CYBRARY

Introduction to Splunk Quiz

Description: By taking this quiz, you will be able to test your knowledge as you prepare for the Introduction to Splunk. This 25 question quiz covers knowledge based questions across multiple domains found in the Introduction to Splunk course.

---

1) Which of the following searches includes a wildcard? (1PT)

a) index=windowsevents Account_Name=Waldo | stats count by Event_Code
b) index=firewall dest_port=3389 src_ip=*
c) sourcetype="cisco:esa" | table _time _raw
d) index=aws username!=Sonya

2) Splunk can be defined as: (1PT)

a) A company
b) Software and data solutions provided by the company Splunk
c) A and B
d) A patented technique for reverse-engineering IoT data

3) Which of the following is a Splunk automation product? (1PT)

a) Phantom
b) VictorOps
c) A and B
d) Chef

4) Which of the following are limitations of Splunk Free when compared to Splunk Enterprise? Consider the answers to apply to a Splunk Free environment after a Splunk Enterprise free trial is over. (1PT)

a) You can only have one user
b) You can only index a maximum of 500MB per day
c) You can only send ten email alerts per day.
d) A and B

5) True or False? You could always pick the newest version of Splunk to install. (1PT)

a) True
b) False

6) Which part of the data pipeline would a Universal Forwarder correspond to? (1PT)

a) Input
b) Parsing
c) Indexing
d) Searching

7) True or False? You can apply data retention policies by index. (1PT)

a) True
b) False

8) True or False? A large company with over a thousand forwarders will likely need to use a non-distributed Splunk environment

a) True
b) False

9) The standard location for installing Splunk on Linux is:

a) /sys
b) /var
c) /opt
d) /tmp

10) Which of the following ports does Splunk use by default?

a) 8000
b) 9997
c) 8089
d) All of the above

11) True or False? You can use a deployment tool like SCCM or Ansible to install a universal forwarder.

a) True
b) False

12) By default, what folder do you run Splunk commands out of?

a) /opt/splunk/bin
b) /opt/splunk/etc
c) /system
d) /programs/commands

13) Under the monitoring console, you can:

a) Run a health check
b) Install a forwarder

c) Change your user account settings
d) All of the above

14) True or False? Splunk comes with no pre-built alerts

a) True
b) False

15) You can set up authentication using the following methods:

a) LDAP
b) Scripted authentication API
c) Splunk Authentication
d) All of the above

16) You can look at running or recently completed searches under the page called _____.

a) Alerts
b) Splunk Status
c) Jobs
d) You can only check through the command line

17) In order to see all event data, you should run your search in:

a) Smart mode
b) Fast mode
c) Extended mode
d) Verbose mode

18) True or False? You can use regex to extract fields from your data

a) True
b) False

19) Configuration files are formatted in:

a) Lua
b) Haikus
c) Stanzas
d) Base58

20) SPL, in the Splunk world, stands for:

a) Standard Platform Logging
b) Secondary Parsing License
c) Search Processing Language
d) Splunk Premier License

21) Fields names are _____ while field values are _____.

a) Case sensitive; not case sensitive
b) Not case sensitive; case sensitive
c) Case sensitive; case sensitive
d) Not case sensitive; not case sensitive

22) AND, OR, and NOT are:

a) Not usable in searches
b) Boolean operators
c) Polar vectors
d) Required entries in every search

23) True or False? You can interchange != and NOT because these are identical

a) True
b) False

24) When an alert triggers, you can set the following trigger actions:

a) Send an email
b) Write results to csv
c) Add to triggered alerts
d) All of the above

25) Which of the following searches could run successfully?

a) index=main sourcetype=access_* status=200
b) index=main ThreatName=Suspicious TLS Evasion | stats count by src_ip
c) Both A and B
d) None of the above

Answer Key

1. **Answer: B**

Explanation: A wildcard looks like this: * . In answer B, the wildcard represents any value for the field src_ip.

2. **Answer: C**

Explanation: Splunk is both a company and its products are often referred to simply as "Splunk."

3. **Answer: A**

Explanation: Phantom was purchased by Splunk and provides automation capabilities

4. **Answer: D**

Explanation: Splunk Free limits the amount of data you can index per day to 500MB. You are also limited to one user and do not have alerting options.

5. **Answer: False**

Explanation: Your system may require an older version of Splunk. You may also choose to use a different version because of known bugs, compatibility with other parts of the environment, or other reasons.

6. **Answer: A**

Explanation: Universal Forwarders take input and pass it along to get parsed and indexed.

7. **Answer: True**

Explanation: You can configure Splunk to remove and move data at different ages or sizes.

8. **Answer: False**

Explanation: A large company will likely need a distributed environment where the parts of Splunk are separated out and they have duplicate machines for different roles.

9. **Answer: C**

Explanation: You have the option of installing Splunk in other locations, but putting it in the /opt directory will allow you to easily follow standard instructions. to simply as "Splunk."

10. **Answer: D**

Explanation: Splunk, by default, uses 8000 for Splunk Web access, 9997 for receiving data from forwarders, and 8089 for management.

11. Answer: True

Explanation: Rather than manually installing forwarders, you can use a deployment tool. This may speed up the process or help you get forwarders installed in places where you don't have access.

12. Answer: A

Explanation: You can navigate to that folder and run a command by going ./splunk or you can type in /opt/splunk/bin/splunk and then add your command.

13. Answer: A

Explanation: When you navigate to the monitoring console on the Splunk Web Interface, you have the option of running health checks, getting an overview of your environment, checking out performance, and other tasks. To install a forwarder, you'll need to work outside of the Web Interface. To change your user account settings, go to Settings > Access Controls > Users.

14. Answer: False

Explanation: Splunk comes with some pre-built health alerts.

15. Answer: D

Explanation: You can set up and manage accounts to authenticate using Splunk authentication, LDAP, and configure authentication to use other external authentication systems such as RADIUS or PAM.

16. Answer: C

Explanation: Under Activity > Jobs, you are able to view currently running and recently completed searches.

17. Answer: D

Explanation: Verbose mode, while a slower way to search, displays as much event data as possible.

18. Answer: True

Explanation: Regular expressions can be useful for extracting data or running searches.

19. Answer: C

Explanation: Configuration files are formatted in stanzas. These begin with text enclosed in brackets and then have configuration parameters defined below.

20. Answer: C

Explanation: The Splunk Search Process Language (SPL) is a powerful way to search data.

21. Answer: A

Explanation: It matters whether or not you capitalize a field name, but capitalization doesn't matter for a field value.

22. Answer: B

Explanation: You can use these Boolean operators to perform Splunk searches.

23. Answer: False

Explanation: When specifying that you do NOT want a field value, you will get results that may or may not have that field name. When you search using the does not equal exclamation and equal sign != you get only results that have that field but not that field value.

24. Answer: D

Explanation: Alerts can be set to send an email, write the search results to a csv file, add the alert to the triggered alerts list, and other actions.

25. Answer: A

Explanation: Given the right data to search from, this search count run successfully. In B, there needs to be quotation marks around the field value for ThreatName.

Score ___/12