21 October 2025

Ứng dụng Log Analysis

Phát hiện Brute-Force Attack

Giảng viên hướng dẫn: Đoàn Trung Sơn
Nhóm thực hiện: Nhóm 11
- Nguyễn Trọng Tuấn - 23010690
- Hoàng Xuân Phong - 23010021

Lý do chọn đề tài

Understanding Brute-Force Attacks and Analysis

•Bối cảnh
-Tấn công dò mật khẩu (brute-force) là mối đe dọa phổ biến và nguy hiểm.
-Phân tích nhật ký (log) thủ công rất tốn thời gian, dễ sai sót.
•Giải pháp
-Cần một công cụ chuyên dụng để tự động hóa quá trình phân tích log.
-Xây dựng công cụ gọn nhẹ, hiệu quả, giúp nhanh chóng xác định hành vi đáng ngờ.

Mục tiêu đề tài

Mục tiêu tổng quát

-Tự động hóa việc phân tích log đăng nhập.
-Phát hiện sớm các cuộc tấn công brute-force.
-Trực quan hóa các cảnh báo an ninh hiệu quả.

Mục tiêu cụ thể

-Xây dựng module đọc và phân tích (parsing) tệp log.
-Thiết kế thuật toán nhận diện IP tấn công dựa trên ngưỡng.
-Phát triển giao diện web (Streamlit) để hiển thị kết quả.
-Xây dựng chức năng xuất báo cáo các IP đáng ngờ ra file CSV.

Cơ sở lý thuyết

Các khái niệm về log hệ thống

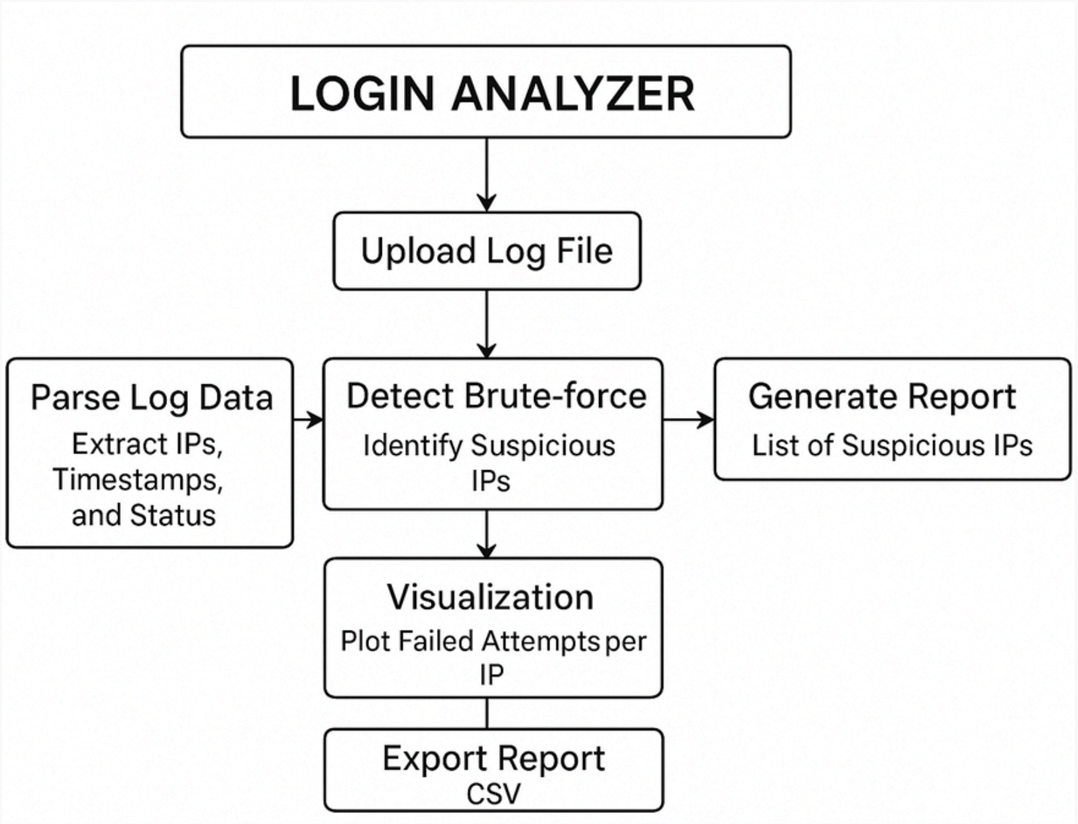
•Nhật ký hệ thống (System Log)
-Là các tệp ghi lại sự kiện hệ thống (VD: /var/log/auth.log).
•Tấn công Brute-Force
-Dấu hiệu: Số lượng lớn đăng nhập thất bại từ cùng một IP trong thời gian ngắn.
•Phương pháp phát hiện dựa trên ngưỡng (Threshold-based)
-IP vượt ngưỡng (vd: >10 lần thất bại / 5 phút) sẽ bị đánh dấu là nghi ngờ.

