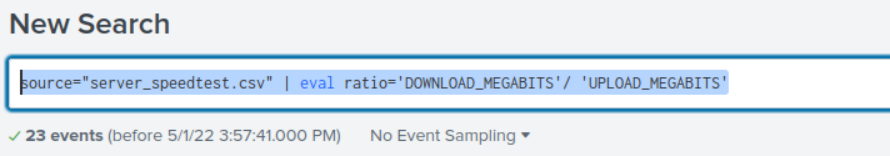
### **Using SIEM Project**

### **Step 1: The Need for Speed**

**Task:** Create a report to determine the impact that the DDOS attack had on download and upload speed. Additionally, create an additional field to calculate the ratio of the upload speed to the download speed.

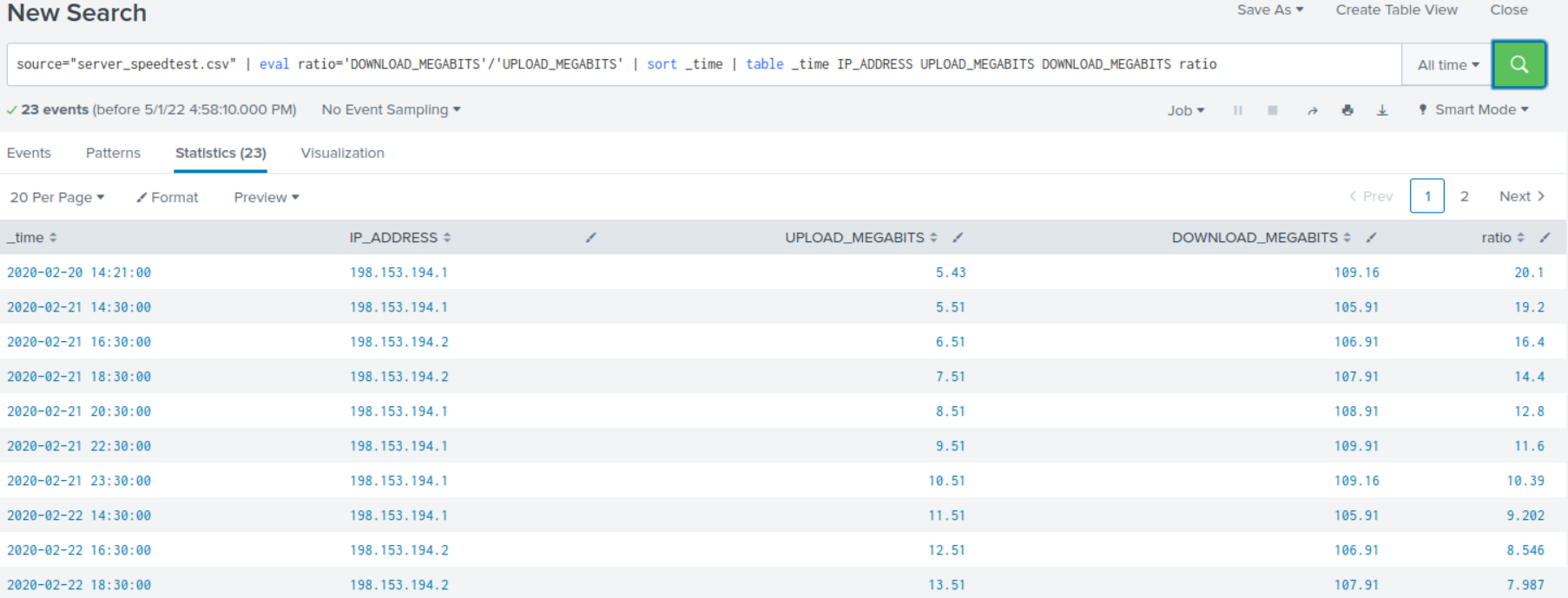
Upload the following file of the system speeds around the time of the attack. Speed Test File

