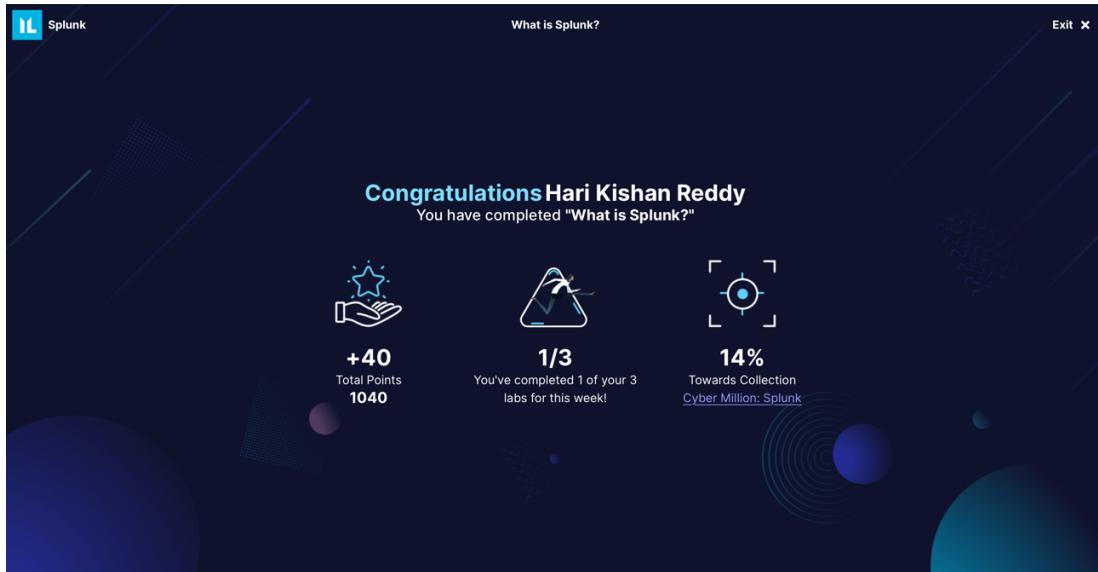


Network Monitoring- Lab 4

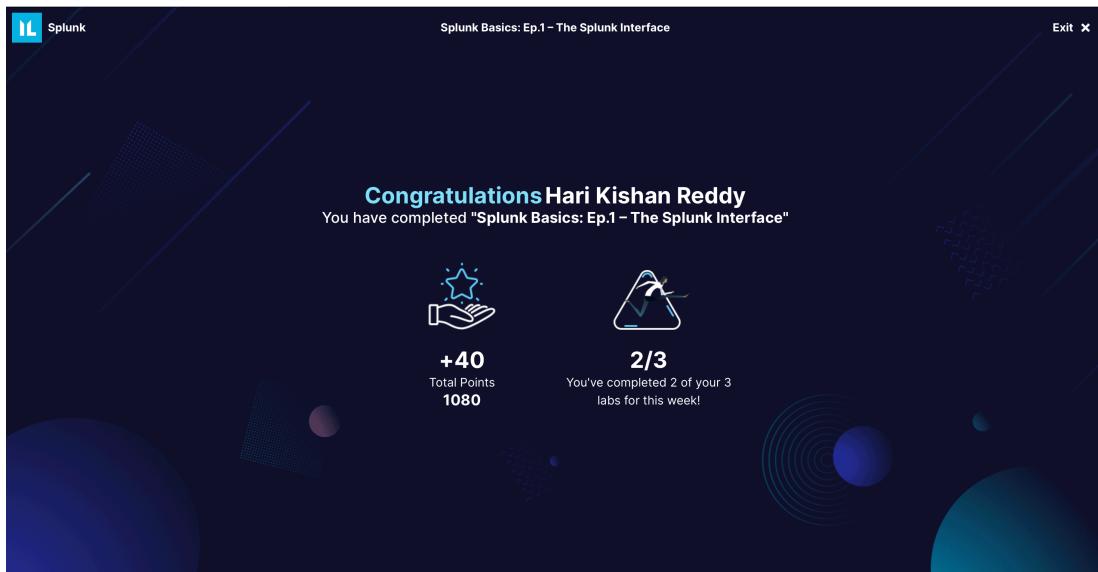
By Hari Kishan Reddy (ha2755)

1. What is Splunk?

Screenshot of lab completion:

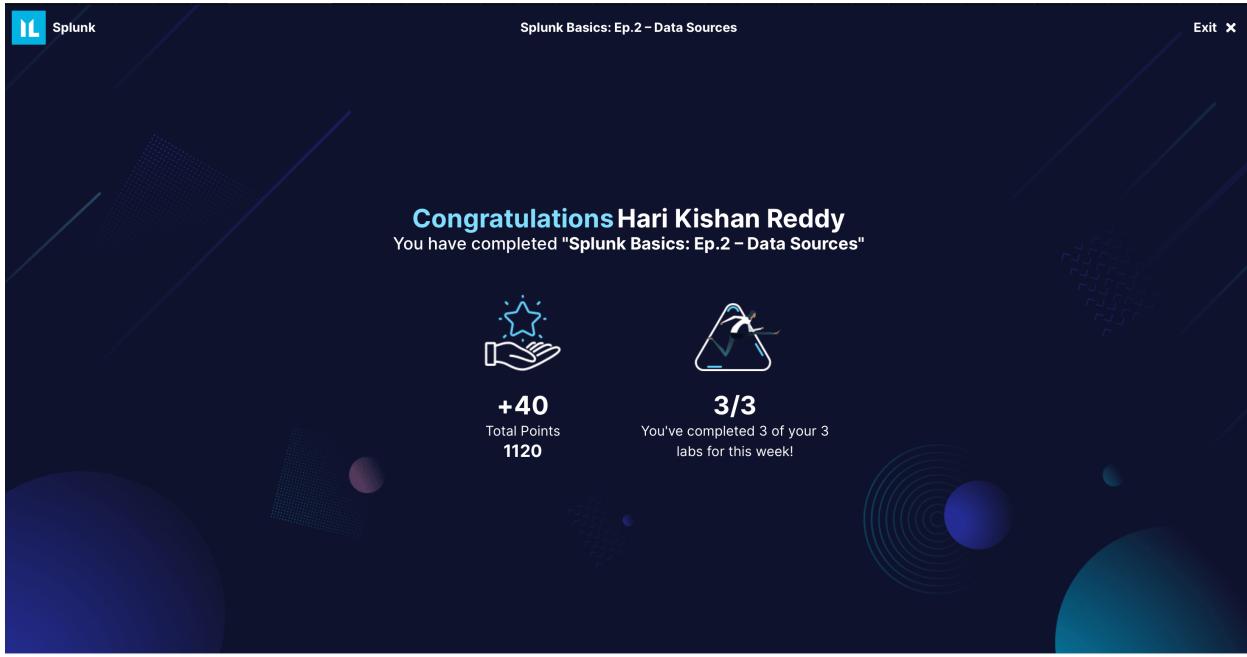


Screenshot of lab completion:



