

LEARNING SPLUNK

Article by-DEEPA LI GUPTA

SPLUNK :

Splunk is a software platform used for monitoring, searching, analyzing and visualizing machine-generated data in real time. It captures, indexes, and correlates real-time data in a searchable container and produces graphs, alerts, dashboards, and visualizations. Splunk is used to monitor and troubleshoot problems with applications, servers, and networks. Developers use Splunk to analyze and search data, create data models, and visualize results for monitoring and examining large amounts of machine-generated data.

MODULE 1: INSTALL SPLUNK ENTERPRISE

INSTALLATION OF SPLUNK :

STEP 1: Go to the website of splunk- splunk.com.

STEP 2: Do the registration.

STEP 3: Go to products and download splunk enterprize.

STEP 4: Download will start and now you can run that msi file to install it on your system.

STEP 5: After installing , we can start with it.

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk>enterprise' and 'Apps'. Below the navigation is a search bar and a sidebar titled 'Hello, Administrator' with a green checkmark icon. The main area has a 'Quick links' section with 'Search & Reporting', 'Splunk Secure Gateway', and 'Upgrade Readiness App'. It also features a 'Find more apps' link. Below this are sections for 'Common tasks' (Add data, Search your data, Visualize your data, Add team members, Manage permissions, Configure mobile devices) and 'Learning and resources' (Product tours, Learn more with Splunk Docs, Get help from Splunk experts, Extend your capabilities, Join the Splunk Community, See how others use Splunk).

Creating new user with administrator rights.

The screenshot shows the 'Users' page in Splunk. At the top right is a 'New User' button. The table lists one user: 'deepali_12' (Actions: Edit, Authentication system: Splunk, Full name: Administrator, Email address: changeme@example.com, Time zone: launcher, Default app: system, Roles: admin, Last Login: 27/2/2024, 9:34:30 am, Status: Active). There are filters and a per-page dropdown at the top.

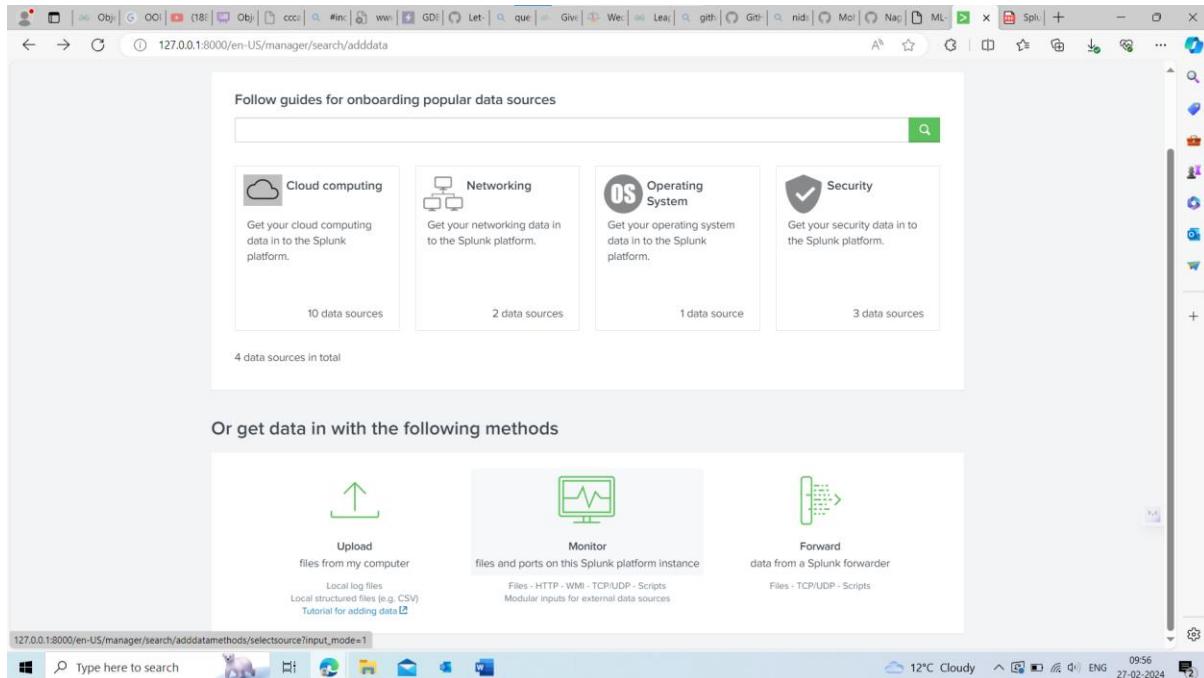
We can add users by:settings -> users-> new user. So ,here I created a new user with name –

The screenshot shows the 'Users' page after adding a new user. Now there are two users listed: 'deepali_12' (same details as before) and 'dipali' (Actions: Edit, Authentication system: Splunk, Full name: dipali, Email address: dipali@example.com, Time zone: launcher, Default app: system, Roles: power, user-dipali, Last Login: 27/2/2024, 9:34:30 am, Status: Active).

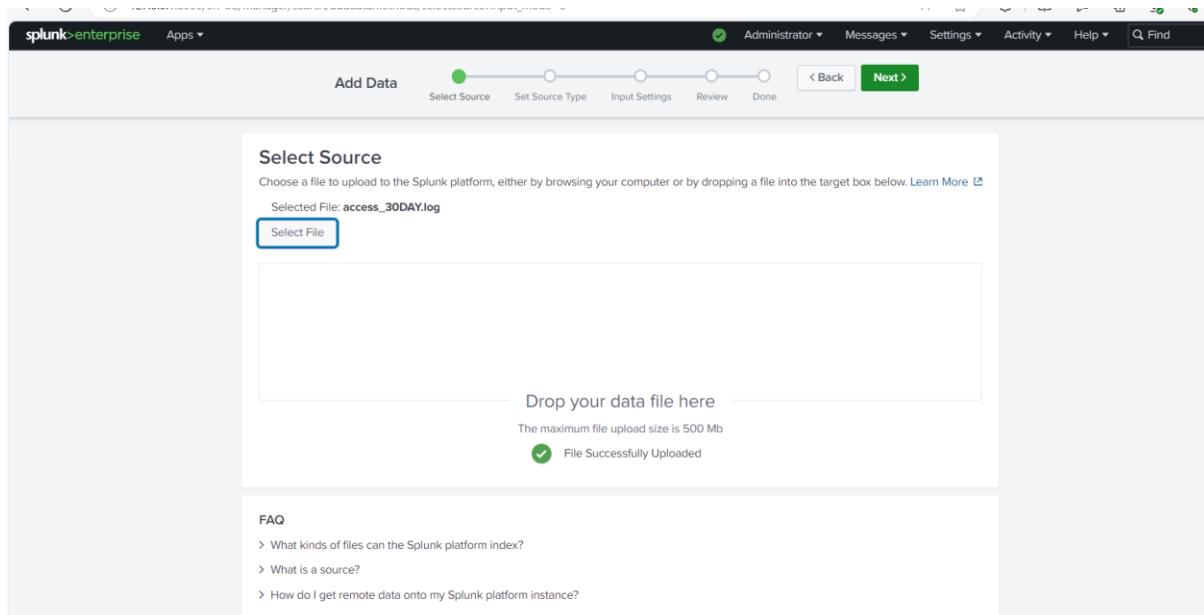
Dipali.

MODULE 2: INGESTING DATA

In this we will upload the file to analyse.



clicking on upload button, we will upload the file .



Now on clicking on next button, This screen will appear.

Splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Add Data

Select Source Set Source Type Input Settings Review Done

Back Next >

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: access_30DAY.log

Source type: access_combined_wcookie ▾ Save As

List ▾ Format 20 Per Page ▾

View Event Summary

Event Breaks Timestamp Advanced

Time Event

1 2 3 4 5 6 7 8 ... Next >

Now we can see in this that splunk has already set the source type.

Splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Add Data

Select Source Set Source Type Input Settings Review Done

Back Next >

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: access_30DAY.log

Source type: access_combined_wcookie ▾ Save As

List ▾ Format 20 Per Page ▾

View Event Summary

Event Breaks Timestamp Advanced

Time Event

1 2 3 4 5 6 7 8 ... Next >

Now we have set the host field value as – web_application .

Add Data

Select Source Set Source Type Input Settings Review Done

Back Review >

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Constant value
 Regular expression on path
 Segment in path

Host field value

Index

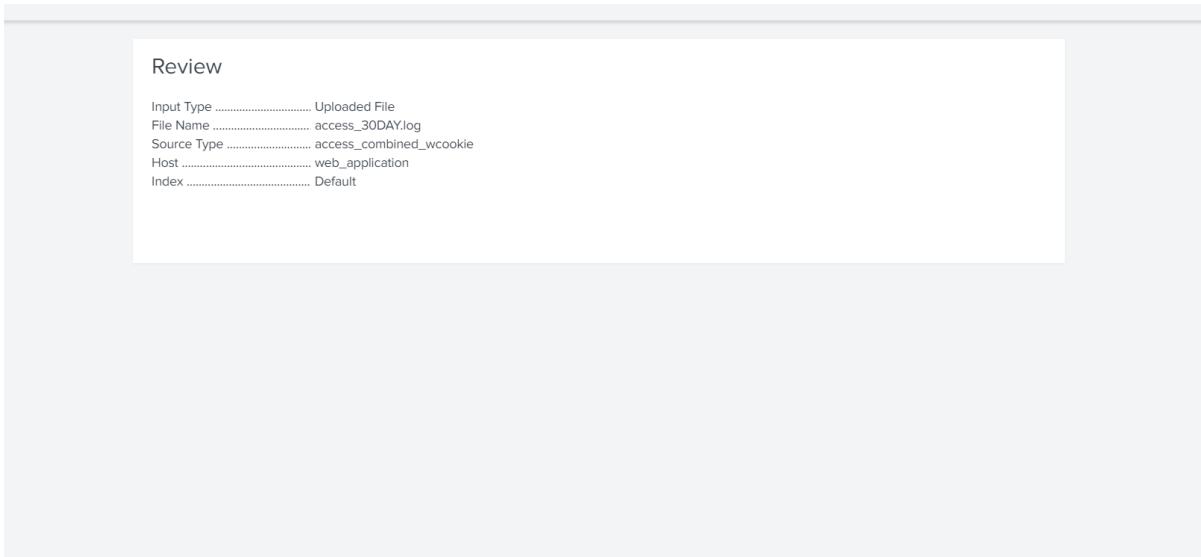
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index Default Create a new index

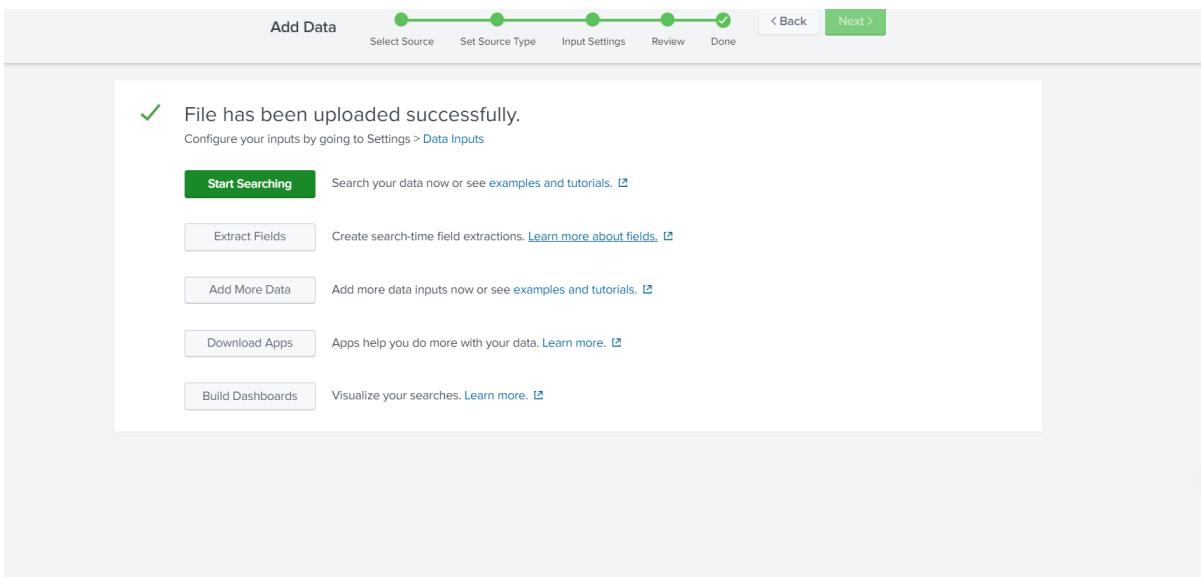
FAQ

> How do indexes work?
> How do I know when to create or use multiple indexes?

Clicking on Review button. We will get the page telling about our file details.



Clicking on submit button , our file will be submitted and we will now go to the task 3.



No we will upload the linux 30 day file by clicking on Add more button -> upload -> linux30day file.

, now source type is to be set which is already set by the splunk.

splunk>enterprise Apps ▾

Add Data

Select Source Set Source Type Input Settings Review Done < Back Next >

Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: linux_s_30DAY.log

Source type: linux_secure ▾ Save As

	Time	Event
1	1/27/24 8:00:05.000 AM	Sat Jan 27 2024 08:00:05 www1 sshd[4741]: Failed password for invalid user zabbix from 208.65.153.253 port 22 ssh2
2	1/27/24 8:00:29.000 AM	Sat Jan 27 2024 08:00:29 www1 sshd[4600]: Failed password for invalid user operator from 208.65.153.253 port 22 ssh2
3	1/27/24 8:01:14.000 AM	Sat Jan 27 2024 08:01:14 www1 sshd[4867]: Failed password for invalid user dba from 208.65.153.253 port 1895 ssh2
4	1/27/24 8:39:04.000 AM	Sat Jan 27 2024 08:39:04 www1 sshd[72408]: pam_unix(sshd:session): session opened for user nsharpe by (uid=0)
5	1/27/24 8:39:04.000 AM	Sat Jan 27 2024 08:39:04 www1 sshd[90106]: Server listening on :: port 22.
6	1/27/24 8:39:04.000 AM	Sat Jan 27 2024 08:39:04 www1 sshd[93022]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)
7	1/27/24 8:41:58.000 AM	Sat Jan 27 2024 08:41:58 www1 sshd[2262]: Failed password for root from 202.179.8.245 port 22 ssh2
8	1/27/24 8:41:59.000 AM	Sat Jan 27 2024 08:41:59 www1 sshd[3346]: Failed password for root from 202.179.8.245 port 22 ssh2

View Event Summary

splunk>enterprise Apps ▾

Add Data

Select Source Set Source Type Input Settings Review Done < Back Review >

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Constant value
 Regular expression on path
 Segment in path

Host field value

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index Create a new index

FAQ

- How do indexes work?
- How do I know when to create or use multiple indexes?

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Q Find

Add Data

Review

Input Type Uploaded File
File Name linux_s_30DAY.log
Source Type linux_secure
Host web_server
Index Default

Done

< Back Submit >

This screenshot shows the 'Review' step of the 'Add Data' wizard. It displays the configuration settings entered by the user: Input Type (Uploaded File), File Name (linux_s_30DAY.log), Source Type (linux_secure), Host (web_server), and Index (Default). The status bar at the top indicates the user is 'Administrator'. The navigation bar includes links for 'Messages', 'Settings', 'Activity', 'Help', and a search bar.

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Q Find

Add Data

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

Selected File: db_audit_30DAY.csv

Select File

Drop your data file here

The maximum file upload size is 500 Mb

✓ File Successfully Uploaded

FAQ

What kinds of files can the Splunk platform index?
What is a source?
How do I get remote data onto my Splunk platform instance?

Next >

This screenshot shows the 'Select Source' step of the 'Add Data' wizard. It features a file upload interface where a CSV file named 'db_audit_30DAY.csv' has been selected. A message indicates the file was successfully uploaded. Below the upload area is a 'FAQ' section with links related to file types, sources, and remote data ingestion. The navigation bar at the top shows the user is 'Administrator'.

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Add Data  Review >

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Constant value
 Regular expression on path
 Segment in path

Host field value

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index Create a new index

FAQ

> How do indexes work?
> How do I know when to create or use multiple indexes?

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Add Data  Review >

Review

Input Type Uploaded File
File Name db_audit_30DAY.csv
Source Type db_audit
Host database
Index Default

MODULE 3: SEARCHING

TASK 1: PERFORM A BASIC SEARCH

1. Performing Search with command : error OR fail*

Time	Event
2/26/24 11:38:49.000 PM	194.8.74.23 - [26/Feb/2024:23:38:49] "POST /cart/error.do?msg=FormError&JSESSIONID=SD8SL5FF4ADFF89311 HTTP/1.1" 200 1253 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 438 host= web_application source = access_30DAY.log sourcetype = access_combined_wcookie
2/26/24 11:57:00.000 PM	67.133.102.54 - [26/Feb/2024:23:15:57] "POST /cart/error.do?msg=CreditNotAccepted&JSESSIONID=SD2SL4FF6ADFF4958 HTTP/1.1" 200 2024 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 620 host= web_application source = access_30DAY.log sourcetype = access_combined_wcookie
2/26/24 11:12:48.000 PM	142.162.221.28 - [26/Feb/2024:23:12:48] "POST /cart/error.do?msg=CreditDoesNotMatch&JSESSIONID=SD0SL4FF2ADFF89269 HTTP/1.1" 200 1382 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)" 744 host= web_application source = access_30DAY.log sourcetype = access_combined_wcookie
2/26/24 11:11:31.000 PM	211.166.11.101 - [26/Feb/2024:23:11:31] "POST /cart/error.do?msg=CreditNotAccepted&JSESSIONID=SD7SL9FF4ADFF89538 HTTP/1.1" 200 2035 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 476 host= web_application source = access_30DAY.log sourcetype = access_combined_wcookie
2/26/24 11:11:20.000 PM	211.166.11.101 - [26/Feb/2024:23:11:20] "POST /cart/error.do?msg=ItemOutOfStock&productId=GT-SC-G01&JSESSIONID=SD7SL9FF4ADFF89538 HTTP/1.1" 200 602 "http://www.buttercupgames.com/cart.do?action=purchase&productId=GT-SC-G01" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 476 host= web_application source = access_30DAY.log sourcetype = access_combined_wcookie

In this , we can observe , we are getting results for both web application and web server.

TASK 2: START A NEW SEARCH. NARROW YOUR RESULTS

2. Performing search with command : fail* AND password

The screenshot shows the Splunk interface with a search bar containing "fail* AND password". Below it, a summary says "450 events (2/26/24 9:30:00.000 AM to 2/27/24 10:15:16.000 AM) No Event Sampling". The main area displays a table of events with columns for Time and Event. The table includes a header row and several event rows. On the left, there are sections for "SELECTED FIELDS" and "INTERESTING FIELDS". The "Event" column contains log entries like "Mon Feb 26 2024 22:56:31 www1 sshd[1389]: Failed password for invalid user ubuntu from 223.213.255.255 port 4411 ssh2 host = web_server source = linux_s_30DAY.log sourcetype = linux_secure". The interface has a "Last 24 hours" dropdown and various navigation and search controls.

Review the results and notice the port values for a few of the events. You want to see users trying to log into the SSH port we have open, port 22.

3. Performing search with cmd : fail* AND password 22

The screenshot shows the Splunk interface with a search bar containing "fail* AND password 22". Below it, a summary says "349 events (2/26/24 9:30:00.000 AM to 2/27/24 10:17:13.000 AM) No Event Sampling". The main area displays a table of events with columns for Time and Event. The table includes a header row and several event rows. On the left, there are sections for "SELECTED FIELDS" and "INTERESTING FIELDS". The "Event" column contains log entries like "Mon Feb 26 2024 22:56:31 www1 sshd[1389]: Failed password for invalid user ubuntu from 223.213.255.255 port 4411 ssh2 host = web_server source = linux_s_30DAY.log sourcetype = linux_secure". The interface has a "Last 24 hours" dropdown and various navigation and search controls.

