

Splunk: Exploring SPL

The "Splunk: Exploring SPL" task on TryHackMe is designed to provide learners with an understanding of the basics of Splunk's Search Processing Language (SPL). This medium-difficulty task, walks participants through the key concepts and functionalities of SPL, enabling them to effectively query and analyze data within Splunk.

The task comprises eight main sections, each focusing on different aspects of SPL. Below is a detailed summary of each section.

Task 1: Introduction

The introduction provides an overview of the task's objectives, emphasizing the importance of SPL in extracting meaningful insights from large datasets. It sets the stage for the subsequent tasks by outlining the key concepts to be covered.

Task 2: Connect with the Lab

In this task, participants are guided on how to connect to the TryHackMe lab environment. This includes starting the AttackBox, which provides a virtual environment to practice using Splunk and SPL.

Task 3: Search & Reporting App Overview

This section introduces the Splunk Search & Reporting app, the primary interface for executing SPL queries. Participants learn about the different components of the app, such as the search bar, time range picker, and the search results area. Key features like saving searches and creating reports are also covered.

Task 4: Splunk Processing Language Overview

Here, the task delves into the fundamentals of SPL. Participants learn about the structure of SPL queries, including the importance of the pipe (|) character in chaining commands. The section also introduces basic SPL commands and their syntax, setting the foundation for more complex queries.

Task 5: Filtering the Results in SPL

This task focuses on filtering search results using SPL. Participants learn how to refine their searches to retrieve specific data points using commands like search, where, and dedup. Practical exercises help solidify understanding by requiring learners to apply these commands to real datasets.

Task 6: SPL - Structuring the Search Results

In this section, participants learn how to structure and format their search results for better readability and analysis. Commands such as table, fields, and rename are introduced. These commands help in organizing the output of SPL queries into a more structured and interpretable format.

Task 7: Transformational Commands in SPL

This task introduces transformational commands, which are used to manipulate and transform data within Splunk. Participants explore commands like stats, eval, and chart, which allow for advanced data analysis and visualization. Practical examples demonstrate how these commands can be used to derive insights from complex datasets.

Task 8: Recap and Conclusion

The final section recaps the key concepts covered in the task and reinforces the importance of SPL in data analysis. Participants are encouraged to review the commands and techniques learned and to continue practicing their SPL skills to become proficient in using Splunk for data analysis.

Screenshot Overview of the tasks

John_Mbithi_Mutave

68°F Mostly cloudy Search [Taskbar icons: File Explorer, Edge, etc.] ENG UK 8:46 AM 7/16/2024 [System tray icons: Network, Volume, etc.]

cs-sa07-24019
John_Mbithi_Mutave

10.10.22.179/.../search/search

TryHackMe | Learn Cy... | TryHackMe Support | Offline CyberChef | Revshell Generator | Reverse Shell Cheat S... | GitHub - sursikrepa/...

spunk - endorpha

Messages | Settings | Activity | Help | Find

Search | Analytics | Datasets | Reports | Alerts | Dashboards

Search & Reporting

Search

Enter search here...

Last 24 hours

No Event Sampling

Verbose Mode

Search History

100

No Time Filter

20 Per Page

1 2 3 4 5 6 7 Next

Search	Actions	Last Run
index = windowslogs	Add to Search	a minute ago
source="Event_Logs" host="cyber-host" index="windowslogs" sourcetype="_base"	Add to Search	Fri Jul 10 2022 00:38:18
index=""	Add to Search	Thu Jul 14 2022 09:25:19
*	Add to Search	Mon Jul 04 2022 00:48:50
index="1 delete	Add to Search	Sun Jul 03 2022 23:24:47
index="1 state count by index	Add to Search	Sun Jul 03 2022 23:24:31
index=windowslogs chart count by Image	Add to Search	Sun Jul 03 2022 23:24:27
index=windowslogs chart count by Image	Add to Search	Sun Jul 03 2022 21:40:14
index=windowslogs chart count by User	Add to Search	Sun Jul 03 2022 21:40:05
index=windowslogs new User	Add to Search	Sun Jul 03 2022 21:38:21
index=windowslogs new EventID	Add to Search	Sun Jul 03 2022 21:38:10
index=windowslogs new Image	Add to Search	Sun Jul 03 2022 21:37:50
index=windowslogs new Image	Add to Search	Sun Jul 03 2022 21:37:28
index=windowslogs top limit 8 Image	Add to Search	Sun Jul 03 2022 21:35:55
index=windowslogs top limit 7 Image	Add to Search	Sun Jul 03 2022 21:35:40
index=windowslogs search cyber	Add to Search	Sun Jul 03 2022 21:08:51
index=windowslogs search cyber	Add to Search	Sun Jul 03 2022 21:08:46
index=windowslogs search "cyber"	Add to Search	Sun Jul 03 2022 21:08:38
index=windowslogs search "Cyber"	Add to Search	Sun Jul 03 2022 21:08:31
index=windowslogs table _time EventID Hostname SourceName debug Hostname reverse	Add to Search	Sun Jul 03 2022 21:05:55

