Analyzing FTP Log Files Using Splunk SIEM

Introduction

FTP (File Transfer Protocol) log files contain valuable information about file transfers within a network. Analyzing FTP logs using Splunk SIEM enables security professionals to monitor file transfer activities, detect anomalies, and identify potential security threats.

Project Overview

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

Prerequisites

Before starting the project, ensure the following:

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

Steps to Upload Sample FTP Log Files to Splunk SIEM

1. Prepare Sample FTP Log Files

- Obtain sample FTP log File in a suitable format (e.g., text files).
- Ensure the log files contain relevant FTP events, including timestamps, source IP, username, commands, filenames, 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 FTP 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 FTP logs (e.g., ftp 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 FTP 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 FTP 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 FTP events are visible.

Steps to Analyze FTP Log Files in Splunk SIEM

1. Search for FTP Events

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

2. Extract Relevant Fields

- Identify key fields in FTP logs such as timestamps, source IP, username, commands, filenames, etc.
- Use Splunk's field extraction capabilities or regular expressions to extract these fields for better analysis.
- Example extraction command:
- #CODE: | rex field=_raw "^(?<timestamp>\d{4}-\d{2}-\d{2}\s+\d{2}:\d{2}:\d{2}).*?(?<source_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}).*?(?<username>\w+).*?(?<command>[A-Z]+).*?(?<file_path>\/[\w\/.-]+)"

Explanation:

- ^: Start of the line.
- (?<timestamp>\d{4}-\d{2}-\d{2}\s+\d{2}:\d{2}:\d{2}): Matches and captures the timestamp in the format "YYYY-MM-DD HH:MM:SS".
- .*?: Matches any character (except for line terminators) as few times as possible.

- (?<source_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}): Matches and captures the source IP address.
- (?<username>\w+): Matches and captures the username (assuming it consists of alphanumeric characters).
- (?<command>[A-Z]+): Matches and captures the FTP command (assuming it consists of uppercase letters).
- (?<file_path>\/[\w\/.-]+): Matches and captures the file path (assuming it starts with "/" and can contain alphanumeric characters, "/", ".", and "-").

3. Analyze File Transfer Activity

- Determine the frequency and volume of file transfers.
- Identify top users or IP addresses involved in file transfers.
- Analyze the types of files being transferred (e.g., documents, executables, archives).
- Use stats command to calculate statistics such as count, sum, avg, etc.

4. Detect Anomalies

- Look for unusual patterns in file transfer activity.
- Analyze sudden spikes or drops in file transfer volume.
- Investigate file transfers to or from suspicious IP addresses.
- Use statistical analysis or machine learning models to detect anomalies.

5. Monitor User Behavior

- Monitor user behavior during file transfers.
- Identify users with multiple failed login attempts or unauthorized access attempts.
- Analyze user activity patterns and deviations from normal behavior.

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.