Using the eval command, create a field called ratio that shows the ratio between the upload and download speeds. Hint: The format for creating a ratio is: | eval new\_field\_name = 'fieldA' / 'fieldB'



Create a report using the Splunk's table command to display the following fields in a statistics report:

* + \_time
  + IP\_ADDRESS
  + DOWNLOAD\_MEGABITS
  + UPLOAD\_MEGABITS
  + ratio

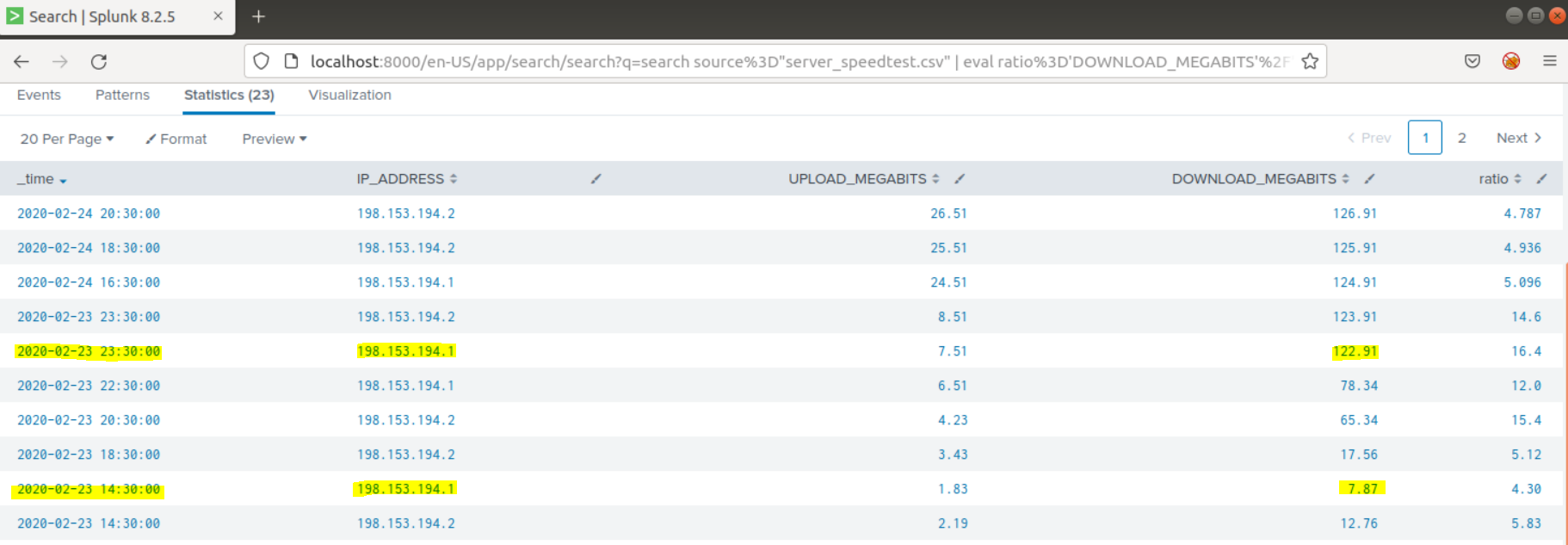


Answer the following questions:  
 Based on the report created, what is the approximate date and time of the attack?

**The attack happened on 2-23-2020 at 14:30 because the download megabits were 7.87.**

How long did it take your systems to recover?

