Lab) Splunk Investigation 1 Solution

Investigation Scenario

Alongside the vulnerability scan our security tools have alerted us to a malicious actor that is brute forcing accounts for the website. We need you to investigate, find out where the attack is coming from, if they were successful, and if they were, what did they do with their access. This is an extremely time-sensitive investigation, every second is potentially more time the attacker has control over systems on the server.

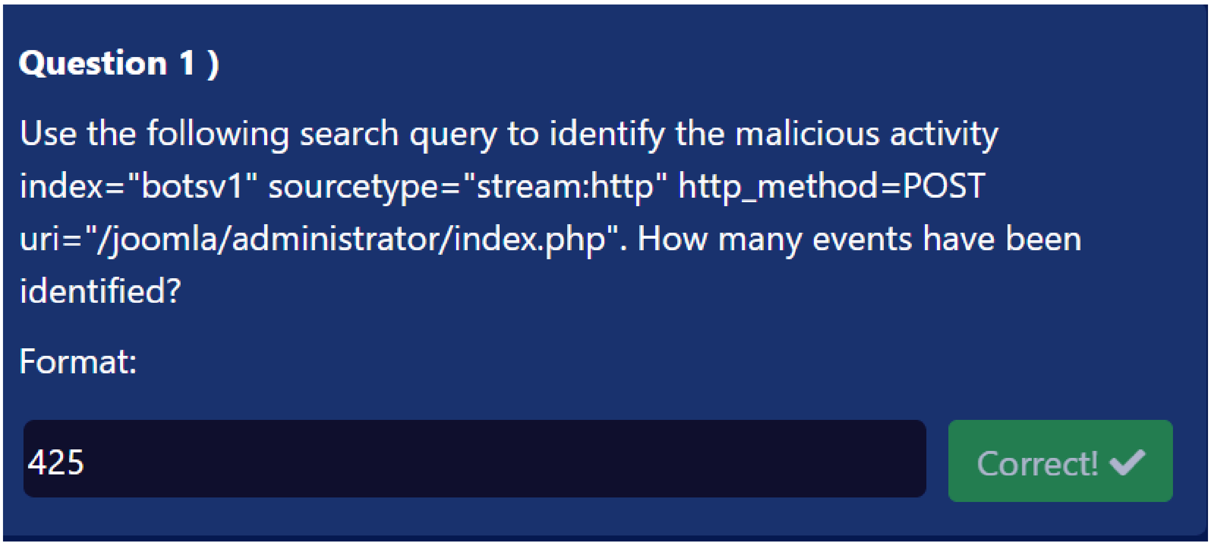
This investigation isn't as simple as looking at one type of event sourcetype. You will need to use your analysis skills to investigate and compare different log types to work out exactly what has happened. As a starting point, we know the administrator URL ishttp://imreallynotbatman.com/joomla/administrator/index.phpand that usernames and passwords will be submitted in an HTTP POST request (http_method=POST). Ensure that event sampling is set to 'No Event Sampling' so we can see every single event. Let's investigate!

Accessing Splunk

Open Firefox from the bottom taskbar and click Restore Session to access Splunk.

Click on the 'Search and Reporting' app in the top right corner and you'll be able to search! Don't forget to ensure Event Sampling is turned off, and your time range (far right of the search field) is set to All Time. All queries must start by referencing the dataset, using`index="botsv1"`. REMEMBER - events take a while to load after a search, be patient otherwise you may be missing results!

This is the solution for the Splunk SIEM investigation and it take me around 20 minutes to complete the task.

