Stellarisys Smart Log Detection Tool

Author: Aadil K.
University: Daffodil International University, Department of Computing and Information System

---

Abstract

Stellarisys is an advanced tool designed for real-time log detection and analysis. It leverages data structures such as linked lists, stacks, queues, graphs, and binary search trees to efficiently identify and mitigate security threats like SQL injection, cross-site scripting (XSS), path traversal, command injection, and brute-force login attempts. By automating the log analysis process, Stellarisys helps system administrators and cybersecurity professionals quickly respond to potential security incidents, with real-time notifications sent via Telegram. The tool is optimized for handling large volumes of log data and ensures efficient threat detection.

---

1. Introduction

Purpose

Stellarisys automates the process of log analysis to detect and alert system administrators about common security threats. The tool provides a comprehensive solution for monitoring system logs and mitigating risks related to SQL injection, XSS, path traversal, command injection, and brute-force login attempts.

Importance

System logs are invaluable for detecting threats, but manual analysis can be slow and prone to errors. Stellarisys automates this process, ensuring quick identification of malicious activities and reducing the risk of overlooked threats. With real-time notifications and an efficient detection system, it supports swift response and remediation.

---

2. Features and Capabilities

- **Real-Time Threat Detection:** Stellarisys scans logs for attack patterns, including SQL injection, XSS, path traversal, command injection, and brute-force login attempts.
- **Alerting System:** Alerts are generated in the terminal and sent to a Telegram bot for real-time notifications.
- **Efficient Data Processing:** The tool uses advanced data structures such as linked lists, stacks, queues, graphs, and binary search trees to process log data efficiently.

- **Color-Coded Output:** Different types of messages (alerts, warnings, safe messages, etc.) are color-coded for easy identification in the terminal.

---

3. System Requirements

- **Perl:** Ensure Perl is installed on the system.
- **Required Perl Module:** Install `LWP::UserAgent` for sending HTTP requests to Telegram.
- **Optional:** Set up a Telegram account, create a bot via the BotFather, and retrieve your bot's token and chat ID for notification configuration.

---

4. Methodology and Architecture

Stellarisys parses logs line by line and matches entries with predefined attack patterns, such as SQL injection (e.g., `union select`), XSS payloads (e.g., `<script>`), path traversal (e.g., `../`), and command injection (e.g., `;` or `|`). Brute-force login attempts are detected by tracking repeated failed login attempts.

Data Structures:

- **Linked List:** Stores dynamically generated alerts.
- **Stack:** Tracks recent events for backtracking.
- **Queue:** Handles brute-force attempts using FIFO processing.
- **Graph:** Models relationships between IP addresses to spot unusual behavior.
- **Binary Search Tree (BST):** Allows for fast searching and detection of repeated access patterns.

Telegram Notifications: Upon detecting a threat, Stellarisys sends an alert to a configured Telegram bot, detailing the attack type and source IP.

---

5. Usage

Installation

1. **Install Perl** if not already installed.
2. Install the required Perl module:
3. Download the **Stellarisys** script and save it to your system.
4. Set up your Telegram bot token and chat ID.

Running the Tool

Once installed, execute the tool with:

```
perl stellarisys.pl
```

The tool will begin processing logs, and upon detecting any security threats, alerts will appear in the terminal and be sent to your Telegram account.

Telegram Notifications

Configure your Telegram bot with the bot token and chat ID. The bot will send real-time notifications with details of any detected threats.

---

6. Conclusion

Stellarisys is a robust log detection tool that enables real-time monitoring of system logs for potential security threats. With its use of efficient data structures and real-time alerts via Telegram, it offers a streamlined solution for system administrators and cybersecurity professionals to quickly detect and mitigate risks. By automating the log analysis process, Stellarisys ensures that threats are addressed promptly, reducing the potential for undetected attacks.

References

1. Williams, L. (2017). *Cybersecurity and Incident Response*. O'Reilly Media.
2. McGraw, G. (2006). *Software Security: Building Security In*. Addison-Wesley Professional.
3. Wichers, D. (2016). *Web Application Security: Exploitation and Countermeasures for Modern Web Applications*. O'Reilly Media.
4. Porcedda, M., & De Martin, J. C. (2013). *Log Analysis and Event Correlation for Intrusion Detection Systems*. Springer.