How to Search

If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Analyze Your Data with Table Views

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics. [View Table Views](#)

Search

ENG UK

cs-sa07-24019
John_Mbithi_Mutave

[illegible]

John_Mbithi_Mutave

[illegible]

John_Mbithi_Mutave

[illegible]

cs-sa07-24019
John_Mbithi_Mutave

The screenshot shows a web browser window with the TryHackMe website. The browser's address bar displays the URL `tryhackme.com/r/room/splunkexploringspl`. The website's navigation bar includes links for 'Dashboard', 'Learn', 'Compete', and 'Other', along with a search icon, a 'Go Premium' button, and a user profile icon. The main content area is titled 'Answer the questions below' and contains five quiz questions, each with a text input field and a 'Correct Answer' button. The questions and their answers are as follows:

- Question 1: How many Events are returned when searching for Event ID 1 AND User as "James"?
Answer: 4
- Question 2: How many events are observed with Destination IP 172.18.39.6 AND destination Port 135?
Answer: 4
- Question 3: What is the Source IP with highest count returned with this Search query?
Search Query: `index=windowslogs Hostname="Salena.Adam" DestinationIp="172.18.38.5"`
Answer: 172.90.12.11
- Question 4: In the index windowslogs, search for all the events that contain the term **cyber** how many events returned?
Answer: 0
- Question 5: Now search for the term **cyber***, how many events are returned?
Answer: 12256

Below the quiz questions, there is a task bar labeled 'Task 5' with the title 'Filtering the Results in SPL'. The browser's status bar at the bottom shows the temperature as 68°F, the weather as 'Mostly cloudy', and the time as 9:04 AM on 7/16/2024.

cs-sa07-24019
John_Mbithi_Mutave

TryHackMe | Learn Cy... | 10.10.222.179/en-US/app/search/search-index%3Ddownload%3D%20table_time_EventID_Hostname_SourceName%20reverse&display.page.search.mode=verbose&dispatch.sample_status=workload_pool&earliest-dates=display.events.fields["host%3D"]

Search | Analytics | Datasets | Reports | Alerts | Dashboards

New Search

Interdependencies
1 | table_time_EventID_Hostname_SourceName
2 | reverse

12,256 events (before 5/16/24 8:35:34.000 PM) No Event Sampling

Events (12,256) | Patterns | Statistics (12,256) | Visualization

100 Per Page | Format | Preview

Time	EventID	Hostname	SourceName
1922-04-15 08:05:48	886	Janez.browne	Powershell
1922-04-15 08:05:48	886	Janez.browne	Powershell
1922-04-15 08:05:48	886	Janez.browne	Microsoft-Windows-PowerShell
1922-04-15 08:05:48	886	Janez.browne	Powershell
1922-04-15 08:05:48	4183	Janez.browne	Microsoft-Windows-PowerShell
1922-04-15 08:05:48	886	Janez.browne	Powershell
1922-04-15 08:05:48	4183	Janez.browne	Microsoft-Windows-PowerShell
1922-04-15 08:05:48	886	Janez.browne	Powershell
1922-04-15 08:05:48	4183	Janez.browne	Microsoft-Windows-PowerShell
1922-04-15 08:05:48	886	Janez.browne	Powershell
1922-04-15 08:05:48	18	Michael.Savon	Microsoft-Windows-Sysmon
1922-04-15 08:05:48	18	Michael.Savon	Microsoft-Windows-Sysmon
1922-04-15 08:05:48	18	Michael.Savon	Microsoft-Windows-Sysmon
1922-04-15 08:05:48	18	Michael.Savon	Microsoft-Windows-Sysmon
1922-04-15 08:05:48	4183	Janez.browne	Microsoft-Windows-PowerShell
1922-04-15 08:05:48	4183	Janez.browne	Microsoft-Windows-PowerShell
1922-04-15 08:05:48	12	Janez.browne	Microsoft-Windows-Sysmon
1922-04-15 08:05:48	18	Michael.Savon	Microsoft-Windows-Sysmon
1922-04-15 08:05:48	18	Michael.Savon	Microsoft-Windows-Sysmon
1922-04-15 08:05:48	18	Michael.Savon	Microsoft-Windows-Sysmon
1922-04-15 08:05:48	18	Michael.Savon	Microsoft-Windows-Sysmon
1922-04-15 08:05:48	18	Michael.Savon	Microsoft-Windows-Sysmon
1922-04-15 08:05:48	18	Michael.Savon	Microsoft-Windows-Sysmon
1922-04-15 08:05:48	18	Michael.Savon	Microsoft-Windows-Sysmon
1922-04-15 08:05:48	18	Michael.Savon	Microsoft-Windows-Sysmon
1922-04-15 08:05:48	18	Michael.Savon	Microsoft-Windows-Sysmon