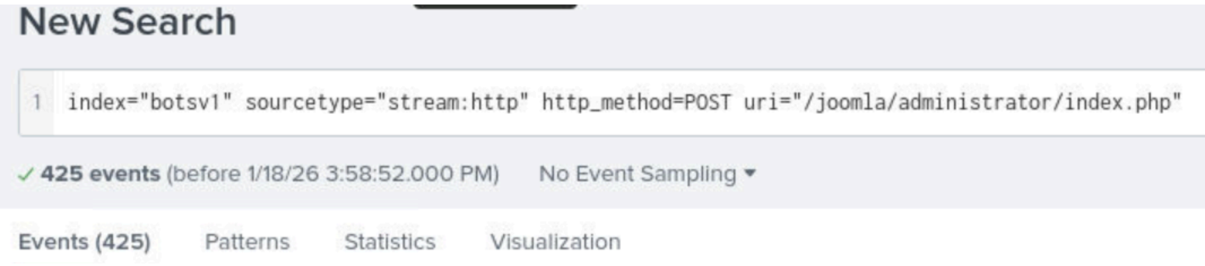


Question 1)

Use the following search query to identify the malicious activity index="botsv1" sourcetype="stream:http" http_method=POST uri="/joomla/administrator/index.php". How many events have been identified?

Format:

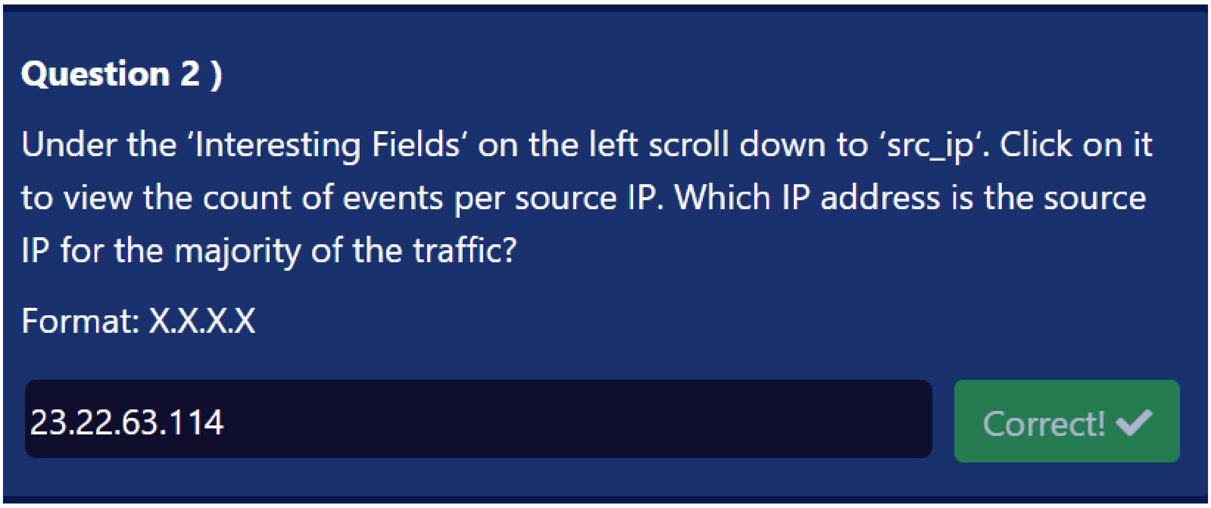
425



New Search

```
1  index="botsv1" sourcetype="stream:http" http_method=POST uri="/joomla/administrator/index.php"
```

