Project Overview

- Title: Log Analyzer Security Tool
- Security monitoring tool built in Python
- Analyzes server log files for suspicious login attempts
- Provides visual and text-based reporting
- Helps identify potential security threats

Key Features

- Core Functionality:
- Automated log file parsing
- Failed login attempt detection
- IP address tracking
- Multiple reporting formats
- Real-time visualization

Technical Implementation

- Technologies Used:
- Python 3
- Tkinter (GUI Framework)
- Matplotlib (Visualization)
- Regular Expressions (Log Parsing)
- File I/O Operations

System Architecture

- Main Components:
- 1. Log Parser: Reads log files, extracts IP addresses, identifies failed attempts
- 2. Analysis Engine: Tracks attempt frequency, identifies patterns, generates statistics
- 3. Reporting System: Creates detailed reports, generates visualizations, saves results to files

Data Processing Flow

- 1. User selects log file
- 2. System parses log entries
- 3. Failed attempts are identified
- 4. IP addresses are extracted
- 5. Data is analyzed
- 6. Reports are generated
- 7. Visualizations are created

Sample Data Analysis

- Log Entry Format:
- Dec 04 10:00:12 server sshd[10234]: Failed password for invalid user admin from 192.168.1.1 port 22 ssh2
- Extracted Information:
- Timestamp
- User type (valid/invalid)
- IP address
- Port number

Visualization Features

- Generated Outputs:
- Bar charts of failed attempts
- IP address frequency distribution
- Time-based analysis
- Color-coded severity indicators

Security Reports

- Report Contents:
- Suspicious IP addresses
- Number of failed attempts
- Timestamp information
- Pattern analysis
- Risk assessment

Project Benefits

- 1. Enhanced Security Monitoring
- 2. Quick Threat Detection
- 3. Visual Pattern Recognition
- 4. Automated Analysis
- 5. Easy-to-use Interface

Future Enhancements

- Potential Additions:
- Real-time monitoring
- Email notifications
- IP geolocation
- Advanced pattern detection
- Integration with security systems
- Machine learning for threat detection