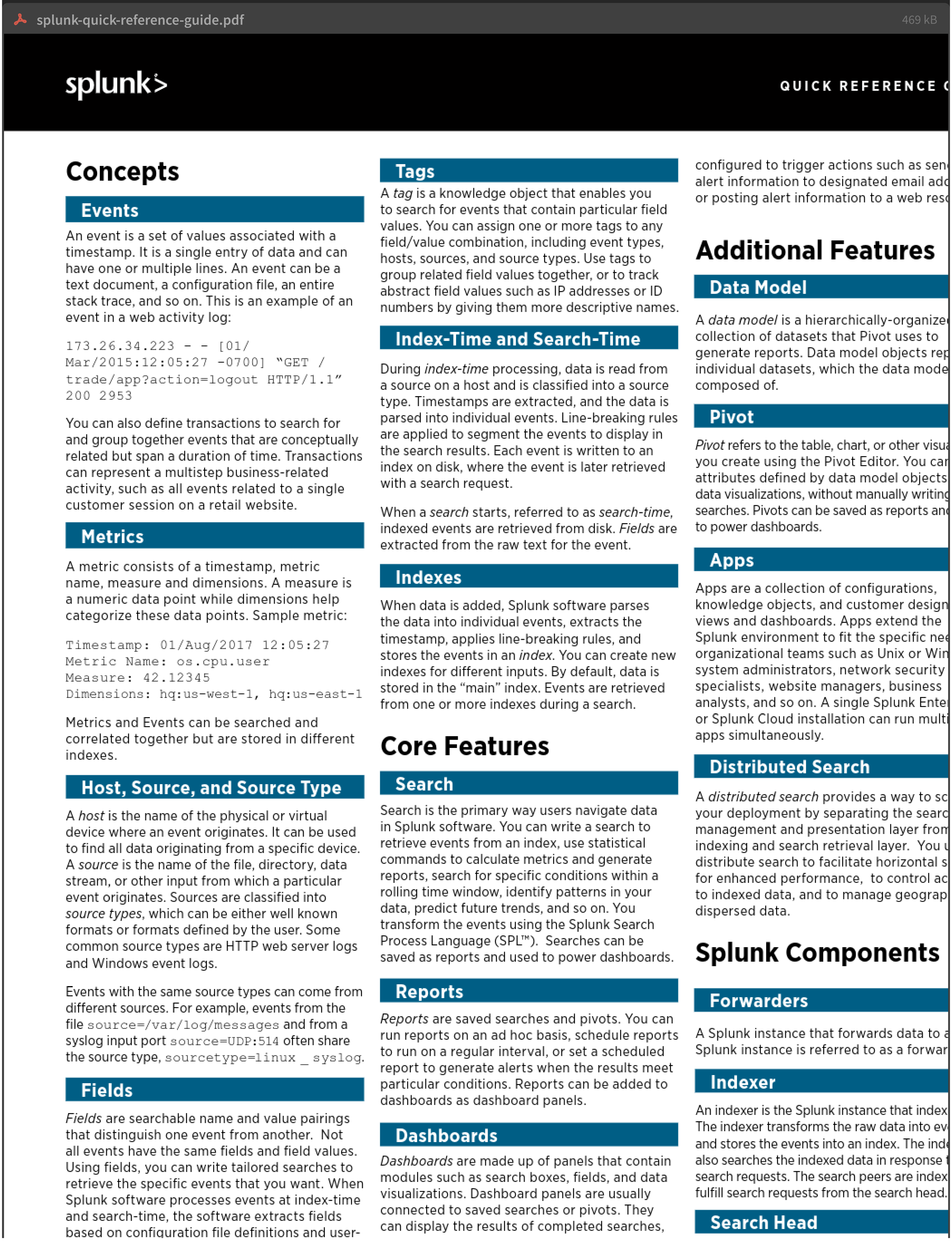
Splunk: 1a (Quiz)

FROM: https://tryhackme.com/room/bpsplunk

TASK 1 Deploy!



splunk-quick-reference-guide.pdf 469 kB

splunk>

QUICK REFERENCE G

Concepts

Events

An event is a set of values associated with a timestamp. It is a single entry of data and can have one or multiple lines. An event can be a text document, a configuration file, an entire stack trace, and so on. This is an example of an event in a web activity log:

```
173.26.34.223 - - [01/
Mar/2015:12:05:27 -0700] "GET /
trade/app?action=logout HTTP/1.1"
200 2953
```

You can also define transactions to search for and group together events that are conceptually related but span a duration of time. Transactions can represent a multistep business-related activity, such as all events related to a single customer session on a retail website.