✓ **425 events** (before 1/18/26 3:58:52.000 PM) No Event Sampling ▾

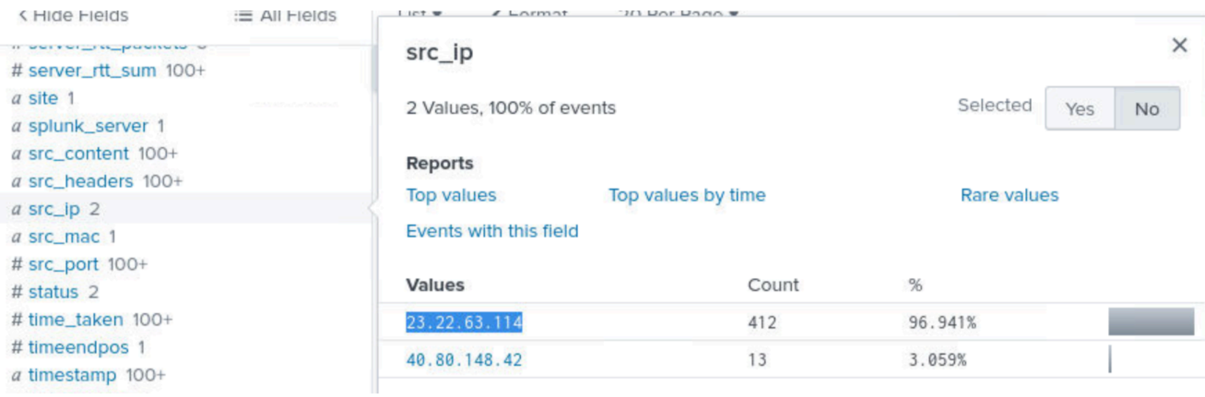


Question 2)

Under the ‘Interesting Fields’ on the left scroll down to ‘src_ip‘. Click on it to view the count of events per source IP. Which IP address is the source IP for the majority of the traffic?

Format: X.X.X.X

23.22.63.114



server_rtt_sum 100+
a site 1
a splunk_server 1
a src_content 100+
a src_headers 100+
a src_ip 2
a src_mac 1
src_port 100+
status 2
time_taken 100+
timeendpos 1
a timestamp 100+

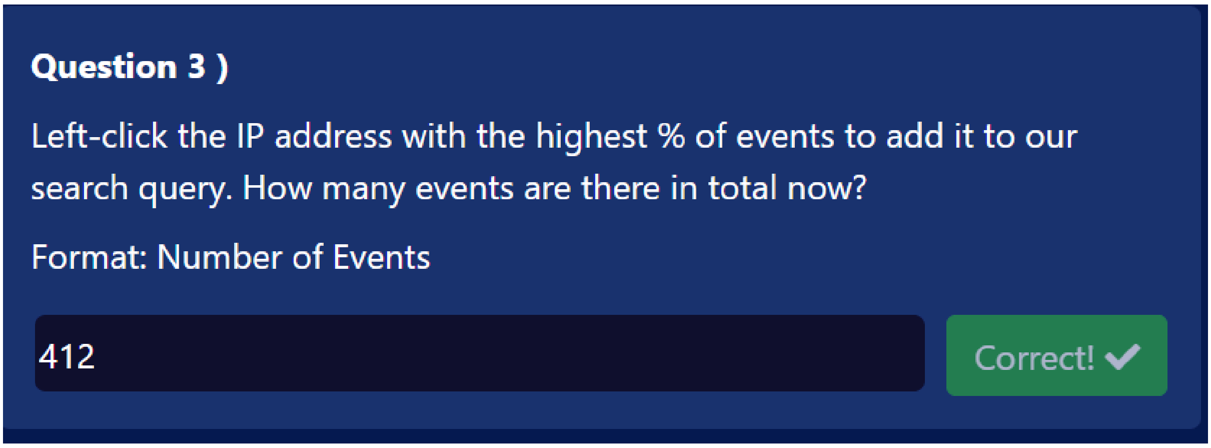
src_ip

2 Values, 100% of events

Selected Yes [✓ No]

Reports

Values	Count	%
23.22.63.114	412	96.941%
40.80.148.42	13	3.059%

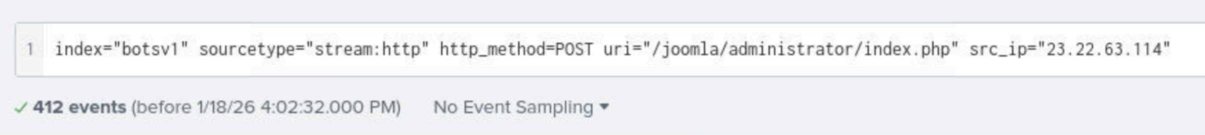


Question 3)

Left-click the IP address with the highest % of events to add it to our search query. How many events are there in total now?