Notice that not only events with port 22 are selected, but any events with the number 22 in them.

4. Performing search with cmd : fail* AND password port 22

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query "fail* AND password port 22". The results table shows 349 events from February 26, 2024, between 9:30:00:000 AM and 10:18:03:000 AM. The events list includes several entries related to failed password attempts on port 22:

Time	Event
Mon Feb 26 2024 22:56:31	www1 sshd[1389]: Failed password for invalid user ubuntu from 233.213.255.255 port 4411 ssh2 host = web_server source = linux_s_30DAY.log sourcetype = linux_secure
Mon Feb 26 2024 22:56:18	www1 sshd[3497]: Failed password for root from 233.213.255.255 port 8000 ssh2 host = web_server source = linux_s_30DAY.log sourcetype = linux_secure
Mon Feb 26 2024 22:56:02	www1 sshd[5001]: Failed password for invalid user tomcat from 192.188.106.240 port 22 ssh2 host = web_server source = linux_s_30DAY.log sourcetype = linux_secure
Mon Feb 26 2024 22:55:44	www1 sshd[2609]: Failed password for invalid user root from 192.188.106.240 port 2263 ssh2 host = web_server source = linux_s_30DAY.log sourcetype = linux_secure
Mon Feb 26 2024 22:55:36	www1 sshd[5938]: Failed password for invalid user noone from 192.188.106.240 port 22 ssh2 host = web_server source = linux_s_30DAY.log sourcetype = linux_secure
Mon Feb 26 2024 22:39:00	www1 sshd[3730]: Failed password for invalid user helpdesk from 142.162.221.28 port 22 ssh2 host = web_server source = linux_s_30DAY.log sourcetype = linux_secure

Notice that you are now only seeing events the entire phase.

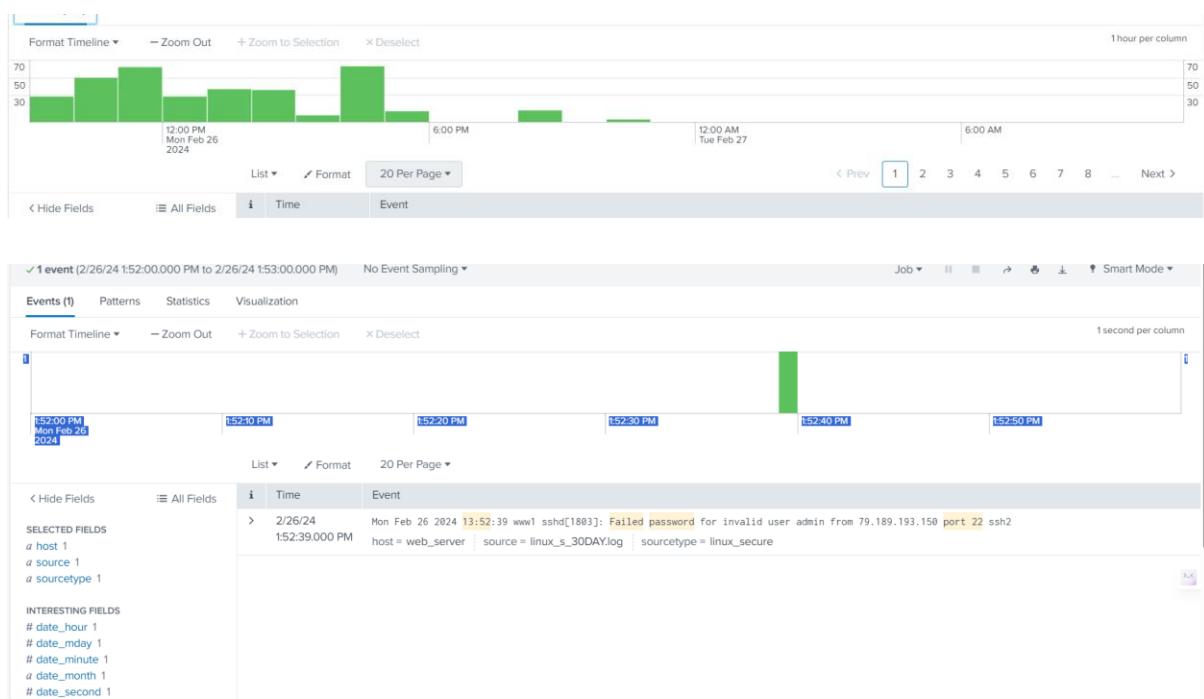
5. Performing search with cmd : fail* AND password "port 22"

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query "fail* AND password \"port 22\"". The results table shows 341 events from February 26, 2024, between 9:30:00:000 AM and 10:19:07:000 AM. The events list includes several entries related to failed password attempts on port 22:

Time	Event
Mon Feb 26 2024 22:56:02	www1 sshd[5001]: Failed password for invalid user tomcat from 192.188.106.240 port 22 ssh2 host = web_server source = linux_s_30DAY.log sourcetype = linux_secure
Mon Feb 26 2024 22:55:36	www1 sshd[5938]: Failed password for invalid user noone from 192.188.106.240 port 22 ssh2 host = web_server source = linux_s_30DAY.log sourcetype = linux_secure
Mon Feb 26 2024 22:39:00	www1 sshd[3730]: Failed password for invalid user helpdesk from 142.162.221.28 port 22 ssh2 host = web_server source = linux_s_30DAY.log sourcetype = linux_secure
Mon Feb 26 2024 20:10:40	www1 sshd[5045]: Failed password for invalid user services from 233.213.255.255 port 22 ssh2 host = web_server source = linux_s_30DAY.log sourcetype = linux_secure
Mon Feb 26 2024 20:09:50	www1 sshd[3877]: Failed password for invalid user postgres from 233.213.255.255 port 22 ssh2 host = web_server source = linux_s_30DAY.log sourcetype = linux_secure
Mon Feb 26 2024 20:09:27	www1 sshd[2691]: Failed password for nobody from 233.213.255.255 port 22 ssh2 host = web_server source = linux_s_30DAY.log sourcetype = linux_secure

TASK 3: USE THE TIMELINE TO LOOK FOR TRENDS IN RESULTS.

6. Timeline :

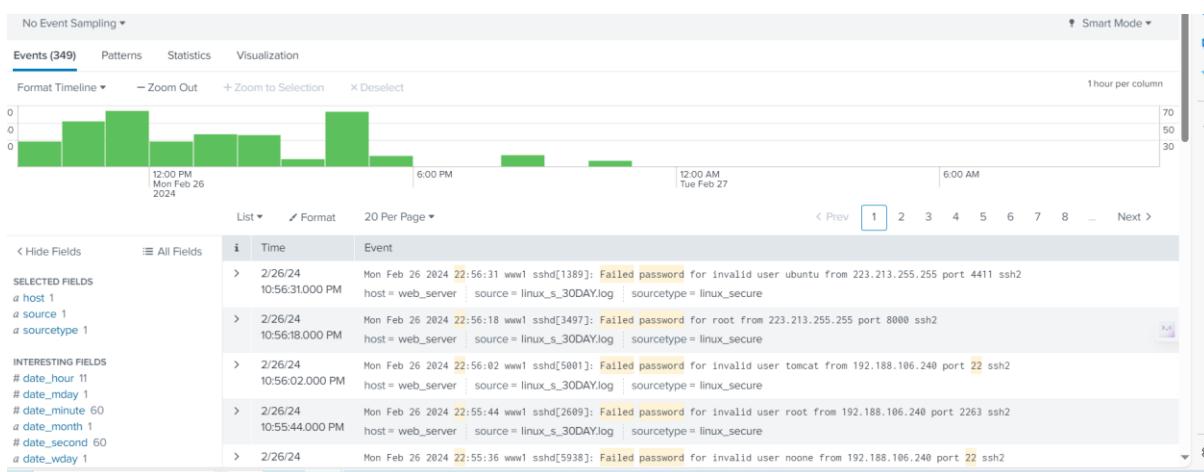


Single click another column. Look at these events. If there are spikes in events that look similar in time, your system may be the target of an attack. If there are no spikes, it has been a good month. Optionally, look at some of the events that were returned and see if you can spot any similarities in IP addresses or ports used.

TASK 4: USE THE OUTPUT OF YOUR SEARCH TO REFINE THE RESULTS.

Click one of the user names in the search results. Note that when you click a user name, a menu of options appears:

User – ubuntu



The screenshot shows a log search interface with the following details:

- Search Query:** fail+ AND password 22 user ubuntu
- Results:** 3 events (2/26/24 10:30:00.000 AM to 2/27/24 10:30:31.000 AM) - No Event Sampling
- Time Range:** Last 24 hours
- Event Timeline:** Format Timeline, Zoom Out, +Zoom to Selection, X Deselect. The timeline shows three green bars representing event times: 12:00 PM Mon Feb 26 2024, 6:00 PM, and 12:00 AM Tue Feb 27.
- Event List:** Shows three entries under the "Event" column, each detailing a failed password attempt for user "ubuntu" from different IP addresses (223.213.255.255, 67.133.102.54, 194.215.205.19) via port 22 (ssh2).
- Fields:** SELECTED FIELDS include host 1, source 1, sourcetype 1. INTERESTING FIELDS include date_hour 3, date_mday 1, date_minute 3, date_month 1, date_second 3, date_wday 1.

TASK 5: SAVE AND SHARE RESULTS. (EXTEND THE DEFAULT SAVE TIME. EXPAND DEFAULT VIEWING PERMISSIONS TO ALL.)

JOBS :

The screenshot shows the "Job Settings" dialog box with the following configuration:

- Owner:** dipali
- App:** search
- Read Permissions:** Private (button) vs Everyone (button)
- Lifetime:** 10 minutes (button) vs 7 days (button, highlighted with a blue border)
- Buttons:** Cancel (gray), Save (green)
- Copy job link:** A button with a link icon.

28: View your list of job histories from the Activity > Jobs menu (on the right side of the Splunk bar, which is the black bar at the top of the browser window).

15 Jobs										
	App: Search & Reporting (search)	Owner: All	Status: All	filter						10 Per Page
	Edit Selected									< Prev 1 2 Next >
>	<input type="checkbox"/> dipali	search	289	208 KB	Feb 27, 2024 10:32:28 AM	Expires	Feb 27, 2024 10:42:44 AM	Runtime	00:00:01	Done
		fail" AND password "port 22"	[2/26/24 10:30:00.000 AM to 2/27/24 10:32:27.000 AM]							
>	<input type="checkbox"/> dipali	search	295	204 KB	Feb 27, 2024 10:31:21 AM	Expires	Feb 27, 2024 10:41:36 AM	Runtime	00:00:01	Done
		fail" AND password 22	[2/26/24 10:30:00.000 AM to 2/27/24 10:31:20.000 AM]							
>	<input type="checkbox"/> dipali	search	199	200 KB	Feb 27, 2024 10:31:17 AM	Expires	Feb 27, 2024 10:41:18 AM	Runtime	00:00:01	Done
		fail" AND password 22 user	[2/26/24 10:30:00.000 AM to 2/27/24 10:31:16.000 AM]							
>	<input type="checkbox"/> dipali	search	3	128 KB	Feb 27, 2024 10:30:32 AM	Expires	Feb 27, 2024 10:41:02 AM	Runtime	00:00:01	Done
		fail" AND password 22 user ubuntu	[2/26/24 10:30:00.000 AM to 2/27/24 10:30:31.000 AM]							
>	<input type="checkbox"/> dipali	search	199	200 KB	Feb 27, 2024 10:30:26 AM	Expires	Feb 27, 2024 10:40:27 AM	Runtime	00:00:01	Done
		fail" AND password 22 user	[2/26/24 10:30:00.000 AM to 2/27/24 10:30:25.000 AM]							
>	<input type="checkbox"/> dipali	search	349	212 KB	Feb 27, 2024 10:29:38 AM	Expires	Feb 27, 2024 10:39:39 AM	Runtime	00:00:01	Done
		fail" AND password port 22	[2/26/24 9:30:00.000 AM to 2/27/24 10:29:38.000 AM]							
>	<input type="checkbox"/> dipali	search	349	212 KB	Feb 27, 2024 10:29:38 AM	Expires	Feb 27, 2024 10:40:24 AM	Runtime	00:00:01	Done
		fail" AND password 22 [2/26/24 9:30:00.000 AM to 2/27/24 10:29:38.000 AM]								
>	<input type="checkbox"/> dipali	search	1	112 KB	Feb 27, 2024 10:29:31 AM	Expires	Feb 27, 2024 10:39:32 AM	Runtime	00:00:01	Done
		* user admin	[2/26/24 1:52:00.000 PM to 2/26/24 1:53:00.000 PM]							

29. Take a moment to review Owner, Events, Expires, Status, and Actions of the jobs. (Note that if a job is running, you can use the button – located under Actions - to stop it. This also sets the job status to Finalized.)

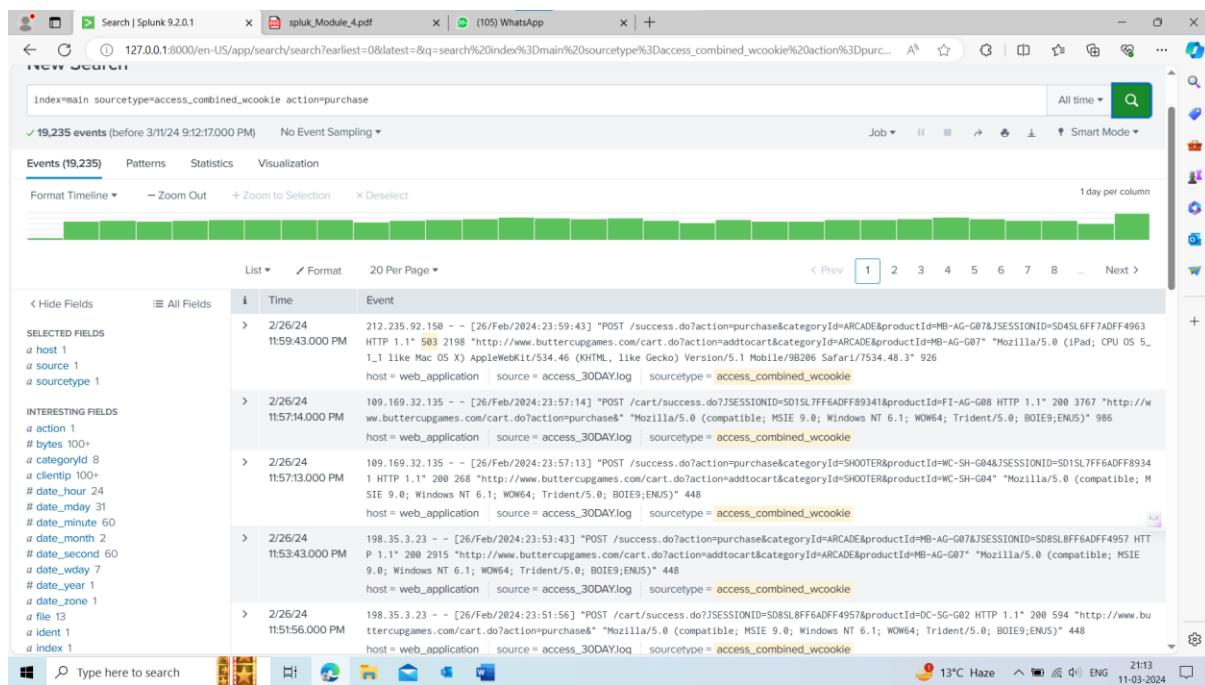
15 Jobs										
	App: Search & Reporting (search)	Owner: All	Status: All	filter						10 Per Page
	Edit Selected									< Prev 1 2 Next >
>	<input type="checkbox"/> dipali	search	289	208 KB	Feb 27, 2024 10:32:28 AM	Expires	Mar 5, 2024 10:36:14 AM	Runtime	00:00:01	Done
		fail" AND password "port 22"	[2/26/24 10:30:00.000 AM to 2/27/24 10:32:27.000 AM]							
>	<input type="checkbox"/> dipali	search	295	204 KB	Feb 27, 2024 10:31:21 AM	Expires	Feb 27, 2024 10:41:36 AM	Runtime	00:00:01	Done
		fail" AND password 22	[2/26/24 10:30:00.000 AM to 2/27/24 10:31:20.000 AM]							
>	<input type="checkbox"/> dipali	search	199	200 KB	Feb 27, 2024 10:31:17 AM	Expires	Feb 27, 2024 10:41:18 AM	Runtime	00:00:01	Done
		fail" AND password 22 user	[2/26/24 10:30:00.000 AM to 2/27/24 10:31:16.000 AM]							
>	<input type="checkbox"/> dipali	search	3	128 KB	Feb 27, 2024 10:30:32 AM	Expires	Feb 27, 2024 10:41:02 AM	Runtime	00:00:01	Done
		fail" AND password 22 user ubuntu	[2/26/24 10:30:00.000 AM to 2/27/24 10:30:31.000 AM]							
>	<input type="checkbox"/> dipali	search	199	200 KB	Feb 27, 2024 10:30:26 AM	Expires	Feb 27, 2024 10:40:26 AM	Runtime	00:00:01	Done
		fail" AND password 22 user	[2/26/24 10:30:00.000 AM to 2/27/24 10:30:25.000 AM]							
>	<input type="checkbox"/> dipali	search	349	212 KB	Feb 27, 2024 10:29:38 AM	Expires	Feb 27, 2024 10:39:38 AM	Runtime	00:00:01	Done
		fail" AND password port 22	[2/26/24 9:30:00.000 AM to 2/27/24 10:29:38.000 AM]							
>	<input type="checkbox"/> dipali	search	349	212 KB	Feb 27, 2024 10:29:38 AM	Expires	Feb 27, 2024 10:40:24 AM	Runtime	00:00:01	Done
		fail" AND password 22 [2/26/24 9:30:00.000 AM to 2/27/24 10:29:38.000 AM]								
>	<input type="checkbox"/> dipali	search	1	112 KB	Feb 27, 2024 10:29:31 AM	Expires	Feb 27, 2024 10:39:31 AM	Runtime	00:00:01	Done
		* user admin	[2/26/24 1:52:00.000 PM to 2/26/24 1:53:00.000 PM]							

MODULE 4: USING FIELDS IN SEARCHES

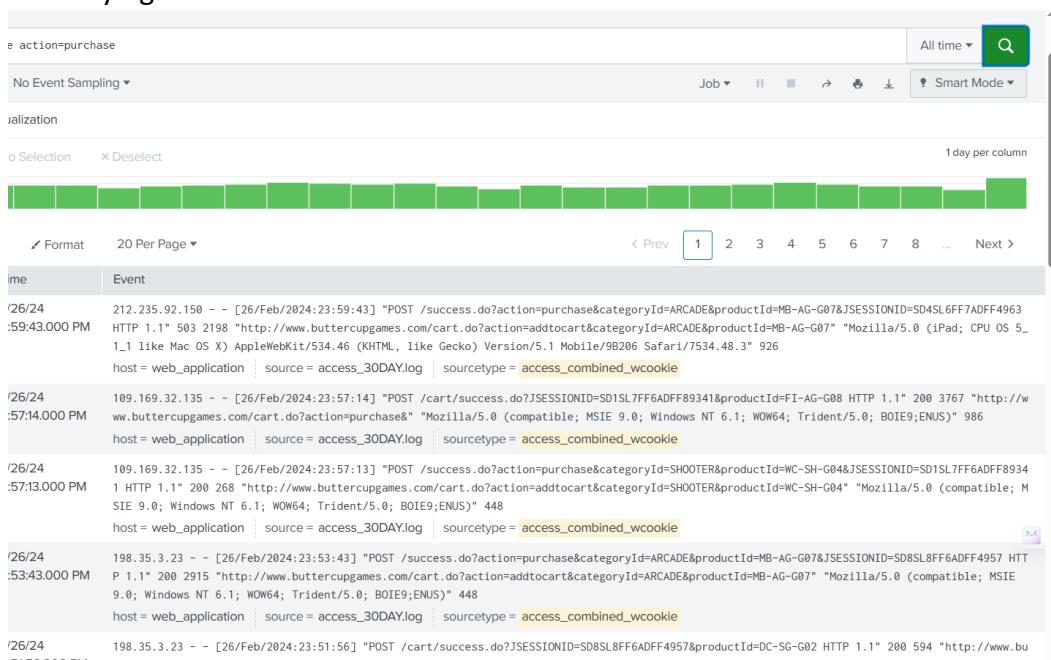
Task 1: Use the Fields sidebar to examine search results.

