Brute Force Attack Detection & Response System

Author: Aziz Ul Haq

Date: January 16, 2026

Executive Summary

This project demonstrates how to detect and respond to brute force attacks using Python. It analyzes simulated authentication logs to identify suspicious login attempts, generates alerts, and simulates IP blocking. The system reflects real-world SOC workflows such as SIEM log analysis, IDS/IPS detection, and automated response actions.

Introduction

A brute force attack occurs when an attacker repeatedly attempts passwords until access is gained. These attacks target SSH servers, web logins, and VPNs. Detecting and responding to such attacks is critical to prevent unauthorized access and data breaches.

Project Setup

1. Authentication Logs: 'auth_logs.txt' simulates login attempts.
2. Detection Script: 'detector.py' reads logs and applies detection logic.
3. Execution: Run the script using 'python detector.py'.
4. Output Files: 'alerts.txt' for alerts and 'blocked_ips.txt' for blocked IPs.

Detection Logic

The script uses threshold-based detection: if an IP has 3 or more failed attempts, it triggers an alert and blocks the IP. This simulates real-world SOC practices like SIEM analysis and IDS/IPS rules.

Alerting & Response

Alerts are generated when suspicious behavior is detected and stored in 'alerts.txt'. Blocked IPs are stored in 'blocked_ips.txt'. This simulates real-world responses like firewall rules or Fail2Ban.

Results

Example alert: [ALERT] Brute Force Attack Detected from IP: 192.168.1.20

Blocked IP: 192.168.1.20

[Screenshots Placeholder]

Cybersecurity Relevance

This project maps to real-world SOC operations:

- Log analysis -> SIEM (Splunk, ELK)

- Threshold detection -> IDS/IPS rules

- Alerts -> SOC monitoring

- IP blocking -> Firewall / Fail2Ban

- Python automation -> SOAR workflows

Conclusion

This project demonstrates practical skills in log analysis, detection, alerting, and automated response. It strengthens a cybersecurity portfolio and prepares for internships and entry-level roles.

References

- OWASP Brute Force Attack Guide

- Fail2Ban Documentation

- Snort IDS Rules

- Splunk SIEM Concepts