**It took the system 9 hours to recover because the download megabits were back up to 122.91 at 23:30 on 2-23-2020.**



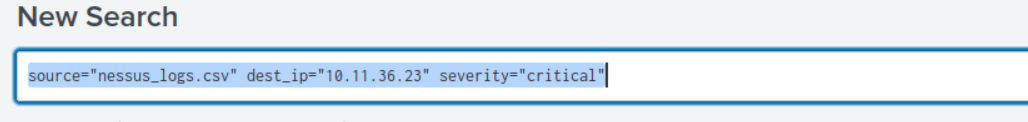
### **Step 2: Are We Vulnerable?**

**Background:** Due to the frequency of attacks, your manager needs to be sure that sensitive customer data on their servers is not vulnerable. Since Vandalay uses Nessus vulnerability scanners, you have pulled the last 24 hours of scans to see if there are any critical vulnerabilities.

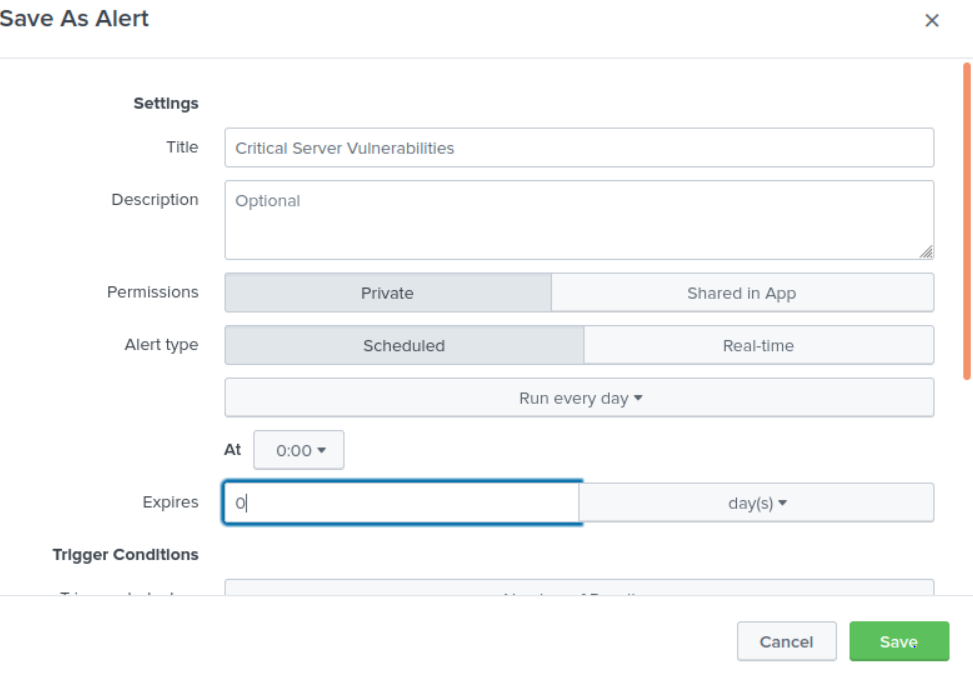
**Task:** Create a report determining how many critical vulnerabilities exist on the customer data server. Then, build an alert to notify your team if a critical vulnerability reappears on this server.