Metrics

A metric consists of a timestamp, metric name, measure and dimensions. A measure is a numeric data point while dimensions help categorize these data points. Sample metric:

```
Timestamp: 01/Aug/2017 12:05:27
Metric Name: os.cpu.user
Measure: 42.12345
Dimensions: hq:us-west-1, hq:us-east-1
```

Metrics and Events can be searched and correlated together but are stored in different indexes.

Host, Source, and Source Type

A *host* is the name of the physical or virtual device where an event originates. It can be used to find all data originating from a specific device. A *source* is the name of the file, directory, data stream, or other input from which a particular event originates. Sources are classified into *source types*, which can be either well known formats or formats defined by the user. Some common source types are HTTP web server logs and Windows event logs.

Events with the same source types can come from different sources. For example, events from the file `source=/var/log/messages` and from a syslog input port `source=UDP:514` often share the source type, `sourcetype=linux_syslog`.

Fields

Fields are searchable name and value pairings that distinguish one event from another. Not all events have the same fields and field values. Using fields, you can write tailored searches to retrieve the specific events that you want. When Splunk software processes events at index-time and search-time, the software extracts fields based on configuration file definitions and user-

Tags

A *tag* is a knowledge object that enables you to search for events that contain particular field values. You can assign one or more tags to any field/value combination, including event types, hosts, sources, and source types. Use tags to group related field values together, or to track abstract field values such as IP addresses or ID numbers by giving them more descriptive names.

Index-Time and Search-Time

During *index-time* processing, data is read from a source on a host and is classified into a source type. Timestamps are extracted, and the data is parsed into individual events. Line-breaking rules are applied to segment the events to display in the search results. Each event is written to an index on disk, where the event is later retrieved with a search request.

When a *search* starts, referred to as *search-time*, indexed events are retrieved from disk. *Fields* are extracted from the raw text for the event.

Indexes

When data is added, Splunk software parses the data into individual events, extracts the timestamp, applies line-breaking rules, and stores the events in an *index*. You can create new indexes for different inputs. By default, data is stored in the "main" index. Events are retrieved from one or more indexes during a search.

Core Features

Search

Search is the primary way users navigate data in Splunk software. You can write a search to retrieve events from an index, use statistical commands to calculate metrics and generate reports, search for specific conditions within a rolling time window, identify patterns in your data, predict future trends, and so on. You transform the events using the Splunk Search Process Language (SPL™). Searches can be saved as reports and used to power dashboards.

Reports

Reports are saved searches and pivots. You can run reports on an ad hoc basis, schedule reports to run on a regular interval, or set a scheduled report to generate alerts when the results meet particular conditions. Reports can be added to dashboards as dashboard panels.

Dashboards

Dashboards are made up of panels that contain modules such as search boxes, fields, and data visualizations. Dashboard panels are usually connected to saved searches or pivots. They can display the results of completed searches,

configured to trigger actions such as sen
alert information to designated email add
or posting alert information to a web reso

Additional Features

Data Model

A *data model* is a hierarchically-organize
collection of datasets that Pivot uses to
generate reports. Data model objects rep
individual datasets, which the data mode
composed of.

Pivot

Pivot refers to the table, chart, or other visu
you create using the Pivot Editor. You can
attributes defined by data model objects
data visualizations, without manually writing
searches. Pivots can be saved as reports and
to power dashboards.

Apps

Apps are a collection of configurations,
knowledge objects, and customer design
views and dashboards. Apps extend the
Splunk environment to fit the specific nee
organizational teams such as Unix or Win
system administrators, network security
specialists, website managers, business
analysts, and so on. A single Splunk Ente
or Splunk Cloud installation can run multi
apps simultaneously.

Distributed Search

A *distributed search* provides a way to sc
your deployment by separating the searc
management and presentation layer from
indexing and search retrieval layer. You u
distribute search to facilitate horizontal s
for enhanced performance, to control ac
to indexed data, and to manage geograp
dispersed data.