1. In the app navigation bar (i.e., the bar towards the top of the browser window,) click Search. If you do not see Search in the application bar – or to clear the previous search - click the App: Search & Reporting in the Splunk bar at the top of the browser window.
2. Search for index=main sourcetype=access_combined_wcookie action=purchase for All time.

Solu: This returns all events where a purchase action was taken.



2. Verifying search executed in smart mode.



3. Sidebar's Interesting Fields list. ProductId is one of the fields extracted by Splunk.

```

a categoryid 8
a clientip 100+
# date_hour 24
# date_mday 31
# date_minute 60
a date_month 2
# date_second 60
a date_wday 7
# date_year 1
a date_zone 1
a file 13
a ident 1
a index 1
a JSESSIONID 100+
# linecount 1
a method 2
# other 100+
a productid 18
a punct 34
a referer 23
a referer_domain 4
a req_time 100+
a root 5
a splunk_server 1
# status 9
# timeendpos 7
# timestamppos 7
a uri 100+
a uri_path 14
a uri_query 100+
a user 1
a useragent 26
# version 1

```

4. Product ids of ten purchased products

The screenshot shows a web browser window with the following details:

- Address Bar:** 127.0.0.1:8000/en-US/app/search/search?earliest=0&latest=&q=search%20index%3Dmain%20sourcetype%3Daccess_combined_wcookie%20action%3Dpurchase
- Toolbar:** Includes icons for back, forward, search, and refresh.
- Sidebar (Interesting Fields):**
 - a categoryid 8
 - a clientip 100+
 - # date_hour 24
 - # date_mday 31
 - # date_minute 60
 - a date_month 2
 - # date_second 60
 - a date_wday 7
 - # date_year 1
 - a date_zone 1
 - a file 13
 - a ident 1
 - a index 1
 - a JSESSIONID 100+
 - # linecount 1
 - a method 2
 - # other 100+
 - a productid 18**
 - a punct 34
 - a referer 23
 - a referer_domain 4
 - a req_time 100+
 - a root 5
 - a splunk_server 1
 - # status 9
 - # timeendpos 7
 - # timestamppos 7
 - a uri 100+
 - a uri_path 14
 - a uri_query 100+
 - a user 1
 - a useragent 26
 - # version 1
- Table (Top 10 Values):**

productId	Count	%
WC-SH-G84	1,422	8.21%
DB-SG-G81	1,389	8.02%
DC-SG-G82	1,368	7.90%
MB-AG-T81	1,268	7.32%
MB-AG-G87	1,262	7.29%
WC-SH-A82	1,238	7.15%
FS-SG-G83	1,199	6.93%
WC-SH-A81	1,141	6.59%
WC-SH-T82	1,116	6.45%
PZ-SG-G85	1,063	6.14%
- Logs (Bottom):**
 - 11:40:15.000 PM: purchase&categoryid=STRATEGY&productId=DC-SG-G82&JSESSIONID=SD8SL8FF6ADFF4957 HTTP 1.1" 200 594 "http://www.buttercupgames.com/cart.do?action=purchase" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BIE9;ENUS)" 448
 - 11:40:15.000 PM: addtocart&categoryid=STRATEGY&productId=DC-SG-G82" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BIE9;ENUS)" 448
 - 11:40:15.000 PM: access_combined_wcookie
 - 11:40:15.000 PM: purchase&categoryid=SHOOTER&productId=WC-SH-G84&JSESSIONID=SD2SL10FF6ADFF4955 HTTP 1.1" 200 816 "http://www.buttercupgames.com/cart.do?action=purchase&categoryid=SHOOTER&productId=WC-SH-G84" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 886
 - 11:40:15.000 PM: addtocart&categoryid=SHOOTER&productId=WC-SH-G84" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 886
 - 11:40:15.000 PM: access_combined_wcookie
 - 11:40:15.000 PM: purchase&categoryid=STRATEGY&productId=PZ-SG-G85 HTTP 1.1" 200 560 "http://www.buttercupgames.com/cart.do?action=purchase&categoryid=STRATEGY&productId=PZ-SG-G85" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BIE9;ENUS)" 971
 - 11:40:15.000 PM: addtocart&categoryid=STRATEGY&productId=PZ-SG-G85" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BIE9;ENUS)" 971
 - 11:40:15.000 PM: access_combined_wcookie

5. Click Status : This field contains the status of the web request. Anything greater than 200 means that the customer interaction ended in an error, and the purchase was not made

The screenshot shows a Splunk search interface with a histogram titled "status". The y-axis represents the count of events, and the x-axis represents the status code. The "200" bin is selected, highlighted in blue. Other visible status codes include 503, 408, 400, 406, 500, 505, 404, and 403. The histogram has a color gradient from light blue for lower counts to dark blue for higher counts.

Values	Count	%
200	17,934	93.236%
503	797	4.143%
408	104	0.541%
400	94	0.489%
406	87	0.452%
500	84	0.437%
505	69	0.359%
404	39	0.203%
403	27	0.14%

6. We can select the status by clicking on it, it will show all the status for each entry.

The screenshot shows a Splunk search interface with a histogram titled "status". The y-axis represents the count of events, and the x-axis represents the status code. The "200" bin is selected, highlighted in blue. Other visible status codes include 503, 408, 400, 406, 500, 505, 404, and 403. The histogram has a color gradient from light blue for lower counts to dark blue for higher counts.

Values	Count	%
200	17,934	93.236%
503	797	4.143%
408	104	0.541%
400	94	0.489%
406	87	0.452%
500	84	0.437%
505	69	0.359%
404	39	0.203%
403	27	0.14%

7. We can status for each entry.

i	Time	Event
>	2/26/24 11:59:43.000 PM	212.235.92.150 - - [26/Feb/2024:23:59:43] "POST /success.do?action=purchase&categoryId=ARCADE&productId=MB-AG-G07&JSESSIONID=SD4SL6FF7ADFF4963 HTTP 1.1" 503 2198 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=ARCADE&productId=MB-AG-G07" "Mozilla/5.0 (iPad; CPU OS 5_1.1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 926 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 503
>	2/26/24 11:57:14.000 PM	109.169.32.135 - - [26/Feb/2024:23:57:14] "POST /cart/success.do?JSESSIONID=SD1SL7FF6ADFF89341&productId=FI-AG-G08 HTTP 1.1" 200 3767 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 986 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 200
>	2/26/24 11:57:13.000 PM	109.169.32.135 - - [26/Feb/2024:23:57:13] "POST /success.do?action=purchase&categoryId=SHOOTER&productId=WC-SH-G04&JSESSIONID=SD1SL7FF6ADFF89341 HTTP 1.1" 200 268 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=SHOOTER&productId=WC-SH-G04" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 200
>	2/26/24 11:53:43.000 PM	198.35.3.23 - - [26/Feb/2024:23:53:43] "POST /success.do?action=purchase&categoryId=ARCADE&productId=MB-AG-G07&JSESSIONID=SD8SL8FF6ADFF4957 HTTP 1.1" 201 2915 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=ARCADE&productId=MB-AG-G07" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 200
>	2/26/24 11:51:56.000 PM	198.35.3.23 - - [26/Feb/2024:23:51:56] "POST /cart/success.do?JSESSIONID=SD8SL8FF6ADFF4957&productId=DC-SG-G02 HTTP 1.1" 200 594 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 200

8. For adding a new search, add and select a status and add to new search , the results displayed are:

In the Fields sidebar, under Selected Fields, click the status field. From the field window, click the value with the highest number (listed at the top). Notice the field and value have been added to the search criteria in the search bar. Also, this selection causes a new search to be executed using the new search criteria.

i	Time	Event
>	2/26/24 11:59:43.000 PM	212.235.92.150 - - [26/Feb/2024:23:59:43] "POST /success.do?action=purchase&categoryId=ARCADE&productId=MB-AG-G07&JSESSIONID=SD4SL6FF7ADFF4963 HTTP 1.1" 503 2198 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=ARCADE&productId=MB-AG-G07" "Mozilla/5.0 (iPad; CPU OS 5_1.1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 926 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 503
>	2/26/24 11:48:44.000 PM	27.102.11.11 - - [26/Feb/2024:23:48:44] "GET /product.screen?productId=SF-BVS-G01&JSESSIONID=SD0SL2FF6ADFF89567 HTTP 1.1" 503 1068 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)" 694 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 503
>	2/26/24 11:38:57.000 PM	194.8.74.23 - - [26/Feb/2024:23:38:57] "GET /product.screen?productId=SF-BVS-G01&JSESSIONID=SD0SL5FF4ADFF89311 HTTP 1.1" 503 431 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 718 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 503
>	2/26/24 11:33:14.000 PM	74.208.173.14 - - [26/Feb/2024:23:33:14] "POST /success.do?action=purchase&categoryId=ARCADE&productId=FI-AG-G08&JSESSIONID=SD0SL4FF2ADFF89562 HTTP 1.1" 503 2316 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=ARCADE&productId=FI-AG-G08" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 159 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 503
>	2/26/24 11:16:00.000 PM	110.138.30.229 - - [26/Feb/2024:23:16:00] "POST /success.do?action=purchase&categoryId=STRATEGY&productId=DC-SG-G02&JSESSIONID=SD0SL5FF7ADFF8928 HTTP 1.1" 503 884 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=STRATEGY&productId=DC-SG-G02" "Mozilla/4.0 (compatible; MSIE 4.01; Windows NT 5.1; .NET CLR 1.1.432.0; .NET4.0C)" 83 host = web_application source = access_30DAY.log sourcetype = access_combined_wcookie status = 503

9. Since the value that shows up in the most results is 200, you are not seeing the server errors. Changing the comparison operator will correct this.

10. For searching status !=200;

Format Timeline ▾ Zoom Out +Zoom to Selection ×Deselect 1 day per column

List ▾ Format 20 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields	All Fields	i Time	Event
SELECTED FIELDS		> 2/26/24 11:59:43.000 PM	212.235.92.150 ~ [26/Feb/2024:23:59:43] "POST /success.do?action=purchase&categoryId=ARCADE&productId=MB-AG-G07&JSESSIONID=SD4SL6FF7ADFF4963 HTTP 1.1" 503 2198 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=ARCADE&productId=MB-AG-G07" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/98206 Safari/7534.48.3" 926 host = web_application source = access_30DAYlog sourcetype = access_combined_wcookie status = 503
INTERESTING FIELDS		> 2/26/24 11:59:13.000 PM	212.235.92.150 ~ [26/Feb/2024:23:59:13] "GET /rush/signals.zip?JSESSIONID=SD4SL6FF7ADFF4963 HTTP 1.1" 404 3986 "http://www.buttercupgames.co m" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/98206 Safari/7534.48.3" 725 host = web_application source = access_30DAYlog sourcetype = access_combined_wcookie status = 404
		> 2/26/24 11:59:10.000 PM	192.188.106.240 ~ [26/Feb/2024:23:59:10] "POST /category.screen?categoryId=NULL&JSESSIONID=SD2SL4FF9ADFF4959 HTTP 1.1" 406 906 "http://www.buttercupgames.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 684 host = web_application source = access_30DAYlog sourcetype = access_combined_wcookie status = 406
		> 2/26/24 11:57:18.000 PM	109.169.32.135 ~ [26/Feb/2024:23:57:18] "GET /hidden/anna_nicole.htm?JSESSIONID=SD1SL7FF6ADFF89341 HTTP 1.1" 404 3410 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 647 host = web_application source = access_30DAYlog sourcetype = access_combined_wcookie status = 404
		> 2/26/24 11:56:25.000 PM	142.162.221.28 ~ [26/Feb/2024:23:56:25] "POST /category.screen?categoryId=NULL" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC_Live_8; InfoPath.2)" 517 host = web_application source = access_30DAYlog sourcetype = access_combined_wcookie status = 500
		> 2/26/24 11:51:07.000 PM	92.46.53.223 ~ [26/Feb/2024:23:51:07] "GET /product.screen?productId=SF-BVS-01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 887 host = web_application source = access_30DAYlog sourcetype = access_combined_wcookie status = 400
		> 2/26/24	92.46.53.223 ~ [26/Feb/2024:23:50:00] "GET /cart.do?action=view&JSESSIONID=SD2SL10FF6ADFF4955 HTTP 1.1" 400 1741 "http://www.google.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 684 host = web_application source = access_30DAYlog sourcetype = access_combined_wcookie status = 400

11.After searching for status not equal to 503.

New Search Save As ▾ Create Table View Close All time ▾

32,154 of 57,970 events matched No Event Sampling ▾ Job ▾ II ■ ▾ Smart Mode ▾

Events (32,154) Patterns Statistics Visualization Format Timeline ▾ Zoom Out +Zoom to Selection ×Deselect 1 day per column Feb 20, 2024

List ▾ Format 20 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields	All Fields	i Time	Event
SELECTED FIELDS		> 2/26/24 11:59:45.000 PM	192.188.106.240 ~ [26/Feb/2024:23:59:45] "GET /category.screen?categoryId=TEE&JSESSIONID=SD2SL4FF9ADFF4958 HTTP 1.1" 200 2958 "http://www.buttercupgames.com/category.screen?categoryId=TEE" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 602 host = web_application source = access_30DAYlog sourcetype = access_combined_wcookie status = 200
INTERESTING FIELDS		> 2/26/24 11:59:41.000 PM	212.235.92.150 ~ [26/Feb/2024:23:59:41] "POST /cart.do?action=addtocart&productId=MB-AG-G07&JSESSIONID=SD4SL6FF7ADFF4963 HTTP 1.1" 200 669 "http://www.buttercupgames.com/product.screen?productId=MB-AG-G07" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/98206 Safari/7534.48.3" 197 host = web_application source = access_30DAYlog sourcetype = access_combined_wcookie status = 200
		> 2/26/24 11:59:39.000 PM	212.235.92.150 ~ [26/Feb/2024:23:59:39] "GET /product.screen?productId=MB-AG-G07&JSESSIONID=SD4SL6FF7ADFF4963 HTTP 1.1" 200 2223 "http://www.buttercupgames.com/category.screen?categoryId=ARCADE" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/98206 Safari/7534.48.3" 332 host = web_application source = access_30DAYlog sourcetype = access_combined_wcookie status = 200
		> 2/26/24	192.188.106.240 ~ [26/Feb/2024:23:59:27] "GET /oldlink?&JSESSIONID=SD2SL4FF9ADFF4959 HTTP 1.1" 200 1911 "http://www.buttercupgames.com/oldlink" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 684 host = web_application source = access_30DAYlog sourcetype = access_combined_wcookie status = 200

12. No of searches which ended in errors are:

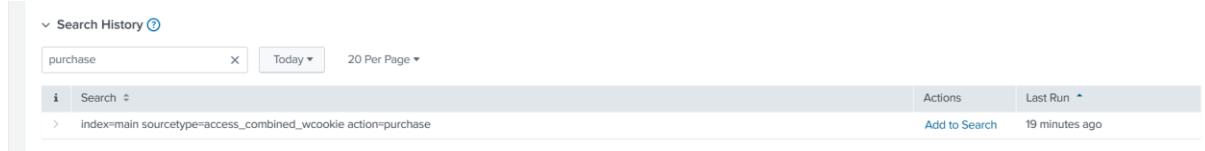
New Search * status!=200 ✓ 15,117 events (before 3/11/24 9:22:26.000 PM) No Event Sampling ▾

Events (15,117) Patterns Statistics Visualization

13. In the Fields sidebar, click status again and select No in the upper right corner next to Selected. This will remove it from the Selected Fields list. Click the x in the upper right corner to close the field window. Click the search link in the Splunk Bar to clear the search results.

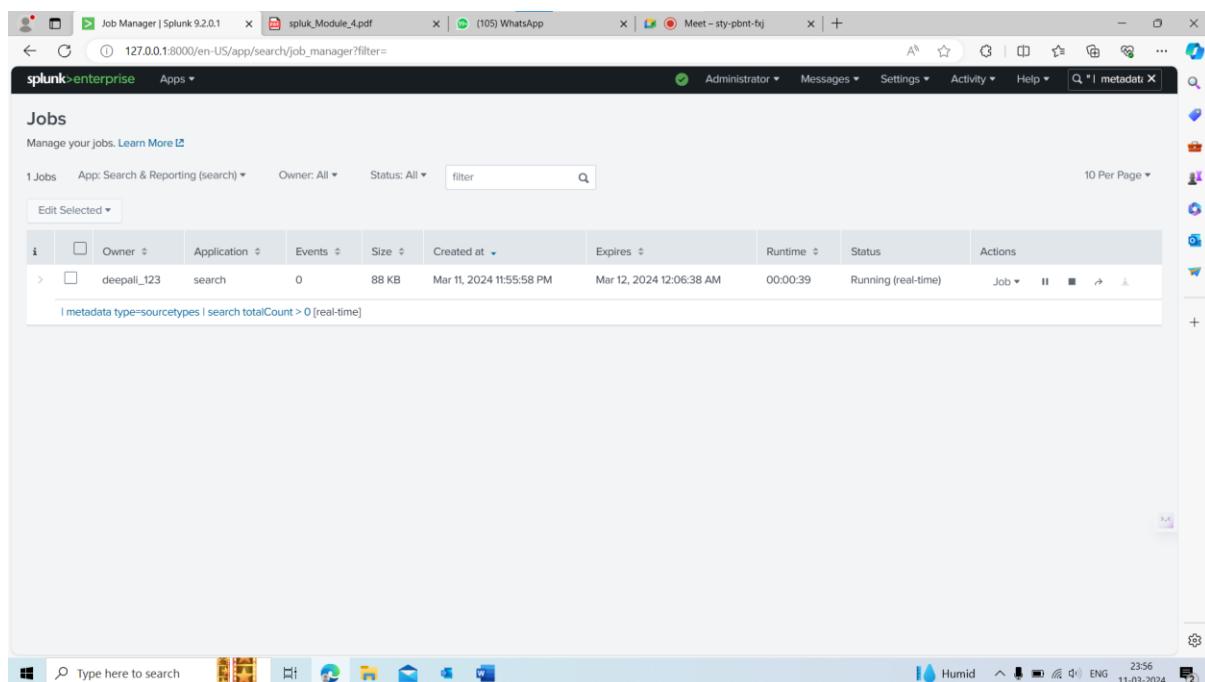
Task 2: Use Search History to browse previously run searches.

14. Search history:



A screenshot of the Splunk search history interface. At the top, there is a search bar with the word "purchase" and a dropdown menu set to "Today". Below the search bar is a table with one row. The row contains the search term "purchase" followed by its details: "index=main sourcetype=access_combined_wcookie action=purchase". To the right of the search term, there are "Actions" and "Last Run" buttons. The "Last Run" button shows "19 minutes ago".

