**Lab Exercise 1 - Exploring the Search Command in Splunk**

**Objective**

In this lab exercise, you will learn how to use Splunk's powerful **search command** to retrieve and analyze data. This command is foundational to working with Splunk and is used in most queries.

**Objectives**

1. Understand the basic syntax of the search command.
2. Perform searches with filtering, fields, and keyword-based queries.
3. Use operators and wildcards to refine your search.
4. Generate meaningful insights using Splunk queries.

**Pre-requisites**

* Access to a Splunk instance (cloud or local installation).
* Data indexed in Splunk (e.g., web server logs, security logs, or any sample dataset).

**Lab Steps**

**Step 1: Access Splunk**

1. Log in to your Splunk Web interface.
2. Navigate to the **Search & Reporting** app.

**Step 2: Basic Search**

1. Run a basic search query:

index=\_internal

* + **Objective**: Retrieve all data from the \_internal index.
  + **Observation**: Notice the timestamps, host, source, and sourcetype fields.

1. Search for a specific keyword:

index=\_internal error

* + **Objective**: Find logs containing the word "error".
  + **Observation**: Logs are filtered based on the keyword.

**Step 3: Field Filtering**

1. Search with a specific field and value:

index=\_internal source="/opt/splunk/var/log/splunk/splunkd.log"

* + **Objective**: Filter results for a specific source field.
  + **Observation**: Logs from the specified source are displayed.

1. Search with multiple field-value pairs:

index=\_internal sourcetype=splunkd log\_level=ERROR

* + **Objective**: Filter results based on sourcetype and log\_level.
  + **Observation**: Only error logs from splunkd are displayed.

**Step 4: Use Wildcards and Comparison Operators**

1. Use a wildcard to match partial values:

index=\_internal source="/opt/splunk/\*"

* + **Objective**: Find all logs from sources starting with /opt/splunk/.

1. Use comparison operators:

index=\_internal duration<1

* + **Objective**: Retrieve logs where the duration field is greater than 5.

**Step 5: Logical Operators**

1. Combine conditions with AND:

index=\_internal sourcetype=splunkd AND log\_level=INFO

* + **Objective**: Retrieve logs that meet both conditions.

1. Use OR for multiple conditions:

index=\_internal sourcetype=splunkd OR sourcetype=access\_combined

* + **Objective**: Retrieve logs matching either sourcetype.

1. Exclude results with NOT:

index=\_internal NOT log\_level=DEBUG

* + **Objective**: Retrieve all logs except debug-level logs.

**Step 6: Time Range Filtering**

1. Search logs within a specific time range:

index=\_internal earliest=-15m@m latest=now

* + **Objective**: Retrieve logs from the last 15 minutes.
  + **Syntax**:
    - earliest: Starting time for the query.
    - latest: Ending time for the query.

1. Use relative time modifiers:

index=\_internal earliest=-7d@d

* + **Objective**: Retrieve logs from the last 7 days starting from midnight.

**Step 7: Display Specific Fields**

1. Use table to display specific fields:

index=\_internal | table \_time source host

* + **Objective**: Display only the \_time, source, and host fields in the output.

1. Use fields to include or exclude fields:

index=\_internal | fields + \_time source

* + **Objective**: Include only the \_time and source fields.

index=\_internal | fields - log\_level

* + **Objective**: Exclude the log\_level field.

**Step 8: Aggregations and Insights**

1. Count the number of events:

index=\_internal | stats count

* + **Objective**: Get the total number of events in the index.

1. Group and count by a field:

index=\_internal | stats count by sourcetype

* + **Objective**: Count the number of events for each sourcetype.

1. Find the top 5 sources:

index=\_internal | top source limit=5

* + **Objective**: List the top 5 sources with the highest event count.

**Step 9: Create a Visualization**

1. Search and generate a chart:

index=\_internal | timechart count by sourcetype

* + **Objective**: Create a time-based chart showing event counts by sourcetype.

1. Save the search:
   * Click **Save As** > **Report** or **Dashboard Panel**.

This lab introduces you to foundational Splunk search techniques, which you can build upon for more advanced analyses like anomaly detection and correlation searches.