Ep.2 – Data Sources

Screenshot of lab completion:

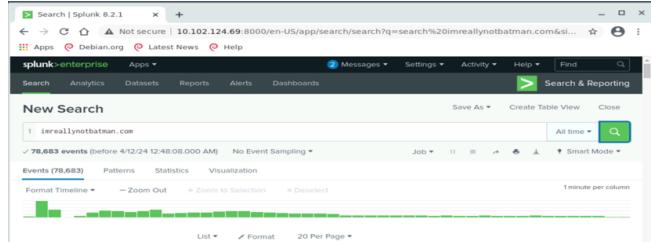


Splunk Basics: Ep.3 – Search

1. Perform a search for the domain "imreallynotbatman.com". How many events are returned?

- **Command:** `domain="imreallynotbatman.com"``

- **Explanation:** The command filters events based on the specified domain, "imreallynotbatman.com", retrieving a total of 78683 events matching this criterion.



2. Perform a search for the domain "imreallynotbatman.com", this time including the field "http_method=POST". How many events are returned?

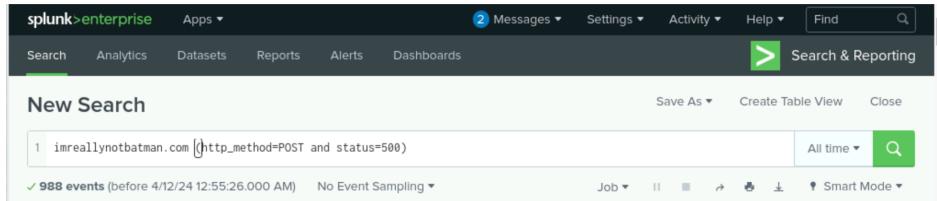
- **Command:** `domain="imreallynotbatman.com" http_method=POST`

- **Explanation:** Adding the `http_method=POST` field filters events further to include only those with a POST HTTP method in addition to the specified domain, resulting in 14238 events.

3. Perform a search for the domain "imreallynotbatman.com", this time including the field "http_method=POST" and the field "status=500". How many events are returned?

- **Command:** `domain="imreallynotbatman.com" http_method=POST status=500`

- **Explanation:** Including both the `http_method=POST` and `status=500` fields narrows down the events to those with a POST method and a status code of 500 for the specified domain, resulting in 988 events.

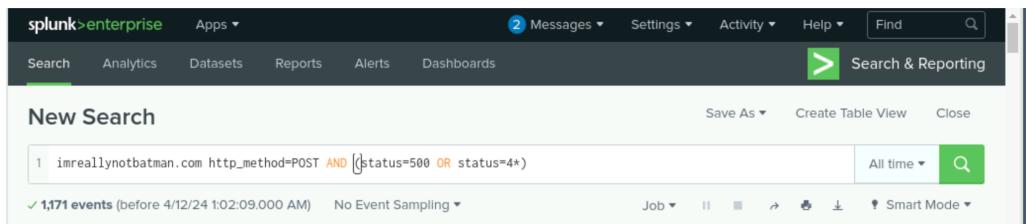


The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: 1 imreallynotbatman.com [http_method=POST and status=500]. The results panel indicates 988 events found, all occurring before April 12, 2024, at 12:55:26.000 AM. There is no event sampling applied.

4. Expand the search query from the previous question to also include all "status=4*" results. How many events are returned?

- **Command:** `domain="imreallynotbatman.com" http_method=POST (status=500 OR status=4*)`

- **Explanation:** By expanding the search to include all status codes starting with "4" in addition to the previous filters, the command retrieves a total of 1171 events.



The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: 1 imreallynotbatman.com http_method=POST AND [status=500 OR status=4*]. The results panel indicates 1,171 events found, all occurring before April 12, 2024, at 1:02:09.000 AM. There is no event sampling applied.

5. Perform a search for the filepath "C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp". How many events does it appear in?

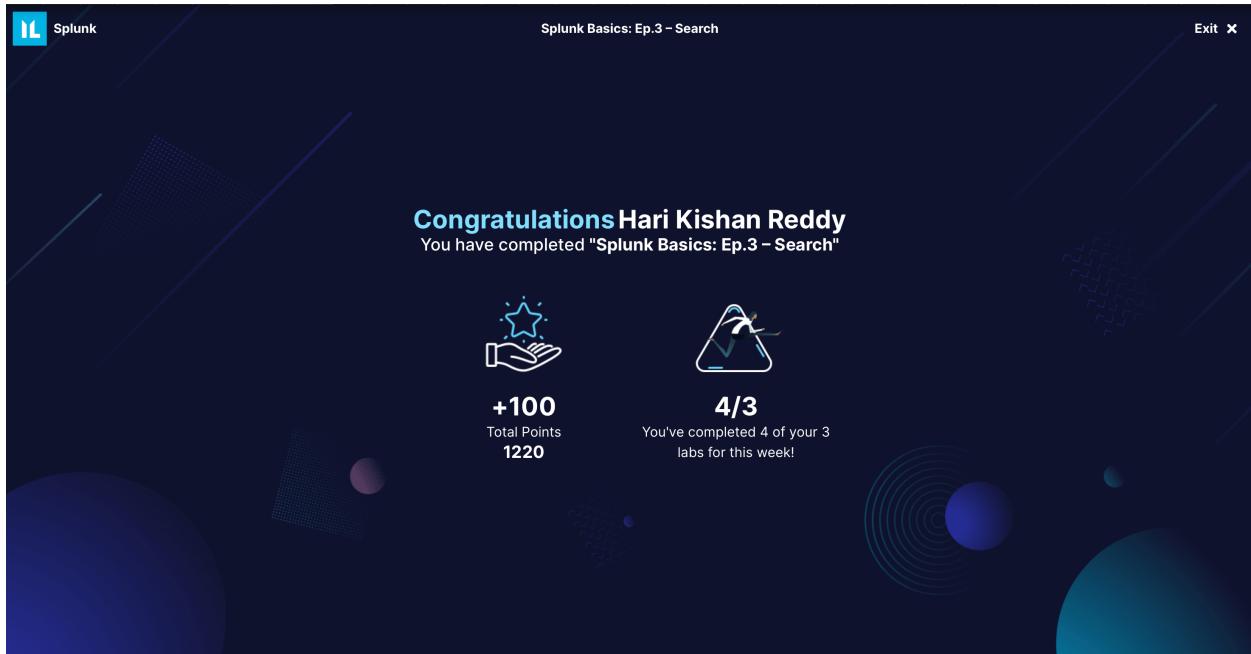
- **Command:** `filepath="C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming\121214.tmp"`

