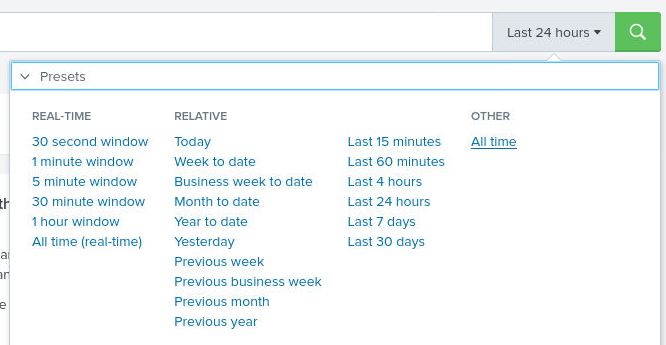
**Lab) Splunk Investigation 1 Solution**

1. Security Information and Event Monitoring
2. Using Splunk SIEM
3. Lab) Splunk Investigation 1 Solution

To get Splunk ready, we'll open a Terminal using the icon on the bottom toolbar and enter in the following command: **sudo systemctl start Splunkd**. After a minute we'll open Firefox and visit **127.0.0.1:8000**. Next we'll click on the ‘Search & Reporting’ app on the left-hand side of the Splunk homepage.

We need to make sure we can see all of the logs as they were generated back in 2020. To do this we'll click on the timeframe selector on the far right and select OTHER > All time on the right.



We're ready to get started with the lab questions!

**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?**

We can copy this search query from the Questions tab to the Clipboard tab, then paste it within the lab machine. Reading the Instructions tab of the lab we can understand what this search query is looking for “As a starting point, we know the administrator URL is [*http://imreallynotbatman.com/joomla/administrator/index.php*](http://imreallynotbatman.com/joomla/administrator/index.php)and that usernames and passwords will be submitted in an HTTP POST request (http\_method=POST)”. Essentially, we're looking for traffic that represents attempted logins to the website.

We should allow the search a few minutes to populate to ensure we don't miss anything important. Remember, Splunk has to search through every single log ingested into the SIEM to find ones that match our query. When the search is complete, we'll see a green tick on the left below the search bar:

A screenshot of a web page

Description automatically generated

The number of events in bold is the answer to this question.

**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?**

Following the steps in the question, we can see that two IPs have sent POST requests to this specific URL, with the IP 23[.]22.63.114 being the most active source IP with almost 97% of the traffic.

A screenshot of a graph

Description automatically generated

**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?**

After clicking the IP address it'll automatically add it to our search. After a few seconds, we can see that this query matches 412 events.

A screenshot of a computer

Description automatically generated

**Question 4 - What is the destination IP? (IP address of our web server hosting imreallynotbatman.com)**

There's two ways we can find the IP address of our web server:

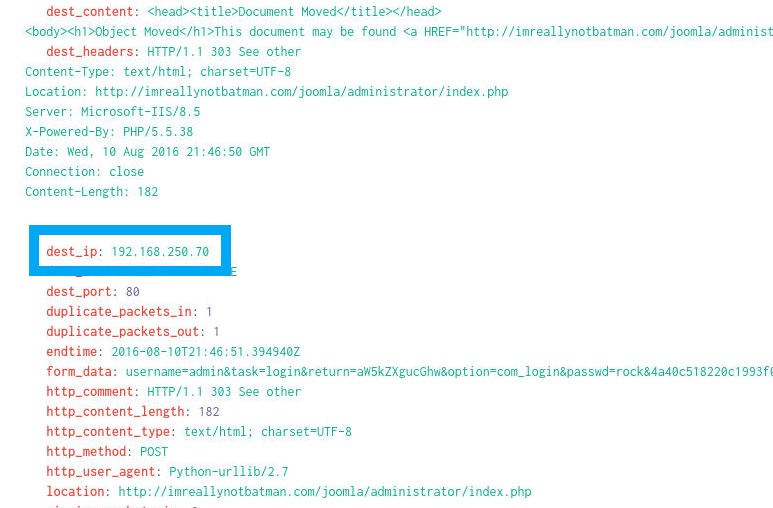
* Option One - Investigate the Interesting Fields panel and look for a property that represents the destination IP field (such as dst\_ip or similar).
* Option Two - Look through any event using the Event Details panel, as our search query is looking specifically at HTTP POST requests to the website, it will definitely contain the destination IP.

Let's go through both of these together. Starting with Option One we'll scroll down the Interesting Fields panel we'll find ‘dest\_ip’. Clicking this will show us the private (internal) IP of the web server!

