Sure! Here are some more Splunk search commands that will help you practice and improve your log analysis skills:

Advanced Filtering & Search Optimization

1. search – Filters results efficiently.

index=your_index error OR failure

2. table – Displays specific fields in a tabular format.

index=your_index | table _time, host, status_code, response_time

3. sort – Sorts results in ascending/descending order.

index=your_index | sort - response_time

4. head & tail – Returns the first or last N results.

index=your_index | head 10

index=your_index | tail 5

Data Enrichment & Lookup

5. inputlookup – Reads data from a lookup table.

| inputlookup user_data.csv

6. outputlookup – Saves results to a lookup table.

index=your_index | table user_id, status | outputlookup status_lookup.csv

Event Correlation & Aggregation

7. bin span= – Groups numerical data into buckets.

index=your_index | bin span=5m _time | stats count by _time

8. stats latest(field_name) by field – Gets the latest value of a field per group.

index=your_index | stats latest(status) by user_id

9. dc (distinct count) – Counts unique occurrences.

index=your_index | stats dc(user_id) as unique_users

Real-Time Monitoring & Alerts

10. predict – Forecasts future values (useful for trends).

index=your_index | timechart avg(cpu_usage) | predict cpu_usage

11. trendline – Calculates trends using moving averages.

index=your_index | timechart avg(response_time) | trendline sma5(response_time)

12. delta – Calculates differences between events.

index=your_index | delta response_time as response_diff

Performance & Debugging

13. metadata – Retrieves information about indexes, sources, or hosts.

| metadata type=hosts index=your_index

14. fields + & fields - – Includes/excludes fields from results.

index=your_index | fields - _raw

15. fieldsummary – Provides a summary of all fields in events.

index=your_index | fieldsummary

Time-Based Analysis

16. earliest= & latest= – Defines time ranges in searches.

index=your_index earliest=-24h latest=now

17. timewrap – Compares time periods side-by-side.

index=your_index | timechart count by host | timewrap 1d

Anomaly Detection & Security

18. anomalies – Detects statistical anomalies.

index=your_index | timechart count | anomalies

19. cluster – Groups similar events together.

index=your_index | cluster showcount=true

20. rare – Identifies uncommon values.

index=your_index | rare host

Bonus: Combining Multiple Commands for Insights

Example 1: Identify servers with high CPU usage spikes

index=your_index sourcetype=cpu_usage | stats avg(cpu) as avg_cpu by host | where avg_cpu > 80

Example 2: Find users who experienced multiple errors within a short time

index=your_index error | transaction user_id maxspan=5m | where eventcount > 5

Example 3: Monitor response time trends and predict future issues

index=your_index | timechart avg(response_time) by host | predict response_time future_timespan=5