- **Explanation:** This command searches for events containing the specified filepath, resulting in 189 events that include this filepath.



The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: 1 C:\\Users\\bob.smith.WAYNECORPINC\\AppData\\Roaming\\121214.tmp. The results panel indicates 189 events found, all occurring before April 12, 2024, at 1:05:40.000 AM. There is no event sampling applied.

Screenshot of lab completion:



Splunk Basics: Ep.4 – Advanced Searching (SPL & Transforming)

The image shows two side-by-side Splunk search interfaces. The left interface is titled 'Splunk Basics: Ep.4 – Advanced Searching (SPL & Transforming)' and displays a 'Tasks' list with three items:

- Perform a search that lists the most common (top) "http_method" field values from the index "botsv1". What percentage is given for the most common http_method present in the dataset? (68.08) - Correct
- Perform a search that lists only the least common (rare) "status" field value from the index "botsv1". What is the status code given? (208) - Correct
- Perform a search using the stats command to count occurrences of each status code present by the field EventID? for the index "botsv1". What is the EventID with the second most events? (4020146.42) - Correct

The right interface is also titled 'Splunk Basics: Ep.4 – Advanced Searching (SPL & Transforming)' and shows a search result for the first task. The search command is `index=botsv1 | top http_method`. The results table shows:

http_method	Count	Percent
POST	14248	68.087547
GET	14339	31.726682
HEAD	31	0.148141
OPTIONS	1	0.000549

- 1. Perform a search that lists the most common (top) "http_method" field values from the index "botsv1". What percentage is given for the most common http_method present in the dataset?**

- **Command:** index=botsv1 | top http_method

- **Explanation:** This command searches the "botsv1" index and uses the stats command to count occurrences of each HTTP method. The top command is then used to identify the most common HTTP method and its percentage 68.08.

The screenshot shows a Splunk search interface with the search command `index=botsv1 | top http_method` entered. The results table shows the following data:

http_method	Count	Percent
POST	14248	68.087547
GET	14339	31.726682
HEAD	31	0.148141
OPTIONS	1	0.000549

- 2. Perform a search that lists only the least common (rare) "status" field value from the index "botsv1". What is the status code given?**

- Command: `index=botsv1 | stats count by status | sort count | head 1`

- Explanation: This command searches the "botsv1" index and uses the stats command to count occurrences of each status code. By sorting the results and selecting the least common (head 1), you identified the rarest status code, which is 206.

The screenshot shows a Splunk search interface with the search command `index=botsv1 | stats count by status | sort count | head 1` entered. The results table shows the following data:

status	Count	Percent
206	1	0.000549
416	1	0.000549
417	1	0.000549

3. Perform a search using the stats command to count the number of events present by the field 'EventID' from the Source 'WinEventLog:Microsoft-Windows-Sysmon/Operational'. What is the EventID with the second most events?

- **Command:** `sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" | stats count by EventID | sort -count

- **Explanation:** This command searches events from the specified source and uses the stats command to count events by EventID. By sorting in descending order and selecting the second entry, you identified the EventID with the second-highest number of events, which is 3.

The screenshot shows the Splunk Enterprise search interface. The search bar contains the command: `source="WinEventLog:Microsoft-Windows-Sysmon/Operational" | stats count by EventID | sort -count`. The results table has two columns: 'EventID' and 'count'. The data is as follows:

EventID	count
7	168374
3	99320
2	1434
1	767
5	684
	18

4. Perform a search for the domain "imreallynotbatman.com" and then use the 'top' command to determine the IP address of an attacker scanning the domain mentioned above for web app vulnerabilities (i.e., the 'top' 'src_ip').

- **Command:** `domain="imreallynotbatman.com" | top src_ip`

- **Explanation:** This command searches for events related to the specified domain and uses the top command to identify the most common source IP address (src_ip) associated with scanning the domain for vulnerabilities.

The screenshot shows the Splunk Enterprise search interface. The search bar contains the command: `imreallynotbatman.com | top src_ip`. The results table has three columns: 'src_ip', 'count', and 'percent'. The data is as follows:

src_ip	count	percent
40.80.148.42	34967	70.865168
192.168.250.70	11493	23.292958
23.22.63.114	2883	5.842774

5. Perform a search using the domain and IP address from the previous question. What is the top 'alert.signature' field value reference?

- **Command:** `domain="imreallynotbatman.com" src_ip=40.80.148.42 | top alert.signature`

- **Explanation:** Building upon the previous search, this command further refines the events by including the specified domain and attacker IP address, then identifies the top 'alert.signature' field value reference related to the attacker's activity.

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

```
1 imreallynotbatman.com AND src_ip=40.80.148.42  
2 | top alert.signature
```

The search results table has the following data:

alert.signature	count	percent
ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	103	21.775899
ET WEB_SERVER Onmouseover= in URI - Likely Cross Site Scripting Attempt	48	10.147992
ET WEB_SERVER Possible XXE SYSTEM ENTITY in POST BODY.	41	8.668076
SURICATA HTTP Host header invalid	35	7.399577
ET WEB_SERVER Possible SQL Injection Attempt SEL	33	6.976744

6. Using the previously discovered 'attacker IP', determine the IP address of the web server being targeted by incoming attacker activity.

- **Command:** `src_ip=40.80.148.42 | top dest_ip`

- **Explanation:** This command focuses on events from the attacker's IP address and uses the top command to identify the most common destination IP address (dest_ip) targeted by the attacker's activity.

