| Cybersecurity |
| --- |
| Module 19 Challenge Submission File |

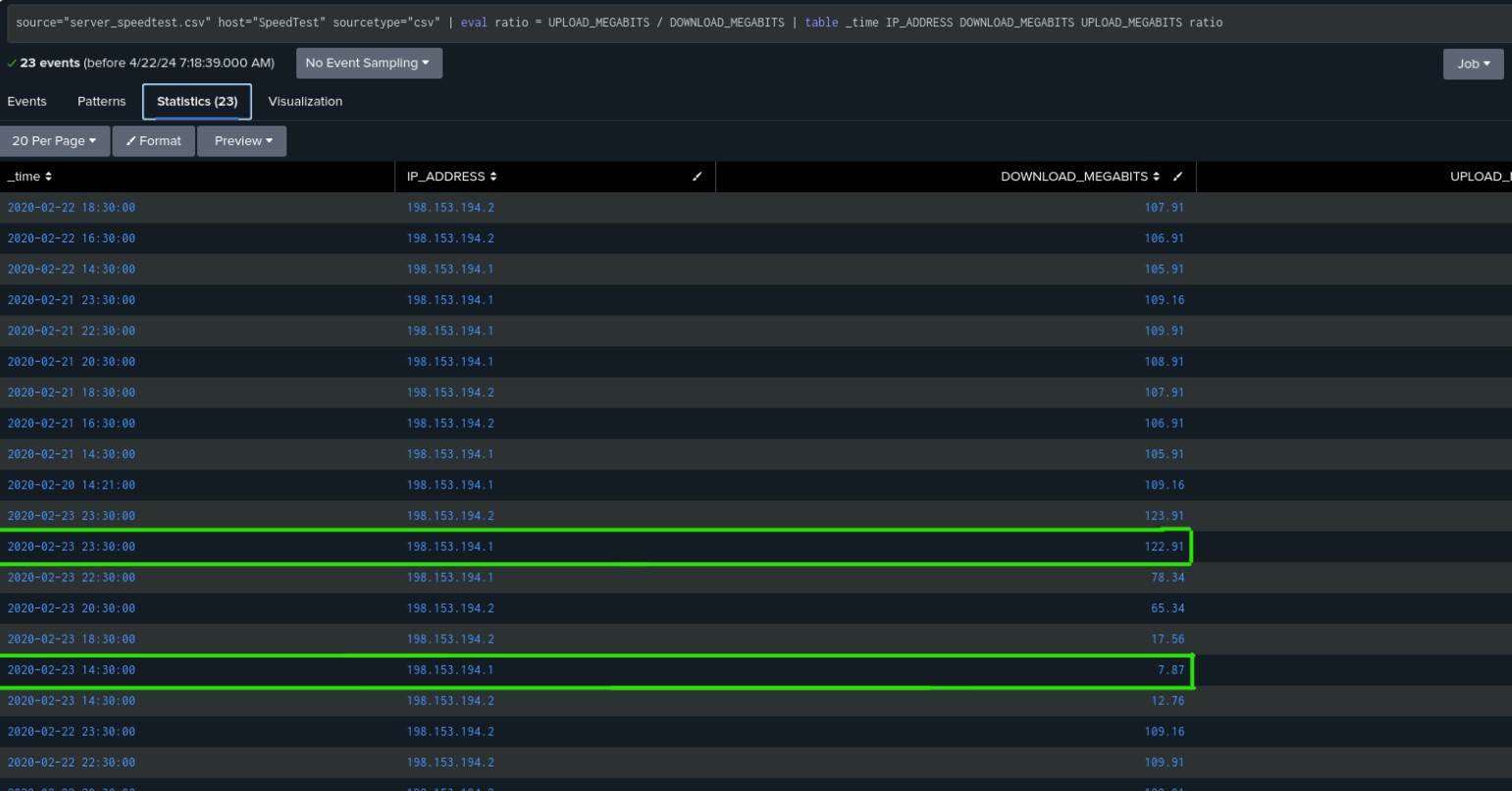
## Let’s Go Splunking!