15. Click inside the Search History filter box, and type purchase. Notice the search list is shortened. Only the searches that contain the word purchase remain.



A screenshot of the Splunk Job Manager. The title bar shows "splunk>enterprise Apps". The main area displays a table titled "Jobs". There is one job listed: "deepali_123" with the application "search", size "0", created at "Mar 11, 2024 11:55:58 PM", expires at "Mar 12, 2024 12:06:38 AM", runtime "00:00:39", and status "Running (real-time)". The table has columns for Owner, Application, Events, Size, Created at, Expires, Runtime, Status, and Actions. A search bar at the top of the table is filled with the query "I metadata type=sourcetypes | search totalCount > 0 [real-time]". The bottom of the screen shows the Windows taskbar with various icons and the system tray.

MODULE 5: BASIC COMMANDS

Task 1: Search for the requested data.

1. Navigate to the Search view. (If you are in the Home app, click Search & Reporting from the column on the left side of the screen. You can also access the Search view by clicking the Search menu option on the bar at the top of the screen.)
2. Enter a search that returns all web application events that include a purchase action with a web status of 200.

Command : index=main sourcetype=access_combined_wcookie action=purchase status=200

The screenshot shows the Splunk 9.2.0.1 interface with the search bar containing the query: * status=200. The search results page displays 116,528 events. The timeline at the top shows the data from 3/11/24 to 3/12/24. Below the timeline, the event list view shows several log entries. One entry is highlighted:

```
> 2/26/24 192.188.106.240 - - [26/Feb/2024:23:59:45] "GET /category.screen?categoryId=TEE&JSESSIONID=SD2SL4FF9ADFF4959 HTTP 1.1" 200 2958 "http://www.buttercupgames.com/category.screen?categoryId=TEE" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 602
```

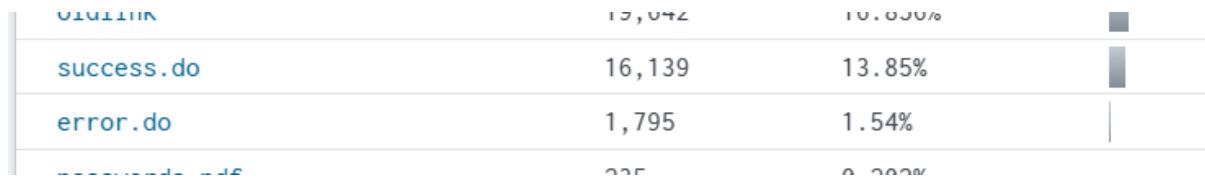
The host is listed as `web_application`, source as `access_30DAY.log`, and sourcetype as `access_combined_wcookie`.

3. Select the file field in the Interesting Fields list.

The screenshot shows the Splunk 9.2.0.1 interface with the search bar containing the query: * status=200. The interesting fields list is displayed, with the 'file' field selected. The 'Top Values' section shows the following data:

Value	Count	%
product.screen	29,417	25.245%
cart.do	29,328	25.168%
category.screen	19,958	17.127%
oldlink	19,642	16.856%
success.do	16,139	13.85%
error.do	1,795	1.54%
passwords.pdf	235	0.202%
userlist	10	0.008%
account	2	0.002%
api	1	0.001%

4. Two files :error.do and success.do, Notice that there are two different files that were returned from the web server. They are: error.do and success.do. Our web development team informs us that the success.do is served when the order is processed and error.do is served when there is an error with the information being processed.



5. The team is only looking for successful purchases, so change your search to only return those.

Command : (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do)

Time	host	source	sourcetype
2/26/24 11:57:14.000 PM	109.169.32.135	-	[26/Feb/2024:23:57:14] "POST /cart/success.do?JSESSIONID=SD1SL7FF6ADFF89341&productId=FI-AG-G08 HTTP 1.1" 200 3767 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 986
2/26/24 11:57:13.000 PM	109.169.32.135	-	[26/Feb/2024:23:57:13] "POST /success.do?action=purchase&categoryId=SHOOTER&productId=WC-SH-G04&JSESSIONID=SD1SL7FF6ADFF89341 HTTP 1.1" 200 268 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=SHOOTER&productId=WC-SH-G04" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448
2/26/24 11:53:43.000 PM	198.35.3.23	-	[26/Feb/2024:23:53:43] "POST /success.do?action=purchase&categoryId=ARCADE&productId=MB-AG-G07&JSESSIONID=SD8SL8FF6ADFF4957 HTTP 1.1" 200 3915 "http://www.buttercupgames.com/cart.do?action=addtocart&categoryId=ARCADE&productId=MB-AG-G07" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448
2/26/24 11:51:56.000 PM	198.35.3.23	-	[26/Feb/2024:23:51:56] "POST /cart/success.do?JSESSIONID=SD8SL8FF6ADFF4957&productId=DC-SG-G02 HTTP 1.1" 200 594 "http://www.buttercupgames.com/cart.do?action=purchase&" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 448

TABLE :

time	host	source	sourcetype
2/25/24 11:45:55.000 PM	database	db_audit_30DAY.csv	db_audit

6. You will see fields that do not matter to the team. Use the fields command to only return the action, JSESSIONID and status fields. Does your search run faster using the command?
Command : (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | fields action, JSESSIONID, status)

Action	JSESSIONID	Status
purchase	SD6SL5FF6ADFF89354	200

7. The fields list looks cleaner, but seeing the events like this might still be confusing for the team.

Task 2: Put the data into an easy to read table.

8. Replace the fields command with the table command to display the data as a table.

Command : (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table action, JSESSIONID, status).

action	JSESSIONID	status
purchase	SD6SL5FF6ADFF89354	200

9. Change the order of the fields so that JSESSIONID is the first column.

Command : (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status)

The screenshot shows the Splunk 9.2.0.1 interface with a search bar containing the command: `index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status`. The search results table has three columns: JSESSIONID, action, and status. The results show 16,139 events, all with status 200 and action purchase. The interface includes a navigation bar with tabs like Search, Analytics, Datasets, Reports, Alerts, Dashboards, and a top menu with Admin, Messages, Settings, Activity, Help, and Find.

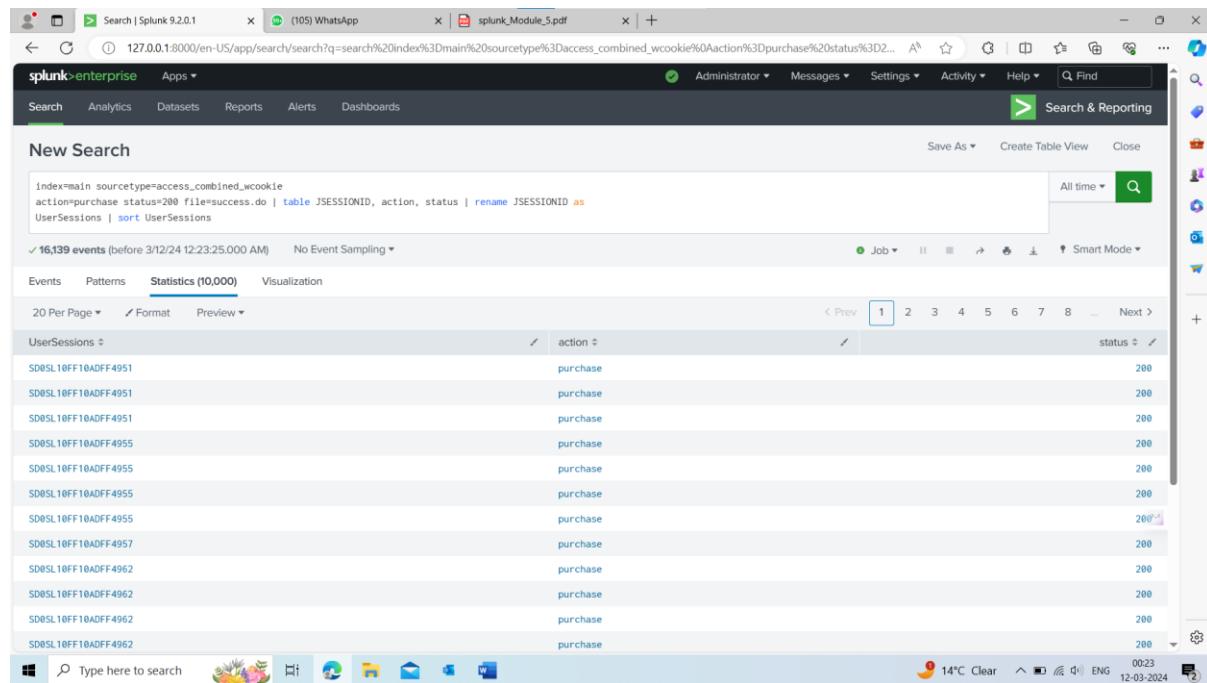
10. Session IDs are called "UserSessions" in the marketing data. Rename JSESSIONID so that your report matches the marketing data.

Command : (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status | rename JSESSIONID as UserSessions)

The screenshot shows the Splunk 9.2.0.1 interface with a search bar containing the command: `index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status | rename JSESSIONID as UserSessions`. The search results table has three columns: UserSessions, action, and status. The results show 16,139 events, all with status 200 and action purchase. The interface includes a navigation bar with tabs like Search, Analytics, Datasets, Reports, Alerts, Dashboards, and a top menu with Admin, Messages, Settings, Activity, Help, and Find.

11. Sort UserSessions using the sort command.

Command: (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status | rename JSESSIONID as UserSessions | sort UserSessions)



The screenshot shows a Splunk search interface with the following search command:

```
index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | table JSESSIONID, action, status | rename JSESSIONID as UserSessions | sort UserSessions
```

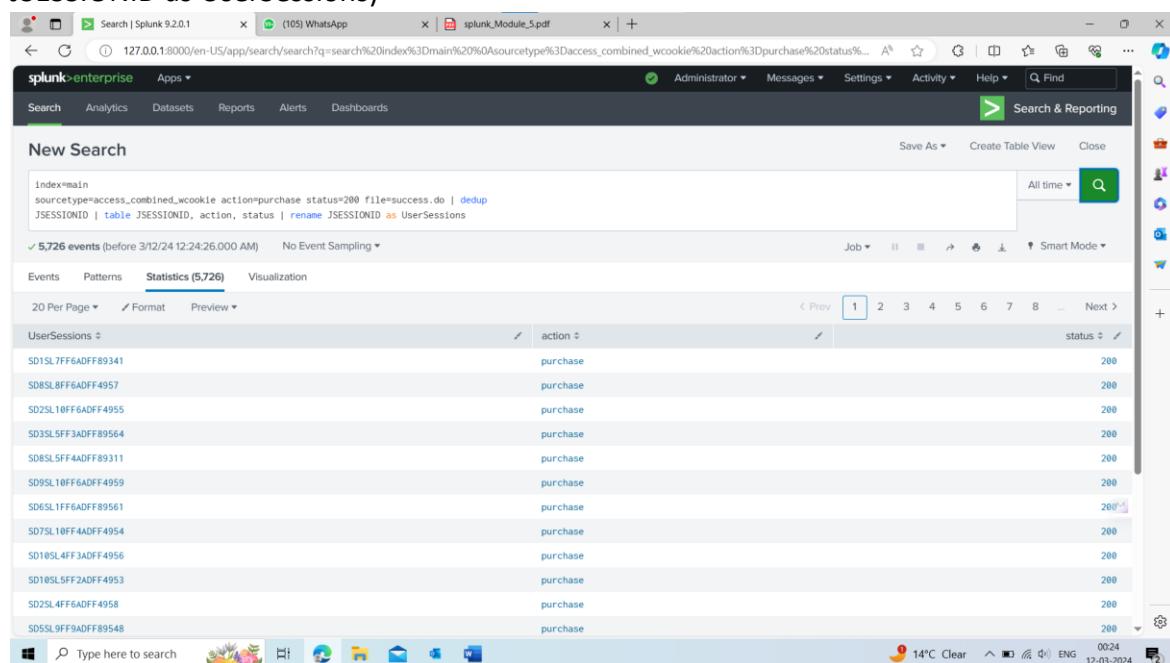
The search results table has columns: UserSessions, action, and status. The status column shows repeated values (200) for different UserSession IDs. The table contains approximately 16,139 events.

UserSessions	action	status
SD0SL10FF10ADFF4951	purchase	200
SD0SL10FF10ADFF4951	purchase	200
SD0SL10FF10ADFF4951	purchase	200
SD0SL10FF10ADFF4955	purchase	200
SD0SL10FF10ADFF4957	purchase	200
SD0SL10FF10ADFF4962	purchase	200

12. Notice that some UserSessions values show up multiple times. Also notice the number of events returned on the Statistics tab.

13. Remove the sort command and use dedup to remove any identical session values.

Command : (index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | dedup JSESSIONID | table JSESSIONID, action, status | rename JSESSIONID as UserSessions)



The screenshot shows a Splunk search interface with the following search command:

```
index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | dedup JSESSIONID | table JSESSIONID, action, status | rename JSESSIONID as UserSessions
```

The search results table has columns: UserSessions, action, and status. The status column shows unique values (200) for each UserSession ID. The table contains approximately 5,726 events.

UserSessions	action	status
SD1SL7FF6ADFF89341	purchase	200
SD0SL8FF6ADFF4957	purchase	200
SD2SL10FF6ADFF4955	purchase	200
SD3SL5FF3ADFF89564	purchase	200
SD0SL5FF4ADFF89311	purchase	200
SD0SL10FF6ADFF4959	purchase	200
SD0SL1FF6ADFF89561	purchase	200
SD0SL10FF4ADFF4954	purchase	200
SD10SL4FF3ADFF4956	purchase	200
SD10SL5FF2ADFF4953	purchase	200
SD2SL4FF6ADFF4958	purchase	200
SD0SL9FF9ADFF89548	purchase	200

14. How many events are now listed on the Statistics tab?

Ans : 5726

15. While having action and status fields displayed was nice for a sanity check of the data, the marketing team will not need to have these displayed. Remove them from your table display.

Command :(index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | dedup JSESSIONID | table JSESSIONID | rename JSESSIONID as UserSessions)

The screenshot shows the Splunk Enterprise search interface. The search bar at the top contains the command: `index=main sourcetype=access_combined_wcookie action=purchase status=200 file=success.do | dedup JSESSIONID | table JSESSIONID | rename JSESSIONID as UserSessions`. Below the search bar, it displays **5,726 events** (before 3/12/24 12:25:03.000 AM) with No Event Sampling. The Statistics tab is selected, showing the count of 5,726. The visualization section shows a list of UserSessions, each represented by a short blue horizontal bar. The sessions listed are: SD1SL7FF6ADFF89341, SD8SL8FF6ADFF4957, SD2SL10FF6ADFF4955, SD3SL5FF3ADFF89564, SD8SL5FF4ADFF89311, SD9SL10FF6ADFF4959, SD6SL1FF6ADFF89561, SD7SL10FF4ADFF4954, SD10SL4FF3ADFF4956, SD10SL5FF2ADFF4953, SD2SL4FF6ADFF4958, and SD5SL9FF9ADFF89548.

MODULE 6 : TRANSFORMING COMMANDS

Task 1: Use the top command to get a list of the best-selling products.

1. Navigate to the Search view. (If you are in the Home app, click Search & Reporting from the column on the left side of the screen. You can also access the Search view by clicking the Search menu option on the bar at the top of the screen.)

The screenshot shows the Splunk search interface with the following search command in the search bar:

```
index=main sourcetype=access_combined_wcookie status=200 file=success.do | top productId
```

The results table has columns for productId, count, and percent. The data is as follows:

productId	count	percent
WC-SH-G04	1360	8.426792
DB-SG-G01	1319	8.172749
DC-SG-G02	1388	8.104591
MB-AG-T01	1285	7.466386
MB-AG-G07	1284	7.460198
WC-SH-A02	1192	7.385836
FS-SG-G03	1155	7.156577
WC-SH-A01	1100	6.815788
WC-SH-T02	1076	6.667080
PZ-SG-G05	1012	6.270525

2. Enter a search that returns all web application events where an item was successfully purchased. Remember that if the success.do file is successfully returned to a user, a purchase was made.

Command : index=main sourcetype=access_combined_wcookie status=200 file=success.do

The screenshot shows the Windows taskbar with the following search results displayed in a window:

```
index=main sourcetype=access_combined_wcookie status=200 file=success.do
```

The results table has columns for _time, host, source, and sourcetype. The data is as follows:

_time	host	source	sourcetype
2/26/24 11:57:14.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:57:13.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:53:43.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:51:56.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:51:56.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:50:48.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:50:48.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:40:15.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:40:12.000 PM	web_application	access_30DAY.log	access_combined_wcookie

3. Use the top command to find the best-selling productIds for all time

Command : (index=main sourcetype=access_combined_wcookie status=200 file=success.do | top productId

The screenshot shows a Splunk search interface with the following search command in the search bar:

```
index=main sourcetype=access_combined_wcookie status=200 file=success.do | top productId
```

The results table displays 10 rows of data:

productId	count	percent
WC-SH-G84	1360	8.426792
DB-SG-G81	1319	8.172749
DC-SG-G82	1388	8.104591
MB-AG-T81	1285	7.466386
MB-AG-G87	1284	7.460190
WC-SH-A82	1192	7.385836
FS-SG-G83	1155	7.156577
WC-SH-A81	1100	6.815788
WC-SH-T82	1076	6.667080
PZ-SG-G85	1012	6.270525

4. Notice that ten rows were returned. You were asked to only return the top 5.

5. Use the limit argument to only return the number of rows requested.

Command: index=main sourcetype=access_combined_wcookie status=200 file=success.do | top productId limit=5

The screenshot shows a Splunk search interface with the following search command in the search bar:

```
index=main sourcetype=access_combined_wcookie status=200 file=success.do | top productId limit=5
```

The results table displays 5 rows of data:

productId	count	percent
WC-SH-G84	1360	8.426792
DB-SG-G81	1319	8.172749
DC-SG-G82	1388	8.104591
MB-AG-T81	1285	7.466386
MB-AG-G87	1284	7.460190

6. Use the showperc option of top to remove percent from the display.

Command : index=main sourcetype=access_combined_wcookie status=200 file=success.do | top productId limit=5 showperc=false

The screenshot shows the Splunk 9.2.0.1 interface with a search bar containing the command: `index=main sourcetype=access_combined_wcookie status=200 file=success.do | top productId limit=5 showperc=false`. The search results table displays 16,139 events. The table has columns for productId and count. The data shows:

productId	count
WC-SH-G04	1360
DB-SG-G01	1319
DC-SG-G02	1308
MB-AG-T01	1205
MB-AG-G07	1204

7. what is the productId of the best-selling product? Please take note as it might be in the quiz. (WC-SHG04)

The screenshot shows a search results table for productId. The table has a single row with the following data:

productId
WC-SH-G04

Task 2: Use the rare command to see what files get accessed the least amount in our web application

8. Enter a search that returns all web application events where a file was successfully served to the user.

Command : (index=main sourcetype=access_combined_wcookie status=200)

The screenshot shows the Splunk 9.2.0.1 interface with a search bar containing the command: `(index=main sourcetype=access_combined_wcookie status=200)`. The search results are visualized as a timeline. The timeline shows multiple green bars representing successful web application events over time. The interface includes a sidebar with selected fields like host, source, and sourcetype, and interesting fields like index, linecount, splunk_server, and status.