Splunk Components

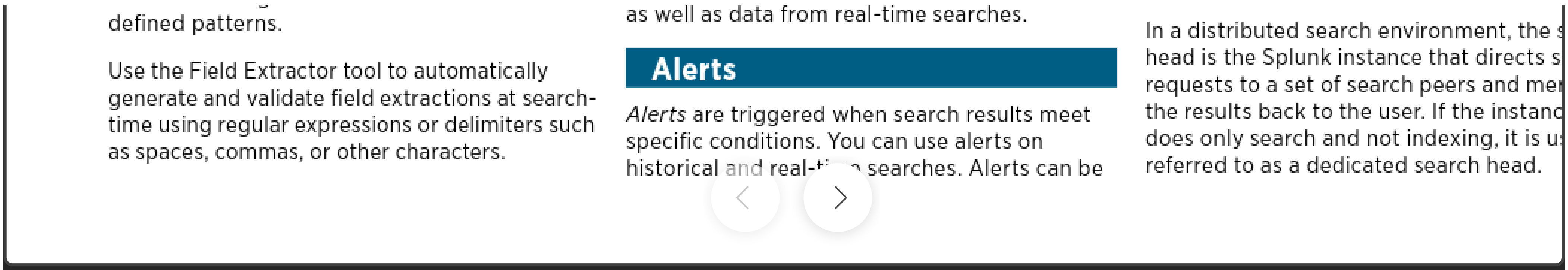
Forwarders

A Splunk instance that forwards data to a
Splunk instance is referred to as a forwar

Indexer

An indexer is the Splunk instance that index
The indexer transforms the raw data into ev
and stores the events into an index. The inde
also searches the indexed data in response t
search requests. The search peers are index
fulfill search requests from the search head.

Search Head



defined patterns.

Use the Field Extractor tool to automatically generate and validate field extractions at search-time using regular expressions or delimiters such as spaces, commas, or other characters.

as well as data from real-time searches.

Alerts

Alerts are triggered when search results meet specific conditions. You can use alerts on historical and real-time searches. Alerts can be

In a distributed search environment, the s head is the Splunk instance that directs s requests to a set of search peers and mer the results back to the user. If the instanc does only search and not indexing, it is u referred to as a dedicated search head.

Splunk queries always begin with this command implicitly unless otherwise specified. What command is this? When performing additional queries to refine received data this command must be added at the start. This is a prime example of a slight trick question.

search

When searching for values, it's fairly typical within security to look for uncommon events. What command can we include within our search to find these?

rare

What about the inverse? What if we want the most common security event?

top

When we import data into splunk, what is it stored under?

index

We can create 'views' that allow us to consistently pull up the same search over and over again; what are these called?

dashboards

Importing data doesn't always go as planned and we can sometimes end up with multiple copies of the same data, what command do we include in our search to remove these copies?

dedup

Splunk can be used for more than just a SIEM and it's commonly used in marketing to track things such as how long a shopping trip on a website lasts from start to finish. What command can we include in our search to track how long these event pairs take?

transaction -- creepy!!!

In a manner similar to Linux, we can 'pipe' search results into further commands, what character do we use for this?

| <--- this is not similar to Linux; this is just like it!!!

In performing data analytics with Splunk (ironically what the tool is at it's core) it's useful to track occurrences of events over time, what command do we include to plot this?

timechart

What about if we want to gather general statistical information about a search?

stats

Data imported into Splunk is categorized into columns called what?

fields

When we import data into Splunk we can view it's point of origination, what is this called? I'm looking for the machine aspect of this here.

host

When we import data into Splunk we can view its point of origination from within a system, what is this called?

source

We can classify these points of origination and group them all together, viewing them as their specific type. What is this called? Use the syntax found within the search query rather than the proper name for this.

sourcetype

When performing functions on data we are searching through we use a specific command prior to the evaluation itself, what is this command?

eval

Love it or hate it regular expression is a massive component to Splunk, what command do we use to specific regex within a search?

rex

It's fairly common to create subsets and specific views for less technical Splunk users, what are these called? ---hey! They're talking about me!

pivot table

What is the proper name of the time date field in Splunk

_time

How do I specifically include only the first few values found within my search?

head

More useful than you would otherwise imagine, how do I flip the order that results are returned in?--Oh! I can imagine a lot!!!

reverse

When viewing search results, it's often useful to rename fields using user-provided tables of values. What command do we include within a search to do this?

lookup

We can collect events into specific time frames to be used in further processing. What command do we include within a search to do just that?

bucket

We can also define data into specific sections of time to be used within chart commands, what command do we use to set these lengths of time? This is different from the previous question as we are no longer collecting for further processing.

span

When producing statistics regarding a search it's common to number the occurrences of an event, what command do we include to do this?

count

Last but not least, what is the website where you can find the Splunk apps at?--liar!!! more questions

splunkbase.splunk.com

We can also add new features into Splunk, what are these called?

apps

What does SOC stand for?

security operations center

TASK 3 BOTS!
https://www.splunk.com/en_us/blog/security/what-you-need-to-know-about-boss-of-the-soc.html
Boss of the SOC is a blue-team jeopardy-style capture-the-flag-esque (CTF) activity