SentinelShield

Advanced Intrusion Detection & Web Protection System

Practical Work Documentation

---

1. Introduction

SentinelShield is a lightweight Intrusion Detection and Web Protection System implemented in a Kali Linux environment. The project simulates the behavior of a Web Application Firewall by inspecting HTTP requests, detecting malicious patterns, monitoring abusive traffic, and generating security logs.

---

2. Objectives

- Understand HTTP request inspection
- Detect common web attacks using signatures
- Monitor abusive behavior using rate limiting
- Analyze security logs
- Generate SOC-style attack summaries

---

3. Environment Details

- OS: Kali GNU/Linux Rolling 2025.4
- Language: Python 3
- Tools: Flask, curl
- Platform: Virtual Lab (Localhost)

---

4. System Architecture

Client requests are inspected by SentinelShield, analyzed using detection rules and behavior thresholds, logged, and summarized for analysis.

---

5. Detection Techniques

5.1 Signature-Based Detection

- SQL Injection
- Cross-Site Scripting (XSS)
- Directory Traversal

5.2 Behavior-Based Detection

- Rate limiting
- Brute-force detection using request frequency

---

6. Practical Execution

Normal and malicious HTTP requests were sent using curl. Malicious payloads were blocked and logged successfully.

---

7. Log Analysis

Security logs recorded timestamps, IP addresses, attack categories, and actions taken. A Python script was used to generate attack summaries.

---

8. Results

The system successfully detected and blocked malicious requests while allowing legitimate traffic. Rate-limit abuse was also identified correctly.

---

9. Conclusion

SentinelShield demonstrates core principles of intrusion detection, web application protection, and SOC-style analysis. This project provides practical exposure to real-world cybersecurity workflows.