9. Use the rare command to find the files that show up the least amount of times in our events.

Commands : (index=main sourcetype=access_combined_wcookie status=200 | rare file)

The screenshot shows the Splunk 9.2.0 interface with a search bar containing the query: "Index=main sourcetype=access_combined_wcookie status=200 | rare file". The search results table displays 116,528 events from before 3/18/24 5:28:53.000 PM. The table has columns for file, count, and percent. The top few rows are:

file	count	percent
api	1	0.000858
account	2	0.001716
userlist	10	0.008582
passwords.pdf	235	0.201678
error.do	1795	1.540416
success.do	16139	13.850009
oldlink	19642	16.856179
category.screen	19958	17.127361
cart.do	29328	25.168416
product.screen	29417	25.244793

10. Do you see anything that might be of a concern for the security team? Make the report even more granular using the by clause to split the rare events by the month in which they happened (date_month).

Command - index=main sourcetype=access_combined_wcookie status=200 | rare file by date_month

The screenshot shows the Splunk 9.2.0 interface with a search bar containing the query: "Index=main sourcetype=access_combined_wcookie status=200 | rare file by date_month". The search results table displays 116,528 events from before 3/18/24 5:34:13.000 PM. The table has columns for date_month, file, count, and percent. The top few rows are:

date_month	file	count	percent
february	api	1	0.000985
february	account	2	0.001970
february	userlist	10	0.009851
february	passwords.pdf	200	0.197023
february	error.do	1602	1.578154
february	success.do	14046	13.836924
february	oldlink	17015	16.761730
february	category.screen	17411	17.151836
february	product.screen	25595	25.214016
february	cart.do	25629	25.247510
january	passwords.pdf	35	0.233085
january	error.do	193	1.285296
january	success.do	2093	13.938466

Task 3: Use the count function of the stats command to find out how many items were added to a cart versus being purchased

11. Enter a search that returns all web application events where an item was successfully added to a cart, or purchased. Remember, when an item is added to the cart the cart.do file is served; the success.do is served when the item is purchased.

Command - index=main sourcetype=access_combined_wcookie file=success.do OR file=cart.do status=200

The screenshot shows a Splunk search interface with the following details:

- Selected Fields:** host, source, sourcetype.
- Interesting Fields:** file, index, linecount, splunk_server, status.
- Extract New Fields:** None.
- Search Results:** A table with columns: _time, host, source, sourcetype. The table contains approximately 10 rows of data, each representing a log entry. Most entries have sourcetype as "access_combined_wcookie". One entry specifically for "cart.do" has sourcetype as "access_30DAY.log".

12. Use the stats count function with a by clause to count events by the file that was served.

Command : index=main sourcetype=access_combined_wcookie file=success.do OR file=cart.do status=200 | stats count by file

The screenshot shows a Splunk search interface with the following details:

- New Search:** The search bar contains the command: index=main sourcetype=access_combined_wcookie file=success.do OR file=cart.do status=200 | stats count by file.
- Statistics (2) Tab:** The Statistics tab is selected, showing the results of the search.
- Results:** A table titled "New Search" with two rows:
 - file: cart.do, count: 29328
 - file: success.do, count: 16139

13. Notice that the count column is labeled count by default. Use an as clause to rename the column to Transactions.

Command : index=main sourcetype=access_combined_wcookie file=success.do OR file=cart.do status=200 | stats count as Transactions by file

file	Transactions
cart.do	29328
success.do	16139

14. Using the rename command, change the name of the file field to Function.

Command : (index=main sourcetype=access_combined_wcookie file=success.do OR file=cart.do status=200 | stats count as Transactions by file | rename file as Function)

Function	Transactions
cart.do	29328
success.do	16139

Task 4: Use the distinct count stats function to count how many times sessions were created for users on the system.

15. Use search terms with the stats dc function to count all sessions (JSESSIONID) that have been used in our web application data.

Command : index=main sourcetype=access_combined_wcookie | stats dc(JSESSIONID)

dc(JSESSIONID)	11455
All time	Search

16. Use the as clause to rename the sessions as Logins.

Command : index=main sourcetype=access_combined_wcookie | stats dc(JSESSIONID) | rename file as Logins

dc(JSESSIONID)	11455
All time	Search

17. Using the by clause, split the Logins by clientip.

Command : index=main sourcetype=access_combined_wcookie | stats dc(JSESSIONID) as Logins by clientip

The screenshot shows the Splunk 9.2.0.1 interface with a search bar containing the command: `index=main sourcetype=access_combined_wcookie | stats dc(JSESSIONID) as Logins by clientip`. The results table has two columns: `clientip` and `Logins`. The data is sorted by `Logins` in descending order. The top entry is 107.3.146.207 with 186 logins. Other entries include 108.65.113.83 (83), 109.169.32.135 (172), 110.138.30.229 (82), 110.159.208.78 (95), 111.161.27.20 (91), 112.111.162.4 (93), 117.21.246.164 (98), 118.142.68.222 (75), 12.130.60.4 (92), 12.130.60.5 (99), 121.254.179.199 (81), and 121.9.245.177 (91). The interface includes a navigation bar with tabs for Events, Patterns, Statistics (185), and Visualization, and a bottom status bar showing weather and system information.

clientip	Logins
107.3.146.207	186
108.65.113.83	83
109.169.32.135	172
110.138.30.229	82
110.159.208.78	95
111.161.27.20	91
112.111.162.4	93
117.21.246.164	98
118.142.68.222	75
12.130.60.4	92
12.130.60.5	99
121.254.179.199	81
121.9.245.177	91

18. Use the sort command to sort Logins so that the clientip with the most Logins is displayed at the top of the list. Make a note of the top clientip you might be asked about it in the quiz.

Command : index=main sourcetype=access_combined_wcookie | stats dc(JSESSIONID) as Logins by clientip | sort -Logins (87.194.216.51)

The screenshot shows the Splunk 9.2.0.1 interface with a search bar containing the command: `index=main sourcetype=access_combined_wcookie | stats dc(JSESSIONID) as Logins by clientip | sort -Logins`. The results table has two columns: `clientip` and `Logins`. The data is sorted by `Logins` in descending order. The top entry is 87.194.216.51 with 186 logins. Other entries include 107.3.146.207 (83), 109.169.32.135 (172), 110.138.30.229 (82), 110.159.208.78 (95), 111.161.27.20 (91), 112.111.162.4 (93), 117.21.246.164 (98), 118.142.68.222 (75), 12.130.60.4 (92), 12.130.60.5 (99), 121.254.179.199 (81), 121.9.245.177 (91), 123.118.73.155 (73), 123.196.113.11 (87), and 123.30.108.208 (95). The interface includes a navigation bar with tabs for Events, Patterns, Statistics (185), and Visualization, and a bottom status bar showing weather and system information.

clientip	Logins
87.194.216.51	186
107.3.146.207	83
109.169.32.135	172
110.138.30.229	82
110.159.208.78	95
111.161.27.20	91
112.111.162.4	93
117.21.246.164	98
118.142.68.222	75
12.130.60.4	92
12.130.60.5	99
121.254.179.199	81
121.9.245.177	91
123.118.73.155	73
123.196.113.11	87
123.30.108.208	95

Task 5: Use the stats sum function to find the total bytes used for the web application

19. Craft search terms that return all events where a file was successfully served to a user.

Command : index=main sourcetype=access_combined_wcookie status=200

_time	host	source	sourcetype
2/26/24 11:59:45.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:59:41.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:59:39.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:59:27.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:59:27.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:57:17.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:57:19.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:57:17.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:57:15.000 PM	web_application	access_30DAY.log	access_combined_wcookie

20. Create a field named TotalBytes by using the sum function of the stats command.

Command : index=main sourcetype=access_combined_wcookie status=200 | stats sum(bytes) as TotalBytes

21. Split the results by the file field using the by clause.

Command : index=main sourcetype=access_combined_wcookie status=200 | stats sum(bytes) as TotalBytes by file

The screenshot shows the Splunk 9.2.0 interface with a search bar containing the command: `index=main sourcetype=access_combined_wcookie status=200 | stats sum(bytes) as TotalBytes by file`. The results table has 'Statistics (10)' selected. The table lists file names and their corresponding TotalBytes values:

file	TotalBytes
account	4238
api	1456
cart.do	61311724
category.screen	42250138
error.do	3747647
oldlink	41349801
passwords.pdf	11103985
product.screen	61672339
success.do	33862989
userlist	27690

22. Use the sort command to sort the file names into alphabetical order.

Command : index=main sourcetype=access_combined_wcookie status=200 | stats sum(bytes) as TotalBytes by file | sort file

The screenshot shows the Splunk 9.2.0 interface with a search bar containing the command: `index=main sourcetype=access_combined_wcookie status=200 | stats sum(bytes) as TotalBytes by file | sort file`. The results table has 'Statistics (10)' selected. The table lists file names and their corresponding TotalBytes values, sorted alphabetically:

file	TotalBytes
account	4238
api	1456
cart.do	61311724
category.screen	42250138
error.do	3747647
oldlink	41349801
passwords.pdf	11103985
product.screen	61672339
success.do	33862989
userlist	27690

23. What is the name of the file that used the least amount of bandwidth? You might be asked about it in the quiz.

Command :

```
account  
api
```

Task 6: Use the stats command's average function to find the average time for each database query being run

24. Search all database events and use the average (avg) function of the stats command to get an average Duration of all queries.

Command : index=main sourcetype=db_audit | stats avg(Duration)

The screenshot shows the Splunk 9.2.0 interface. The search bar contains the query: `index=main sourcetype=db_audit | stats avg(Duration)`. The results section displays the following information:

- 44,096 events (before 3/18/24 6:04:38.000 PM)
- No Event Sampling
- Statistics tab selected
- 20 Per Page
- Format: Preview
- avg(Duration) ≈ 239.4764303178484

25. Use as and by clauses to rename the average field to time to complete and split by the Command.

Command : index=main sourcetype=db_audit | stats avg(Duration) as "time to complete" by Command.

The screenshot shows a Splunk search interface with the following command:

```
index=main sourcetype=db_audit | stats avg(Duration) as "time to complete" by Command
```

The results table has columns: Command, time to complete. The data includes:

Command	time to complete
ALTER TABLE users ADD COLUMN attention NOT NULL DEFAULT HACKED: send 100 bitcoin to 12TFVXGDWF3GMSDjftnfKlipyEhgsW90ymN or be exposed!	3000
CREATE USER allurbase@localhost IDENTIFIED WITH mysql_native_password AS <secret>	87
Database server started	24
GRANT CREATE ROUTINE, CREATE VIEW, CREATE USER, ALTER, SHOW VIEW, CREATE, ALTER ROUTINE, EVENT, SUPER, INSERT, RELOAD, SELECT, DELETE, FILE, SHOW DATABASES, TRIGGER, SHUTDOWN, REPLICATION CLIENT, GRANT OPTION, PROCESS, REFERENCES, UPDATE, DROP, REPLICATION SLAVE, EXECUTE, LOCK TABLES, CREATE TEMPORARY TABLES, INDEX ON *.* TO allurbase@localhost	32
INSERT INTO users (username, password, fname, lname, email) VALUES (aaron09, 80b3e8c48a355793fe4faa91dcf4ebd40161e116, Matthew, Anderson, zwhite@mitchell.com)	30
INSERT INTO users (username, password, fname, lname, email) VALUES (aaron04, 72a091f8d6df41047ef530725b75161775971e, Sean, Robinson, johnsonsus@gmail.com)	21
INSERT INTO users (username, password, fname, lname, email) VALUES (aaron19, 0e2261e4fa5b1ff898e044978a26d16331f0ccb, Robert, Rivera, chrisklein@murphy-payne.com)	20
INSERT INTO users (username, password, fname, lname, email) VALUES (aaron30, 7ca9ace06710d774a973a7a440755bd5b83bd9, Timothy, Kennedy, eatontiffany@fuentes.com)	16
INSERT INTO users (username, password, fname, lname, email) VALUES (aaron48, 11dd577eb10fa2c8743e032b95cd2ee506e68eb, Kevin, Austin, ekennedy@salinas.com)	24
INSERT INTO users (username, password, fname, lname, email) VALUES (aaron59, ac8c5de0928857bbf0d503ba3828797206f0f, Jeremy, Bird, fullermeivin@hotmail.com)	30
INSERT INTO users (username, password, fname, lname, email) VALUES (aaron97, e73886ef59fa95fd4ce013e521db7334e0dea4, Derrick, Riggs, leah33@mckenzie.com)	3
INSERT INTO users (username, password, fname, lname, email) VALUES (aaron98, 57d3bc5f46e0999e28628f031121e78b5d6b0b135, Mark, Blevins, williamsbrandon@gmail.com)	10
INSERT INTO users (username, password, fname, lname, email) VALUES (aaronbell, 7b75ce05b3623b1c491d4ba69a6eadcf0b58b, Andre, Brown, robinsonhannah@hotmail.com)	19
INSERT INTO users (username, password, fname, lname, email) VALUES (aaronfreeman, 1e80a4ce5b033737c8ed9ceb22276e4f620a197t, Kenneth, Meadows, cbender@gmail.com)	22

26. Sort the time to complete so that Command values that take the longest are shown first.

Command : index=main sourcetype=db_audit | stats avg(Duration) as "time to complete" by Command | sort - "time to complete"

The screenshot shows a Splunk search interface with the following command:

```
index=main sourcetype=db_audit | stats avg(Duration) as "time to complete" by Command | sort - "time to complete"
```

The results table has columns: Command, time to complete. The data includes:

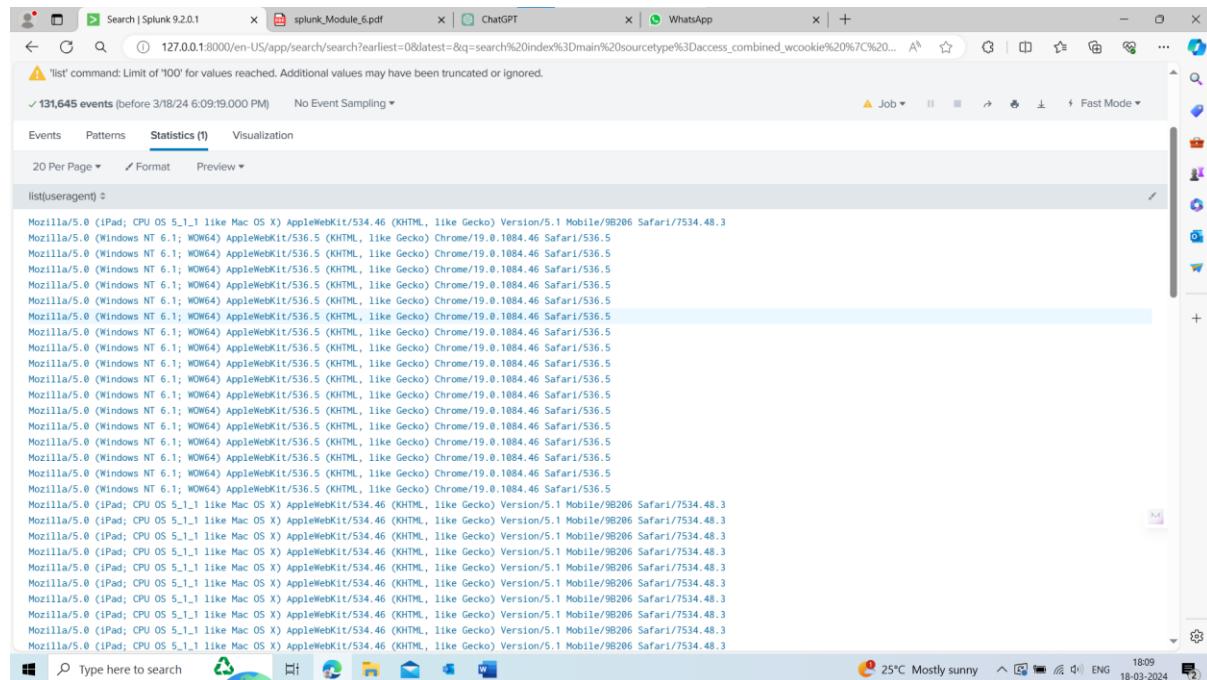
Command	time to complete
ALTER TABLE users ADD COLUMN attention NOT NULL DEFAULT HACKED: send 100 bitcoin to 12TFVXGDWF3GMSDjftnfKlipyEhgsW90ymN or be exposed!	3000
CREATE USER allurbase@localhost IDENTIFIED WITH mysql_native_password AS <secret>	87
Database server started	24
GRANT CREATE ROUTINE, CREATE VIEW, CREATE USER, ALTER, SHOW VIEW, CREATE, ALTER ROUTINE, EVENT, SUPER, INSERT, RELOAD, SELECT, DELETE, FILE, SHOW DATABASES, TRIGGER, SHUTDOWN, REPLICATION CLIENT, GRANT OPTION, PROCESS, REFERENCES, UPDATE, DROP, REPLICATION SLAVE, EXECUTE, LOCK TABLES, CREATE TEMPORARY TABLES, INDEX ON *.* TO allurbase@localhost	32
INSERT INTO users (username, password, fname, lname, email) VALUES (aaron09, 80b3e8c48a355793fe4faa91dcf4ebd40161e116, Matthew, Anderson, zwhite@mitchell.com)	30
INSERT INTO users (username, password, fname, lname, email) VALUES (aaron04, 72a091f8d6df41047ef530725b75161775971e, Sean, Robinson, johnsonsus@gmail.com)	21
INSERT INTO users (username, password, fname, lname, email) VALUES (aaron19, 0e2261e4fa5b1ff898e044978a26d16331f0ccb, Robert, Rivera, chrisklein@murphy-payne.com)	20
INSERT INTO users (username, password, fname, lname, email) VALUES (aaron30, 7ca9ace06710d774a973a7a440755bd5b83bd9, Timothy, Kennedy, eatontiffany@fuentes.com)	16
INSERT INTO users (username, password, fname, lname, email) VALUES (aaron48, 11dd577eb10fa2c8743e032b95cd2ee506e68eb, Kevin, Austin, ekennedy@salinas.com)	24
INSERT INTO users (username, password, fname, lname, email) VALUES (aaron59, ac8c5de0928857bbf0d503ba3828797206f0f, Jeremy, Bird, fullermeivin@hotmail.com)	30
INSERT INTO users (username, password, fname, lname, email) VALUES (aaron97, e73886ef59fa95fd4ce013e521db7334e0dea4, Derrick, Riggs, leah33@mckenzie.com)	3
INSERT INTO users (username, password, fname, lname, email) VALUES (aaron98, 57d3bc5f46e0999e28628f031121e78b5d6b0b135, Mark, Blevins, williamsbrandon@gmail.com)	10
INSERT INTO users (username, password, fname, lname, email) VALUES (aaronbell, 7b75ce05b3623b1c491d4ba69a6eadcf0b58b, Andre, Brown, robinsonhannah@hotmail.com)	19
INSERT INTO users (username, password, fname, lname, email) VALUES (aaronfreeman, 1e80a4ce5b033737c8ed9ceb22276e4f620a197t, Kenneth, Meadows, cbender@gmail.com)	22
INSERT INTO users (username, password, fname, lname, email) VALUES (aaron90, 0a9246e45cdf5d096cf25ec7950e3638869c7c2, Cody, Hart, charles14@moore.com)	16
INSERT INTO users (username, password, fname, lname, email) VALUES (aaronwilson, 9b2ce37fe55a1bdf7358d80f32370a5cccef520, James, Hutchinson, phillipsrichard@hotmail.com)	26
INSERT INTO users (username, password, fname, lname, email) VALUES (aaklins, 08c22739d3863d0447ac5f31cf9a3a1fff69623f, Joshua, Brown, collinsrobert@yahoo.com)	18
INSERT INTO users (username, password, fname, lname, email) VALUES (abaker, bd1da96e9612e70ff871295a8e5465395672ff2, Zachary, Norton, jessica610myers.com)	16

Notice anything about the Command values that are taking the longest to complete?

Task 7: Use the lists and values functions of the stats command to run a report of the browsers users are using to access the web application from.