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

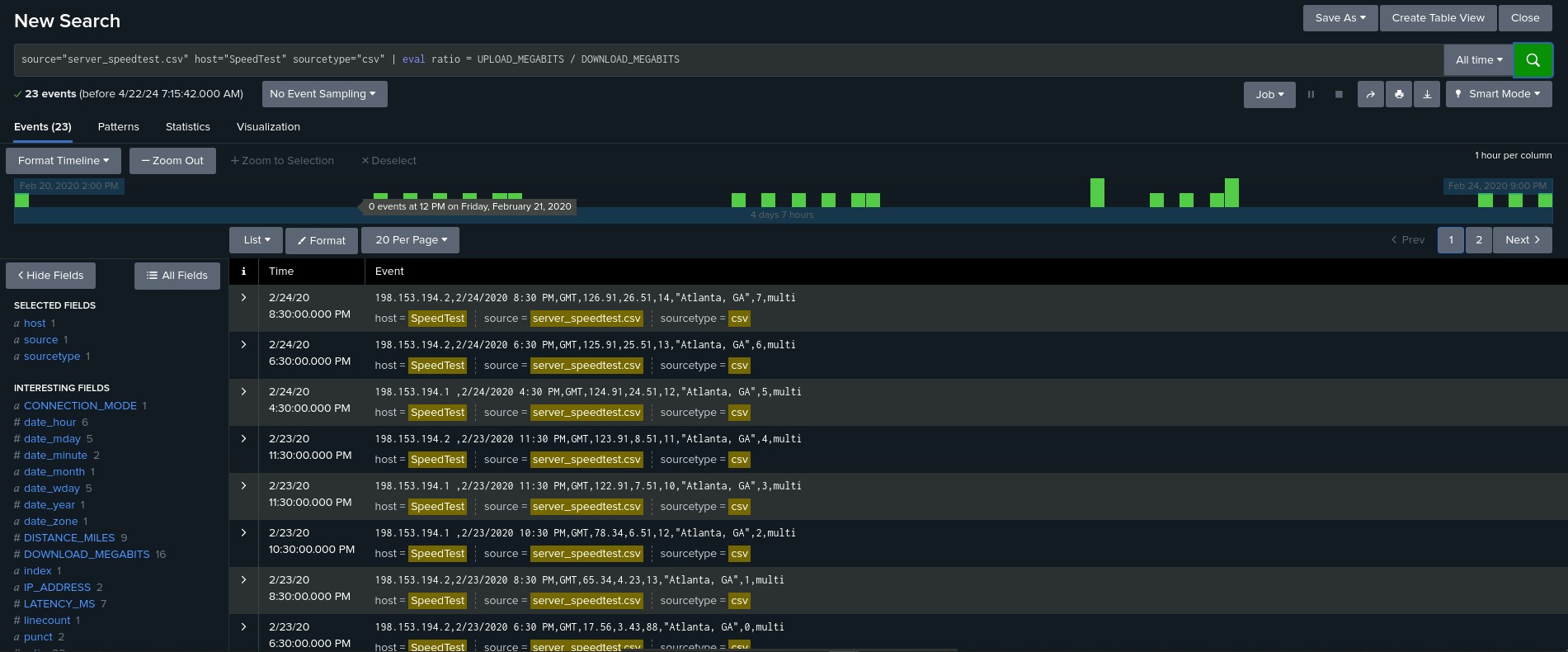
1. Based on the report you created, what is the approximate date and time of the attack?

The attack started on 23/02/2020 at approximately 11:30 as shown from this data



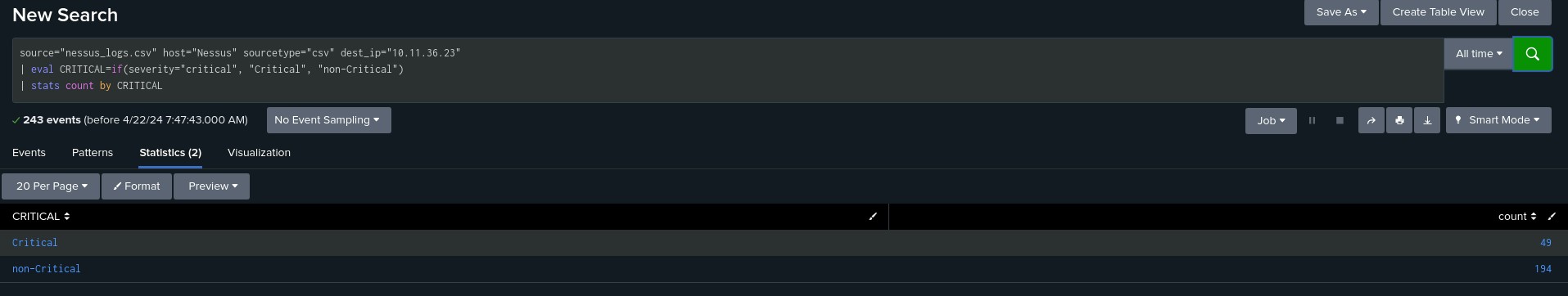
1. How long did it take your systems to recover?