BT
lostly cloudy

Search

ENG UK 9:06 AM 7/16/2024

TryHackMe | Learn Cy... | 10.10.222.179/en-US/app/search/search-index%3Ddownload%3D%20table_time_EventID_Hostname_SourceName%20dedupHostname%20reverse&display.page.search.mode=verbose&dispatch.sample_status=workload_pool&earliest-dates=display.events.fields["host%3D"]

Search | Analytics | Datasets | Reports | Alerts | Dashboards

New Search

Interdependencies
1 | table_time_EventID_Hostname_SourceName
2 | dedup_Hostname
3 | reverse

12,268 events (before 5/16/24 8:39:02.000 PM) No Event Sampling

Events (12,268) | Patterns | Statistics (12,268) | Visualization

100 Per Page | Format | Preview

Time	EventID	Hostname	SourceName
1922-04-15 08:06:38	3	Michael.Savon	Microsoft-Windows-Sysmon
1922-07-14 21:37:59	5158	Janez.browne	Microsoft-Windows-Security-Auditing
1922-07-14 21:37:59	18	Michael.Savon	Microsoft-Windows-Sysmon

BT
ostly cloudy

Search

ENG UK 9:07 AM 7/16/2024

John_Mbithi_Mutave

[illegible]

John_Mbithi_Mutave

68°F Mostly cloudy Search [Taskbar icons: File Explorer, Edge, Chrome, etc.] ENG UK 9:14 AM 7/16/2024 [System tray icons: Network, Volume, etc.]

John_Mbithi_Mutave

The following query will display the Image chart based on the time.

Search Query: `index=windowslogs | timechart count by Image`

Answer the questions below

List the top 8 Image processes using the top command - what is the total count of the 6th Image?

✓ Correct Answer

Using the rare command, identify the user with the least number of activities captured?