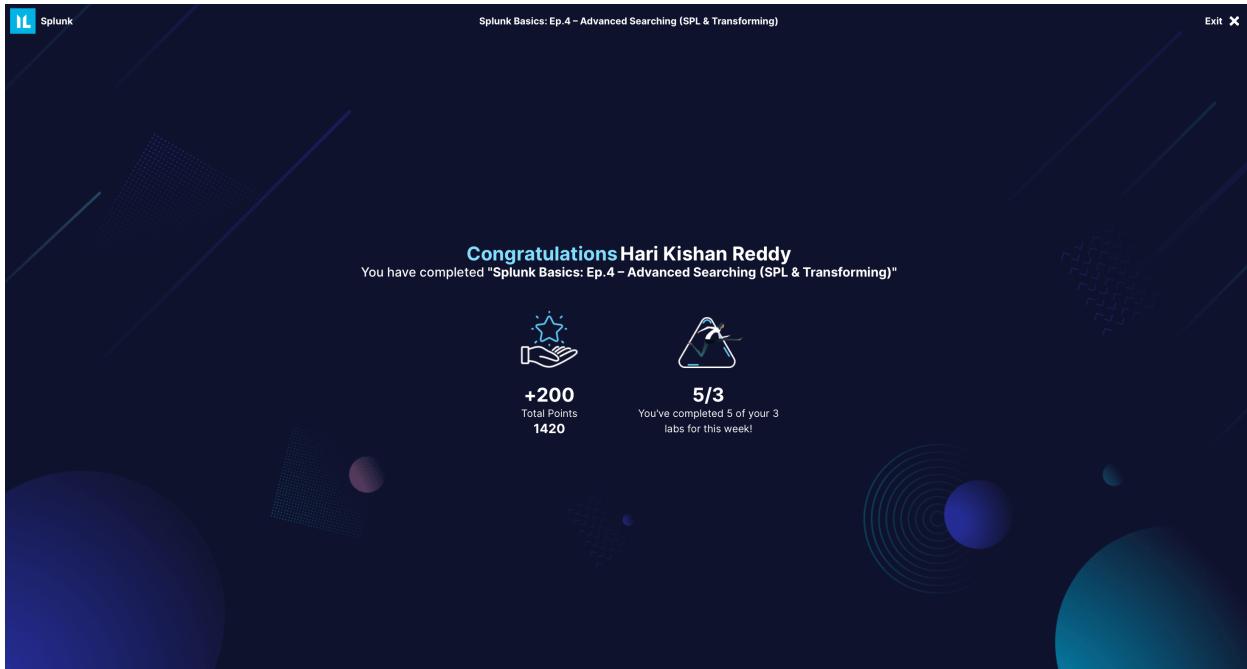
The screenshot shows a Splunk search interface with the following search command in the search bar:

```
1 imreallynotbatman.com AND src_ip=40.80.148.42  
2 | top dest_ip
```

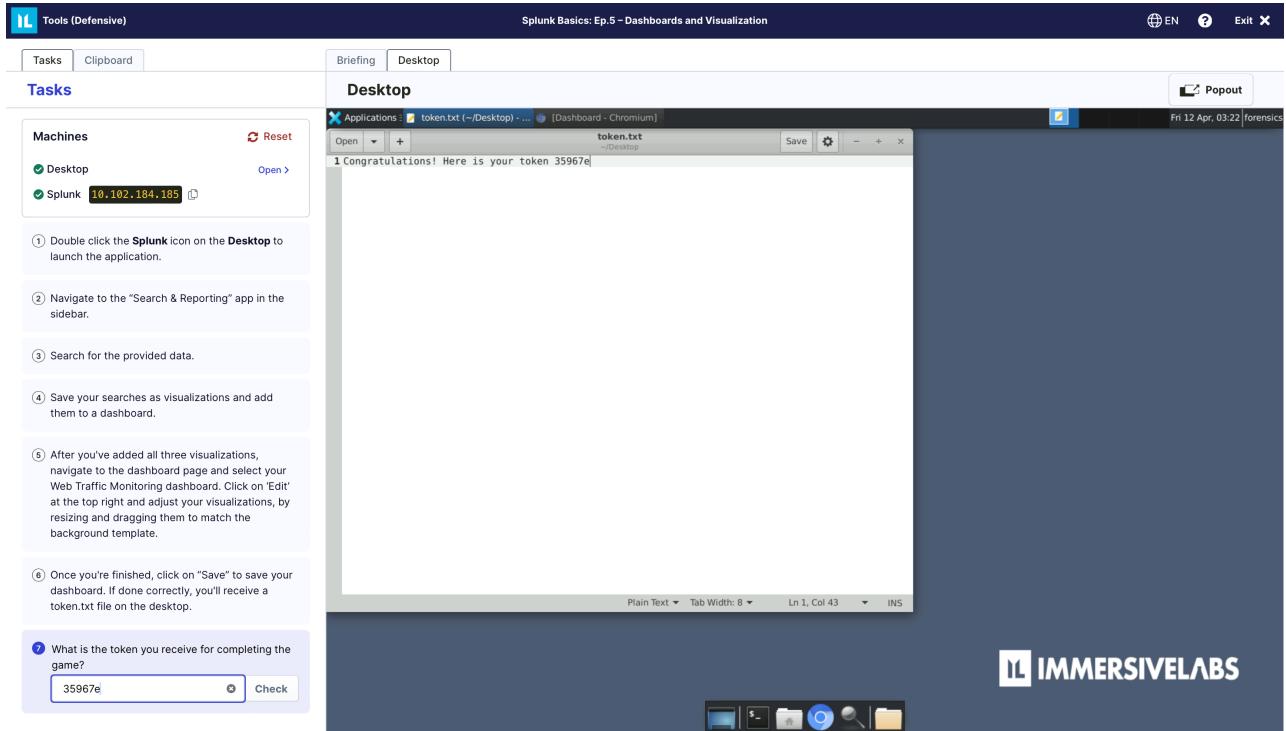
The search results table has the following data:

dest_ip	count	percent
192.168.250.70	34965	99.994280
192.168.250.40	2	0.005720

Screenshot of lab completion:



Splunk Basics: Ep.5 - Dashboards and Visualization



What is the token you receive for completing the game?

1. Double-clicked the Splunk icon on the Desktop to launch the application.
2. Navigated to the "Search & Reporting" app in the sidebar.
3. Searched for the provided data and saved your searches as visualizations.
4. Added the visualizations to a dashboard.
5. Edited the dashboard by resizing and dragging the visualizations to match the background template.
6. Saved the dashboard, resulting in receiving a token.txt file on the desktop with the token "35967e."