| It took about 9 hours to recover |
| --- |

Provide a screenshot of your report:

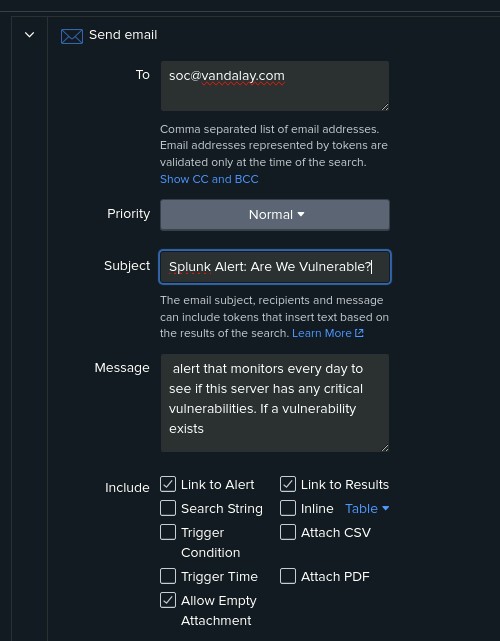
### Step 2: Are We Vulnerable?

Provide a screenshot of your report:



Provide a screenshot showing that the alert has been created:





### Step 3: Drawing the (Base)line

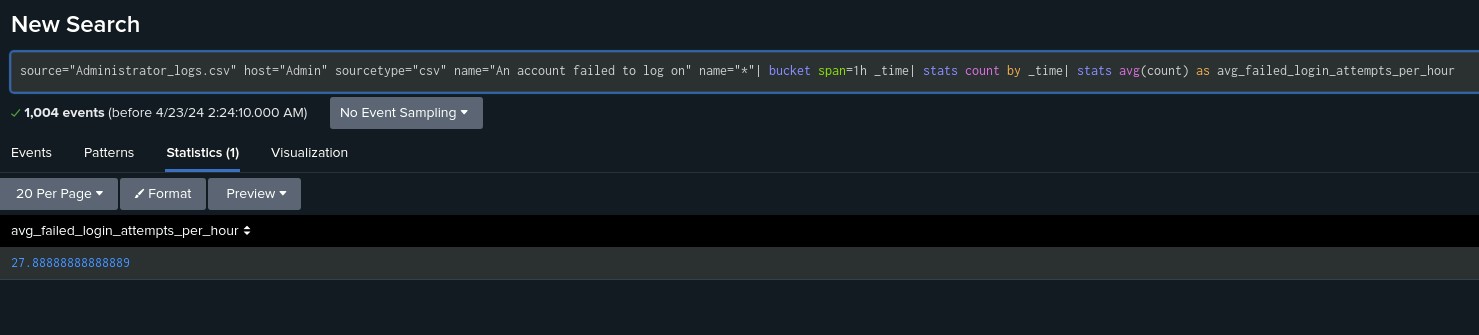
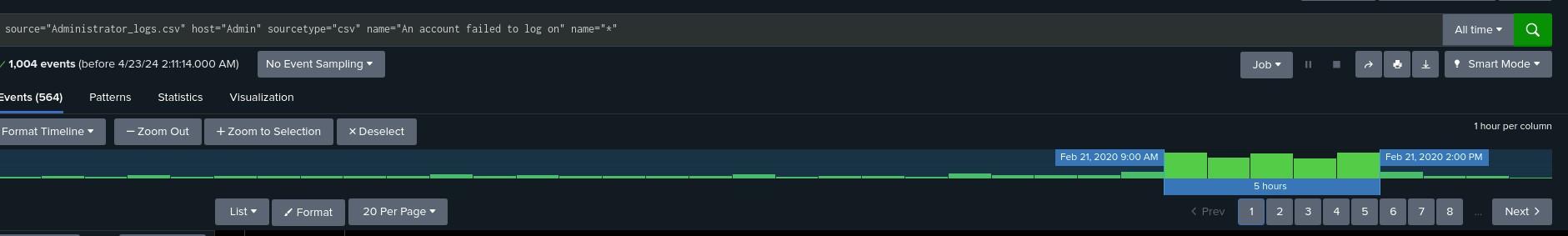
1. When did the brute force attack occur?

| The brute force attack happened on february 21st of 2020 at 9:00am and finished on february 21st of 2020 at 2:00pm the attack lasted 5 hours |
| --- |

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

Over the 36 hours that was recorded of the failed login attempts, none of them go over 30 failed attempts, with the outlier being the brute force attack. The threshold should be set at 40 due to the average of failed attempts being 27 from this query I created.





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



© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.