Analyzing HTTP Log Files Using Splunk SIEM

Introduction

HTTP (Hypertext Transfer Protocol) log files contain valuable information about web server activity, including requests, responses, user agents, and more. Analyzing HTTP logs using Splunk SIEM enables security professionals to monitor web traffic, detect anomalies, and identify potential security threats.

Project Overview

In this project, we will upload sample HTTP log files to Splunk SIEM and perform various analyses to gain insights into web server activity within the network.

Prerequisites

Before starting the project, ensure the following:

- Splunk instance is installed and configured.
- HTTP log data sources are configured to forward logs to Splunk.

Steps to Upload Sample HTTP Log Files to Splunk SIEM

1. Prepare Sample HTTP Log Files

- Obtain sample HTTP log File in a suitable format (e.g., text files).
- Ensure the log files contain relevant HTTP events, including timestamps, request methods, URLs, response codes, user agents, etc.
- Save the sample log files in a directory accessible by the Splunk instance.

2. Upload Log Files to Splunk

- Log in to the Splunk web interface.
- Navigate to **Settings** > **Add Data**.
- Select **Upload** as the data input method.

3. Choose File

- Click on **Select File** and choose the sample HTTP log file you prepared earlier.

4. Set Source Type

- In the **Set Source Type** section, specify the source type for the uploaded log file.
- Choose the appropriate source type for HTTP logs (e.g., access_combined or a custom source type if applicable).

5. Review Settings

- Review other settings such as index, host, and sourcetype.
- Ensure the settings are configured correctly to match the sample HTTP log file.

6. Click Upload

- Once all settings are configured, click on the **Review** button.
- Review the settings one final time to ensure accuracy.
- Click **Submit** to upload the sample HTTP log file to Splunk.

7. Verify Upload

- After uploading, navigate to the search bar in the Splunk interface.
- Run a search query to verify that the uploaded HTTP events are visible.

Steps to Analyze HTTP Log Files in Splunk SIEM

1. Search for HTTP Events

- Open Splunk interface and navigate to the search bar.
- Enter the following search query to retrieve HTTP events:
- #CODE: index=<your_http_index> sourcetype=<your_http_sourcetype>

2. Extract Relevant Fields

- Identify key fields in HTTP logs such as timestamps, request methods, URLs, response codes, user agents, etc.
- Use Splunk's field extraction capabilities or regular expressions to extract these fields for better analysis.
- Example extraction command:
- #CODE: | rex field=_raw "<regex_pattern>"

3. Analyze Web Traffic Patterns

- Determine the distribution of request methods (GET, POST, etc.) to understand web traffic patterns.
- #CODE: index=<your_http_index> sourcetype=<your_http_sourcetype> | stats count by method
- Identify top URLs or endpoints accessed by users.

- #CODE: index=<your_http_index> sourcetype=<your_http_sourcetype> | top limit=10 uri
- Analyze response codes to identify errors or successful requests.
- #CODE: index=<your_http_index> sourcetype=<your_http_sourcetype> | stats count by status

4. Detect Anomalies

- Look for unusual patterns in file transfer activity.
- #CODE: index=<your_http_index> sourcetype=<your_http_sourcetype> | timechart span=1h count by _time
- Analyze high volumes of error responses:
- #CODE: index=<your_http_index> sourcetype=<your_http_sourcetype> | stats count by status | where status >= 400
- Investigate file transfers to or from suspicious IP addresses.
- #CODE: index=<your_http_index> sourcetype=<your_http_sourcetype> | search src_ip="suspicious_ip"

5. Monitor User Behavior

- Identify users with multiple failed login attempts or unauthorized access attempts:
- #CODE: index=<your_http_index> sourcetype=<your_http_sourcetype> | search action="login" status="failed" | stats count by user
- Analyze user session durations and access patterns:
- #CODE: index=<your_http_index> sourcetype=<your_http_sourcetype> | stats range(_time) as session_duration by session_id | stats avg(session_duration) as avg_session_duration by user

Conclusion

Analyzing FTP log files using Splunk SIEM provides valuable insights into file transfer activities within a network. By monitoring FTP events, detecting anomalies, and correlating with other logs, organizations can enhance their security posture and protect against various cyber threats.

Feel free to customize these steps according to your specific use case and requirements.