28. Use the stats.list function to generate a list of all useragent values that have accessed the web application.

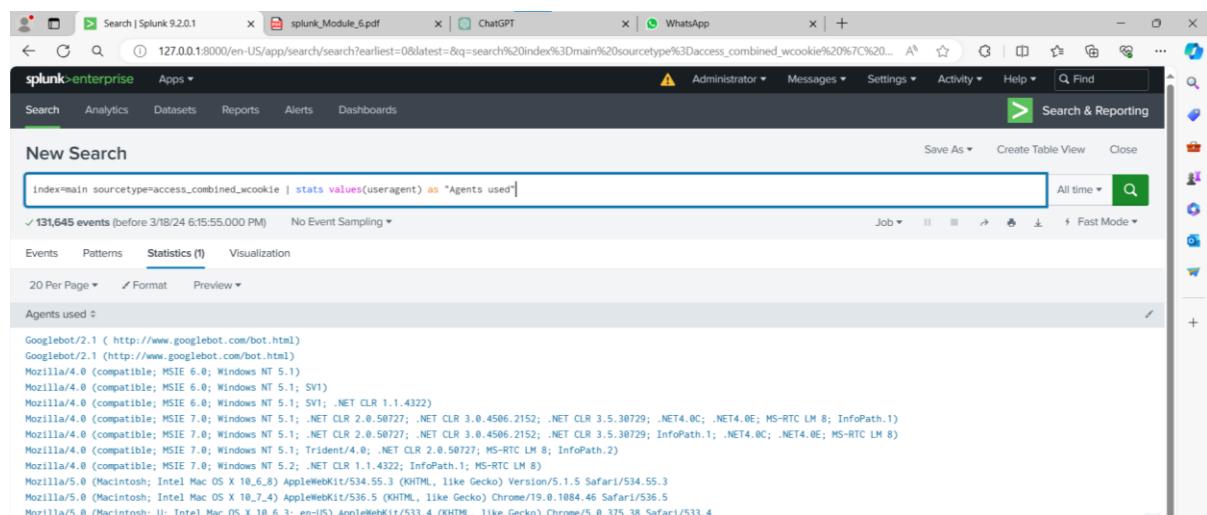
Command : index=main sourcetype=access_combined_wcookie | stats list(useragent)



29. Notice that most of the useragent values show up multiple times in the results.

30. Use the stats values function to only return one instance of each useragent. Add an as clause to name the result as Agents used.

Command : index=main sourcetype=access_combined_wcookie | stats values(useragent) as "Agents used"



31. This report would be much more useful if we knew the number of times each useragent was used. Add a count function to the stats command that counts the events by useragent as Times used.

Command : index=main sourcetype=access_combined_wcookie | stats values(useragent) as "Agents used" count as "Times used" by useragent

The screenshot shows a Splunk search interface with the following search command:

```
index=main sourcetype=access_combined_wcookie | stats values(useragent) as "Agents used" count as "Times used" by useragent
```

The results table has two columns: "Agents used" and "Times used". The data includes:

Agents used	Times used
Googlebot/2.1 (http://www.googlebot.com/bot.html)	1277
Googlebot/2.1 (http://www.googlebot.com/bot.html)	1327
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)	2155
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	2170
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)	1825
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C; .NET4.0E; MS-RTC LM 8; InfoPath.1)	1563
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; InfoPath.1; .NET4.0C; .NET4.0E; MS-RTC LM 8)	1667
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)	10827
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)	10225
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.55.3 (KHTML, like Gecko) Version/5.1.5 Safari/534.55.3	5249
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5	10501
Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.38 Safari/533.4	1735

32. Put the results of Agents used and Times used into a table.

Command : index=main sourcetype=access_combined_wcookie | stats values(useragent) as "Agents used" count as "Times used" by useragent | table "Agents used", "Times used"

The screenshot shows a Splunk search interface with the same search command as the previous one:

```
index=main sourcetype=access_combined_wcookie | stats values(useragent) as "Agents used" count as "Times used" by useragent
```

The results table is identical to the one in the previous screenshot, showing the same list of useragents and their corresponding "Agents used" and "Times used" counts.

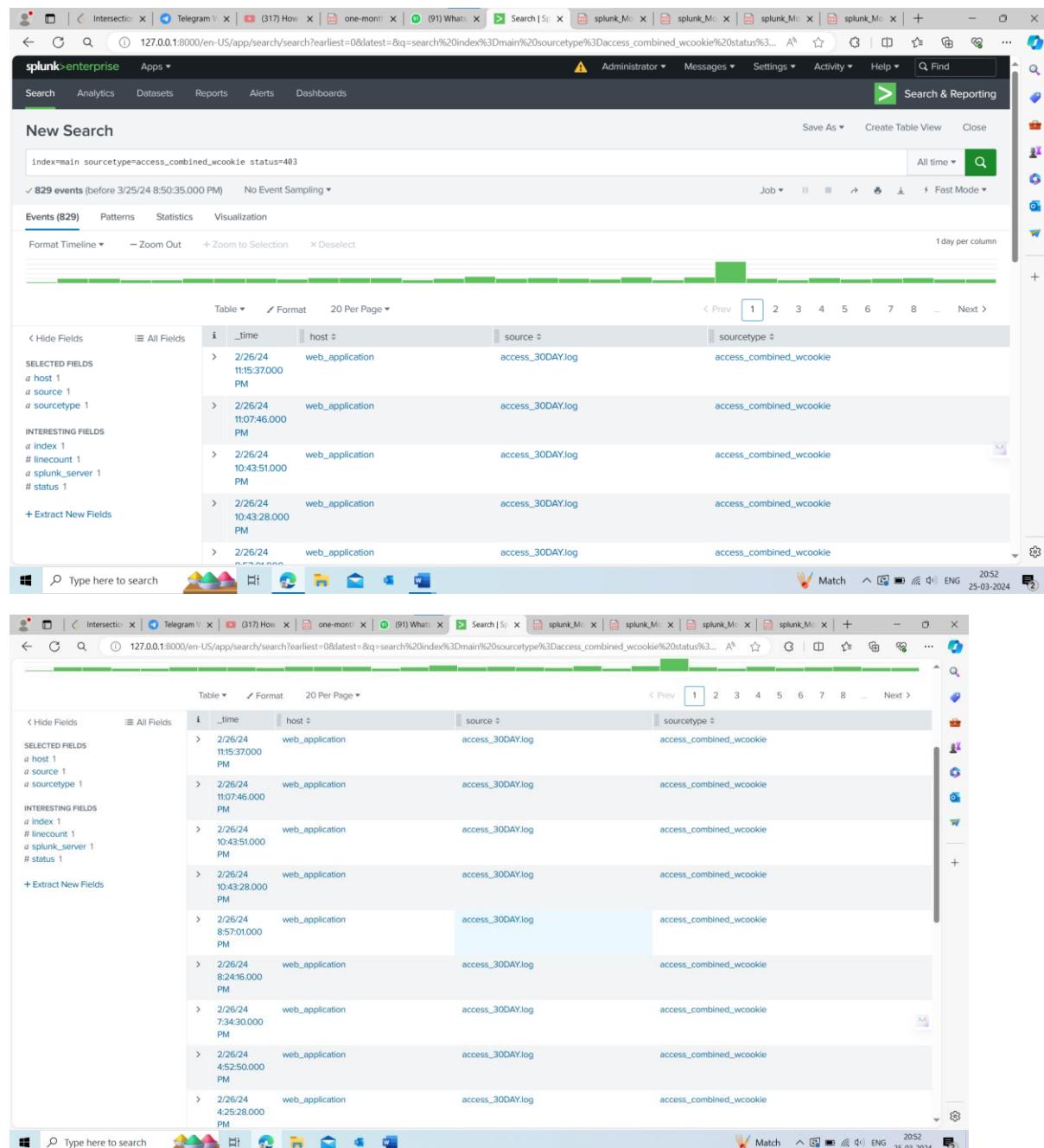
MODULE 7: – Creating Reports and Dashboards

Task 1: Use the stats count function to get a report of users trying to access forbidden pages in the Buttercup Games web application.

1. Navigate to the Search view. (If you are in the Home app, click Search & Reporting from the column on the left side of the screen. You can also access the Search view by clicking the Search menu option on the bar at the top of the screen.)

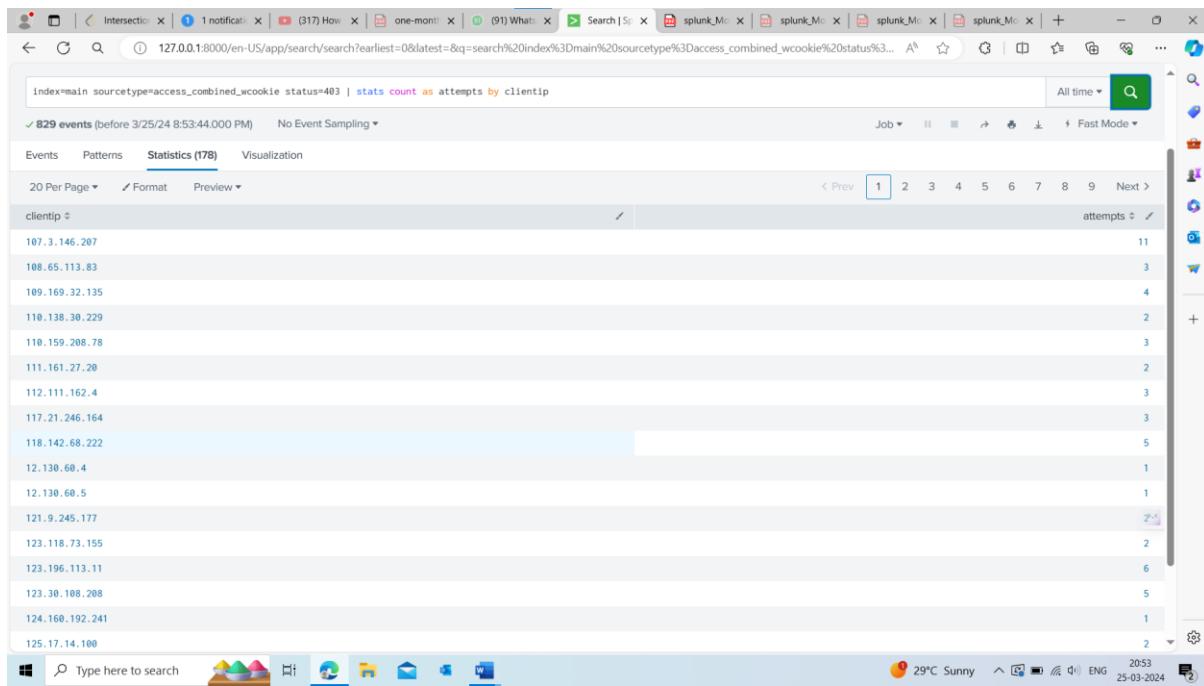
2. Enter a search that returns all web application events with a forbidden status (403).

Command: (index=main sourcetype=access_combined_wcookie status=403)



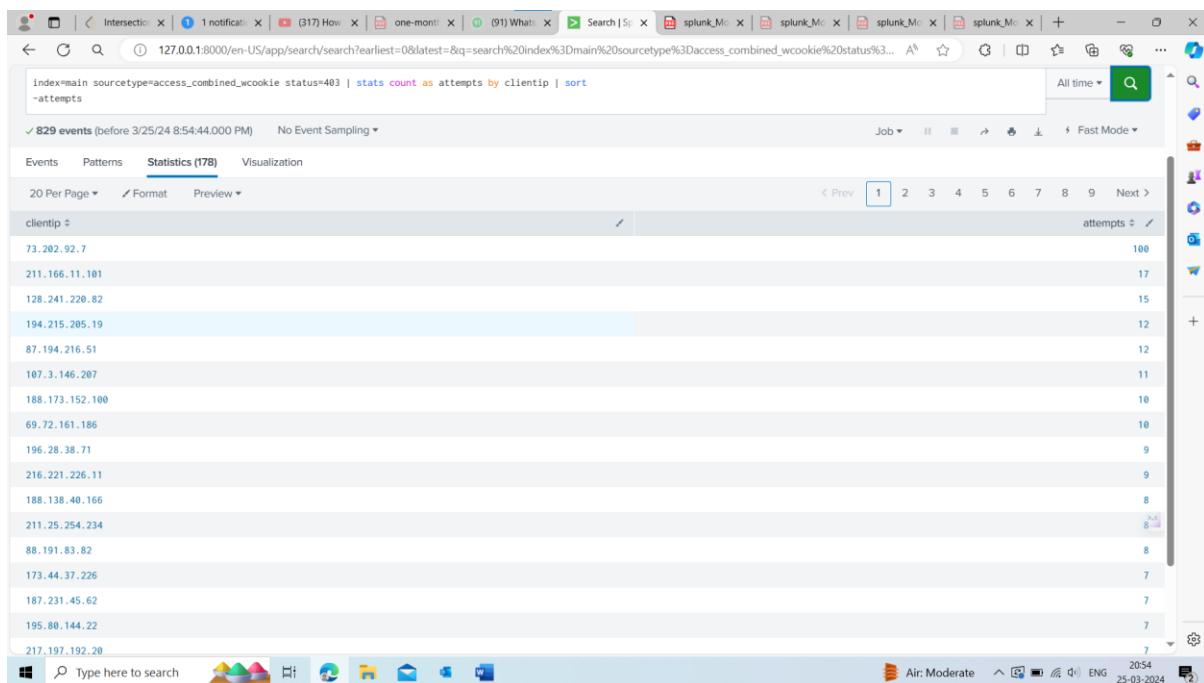
3. Use the stats count function to count the events by clientip and rename the count to attempts.

Command : (index=main sourcetype=access_combined_wcookie status=403 | stats count as attempts by clientip)



4. Use the sort command to display the results so that the clientip with the highest attempts appears first.

Command : index=main sourcetype=access_combined_wcookie status=403 | stats count as attempts by clientip | sort -attempts

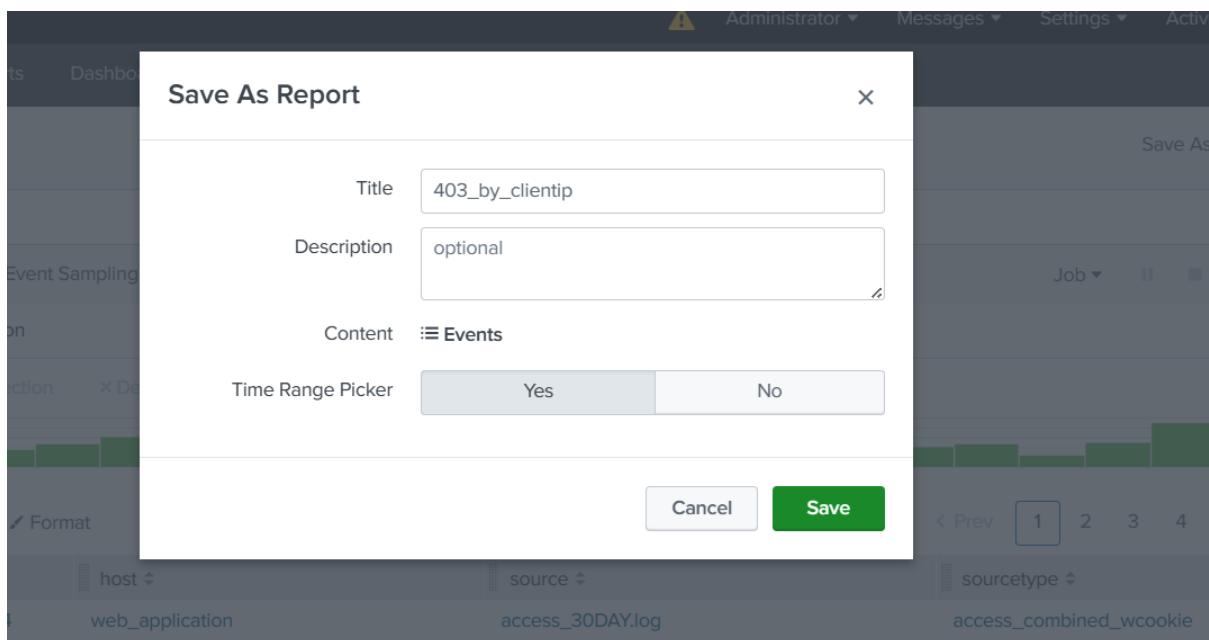


5. For the clientip with the most attempts, what was the total number of attempts? This might show up during the quiz module.

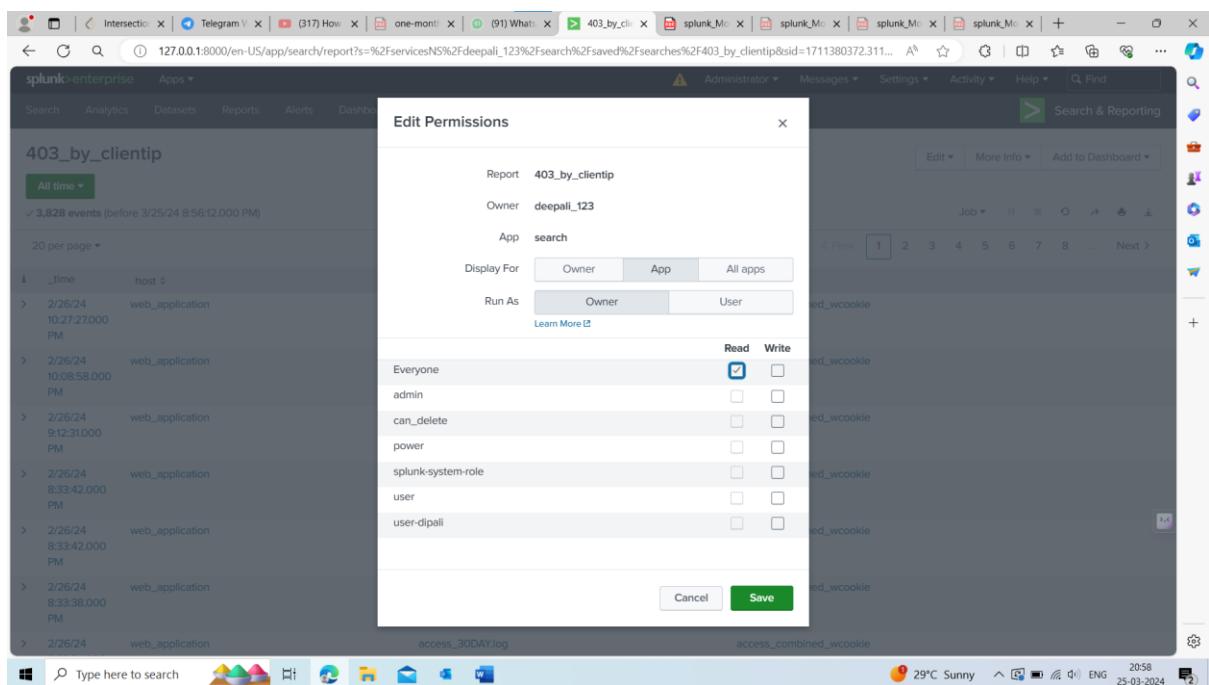
Ans: 100

6. Use the Save As menu (above the time range picker) to select Report.

7. Enter a Title of 403_by_clientip for the report and click Save.



8. Use the Permissions link to make the report display for the App, run as Owner, and be readable by Everyone. Click Save.



9. Access a list of the reports available to you using the Reports menu option on the bar at the top of the screen.

10.

