incidents were stored in CSV format for review and auditing.

Conclusion :

The Log File Analyzer provides an automated, efficient approach to detecting and analyzing suspicious activities from log files. It helps system administrators identify early warning signs of intrusion attempts, offering insights into access behavior and attack trends. The project demonstrates how Python-based data analysis can strengthen cybersecurity operations and improve monitoring efficiency