Cybersecurity

Module 19 Challenge Submission File

Let's Go Splunking!

Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

Step 1: The Need for Speed

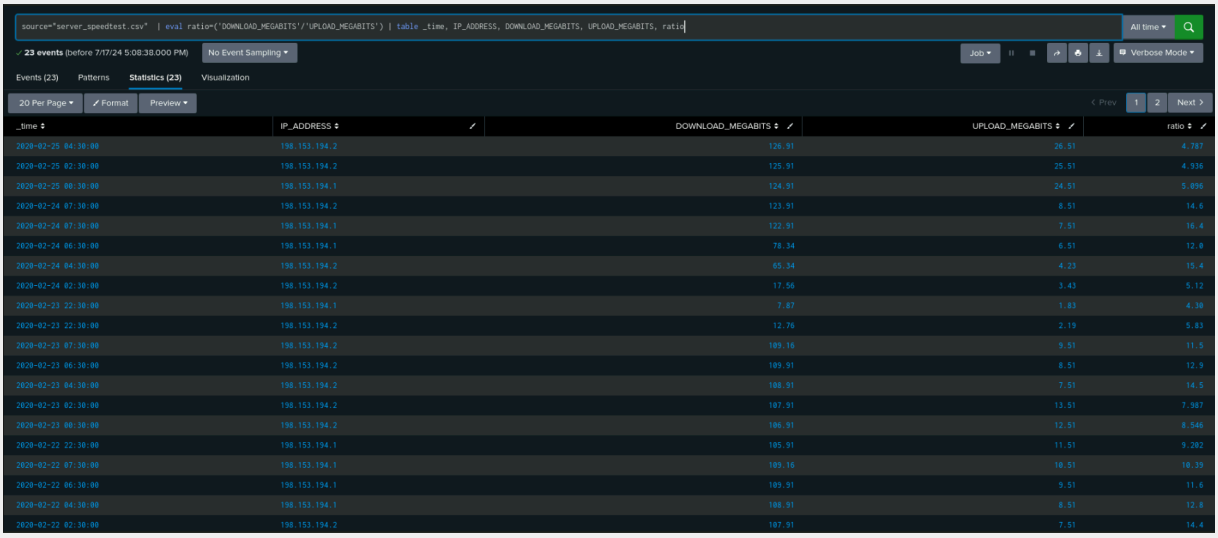
1. Based on the report you created, what is the approximate date and time of the attack?

```
DDOS attack occurred approx 830pm on 23.02.2020. This is where the download
and upload speeds significantly drop compared to the average speeds.
```

2. How long did it take your systems to recover?

```
The speeds get back to normal indicating that the attack ends approx 730am
24.02.2020, making the attack last for about 11 hours.
```

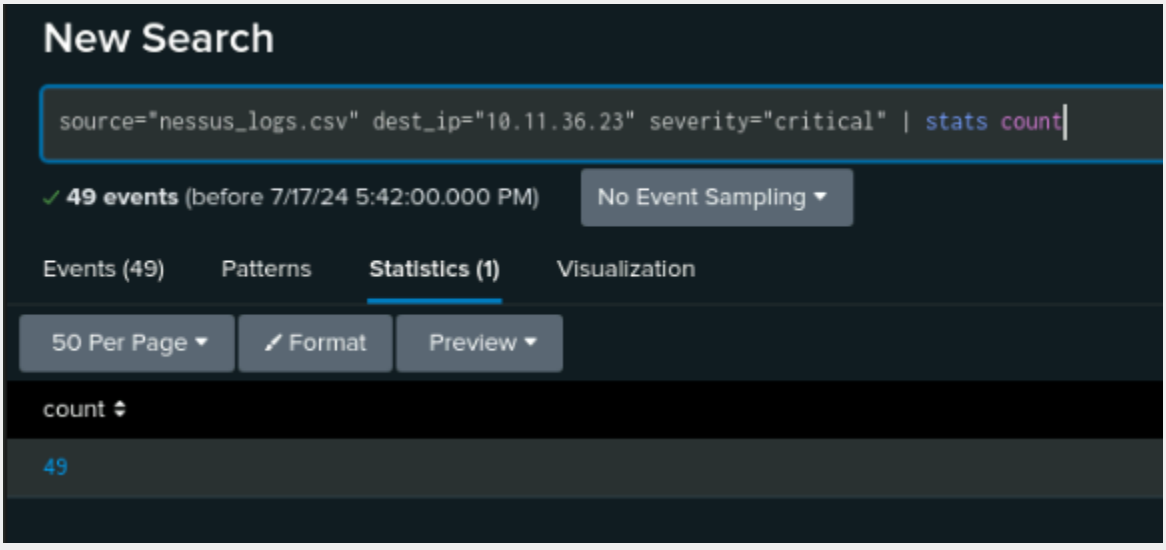
Provide a screenshot of your report:



Step 2: Are We Vulnerable?

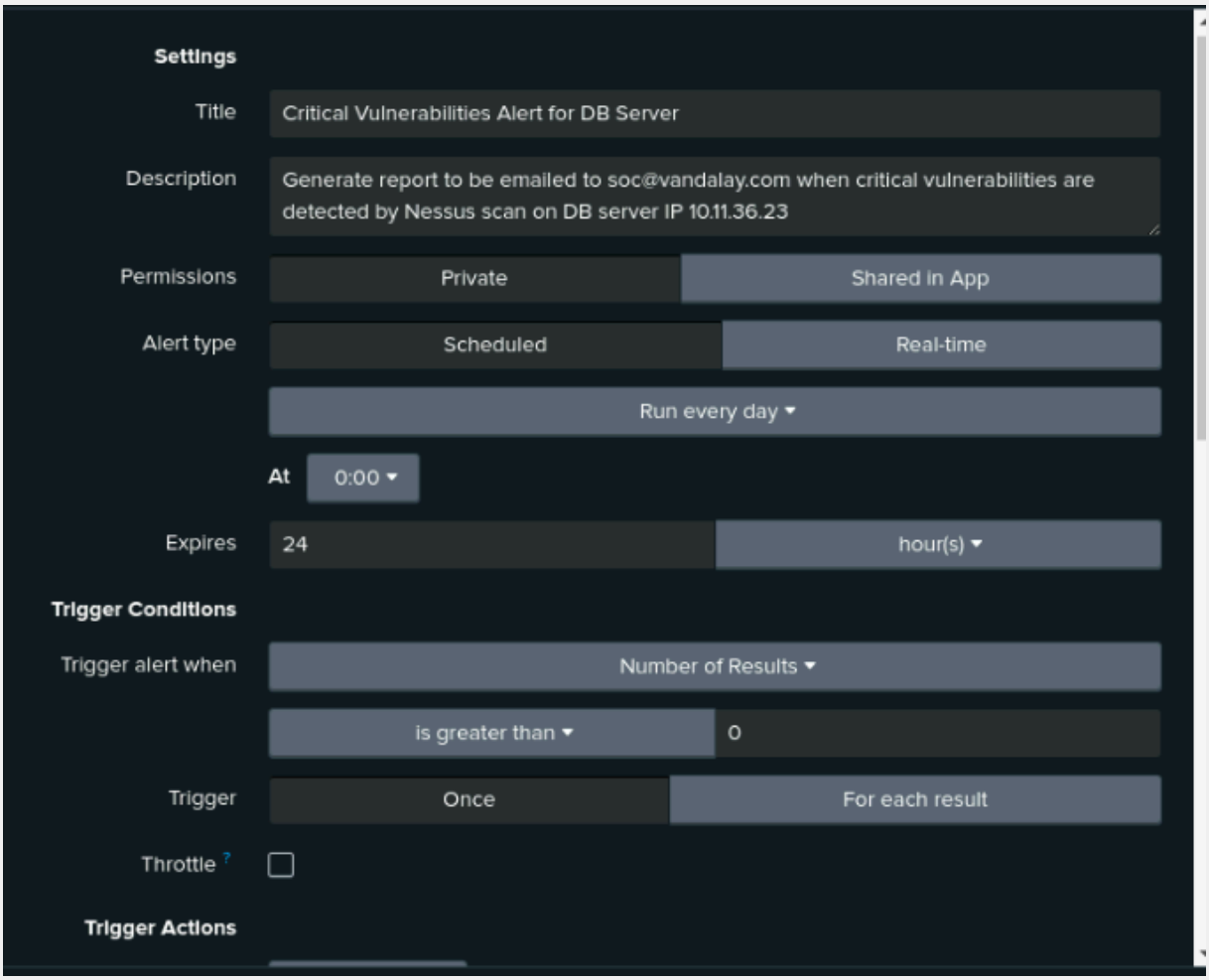
Provide a screenshot of your report:

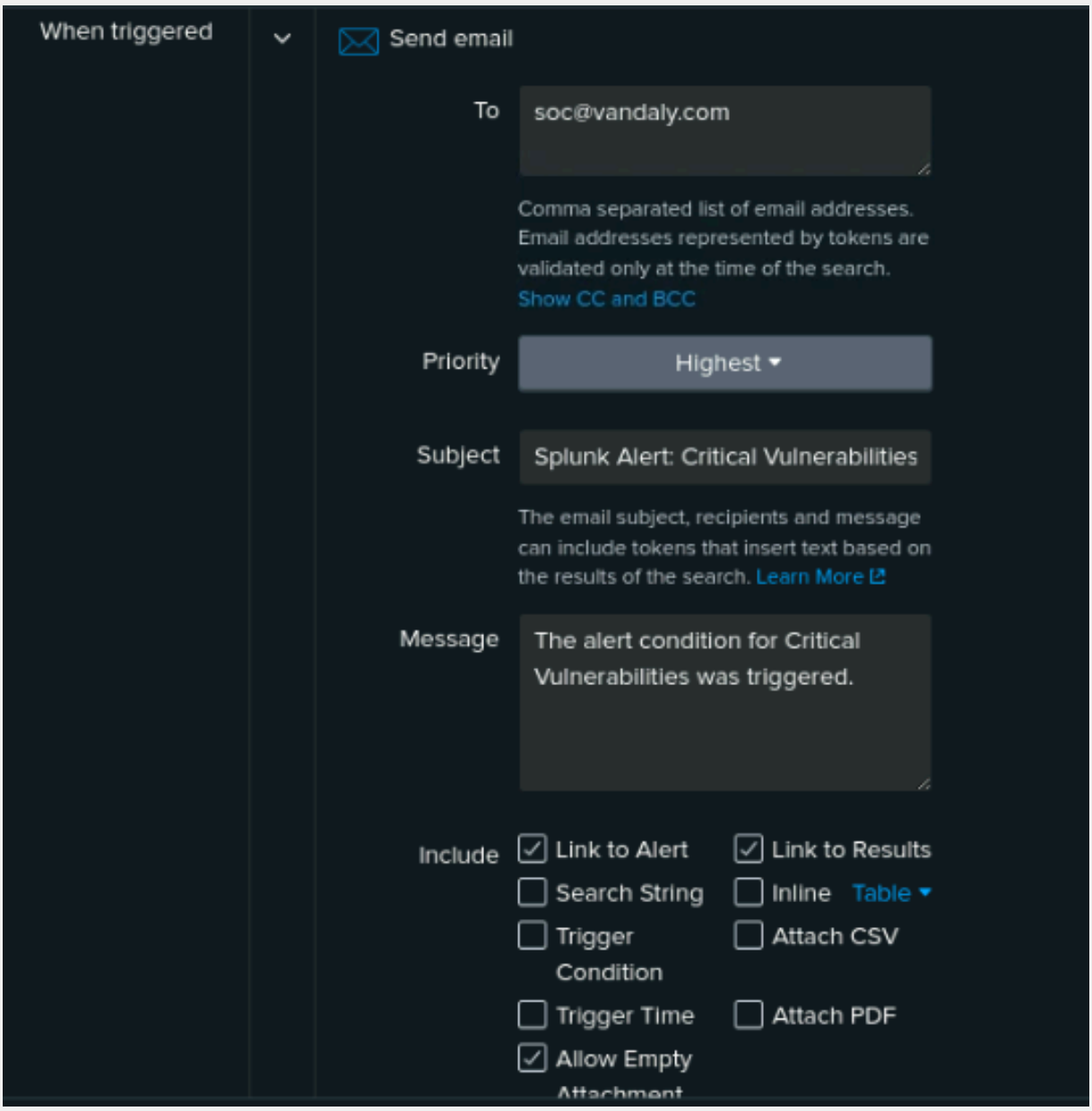
```
Using the below command, we can see that there are 49 counts of critical vulnerabilities for the provided IP address.

source="nessus_logs.csv" dest_ip="10.11.36.23" severity="critical" | stats count
```