Steps I followed are shown below:

Screenshot 1: Splunk 8.2.1 - New Search

Search bar: `index=botsv1 source="stream:http" | top limit=10 status | fields - percent`

Panel Title: "HTTP Status Codes Breakdown"

Visualization Type: Pie Chart

Pie Chart Data:

status	count
303	11365
200	4365
404	2416
304	304
403	403
500	500
404	404

Screenshot 2: Splunk 8.2.1 - New Search

Search bar: `index=botsv1 source="stream:http" | stats count by src_ip | sort - count`

Panel Title: "Web Activity By IP"

Visualization Type: Bar Chart

Bar Chart Data:

src_ip	count
40.80.148.42	17547
23.22.63.114	1429
192.168.2.50	818
192.168.250.70	0
23.22.63.114	11365
40.80.148.42	17547
192.168.2.50	818

Screenshot 3: Splunk Enterprise - New Search

Search bar: `index=botsv1 source="stream:http" | chart count over src_ip by http_method`

Panel Title: "Ip Activity by HTTP Method"

Visualization Type: Line Chart

Line Chart Data:

src_ip	CONNECT	GET	HEAD	OPTIONS	POST	PROPFIND	TRACE	NULL
23.22.63.114	8	8	8	8	412	8	8	0
40.80.148.42	1	4679	8	5	12844	1	1	16
192.168.2.50	8	815	0	0	0	0	0	3

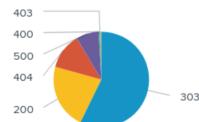
Web Traffic Monitoring

This is for the dashboard description.

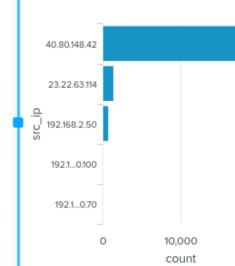
Global Time Range

Last 24 hours

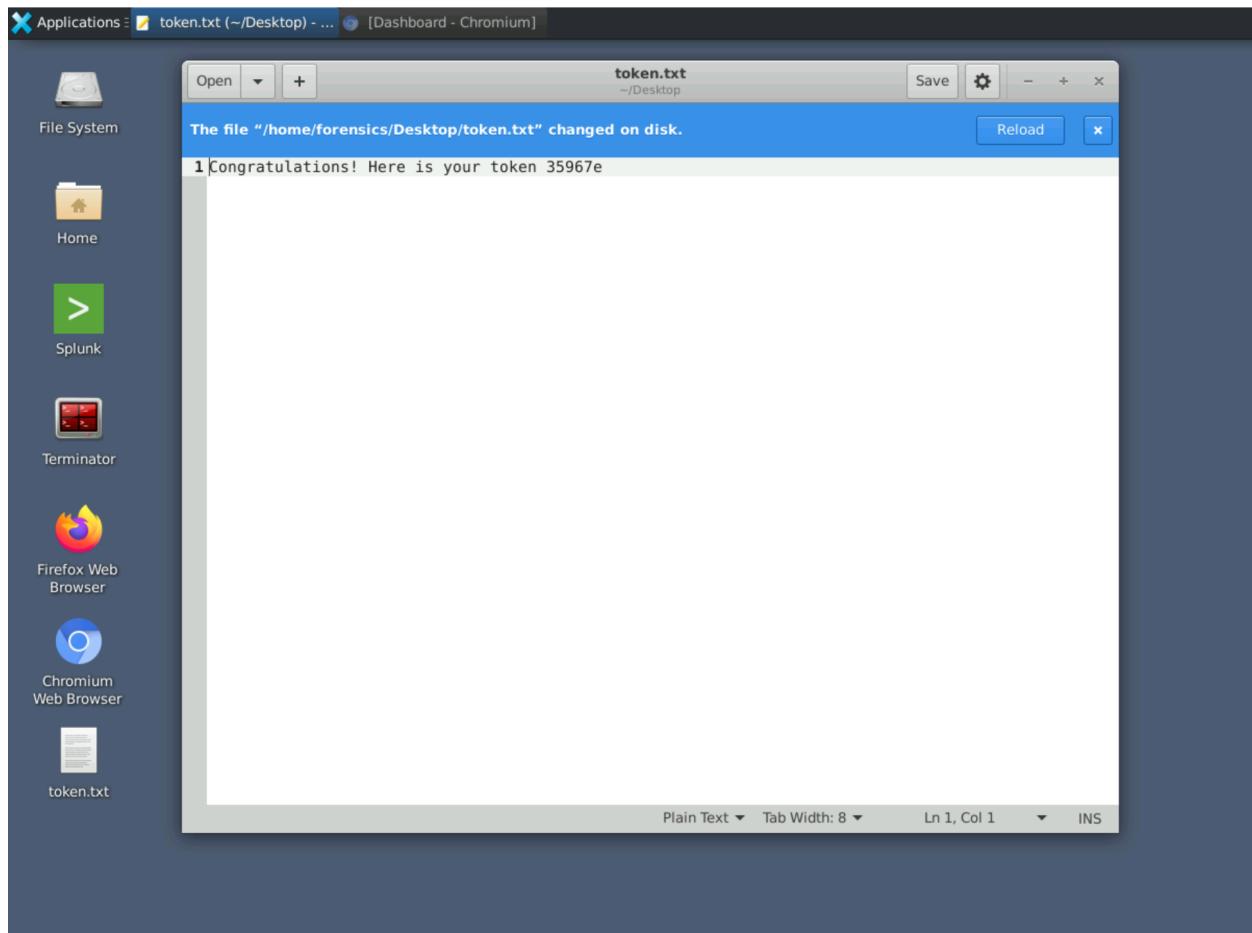
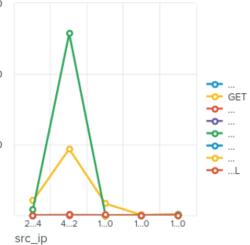
HTTP Status Codes Breakdown