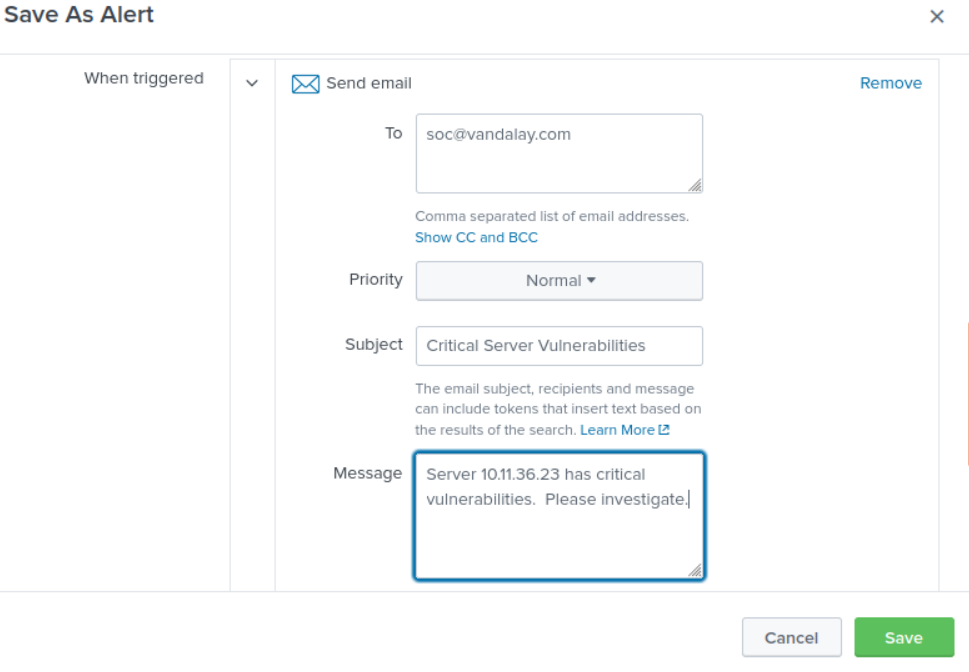
Upload the following file from the Nessus vulnerability scan. Nessus Scan Results

Create a report that shows the count of critical vulnerabilities from the customer database server. The database server IP is 10.11.36.23. The field that identifies the level of vulnerabilities is severity.



Build an alert that monitors every day to see if this server has any critical vulnerabilities. If a vulnerability exists, have an alert emailed to [soc@vandalay.com](mailto:soc@vandalay.com).



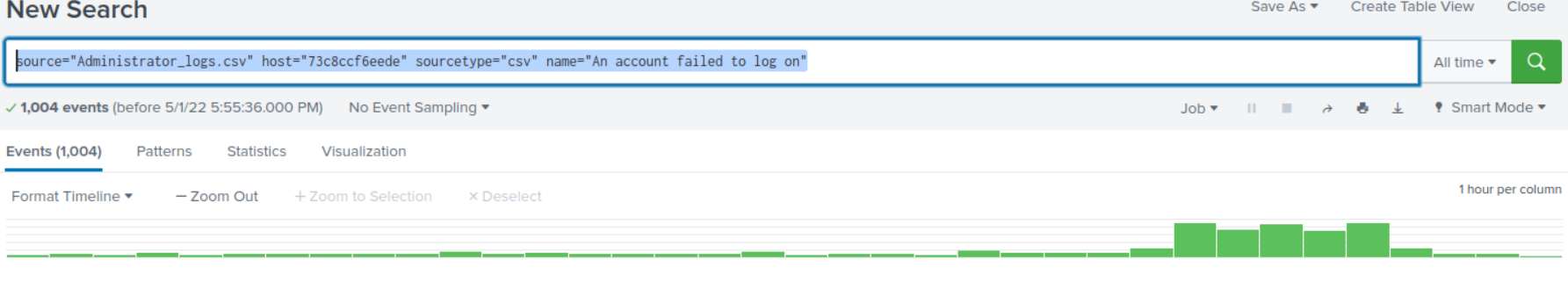


### **Step 3: Drawing the (base)line**

**Background:** A Vandaly server is also experiencing brute force attacks into their administrator account. Management would like you to set up monitoring to notify the SOC team if a brute force attack occurs again.

**Task:** Analyze administrator logs that document a brute force attack. Then, create a baseline of the ordinary amount of administrator bad logins and determine a threshold to indicate if a brute force attack is occurring.

Upload the administrator login logs. When did the brute force attack occur?



The brute force attack occurred on 2-21-2020 at 8:00 am. From 8:00 am to 2:00 pm on 2-21-2020, login attempts escalated from 34 events up to 124 events within a six hour span. Between the hours of 9:00 am to 2:00 pm the number of events rose to 124 events.

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

**I determined that 16 is my baseline for “account failed to log on”.**

Design an alert to check the threshold every hour and email the SOC team at SOC@vandalay.com if triggered.