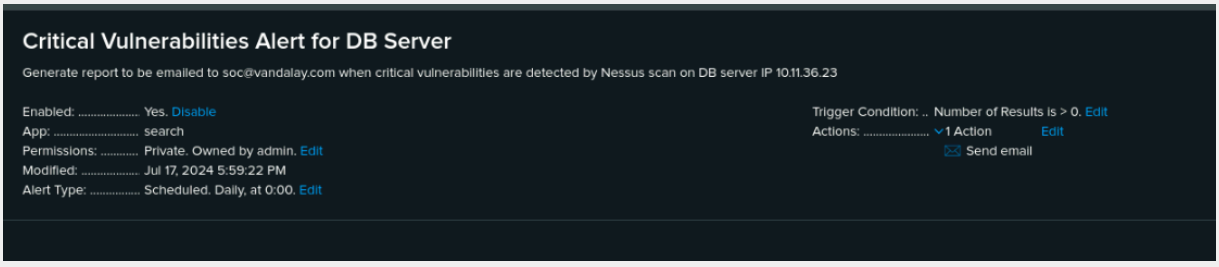
Provide a screenshot showing that the alert has been created:

Create the alert by clicking 'save as' and then 'alert' after we've generated our results from the query above:





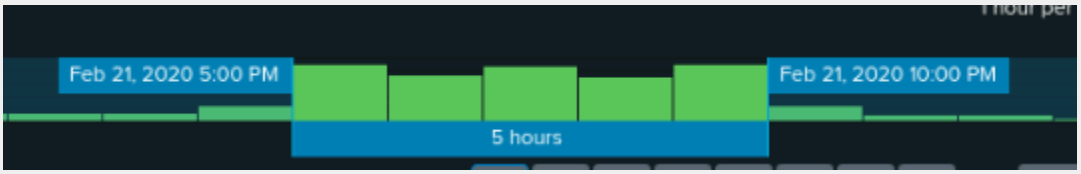
Then once saved, we can see the alert.



Step 3: Drawing the (Base)line

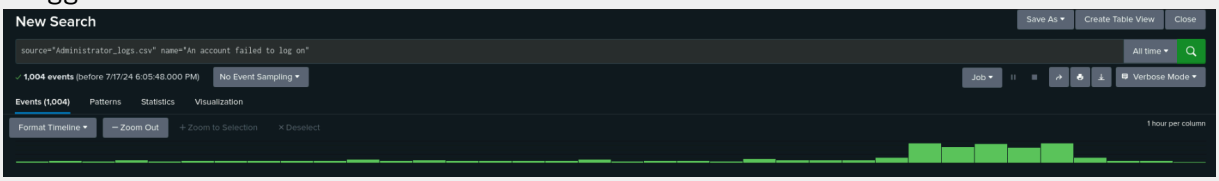
1. When did the brute force attack occur?

```
The brute force attack occurred at approx 5pm on 21.02.2020 and lasted for
approx 5 hours, finishing around 10pm.
```