Format: Number of Events

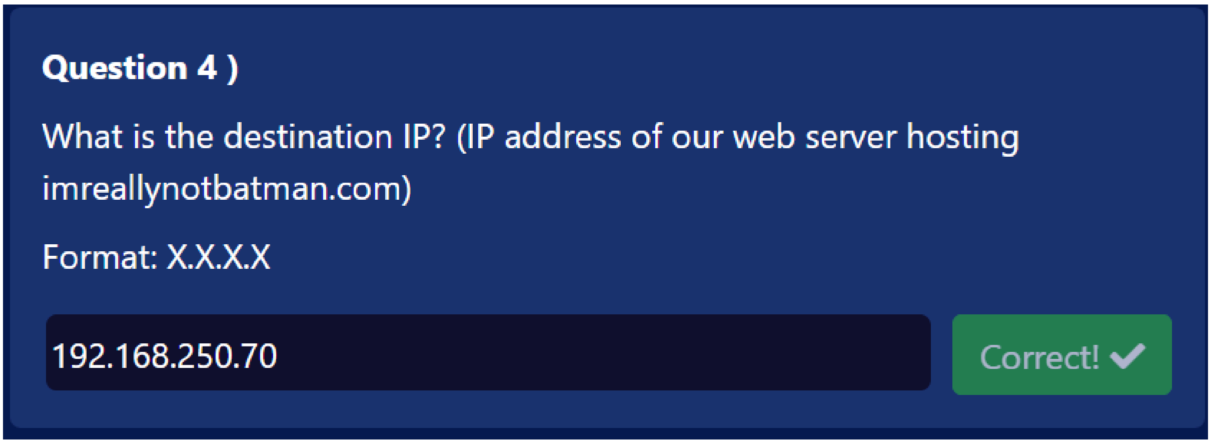
412



```
index="botsv1" sourcetype="stream:http" http_method=POST uri="/joomla/administrator/index.php" src_ip="23.22.63.114"
```

✓ **412 events** (before 1/18/26 4:02:32.000 PM)

Ju I clicked in the ip and I had the events.

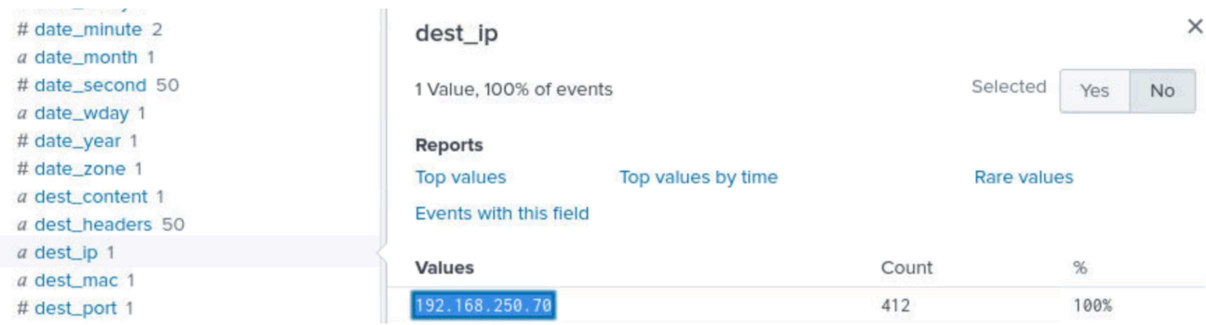


Question 4)

What is the destination IP? (IP address of our web server hosting imreallynotbatman.com)

Format: X.X.X.X

192.168.250.70



date_minute 2
a date_month 1
# date_second 50
a date_wday 1
# date_year 1
# date_zone 1
a dest_content 1
a dest_headers 50
a dest_ip 1
a dest_mac 1
# dest_port 1