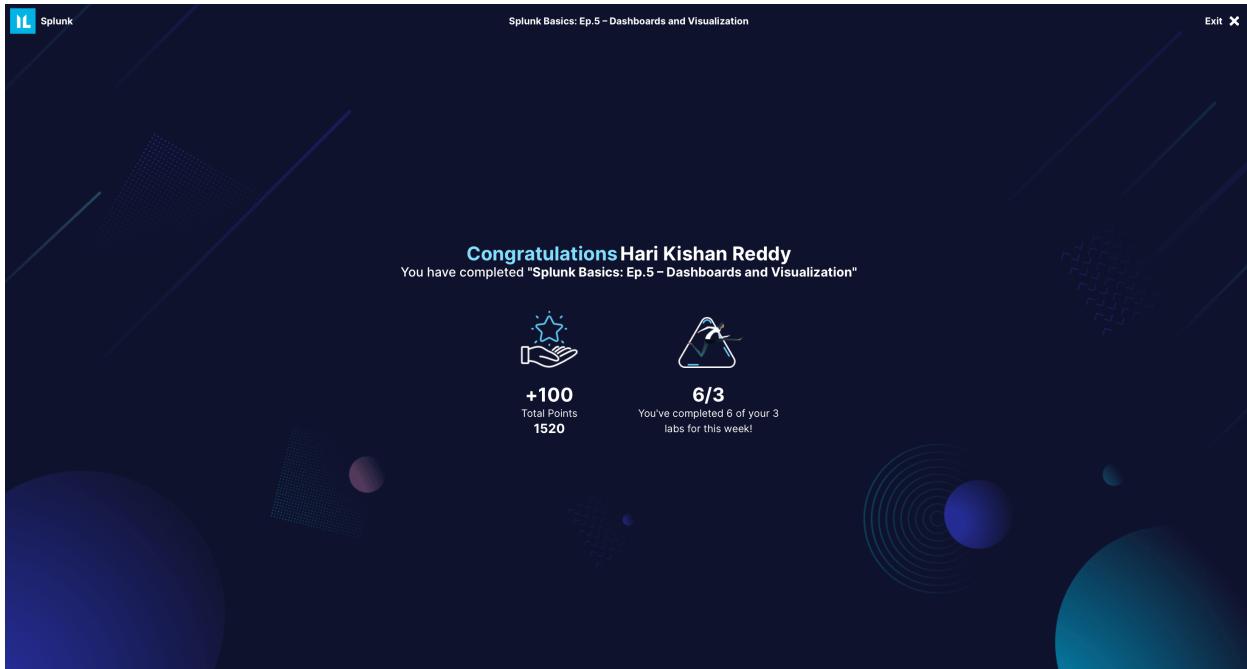
Web Activity By IP



Activity by HTTP Method



Screenshot of lab completion:



Demonstrate Your Skills: Splunk Basics

The screenshot displays the 'Tasks' and 'Desktop' sections of the Splunk Basics interface.

Tasks:

- Q Use SPL queries to look through the dataset and answer the questions.
- Q Select the Data Summary on the Search and Reporting App home page. How many hosts are there?
 - Correct
- Q Looking at the data summary, which source has the highest count?
 - Microsoft-Windows-Sysmon/Operational
 - Correct
- Q Looking at the data summary, provide one of the two sourcetypes with the lowest count.
 - stream:ip
 - Correct
- Q Navigate to the dashboard called WebTraffic Monitoring. Which status code appears the most?
 - 302
 - Correct
- Q Which of the active IP addresses has the lowest number of requests?
 - 192.168.250.70
 - Correct
- Q Which IP has the highest number of POST requests?
 - 49.80.148.42
 - Correct
- Q Search for the host web010desk, source WinEventLog:Security, and the 192.168.250.20 Destination. How many events are returned?
 - 908
 - Correct
- Q Looking at the results from the previous question, find the host name of the service server. What is the host name?
 - web010desk
 - Correct
- Q Search for the keyword 'failure' using the search bar and count the results by the fields alert-signature and alert-signature_id. What is the count of the alert that appeared the fewest times?
 - 28103
 - Correct

Desktop:

The desktop view shows the Splunk UI with various dashboards and search results. One search result table is shown below:

Source	Count	Last Update
CIMI_NOCM_Knowmee/Worker_Error_1	200073	8/24/16 6:27:44.000 PM
CIMI_NOCM_Knowmee/Worker_Error_SOP_Responses	300074	8/24/16 6:27:44.000 PM
CIMI_NOCM_Knowmee/Worker_Error_Status_1	200076	8/24/16 6:27:44.000 PM

1. Select the Data Summary on the Search and Reporting App home page. How many hosts are there?

- **Action:** Accessed the Data Summary on the Search and Reporting App home page.

- **Answer:** 7

Host	Count	Last Update
192.168.2.50	65	8/24/16 4:34:37.000 PM
192.168.250.1	80,922	8/24/16 6:27:44.000 PM
splunk-02	293,579	8/24/16 6:27:43.000 PM
suricata-ids.waynecorpinc.local	125,584	8/24/16 6:27:43.000 PM
we1149srv	121,348	8/24/16 6:27:31.000 PM
we8105desk	244,009	8/24/16 6:27:42.000 PM
we9041srv	90,300	8/24/16 6:27:37.000 PM

2. Looking at the data summary, which source has the highest count?

- **Action:** Examined the data summary to identify the source with the highest count.

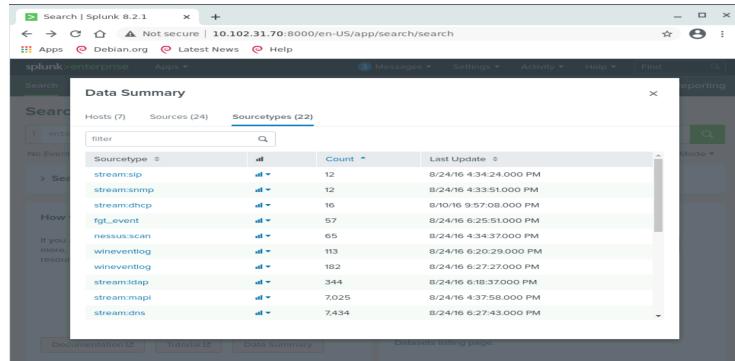
- **Answer:** WinEventLog:Microsoft-Windows-Sysmon/Operational

Source	Count	Last Update
WinEventLog:Microsoft-Windows-Sysmon/Operational	270,597	8/24/16 6:27:40.000 PM
stream:smb	151,568	8/24/16 6:27:38.000 PM
/var/log/suricata/eve.json	125,584	8/24/16 6:27:43.000 PM
WinEventLog:Security	87,430	8/24/16 6:27:41.000 PM
udp:514	80,922	8/24/16 6:27:44.000 PM
WinRegistry	74,720	8/24/16 6:27:42.000 PM
stream:ip	62,083	8/24/16 6:27:43.000 PM
stream:tcp	28,291	8/24/16 6:27:43.000 PM
stream:http	23,936	8/24/16 6:11:45.000 PM
C:\inetpub\logs\LogFiles\W3SVC1\w3_ext60810.log	22,401	8/10/16 10:22:48.000 PM

3. Looking at the data summary, provide one of the two sourcetypes with the lowest count.

- **Action:** Examined the data summary to identify one of the sourcetypes with the lowest count.