✓ Correct Answer

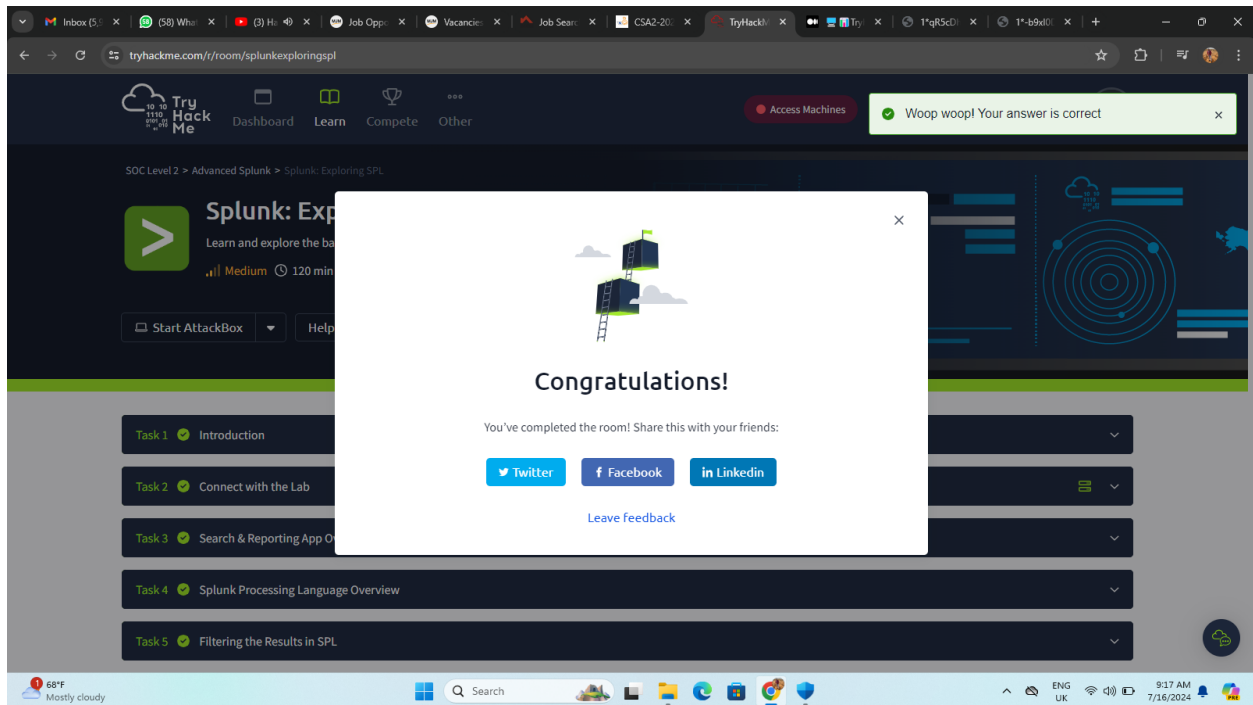
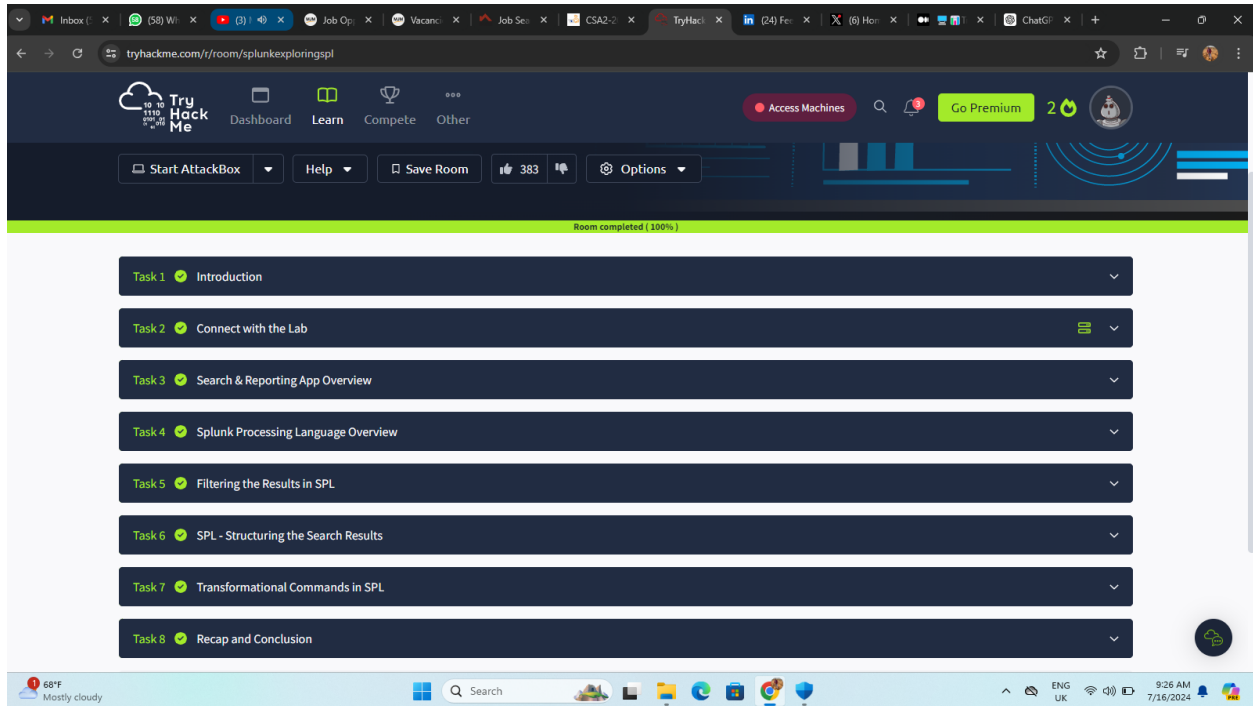
Create a pie-chart using the chart command - what is the count for the conhost.exe process?

✓ Correct Answer

Task 8 ○ Recap and Conclusion

Created by	Room Type	Users in Room	Created
<div> 68°F Mostly cloudy </div> <div> </div> <div> ENG UK 9:16 AM 7/16/2024 </div>			

cs-sa07-24019
John_Mbithi_Mutave



Shareable link - <https://tryhackme.com/r/room/splunkexploringspl>

Conclusion

The "Splunk: Exploring SPL" task on TryHackMe provides a comprehensive introduction to Splunk's Search Processing Language. Through a series of well-structured tasks, participants gain hands-on experience in using SPL to query, filter, and analyze data. By completing this task, learners build a strong foundation in SPL, which is essential for leveraging Splunk's capabilities in real-world data analysis scenarios.