Các công nghệ sử dụng

- Ngôn ngữ chính: Python
- Giao diện Web: Streamlit
- Xử lý dữ liệu: Pandas
- Trực quan hóa: Matplotlib, Plotly
- Hỗ trợ khác: Seaborn, Scikit-learn, Numpy

Kiến trúc hệ thống

Sơ đồ tổng quan kiến trúc và luồng hoạt động của ứng dụng "Login Analyzer".



Các Module Chính

- Ngôn ngữ chính: Python
- Giao diện Web: Streamlit
- Xử lý dữ liệu: Pandas
- Trực quan hóa: Matplotlib, Plotly
- Hỗ trợ khác: Seaborn, Scikit-learn, Numpy

Key Use Cases

Upload Log

Người dùng có thể dễ dàng tải tệp nhật ký (log files) lên ứng dụng, cho phép xử lý và phân tích hiệu quả các kiểu tấn công brute-force tiềm ẩn từ nhiều nguồn khác nhau.

Parse Data

Mô-đun phân tích nhật ký (log parser) sẽ phân tích và trích xuất dữ liệu liên quan một cách có hệ thống, chuyển đổi nhật ký thô thành các định dạng có cấu trúc, giúp việc xác định và đánh giá các mối đe dọa bảo mật trở nên dễ dàng hơn.

View Statistics

Người dùng có thể trực quan hóa các nhật ký đã được xử lý thông qua các thống kê tương tác, cho phép nhanh chóng nắm bắt thông tin về các lần thử đăng nhập và những hoạt động đáng ngờ, từ đó nâng cao khả năng giám sát an ninh tổng thể.

Hướng dẫn sử dụng

Environment Setup

Để bắt đầu, hãy đảm bảo hệ thống của bạn đã cài đặt Python cùng với các gói cần thiết được liệt kê trong tệp requirements.txt để hỗ trợ ứng dụng.

Running the App

Khởi chạy ứng dụng bằng cách thực thi tệp script Python chính. Thao tác này sẽ khởi động máy chủ, cho phép bạn truy cập công cụ từ trình duyệt web của mình.

Accessing via Browser

Mở trình duyệt web bạn hay dùng và điều hướng đến địa chỉ máy chủ cục bộ (local server) được cung cấp trong terminal để tương tác liền mạch với ứng dụng.

Kết quả và đánh giá

Stable Operation

Ứng dụng thể hiện hiệu suất ổn định, xử lý các tệp nhật ký với nhiều kích thước khác nhau mà không gặp lỗi, đảm bảo độ tin cậy trong quá trình phân tích quan trọng các sự kiện bảo mật và hoạt động của người dùng.

Fast Log Processing

Dữ liệu nhật ký được xử lý nhanh chóng, cho phép phát hiện các cuộc tấn công brute-force trong thời gian thực, giúp nâng cao khả năng phản hồi của hệ thống và giảm thiểu thời gian từ lúc phát hiện đến khi hành động.

Simple Interface

Người dùng được hưởng lợi từ một giao diện trực quan giúp đơn giản hóa quy trình phân tích nhật ký, giúp người dùng với các trình độ kỹ thuật khác nhau có thể tiếp cận và diễn giải kết quả một cách hiệu quả.

Kết luận

Thành tựu và Hướng phát triển của Ứng dụng "Login Analyzer"

- Đã thành công trong việc phát triển ứng dụng "Login Analyzer".
- Ứng dụng có khả năng xử lý log thực tế và phát hiện các cuộc tấn công một cách hiệu quả.

Hướng phát triển trong tương lai

- Giám sát theo thời gian thực.
- Tích hợp hệ thống cảnh báo qua email hoặc chat.
- Hỗ trợ nhiều định dạng log hơn.