- **Answer:** stream:sip



The screenshot shows the Splunk Data Summary interface. The table lists sourcetypes along with their count and last update time. The columns are SourceType, Count, and Last Update. The data is sorted by Count in descending order.

SourceType	Count	Last Update
stream:sip	12	8/24/16 4:34:24,000 PM
stream:snmp	12	8/24/16 4:33:51,000 PM
stream:dhcp	16	8/10/16 9:57:08,000 PM
fgt_event	57	8/24/16 6:25:51,000 PM
nessus:scan	65	8/24/16 4:34:37,000 PM
wireeventlog	113	8/24/16 6:20:29,000 PM
wireeventlog	182	8/24/16 6:27:27,000 PM
stream:idap	344	8/24/16 6:18:37,000 PM
stream:mapi	7,025	8/24/16 4:37:58,000 PM
stream:dns	7,434	8/24/16 6:27:43,000 PM

4. Navigate to the dashboard called Web Traffic Monitoring. Which status code appears the most?

- **Action:** Accessed the Web Traffic Monitoring dashboard and identified the status code with the highest count.

- **Answer:** 303

5. Which of the active IP addresses has the lowest number of requests?

- **Action:** Analyzed active IP addresses and determined the one with the lowest request count.

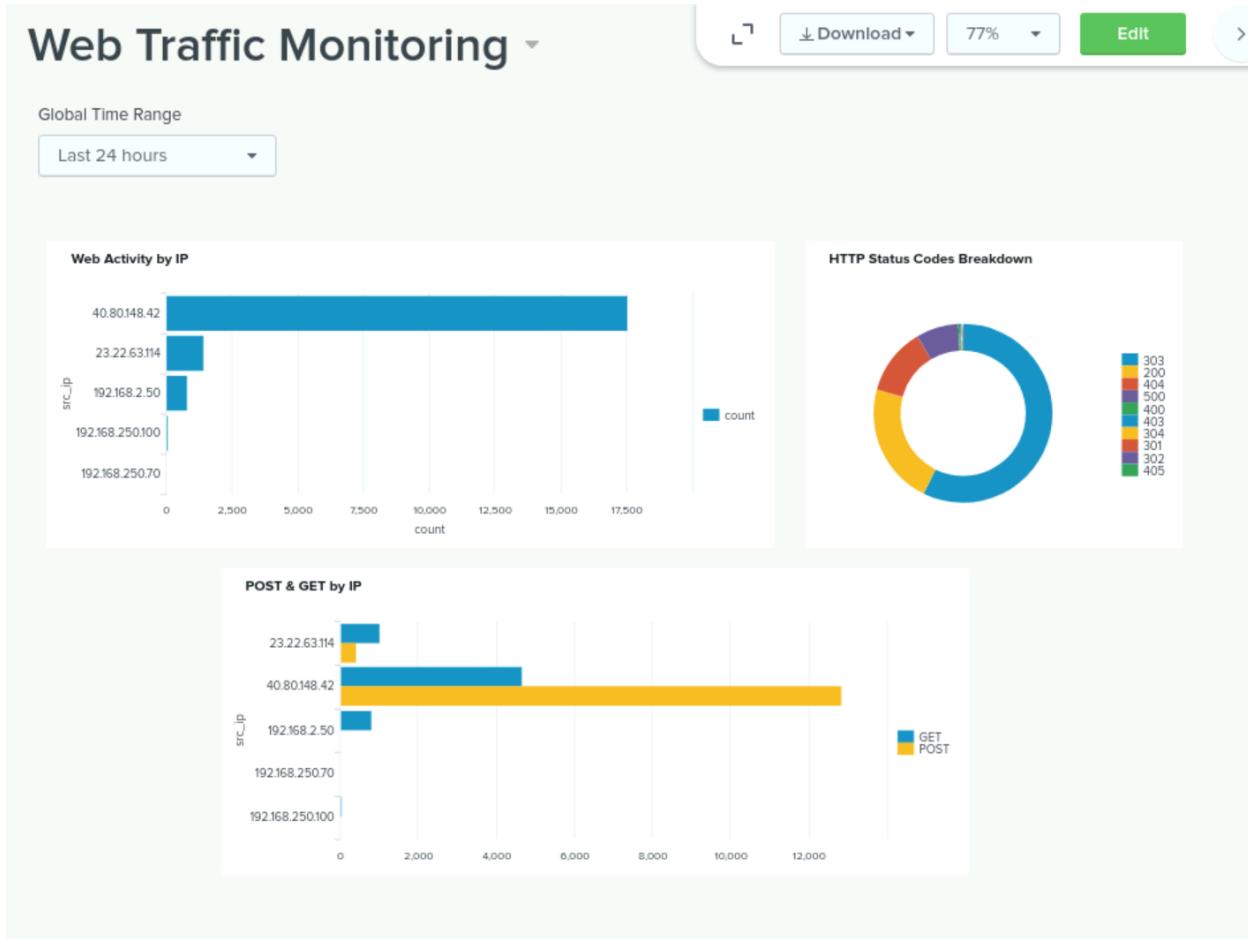
- **Answer:** 192.168.250.70

6. Which IP has the highest number of POST requests?

- **Action:** Analyzed POST requests and identified the IP with the highest count of POST requests.

- **Answer:** 40.80.148.42

For 4,5,6 questions:



7. Search for the host we8105desk, source WinEventLog:Microsoft-Windows-Sysmon/Operational, and the 192.168.250.20 DestinationIp. How many events are returned?

- **Command:** `host=we8105desk sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" dest_ip=192.168.250.20 | stats count`

- **Answer:** 1608

The search results show the following query and statistics:

```
1 host=we8105desk source="WinEventLog:Microsoft-Windows-Sysmon/Operational" DestinationIp=192.168.250.20
2 | stats count
```

1,608 events (before 4/12/24 5:04:11.000 PM) No Event Sampling

Events Patterns Statistics (1) Visualization

Your search did not return any events because you are in Smart Mode. Search in Verbose Mode to view events.

