Splunk Log Search & Analysis Project

Project Overview

This project demonstrates how to upload log data into Splunk Enterprise, perform basic searches, and identify patterns or errors in the data. The objective was to find entries containing the keyword 'error' and analyze them.

Tools Used

- Splunk Enterprise
- Apache Log Dataset

Steps Taken

1. Installed Splunk Enterprise from https://www.splunk.com/en_us/download/splunk-enterprise.html.
2. Started Splunk service and logged into http://localhost:8000.
3. Downloaded Apache log data from GitHub public dataset.
4. Uploaded the file to Splunk under the index 'testlogs'.
5. Navigated to Search & Reporting.
6. Ran the search 'index=testlogs error' to find all log entries containing the word 'error'.
7. Filtered results to All time to ensure no entries were missed.

Findings

- Total error entries found: 202

What I Learned

- How to ingest log data into Splunk.
- How to filter and search for the total number of error messages