The screenshot shows the Splunk Enterprise web interface. The top navigation bar includes links for 'Intersection', '1 notification', '(317) How', 'one-month', '(91) What', 'Reports', 'splunk_Mo', 'splunk_Mo', 'splunk_Mo', 'splunk_Mo'. The main menu bar has options like 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below the menu is a sidebar with icons for 'Search & Reporting', 'Alerts', 'Dashboards', and other system status indicators. The main content area is titled 'Reports' and displays a table of 8 reports. The table columns are 'Title', 'Actions', 'Next Scheduled Time', 'Owner', 'App', and 'Sharing'. The reports listed are: '403_by_clientip', 'Bucket Merge Retrieve Conf Settings', 'Errors in the last 24 hours', 'Errors in the last hour', 'License Usage Data Cube', 'Messages by minute last 3 hours', 'Orphaned scheduled searches', and 'Splunk errors last 24 hours'. Each report entry includes a 'View' link and an 'Edit' dropdown. The bottom of the screen shows a taskbar with various icons and a system tray indicating '29°C Sunny' and the date '25-03-2024'.

10. Notice that the 403_by_clientip report is in the list. Click on the report title to run the report.

The screenshot shows the Splunk Enterprise web interface with the '403_by_clientip' report selected. The top navigation bar and sidebar are identical to the previous screenshot. The main content area now displays the details of the '403_by_clientip' report. It shows a summary of '3,828 events (before 3/25/24 9:00:07.000 PM)' and a table of log entries. The table has columns for '_time', 'host', 'source', and 'sourcetype'. The log entries show multiple instances of 'web_application' access logs from March 26, 2024, at various times between 10:27:27.000 PM and 8:33:42.000 PM. Each entry is associated with 'access_30DAY.log' and 'access_combined_wcookie' sourcetype. The bottom of the screen shows a taskbar with various icons and a system tray indicating '29°C Sunny' and the date '25-03-2024'.

Task 2: Use stats functions to create visualizations of products sold, and add them to a dashboard.

11. Navigate to a new Search view. (Access the Search view by clicking the Search menu option on the bar at the top of the screen.)

12. Enter a search that returns all web application events for all time where an item was successfully purchased. Remember, when an item is successfully purchased a success.do file is served and a 200 status is returned.

command : (index=main sourcetype=access_combined_wcookie file=success.do status=200)

The screenshot shows the Splunk interface with a search results page. The search bar contains the command: "index=main sourcetype=access_combined_wcookie file=success.do status=200". The results table shows 16,139 events from March 25, 2024, at 9:07:21.000 PM. The table includes columns for _time, host, source, and sourcetype. The sourcetype column consistently shows "access_combined_wcookie". The interface also displays a timeline visualization above the table and various navigation and search controls.

13. Use the stats count function with a by clause to count events by the productid.

Command : index=main sourcetype=access_combined_wcookie file=success.do status=200 | stats count by productid

The screenshot shows the Splunk interface with a search results page. The search bar contains the command: "index=main sourcetype=access_combined_wcookie file=success.do status=200 | stats count by productid". The results table shows 16,139 events from March 25, 2024, at 9:08:13.000 PM. The table includes columns for productid and count. The count column shows values such as 935, 1319, 1388, 988, 1155, and 61. The interface also displays a table view above the results and various navigation and search controls.

14. Select the Visualization tab and choose the Column Chart from the visualization selections.

The screenshot shows the 'Splunk Visualizations' page. At the top, there's a grid of nine preview images for different visualization types: Line, Area, Bar, Horizontal Bar, Pie, Scatter, Bubble, Gauge, and Map. Below the grid is a link 'Find more visualizations'. A vertical sidebar on the left has a 'Count' button. The main content area features a section for 'Choropleth Map' with the description 'Show how values vary over a geographic region.' and a 'Search Fragment' section containing the following SPL command:

```
| stats count by featureId | geom geo_countries  
featureIdField=featureId
```

A blue bar at the bottom contains the text 'CLU-PG-G06'.

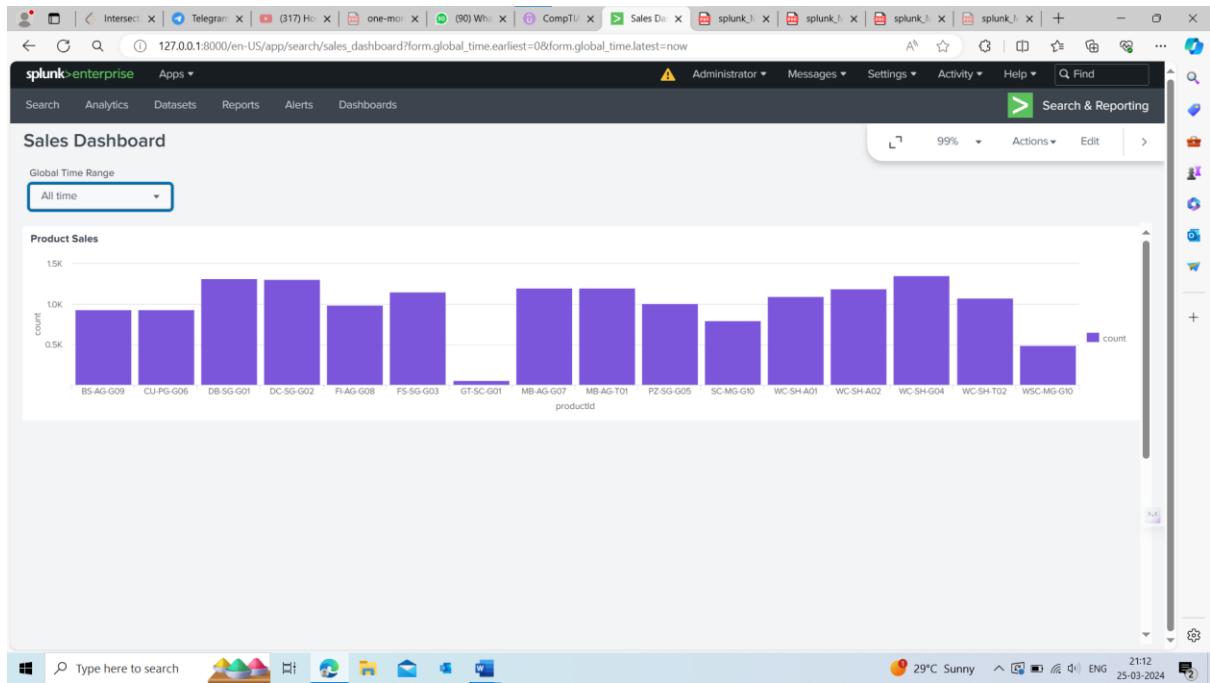
15. Use the Save As menu to select Dashboard Panel.

16. Save the dashboard with these values:

- Dashboard: New
- Dashboard Title: Sales Dashboard
- Panel Title: Product Sales

The screenshot shows the 'Save Panel to New Dashboard' dialog. It has fields for 'Dashboard Title' (Sales Dashboard), 'Description' (Optional), and 'Permissions' (Private). Below these are options for building the dashboard: 'Classic Dashboards' (The traditional Splunk dashboard builder) and 'Dashboard Studio' (A new builder to create visually-rich, customizable dashboards). Under 'Panel Title', it says 'Product Sales'. Under 'Visualization Type', 'Column Chart' is selected. At the bottom are 'Cancel' and 'Save to Dashboard' buttons.

17. Once saved, click View Dashboard



18. Roll over the columns in the chart to see the interaction, and notice the tools at the bottom of the panel.

19. Use the Open in Search icon at the bottom of the panel, to open the search view and run the search.



20. Remove the by clause from the search to return the total count of products sold.

Command : (index=main sourcetype=access_combined_wcookie file=success.do status=200 | stats count)

The screenshot shows a Splunk search interface with the following search command:

```
index=main sourcetype=access_combined_wcookie file=success.do status=200 | stats count
```

The results table has the following data:

productId	count
BS-AC-G09	935
CU-PG-G06	935
DB-SG-G01	1319
DC-SG-G02	1308
FT-AC-G08	988
FS-SG-G03	1155
GT-SC-G01	61
MB-AC-G07	1204
MB-AG-T01	1205
PZ-SG-G05	1012
SC-MG-G10	795
WC-SH-A01	1100
WC-SH-A02	1192
WC-SH-G04	1368
WC-SH-T02	1076
WSC-MG-G10	494

The screenshot shows a new Splunk search with the following search command:

```
index=main sourcetype=access_combined_wcookie file=success.do status=200 | stats count
```

The results table has the following data:

count
16139

The screenshot shows a Splunk dashboard with a large visual element displaying the value "16,139". Below it is a table with the following data:

count
16139

A tooltip for the visual element says:

Snip saved to clipboard
Select here to mark up and share the image.

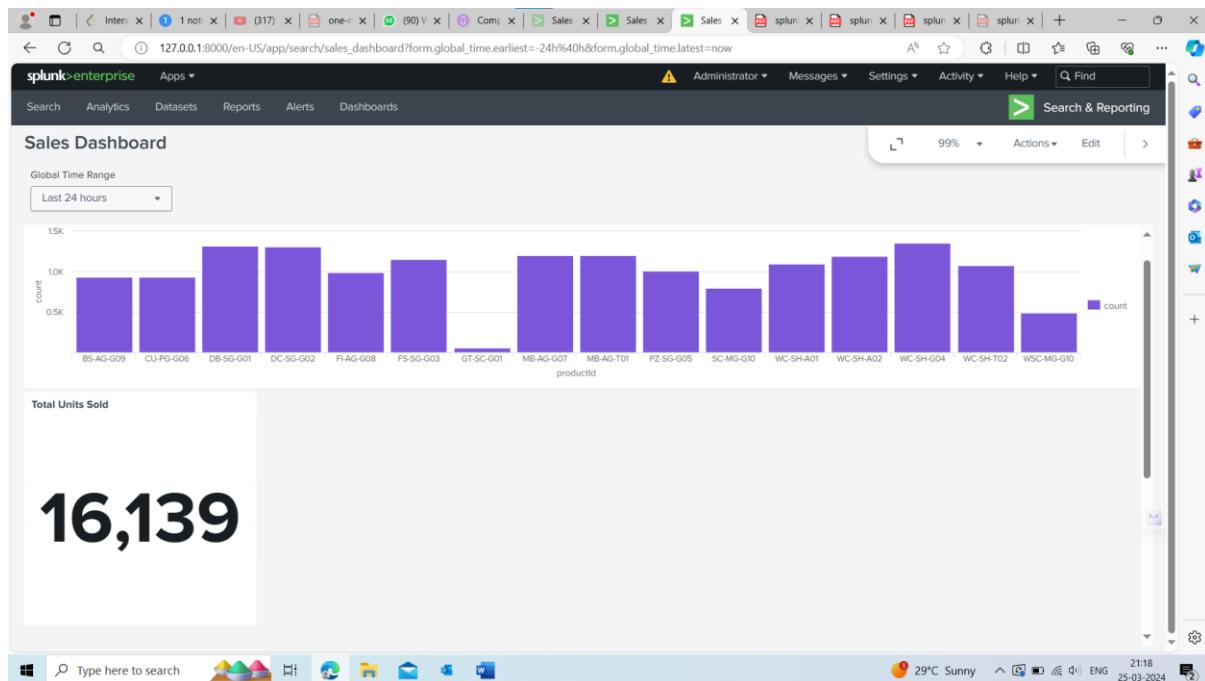
21. Select the Visualization tab and choose the Single Value visualization from the Splunk Visualizations menu.

22. Use the Save As menu to select Dashboard Panel.

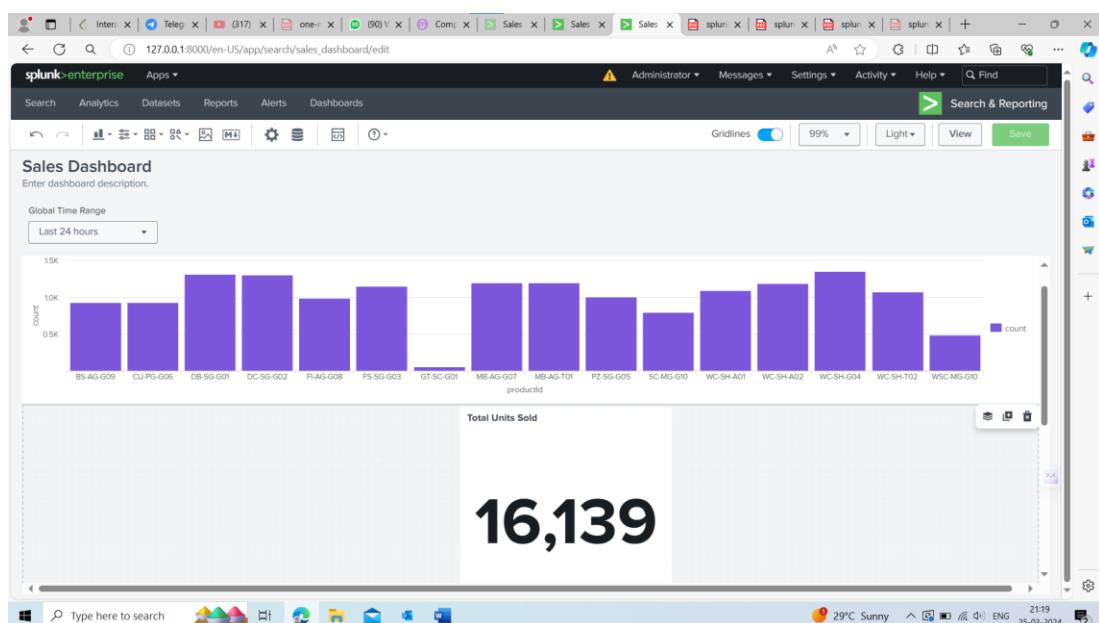
23. Save the dashboard with these values:

- Dashboard: Existing
- Dashboard Title: Sales Dashboard
- Panel Title: Total Units Sold

24. Once saved, click View Dashboard.



25. The Total Units Sold panel is probably the first item our CFO will want to see. Click the Edit button at the top of the dashboard.



26. Click and hold the bar at the top of the Total Units Sold panel and drag the panel to the top of the dashboard. Once in place, drop and click Save.

MODULE 8: USING PIVOT

Task 1: Use a non-transforming command with instant Pivot.

1. Navigate to the Search view. (If you are in the Home app, click Search & Reporting from the column on the left side of the screen. You can also access the Search view by clicking the Search menu option on the green bar at the top of the screen.)
2. Enter in a search that returns all web application events for all time.

Command : index=main sourcetype=access_combined_wcookie

The screenshot shows the Splunk search interface with the following details:

- Search Bar:** index=main sourcetype=access_combined_wcookie
- Results Summary:** 131,645 events (before 3/25/24 9:45:18.000 PM) No Event Sampling
- Event View:** A table showing log entries with columns: _time, host, source, and sourcetype. The first few rows are:

_time	host	source	sourcetype
2/26/24 11:59:45.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:59:43.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:59:41.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:59:39.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:59:27.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:59:27.000 PM	web_application	access_30DAY.log	access_combined_wcookie

- Left Panel:** Shows selected fields (host, source, sourcetype), interesting fields (index, _index, _score, _type), and extract new fields.
- Bottom Bar:** Type here to search, navigation icons, and timestamp 21:45 25-03-2024.

3. Click on the Visualization tab to see three icons: Pivot, Quick Reports, and Search Command.

The screenshot shows the Splunk Search & Reporting interface with the following details:

- Search Bar:** index=main sourcetype=access_combined_wcookie
- Results Summary:** 131,645 events (before 3/25/24 9:45:18.000 PM) No Event Sampling
- Event View:** A table showing log entries with columns: _time, host, source, and sourcetype. The first few rows are:

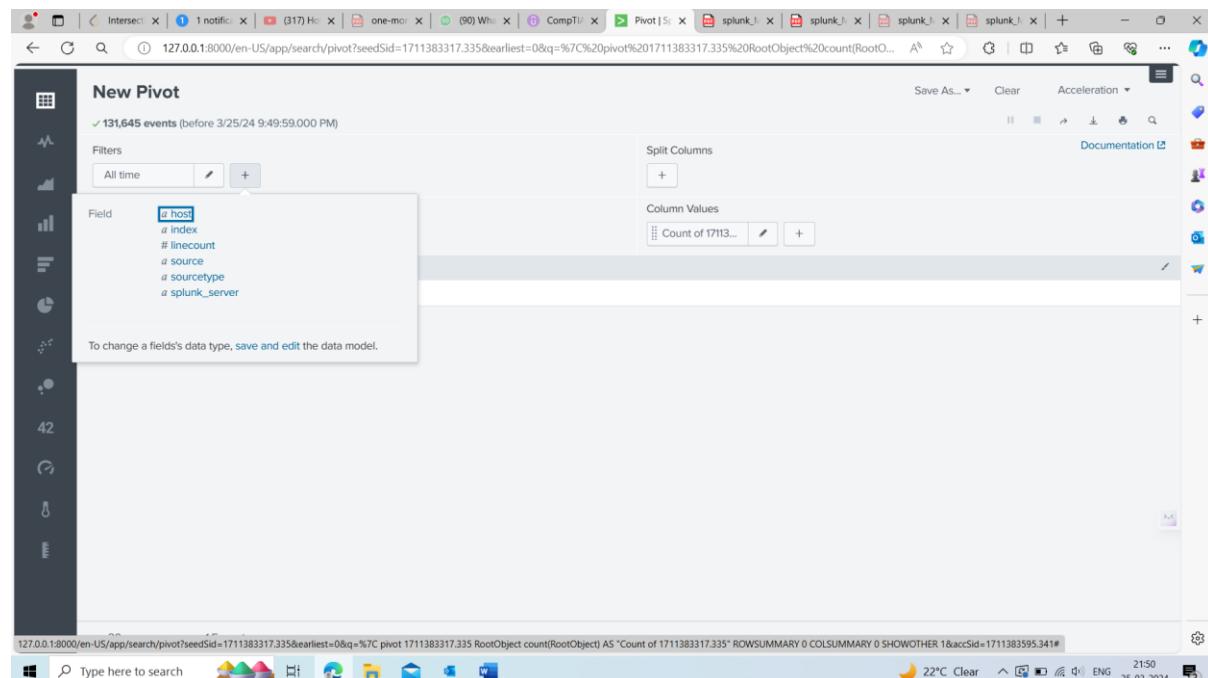
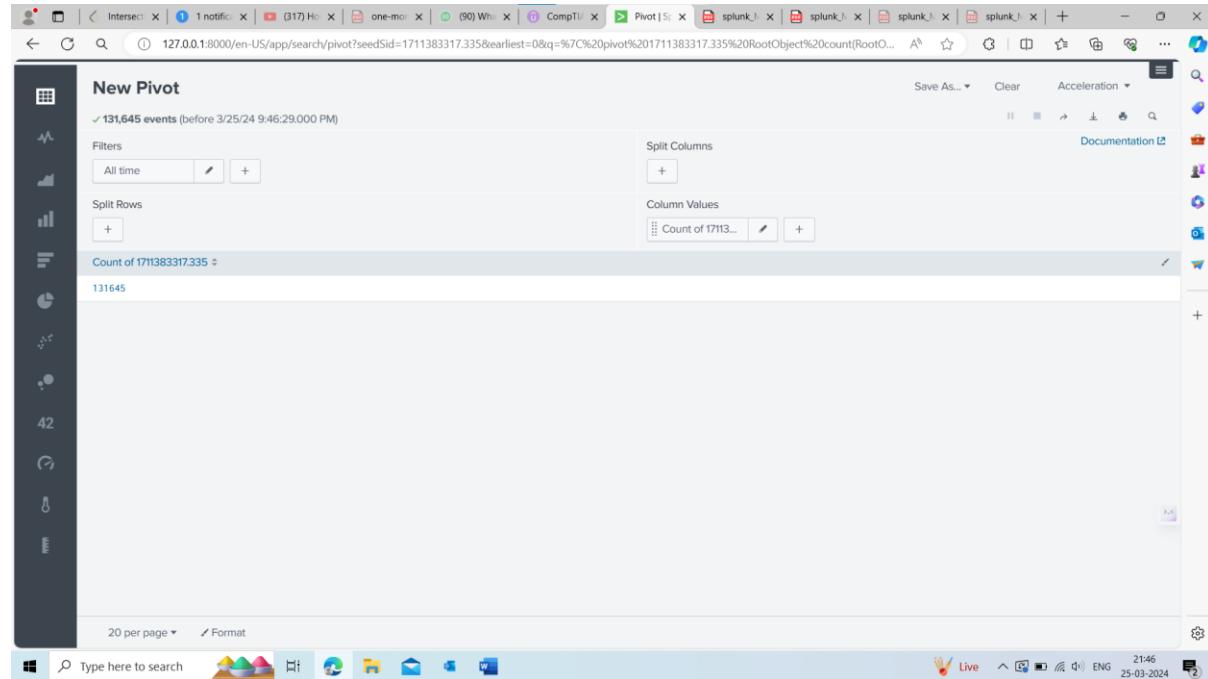
_time	host	source	sourcetype
2/26/24 11:59:45.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:59:43.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:59:41.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:59:39.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:59:27.000 PM	web_application	access_30DAY.log	access_combined_wcookie
2/26/24 11:59:27.000 PM	web_application	access_30DAY.log	access_combined_wcookie

- Left Panel:** Shows search history and recent apps.
- Right Panel:** Three icons for visualization: Pivot (green icon), Quick Reports (blue icon), and Search Commands (orange icon).
- Bottom Bar:** Type here to search, navigation icons, and timestamp 21:46 25-03-2024.