8. Looking at the results from the previous question, find the host name of the remote server. What is the Destination Hostname?

- **Action:** Examined the results of the previous search and added Destination Hostname.

- **Answer:** we9041srv

A screenshot of a Splunk search interface titled "New Search". The search bar contains the query: "host=we8105desk source="WinEventLog:Microsoft-Windows-Sysmon/Operational" DestinationIp=192.168.250.20 | table DestinationHostname". The results show 1,608 events. The "Statistics" tab is selected, displaying the count of 1,608 events. The "DestinationHostname" field has a value of "we9041srv" repeated 1,608 times. The interface includes standard Splunk navigation and search controls.

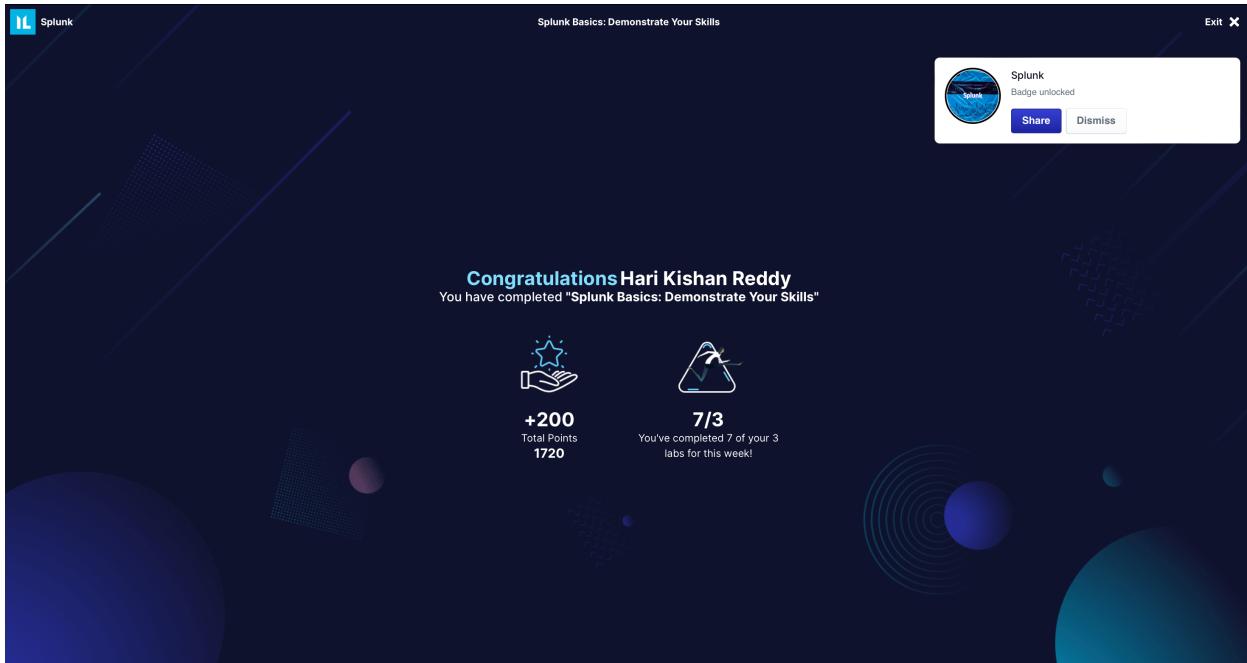
9. Search for the keyword "cerber" using the Suricata sourcetype and count the results by the fields alert.signature and alert.signature_id. What is the signature_id of the alert that appeared the fewest times?

- **Command:** `sourcetype=suricata "cerber" | stats count by alert.signature_id | sort count`

- **Answer:** 2816763

A screenshot of a Splunk search interface titled "New Search". The search bar contains the query: "sourcetype=Suricata \"cerber\" | stats count by alert.signature, alert.signature_id | sort count". The results show 5 events. The "Statistics" tab is selected, displaying the count of 5 events. The "alert.signature_id" field has values 2816763, 2816764, and 2820156, with counts 1, 2, and 2 respectively. The interface includes standard Splunk navigation and search controls.

Screenshot of lab completion:



Write Up

My key learnings and takeaways:

Network Monitoring with Splunk: A Comprehensive Overview

Splunk has proven to be a powerful tool in network monitoring, offering extensive capabilities to gather, analyze, and visualize data from various sources. Through hands-on tasks and modules, I've gained valuable insights into the fundamental aspects of network monitoring using Splunk.

Data Collection and Analysis

One of the core functionalities of Splunk is its ability to collect and index data from diverse sources such as logs, events, and metrics. Using SPL queries, I learned how to search and filter data effectively, allowing me to extract valuable information and perform in-depth analysis.

Visualizations and Dashboards

Splunk's visualization features have been instrumental in creating meaningful representations of data. By creating visualizations such as charts, graphs, and data summaries, I gained a deeper understanding of network trends, anomalies, and performance metrics. Dashboards further enhanced my ability to monitor key indicators in real-time and make informed decisions.

Alerting and Monitoring

Splunk's alerting capabilities proved invaluable in proactive network monitoring. By setting up alerts based on predefined criteria, I was able to detect and respond to potential issues promptly. This proactive approach helped in ensuring network stability and security.

Incident Investigation and Response

In scenarios requiring detailed investigation, Splunk's ability to correlate and analyze vast amounts of data came to the forefront. By conducting searches across multiple data sources and applying statistical analysis, I could identify patterns, anomalies, and potential security threats. This deep dive into incident investigation enhanced my skills in threat detection and response.

Integration and Automation

Splunk's integration capabilities with other tools and systems allowed for seamless data exchange and automation of workflows. Integrating with security tools, for example, enabled me to streamline threat intelligence and incident response processes, enhancing overall network security posture.

Performance Optimization

Through performance monitoring modules, I learned to monitor network traffic, analyze resource utilization, and optimize network performance. This holistic approach to performance management ensures optimal network functioning and user experience.

Conclusion

Overall, my experience with Splunk in network monitoring was good. The platform's robust features, coupled with hands-on exercises and modules, have equipped me with essential skills in data analysis, visualization, alerting, incident response, and performance optimization. Splunk stands out as a versatile and comprehensive solution for effective network monitoring and security.