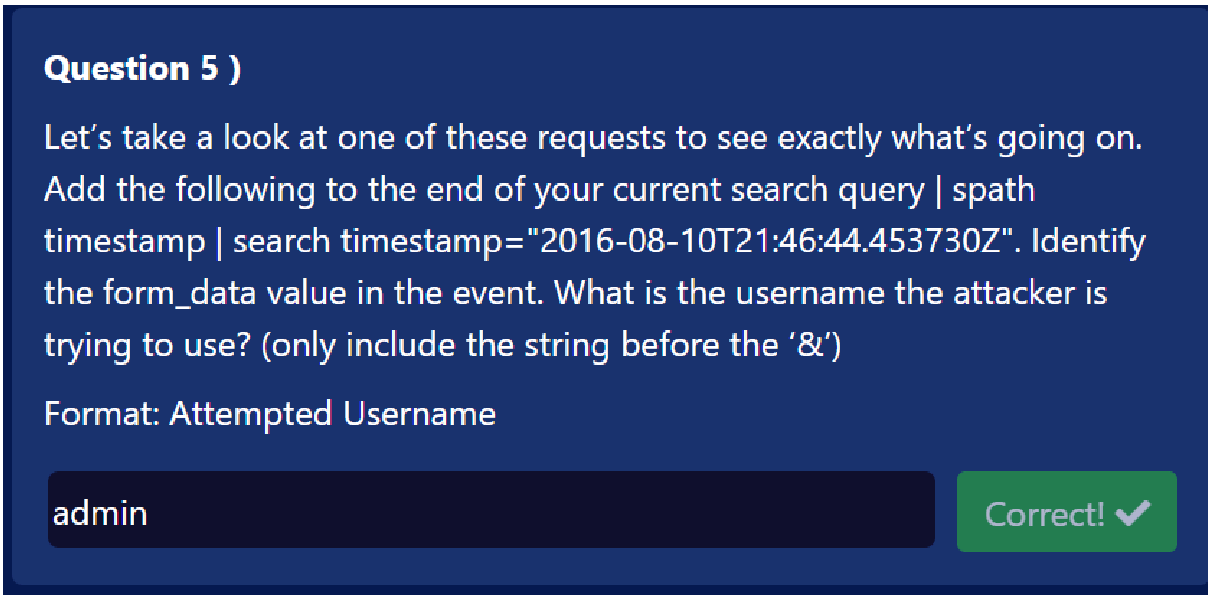
dest_ip

1 Value, 100% of events

Selected: Yes [✓ No]

Reports

Values	Count	%
192.168.250.70	412	100%

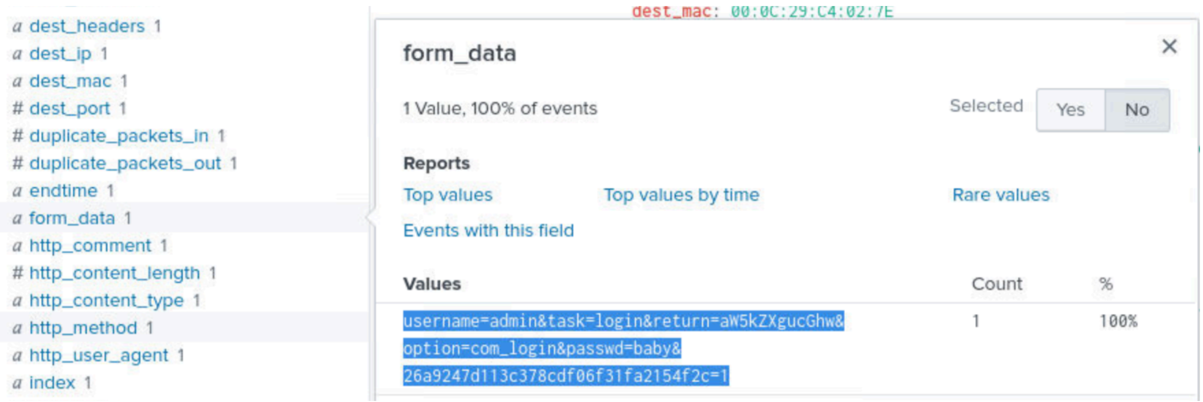


Question 5)