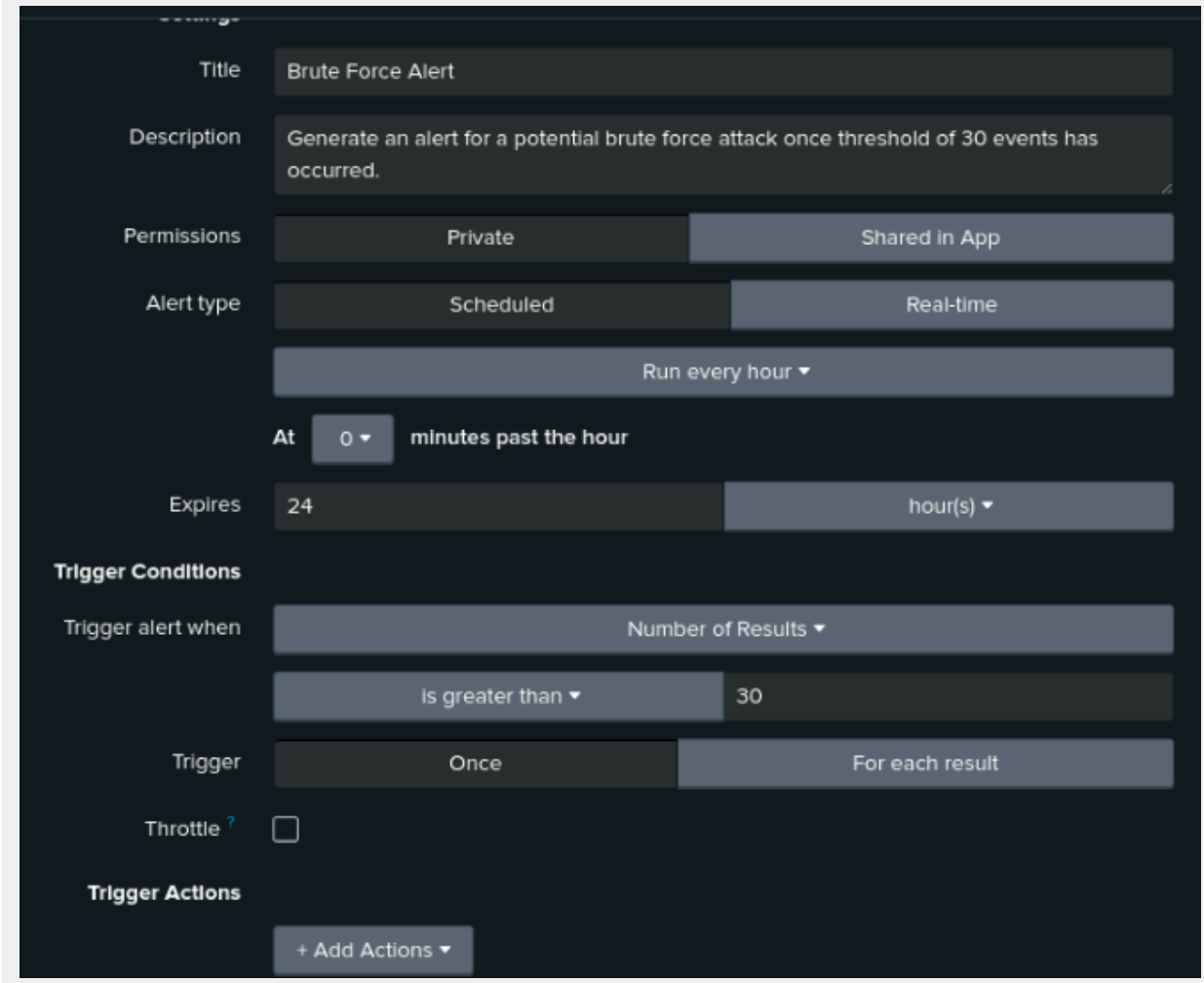
2. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring:

```
Considering that the range of events is 6 to 34 pre and post attack, we can
assume a normal baseline of 30 events. I would set a scale for alert as

0 - 25  = green alert
25 - 50 = amber alert
50+     = red alert

The threshold I will be setting in the alert will be 30 events, which will
trigger an email to be sent to the soc team.
```



3. Provide a screenshot showing that the alert has been created:

```
Same as above, used the Save As > Alert tabs to create the alert.
Set to run every hour triggered when 30 events occur, sending a highest
priority email to the soc team for further investigation.
```


Title
Brute Force Alert
Description
Generate an alert for a potential brute force attack once threshold of 30 events has occurred.
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every hour
At
0
minutes past the hour
Expires
24
hour(s)
Trigger Conditions
Trigger alert when
Number of Results
is greater than
30
Trigger
Once
For each result
Throttle
Trigger Actions
+ Add Actions