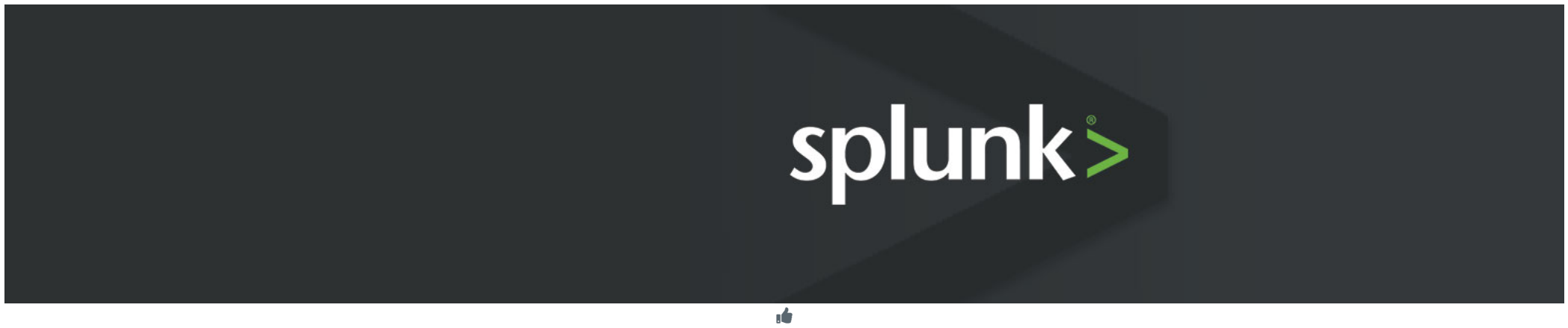


153

Splunk

Start AttackBox | Awards | Help | Options

Part of the Blue Primer series, learn how to use Splunk to search through massive amounts of information

Chart | Scoreboard | Discuss | Writeups | More

Difficulty:

Active Machine Information

Title	IP Address	Expires	
Splunk-AO	10.10.95.97	57m 26s	Add 1 hour / Terminate

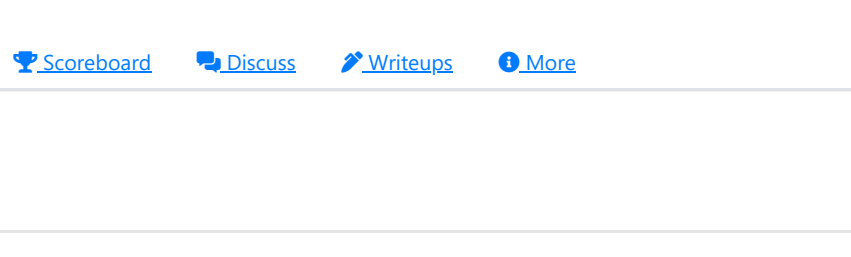
57%

Task 1 Deploy!

Task 2 Can you dig it?

A short quiz over the base search commands that are useful for Splunk. All you'll need for this is the attached quick reference guide and possibly the magic of Google. Include all parts of the search query unless otherwise instructed.

Download



Enjoy the room! For future rooms and write-ups, follow @darkstar7471 on Twitter.

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 — Correct Answer — Hint

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 — Correct Answer

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

top Correct Answer

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

index Correct Answer Hint

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

dashboards Correct Answer Hint

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 Correct Answer

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 Correct Answer Hint

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

| Correct Answer

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 Correct Answer

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

stats Correct Answer

Data imported into Splunk is categorized into columns called what?

fields Correct Answer Hint

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 Correct Answer

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

source Correct Answer Hint

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 Correct Answer

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

eval Correct Answer

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 Correct Answer

It's fairly common to create subsets and specific views for less technical Splunk users, what are these called?

pivot table Correct Answer Hint

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

_time Correct Answer

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

head Correct Answer

More useful than you would otherwise imagine, how do I flip the order that results are returned in?

reverse Correct Answer

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 Correct Answer

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 Correct Answer Hint

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 | Correct Answer | Hint

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 | Correct Answer

Last but not least, what is the website where you can find the Splunk apps at?

splunkbase.splunk.com | Correct Answer

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

apps | Correct Answer | Hint

What does SOC stand for?

Security Operations Center | Correct Answer

What does SIEM stand for?

security information events management | Correct Answer

How about BOTS?

boss of the soc | Correct Answer | Hint

And CIM?

common information model | Correct Answer

what is the website where you can find the Splunk forums at?

answers.splunk.com | Correct Answer

Task 3 ✔ BOTS!

Task 4 ✔ Halp, I'm drowning in logs!

Task 5 ○ Advanced Persistent Threat

Task 6 ○ Ransomware

Created by DarkStar7471

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 6086 users are in here and this room is 574 days old.