Let’s take a look at one of these requests to see exactly what’s going on. Add the following to the end of your current search query | spath timestamp | search timestamp="2016-08-10T21:46:44.453730Z". Identify the form_data value in the event. What is the username the attacker is trying to use? (only include the string before the ‘&’)

Format: Attempted Username

admin



dest_mac: 00:0C:29:C4:02:7E

```
a dest_headers 1
a dest_ip 1
a dest_mac 1
# dest_port 1
# duplicate_packets_in 1
# duplicate_packets_out 1
a endtime 1
a form_data 1
a http_comment 1
# http_content_length 1
a http_content_type 1
a http_method 1
a http_user_agent 1
a index 1
```

form_data

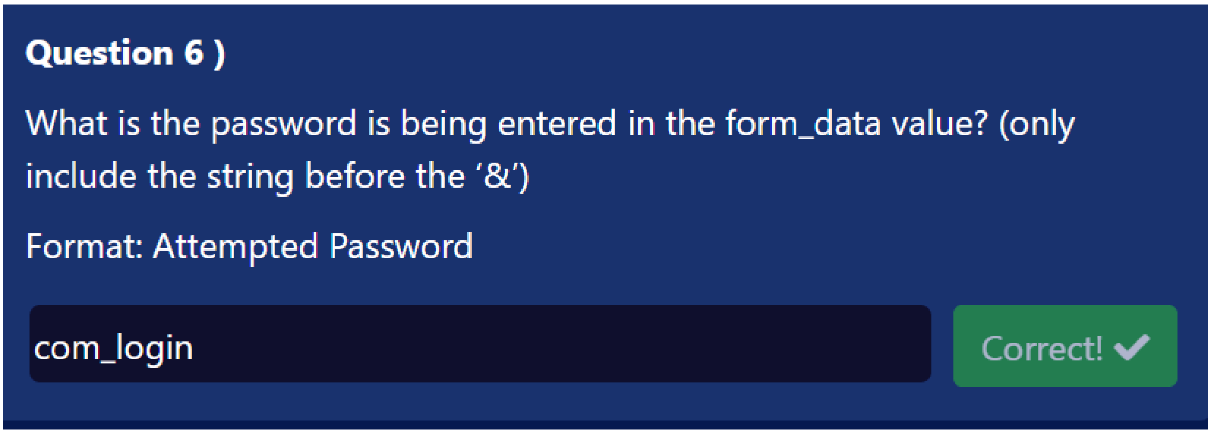
1 Value, 100% of events

Selected: Yes [✓ No]

Reports

Values	Count	%

username=admin&task=login&return=aW5kZXgucGhw&
option=com_login&passwd=baby&
26a9247d113c378cdf06f31fa2154f2c=1
	1	100%