A screenshot of a cell phone

Description automatically generated

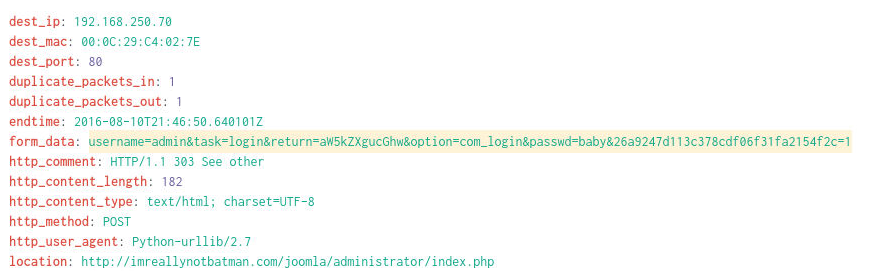
Alternatively, we could look at the details for any event. Looking through the properties and values, we can find dest\_ip this way too!



**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 ‘&’)**

By copying this query text into our current search query we are selecting any events at the specific timestamp, which results in 1 event being shown. We're in a situation similar to the previous question, where we can either look at the Interesting Fields to find the form\_data property and values or look through the raw event details.

Scrolling through the event details, we can find the property we're interested in.



From the above screenshot we can see the username and password that were submitted by the login form to the web server.

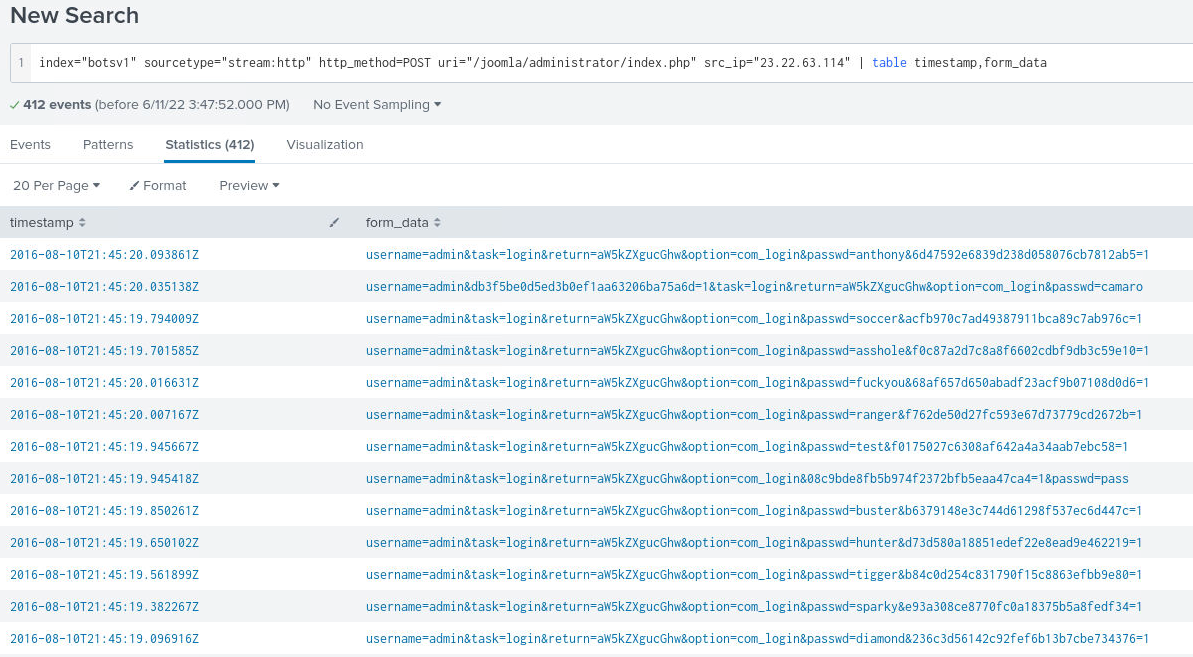
**Question 6 - What is the password is being entered in the form\_data value? (only include the string before the ‘&’)**

Looking at the screenshot above in Q5, we can see the password required to answer this question.

**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 ‘&’)**

By removing the section of our query regarding timestamps, and adding in the text from this question, our final search query will be **index="botsv1" sourcetype="stream:http" http\_method=POST uri="/joomla/administrator/index.php" src\_ip="23.22.63.114" | table timestamp,form\_data**.

By creating a table showing only the timestamp and form\_data fields, it's much easier for us to view the usernames and passwords used in this apparent bruteforce attack against a login form.



To find the first password used in the attack, we can click on the ‘Timestamp’ column heading to change the sorting. Clicking it once will show a down arrow, so the first result is the most recent. Clicking it again will show an up arrow, so the first result is the oldest, which is what we want!