Splunk Certified Power User – POST TEST MCQs

1. What is the main purpose of Splunk's Search Processing Language (SPL)?

   A) To create dashboards
   B) To search, filter, and analyze data
   C) To manage user access
   D) To configure data inputs

Answer: B) To search, filter, and analyze data

2. What is the function of the index in Splunk?

   A) To display data in reports
   B) To store raw event data for searching
   C) To create data alerts
   D) To schedule searches

Answer: B) To store raw event data for searching

3. Which of the following is a valid Splunk search command?

   A) start
   B) extract
   C) fetch
   D) search

Answer: D) search

4. What is the purpose of the stats command in Splunk?

   A) To filter events based on time range
   B) To calculate summary statistics like count, sum, avg, etc.
   C) To search for raw events
   D) To manage user permissions

Answer: B) To calculate summary statistics like count, sum, avg, etc.

5. Which field is typically used to correlate events in Splunk?

   A) _time
   B) host
   C) source
   D) sourcetype

Answer: A) _time

6. What does the timechart command do in Splunk?

   A) Creates a table of time-based events
   B) Shows the correlation of events over time
   C) Creates a time series chart
   D) Visualizes the distribution of raw events over time

Answer: C) Creates a time series chart

7. Which operator is used to combine multiple search criteria in Splunk?

   A) AND
   B) OR
   C) NOT
   D) All of the above

Answer: D) All of the above

8. Which of the following is a common use case for the eval command?

   A) To change the timestamp of events
   B) To perform calculations or field transformations
   C) To generate reports
   D) To schedule a search

Answer: B) To perform calculations or field transformations

9. What is the purpose of using the lookup command in Splunk?

   A) To apply custom user permissions
   B) To enrich event data by adding additional fields from external data
   C) To send search results via email
   D) To create real-time alerts

Answer: B) To enrich event data by adding additional fields from external data

10. What is a common use of the rex command in Splunk?

   A) To extract fields from raw event data using regular expressions
   B) To summarize event data
   C) To create a report
   D) To filter events by date range

Answer: A) To extract fields from raw event data using regular expressions

11. Which Splunk component is responsible for indexing raw event data?

   A) Splunk Web
   B) Splunk Indexer

C) Splunk Forwarder
D) Splunk Search Head

Answer: B) Splunk Indexer

12. How can you make a search more efficient in Splunk?

A) By using more complex queries
B) By indexing all fields
C) By using time range filters and specifying exact field names
D) By allowing all users to run searches simultaneously

Answer: C) By using time range filters and specifying exact field names

13. Which of the following is NOT a type of Splunk app?

A) Data Input App
B) Data Processing App
C) Visualization App
D) Reporting App

Answer: B) Data Processing App

14. Which Splunk command is used to display events in a table format?

A) stats
B) table
C) timechart
D) search

Answer: B) table

15. How can you specify a time range for a search in Splunk?

A) By using the timepicker command
B) By specifying the time range in the search bar
C) By using the timestamp command
D) By using the range command

Answer: B) By specifying the time range in the search bar

16. What is the purpose of Splunk's Field Extractor tool?

A) To extract fields automatically from the raw event data
B) To generate real-time alerts
C) To configure data inputs
D) To monitor system performance

Answer: A) To extract fields automatically from the raw event data

17. What is the purpose of the dedup command in Splunk?

A) Removes duplicates from the search results
B) Filters events based on specific criteria
C) Creates a summary of search results
D) Sorts the search results by timestamp

Answer: A) Removes duplicates from the search results

18. What is a key benefit of creating saved searches in Splunk?

A) They allow you to automate the indexing process
B) They provide real-time alerts
C) They store commonly used searches for reuse
D) They allow you to change the data input configuration

Answer: C) They store commonly used searches for reuse

19. Which of the following is an example of a search transformation command?

A) table
B) search
C) stats
D) lookup

Answer: A) table

20. What is the purpose of Splunk's Search Processing Language (SPL)?

A) To create dashboards
B) To search, filter, and analyze data
C) To manage user access
D) To configure data inputs

Answer: B) To search, filter, and analyze data