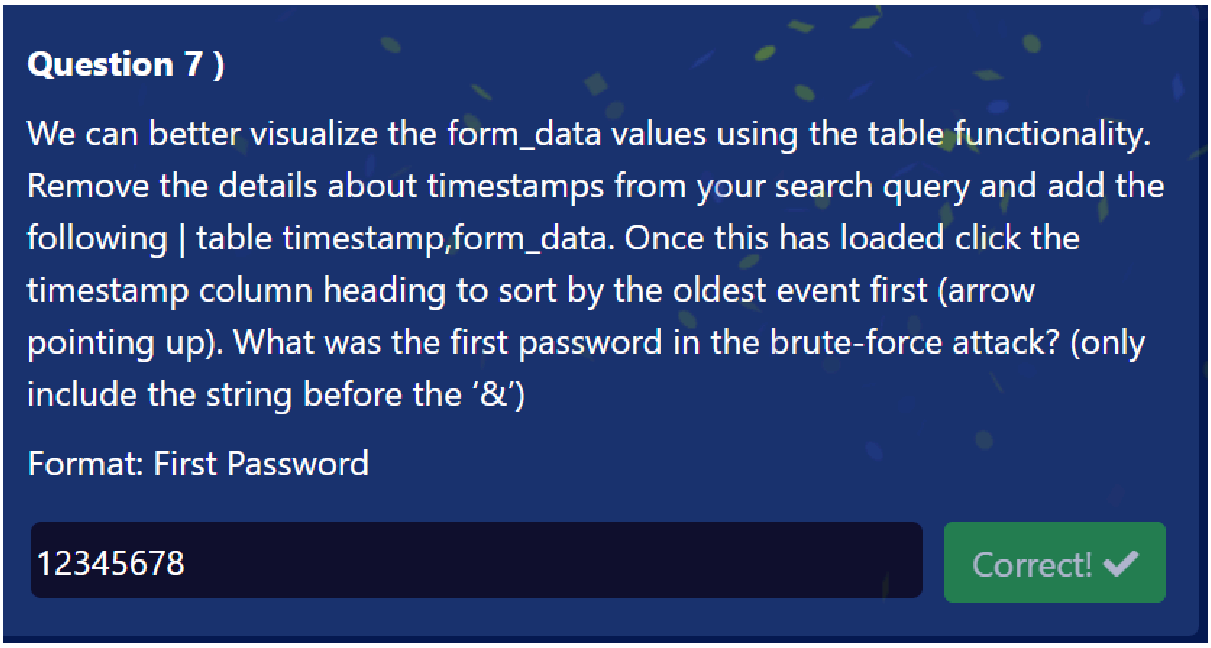
Question 6)

What is the password is being entered in the form_data value? (only include the string before the ‘&’)

Format: Attempted Password

com_login

I answer this question with the same information I had in question 5.

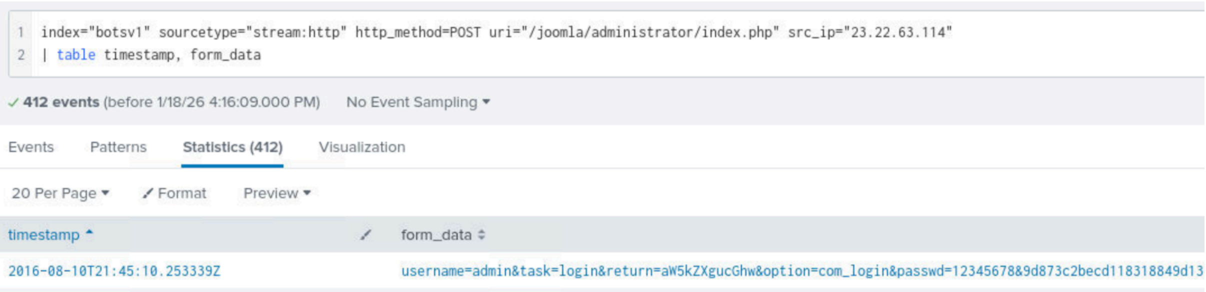


Question 7)

We can better visualize the form_data values using the table functionality. Remove the details about timestamps from your search query and add the following | table timestamp,form_data. Once this has loaded click the timestamp column heading to sort by the oldest event first (arrow pointing up). What was the first password in the brute-force attack? (only include the string before the '&')

Format: First Password

12345678



```
index="botsv1" sourcetype="stream:http" http_method=POST uri="/joomla/administrator/index.php" src_ip="23.22.63.114"
| table timestamp, form_data
```

✓ **412 events** (before 1/18/26 4:16:09.000 PM)

timestamp ▴	form_data ⇕
2016-08-10T21:45:10.253339Z	username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=12345678&9d873c2becd118318849d13