Log File Analyzer for Intrusion Detection

Introduction

This project focuses on analyzing server log files to detect suspicious activities such as brute-force login attempts. It uses Python to parse Apache-style logs and flag IPs with repeated failed login attempts.

Abstract

The tool scans log files and identifies IP addresses that have multiple failed login attempts. By flagging such activity, it helps identify possible intrusion attempts. This project is ideal for SOC analysts and cybersecurity students to understand basic log analysis.

Tools Used

- Python 3.x
- re (Regular Expressions)
- Sample Apache-style logs
- VS Code or Kali

Steps Involved

1. Load a log file.
2. Use regex to find failed login attempts.
3. Count the number of failed attempts per IP.
4. Print and export IPs with repeated failures.
5. Save results to 'detected_ips.txt'.

Conclusion

This project demonstrates how to detect potential intrusions through log analysis. It simulates real-world scenarios a SOC analyst would investigate.