4. Click on the Pivot icon.
 5. In the modal window, select to show All Fields and click OK.

Task 2: Build a report using the Pivot interface.

6. Under Filters, click , to open the filter selector, and select file from the Fields list.



MODULE 9 : CREATING LOOKUPS

Task 1: Download and examine the lookup file.

1. Open a new browser window and direct it to <http://splk.it/productdata>.
2. The file products.zip will be downloaded to your system.
3. Use an archive tool to unarchive the file.
4. Once unarchived, you will see a file named products.csv.
5. Return to the browser window for your instance of Splunk Web or open a new one.
6. Navigate to the Search view. (If you are in the Home app, click Search & Reporting from the column on the left side of the screen. You can also access the Search view by clicking the Search menu option on the bar at the top of the screen.)

This PC > New Volume (D:) > college material > SIXTH SEMESTER > ISG LAB > products >				
New Volume (D:)	Name	Date modified	Type	Size
ALL FORENSICS	_MACOSX	25-03-2024 21:57	File folder	
AMCAT	products	25-03-2024 21:57	Microsoft Excel Co...	1 KB
Business Relate				
C AND C++				
cfrbackup-TWF				

Task 2: Add a lookup file and create a lookup definition.

7. Navigate to: Settings > Lookups > Lookup table files.
8. Click New Lookup Table File.
9. Save the lookup table file with these values:
 - Destination app: search
 - File: products.csv file
 - Destination filename: products.csv
10. Navigate to Settings > Lookups > Lookup definitions.
11. Make sure Search & Reporting is selected for App context and Click New Lookup Definition
12. Save the lookup table file with these values:
 - Destination app: search
 - Name: products_lookup
 - Type: File-based
 - Lookup file: products.csv
13. Return to the Search view.

14. Use inputlookup command to verify the lookup definition was created correctly.

Command : | inputlookup products_lookup

The screenshot shows the Splunk Enterprise search interface. The search bar contains the command: | inputlookup products_lookup|. The results table displays 16 rows of data from the products_lookup table. The columns are: Code, categoryId, price, productId, and productName. The data includes various product categories like STRATEGY, SHOOTER, TEE, etc., with prices ranging from 4.99 to 24.99 and product names like "Mediocre Kingdoms" and "World of Cheese".

Task 3: Use the lookup in a search.

15. Search the web application data for all events where a user purchased a product successfully.

Command : (index=main sourcetype=access_combined_wcookie status=200 file=success.do)

The screenshot shows the Splunk Enterprise search interface. The search bar contains the command: index=main sourcetype=access_combined_wcookie status=200 file=success.do. The results table displays 16,139 events. The columns are: _time, host, source, and sourcetype. The data shows multiple entries for the same host and source, indicating multiple successful purchases. The time column shows dates from 2/26/24 at 11:57:14 PM to 2/26/24 at 11:50:48.000 PM.

16. Use the lookup command and reference the lookup table you just created. Match the productId in lookup table to the productId field in the event data. Use the OUTPUT function to output the product_name lookup table data to a ProductName field.

Command : (index=main sourcetype=access_combined_wcookie status=200 file=success.do | lookup products_lookup productId as productId OUTPUT product_name as ProductName)

The screenshot shows a Splunk search interface with the following search command in the search bar:

```
index=main sourcetype=access_combined_wcookie status=200 file=success.do | lookup products_lookup  
productId as productId OUTPUT product_name as ProductName
```

The results table displays 16,139 events from 2/26/24. The table includes columns for _time, host, source, and sourcetype. A new column, ProductName, has been added to the right of the sourcetype column, showing the mapped product names for each event.

_time	host	source	sourcetype	ProductName
2/26/24 11:57:14.000 PM	web_application	access_30DAY.log	access_combined_wcookie	Product A
2/26/24 11:57:13.000 PM	web_application	access_30DAY.log	access_combined_wcookie	Product B
2/26/24 11:53:43.000 PM	web_application	access_30DAY.log	access_combined_wcookie	Product C
2/26/24 11:51:56.000 PM	web_application	access_30DAY.log	access_combined_wcookie	Product D
2/26/24 11:51:56.000 PM	web_application	access_30DAY.log	access_combined_wcookie	Product E
2/26/24 11:50:48.000 PM	web_application	access_30DAY.log	access_combined_wcookie	Product F

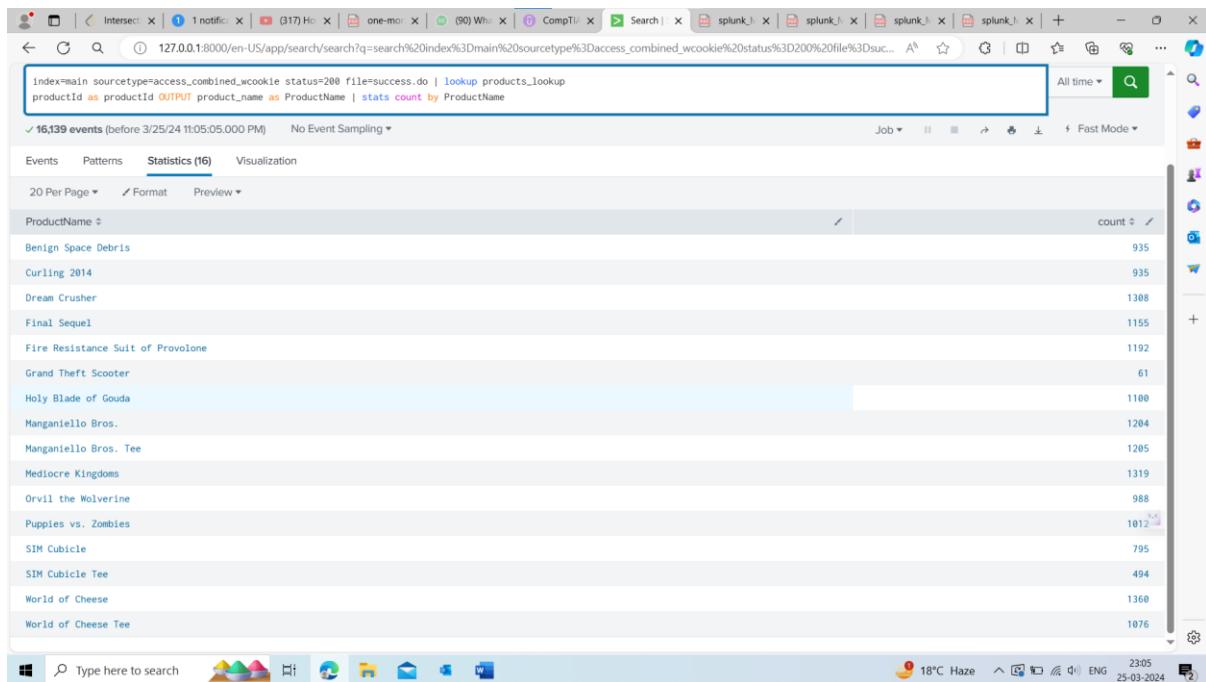
17. Notice that there is now a ProductName field in the fields list

INTERESTING FIELDS

a file 1
a index 1
linecount 1
a productId 16
a ProductName 16
a splunk_server 1
status 1

18. Change the search to use a stats count function to count events by ProductName.

Command : (index=main sourcetype=access_combined_wcookie status=200 file=success.do | lookup products_lookup productId as productId OUTPUT product_name as ProductName | stats count by ProductName)



Task 4: Create an automatic lookup definition.

19. Navigate to Settings > Lookups > Automatic lookups

20. Save the automatic lookup with these values:

- Destination app: search
- Name: products_auto_lookup
- Lookup table: products_lookup
- Apply to: sourcetype
- named: access_combined_wcookie
- Lookup input fields: productId = productId
- Lookup output fields: product_name = ProductName
price = Price

The configuration page shows the following settings for the 'products_auto_lookup' automatic lookup:

- Destination app: search
- Name: products_auto_lookup
- Lookup table: products_lookup
- Apply to: sourcetype (selected), named (access_combined_wcookie)
- Lookup input fields: productId = productId
- Lookup output fields: product_name = ProductName, price = Price

There is also an unchecked checkbox for Overwrite field values.

Task 5: Verify your automatic lookup is working.

21. Return to the Search view.

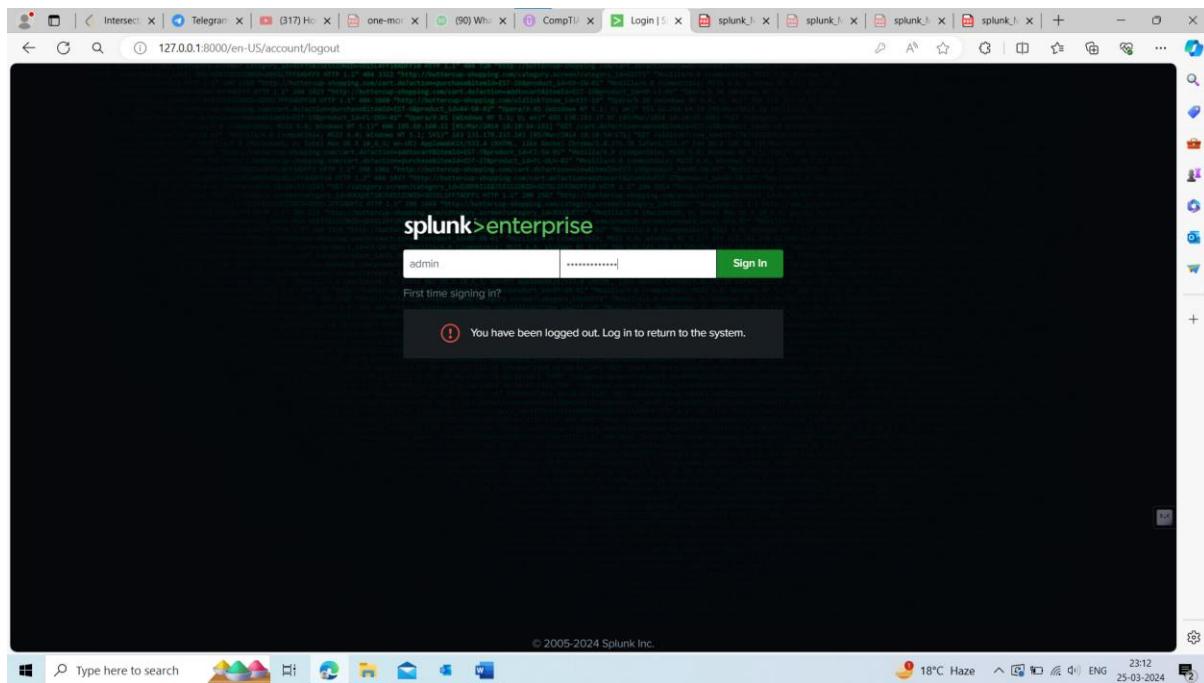
22. Search the web application data for all events where a user purchased a product successfully. Use the stats sum function to sum the Price field by ProductName. Name the resulting field Revenue.

Command : index=main sourcetype="access_combined_wcookie" file=success.do
status=200 | stats sum(Price) as Revenue by ProductName

MODULE 10: CREATING ALERTS

Task 1: Change user account and run a sample search.

1. Log out of Splunk Enterprise using the uname > Logout menu
2. Enter admin for user name and the password of WrongPassword.

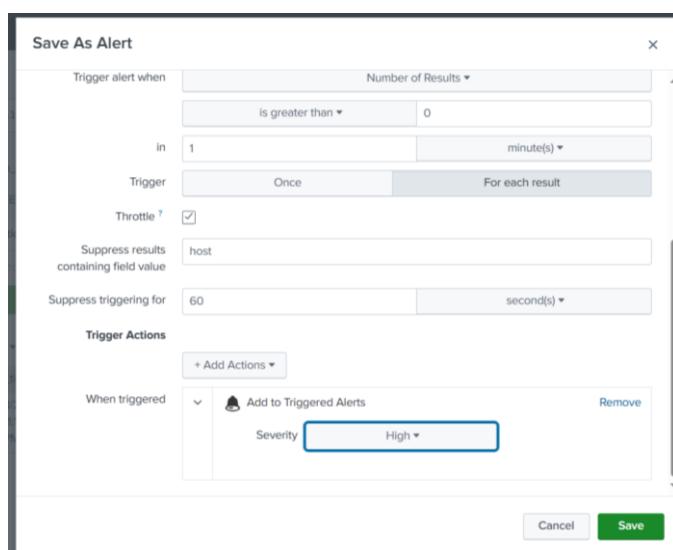
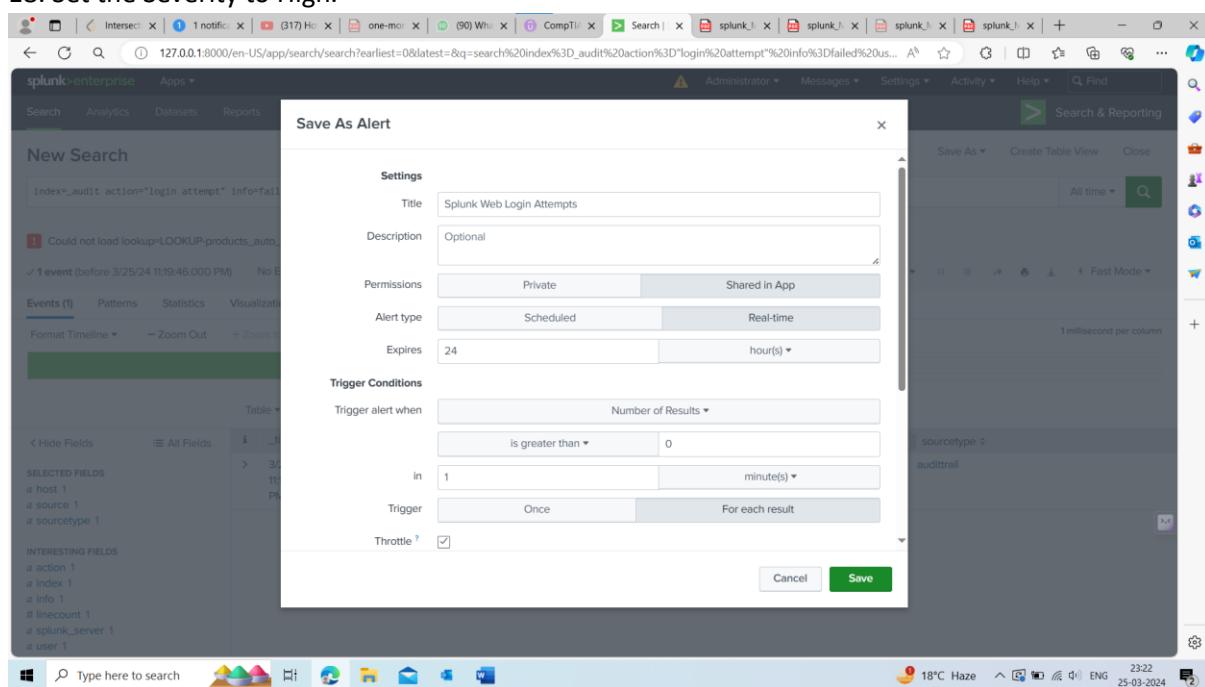


3. Now, enter admin for user name and the password you selected in Module
4. Navigate to the Search view. (If you are in the Home app, click Search & Reporting from the column on the left side of the screen. You can also access the Search view by clicking the Search menu option on the bar at the top of the screen.)
5. Search the _audit index for events where the action of "login attempt" returned a "failed" info value for the username of admin over the Last 15 Minutes.

Command : index=_audit action="login attempt" info=failed user=admin

Task 2: Create an alert.

6. From the Save As menu, select Alert.
7. Title the alert: Splunk Web Login Attempts
8. For Permissions, select Shared in App.
9. For Alert type, select Real-time
10. For Trigger alert when, select Number of Results.
11. Set the number of results to: is greater than 0.
12. The in field should be set to 1 minute
13. For Trigger, select For each result.
14. Check the Throttle checkbox
15. For Suppress results containing field value, type: host
16. Make sure Suppress triggering for is set to 60 seconds.
17. Click Add Actions and select Add to Triggered Alerts.
18. Set the Severity to High.



19. Click Save and Click View Alert.

The screenshot shows the Splunk Web interface with the title 'Splunk Web Login Attempts'. The alert is configured with the following details:

- Enabled: Yes. Disable
- App: search
- Permissions: Shared in App. Owned by deepali_123. [Edit](#)
- Modified: Mar 25, 2024 11:25:53 PM
- Alert Type: Real-time. [Edit](#)

The trigger condition is set to 'Number of Results is > 0 in 1 minute'. There are no fired events for this alert.

20. Log out of Splunk Enterprise using the Administrator > Logout menu

21. Enter admin for user name and the password of WrongPassword three times in a row.

22. Now, enter admin for user name and the correct password.

23. From the Splunk bar, click Activity > Triggered Alerts.

24. Make sure Search & Reporting is selected for App.

The screenshot shows the 'Triggered Alerts' page in Splunk Web. The results table displays two entries:

Time	Fired Alerts	App	Type	Severity	Mode	Actions
2024-03-25 23:28:10 India Standard Time	Splunk Web Login Attempts	search	Real-time	High	Per Result	View Results Edit Search Delete
2024-03-25 23:27:08 India Standard Time	Splunk Web Login Attempts	search	Real-time	High	Per Result	View Results Edit Search Delete

25. Click the View results link on a triggered alert to see the event(s) that caused the alert.

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index=_audit action="login attempt" info=failed user=admin`. The search results table shows one event from 3/25/24 at 11:27:10.000 PM to 3/25/24 at 11:28:10.000 PM. The event details are as follows:

_time	host	source	sourcetype
3/25/24 11:27:15.535 PM	DESKTOP-JOGBSLJ	audittrail	audittrail

Ques: Difference between fast mode , smart mode and verbose mode in splunk.

Ans : The **Fast mode turns off field discovery for event searches. The field and event data is turned off for searches with the stats command.** The **Smart mode turns on field discovery for event searches. The Smart mode is the default setting.** The **Verbose mode returns all field and event data.**