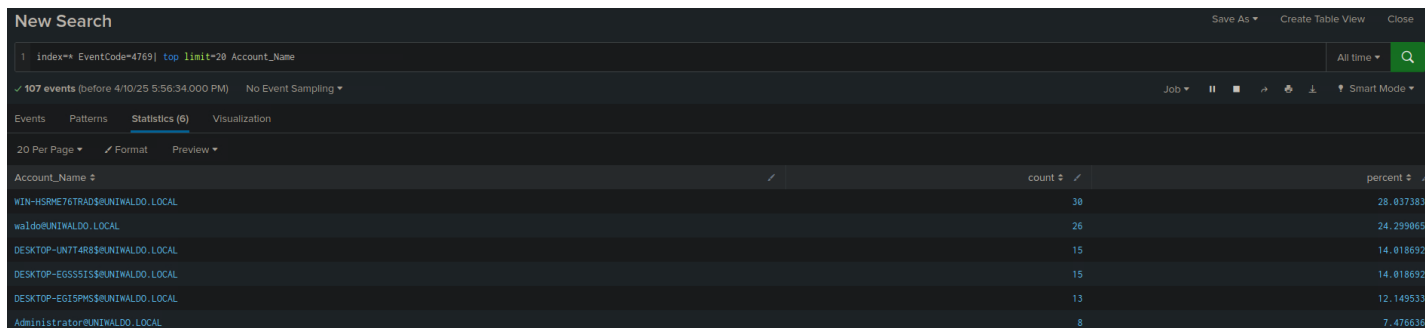


Introduction To Splunk & SPL in HTB

For this lab, I'm utilizing a Splunk Enterprise instance from Hack the Box's SOC Analyst course. During the lab I will be performing a couple of queries in relation to Kerberos authentication requests and computers accessed by the SYSTEM account.

Finding the account with the Kerberos authentication ticket requests:



The screenshot shows the Splunk Search interface with a search query: `index=* EventCode=4769 | top limit=20 Account_Name`. The search results are displayed in a table with columns: Account_Name, count, and percent. The results show the top 20 accounts with the highest number of Kerberos authentication ticket requests.

Account_Name	count	percent
WIN-HSRME76TRAD\$RUNTALDO_LOCAL	30	28.037383
walder@UNTALDO_LOCAL	26	24.299065
DESKTOP-UNT4R8\$RUNTALDO_LOCAL	15	14.018692
DESKTOP-EGSSS1\$RUNTALDO_LOCAL	15	14.018692
DESKTOP-EG15PHS\$RUNTALDO_LOCAL	13	12.149533
Administrator@UNTALDO_LOCAL	8	7.476636

Found the top accounts with Kerberos Authentication ticket requests with the following query:

index=* EventCode=4769 | top limit=20 Account_Name

index=*: Searches through all available indexes

EventCode=4769 = Searches specifically for Kerberos authentication ticket requests

Top limit= Sorts the data by highest counts

Account_Name= Displays account name for each result in the table

Find the number of distinct computers accessed by the SYSTEM account:

The screenshot shows the Splunk search results interface. The search bar contains the query: `1 index=* EventCode=4624 Account_Name=SYSTEM`. Below the search bar, it indicates **6,990 events** (before 4/10/25 6:22:35.000 PM) with **No Event Sampling**. The interface has tabs for **Events (6,990)**, **Patterns**, **Statistics**, and **Visualization**. Below the tabs are controls for **Format Timeline**, **Zoom Out**, **Zoom to Selection**, and **Deselect**. A table of results is displayed with columns for **Time** and **Event**. The first row shows a timestamp of 11/8/22 2:50:26.000 PM and event details including `LogName=Security`, `EventCode=4624`, `EventType=0`, and `ComputerName=DESKTOP-UN`. A red arrow points to the **ComputerName** field in the **INTERESTING FIELDS** list on the left, which also shows `Account_Domain`, `Account_Name`, `Authentication_Package`, and `ComputerName`.

The screenshot shows the Splunk search results interface for the same query: `1 index=* EventCode=4624 Account_Name=SYSTEM`. The second line of the query is `2 | stats dc(ComputerName)`. The results show **6,990 events** (before 4/10/25 6:21:31.000 PM) with **No Event Sampling**. The interface has tabs for **Events (6,990)**, **Patterns**, **Statistics (1)**, and **Visualization**. Below the tabs are controls for **20 Per Page**, **Format**, and **Preview**. The results section shows the command `dc(ComputerName)` and the count **10**.

I found two easy ways to grab this:

One way is the query for all indexes using the 4624 event code and filter for the SYSTEM account name: **index=* EventCode=4624 Account_Name=SYSTEM**. Using Splunk's given interesting fields, you can view the count of Computer names.

A cleaner way to do it is to add a pipe to the query to display the discount count of computer names

in the statistics tab. **index=* EventCode=4624 Account_Name=SYSTEM | stats**

dc(ComputerName)