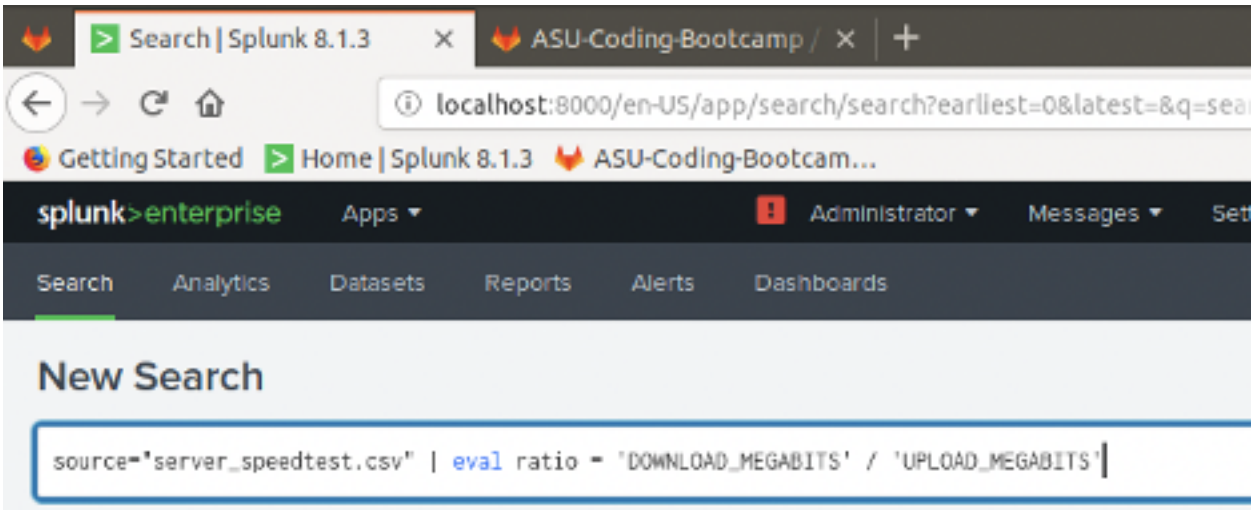
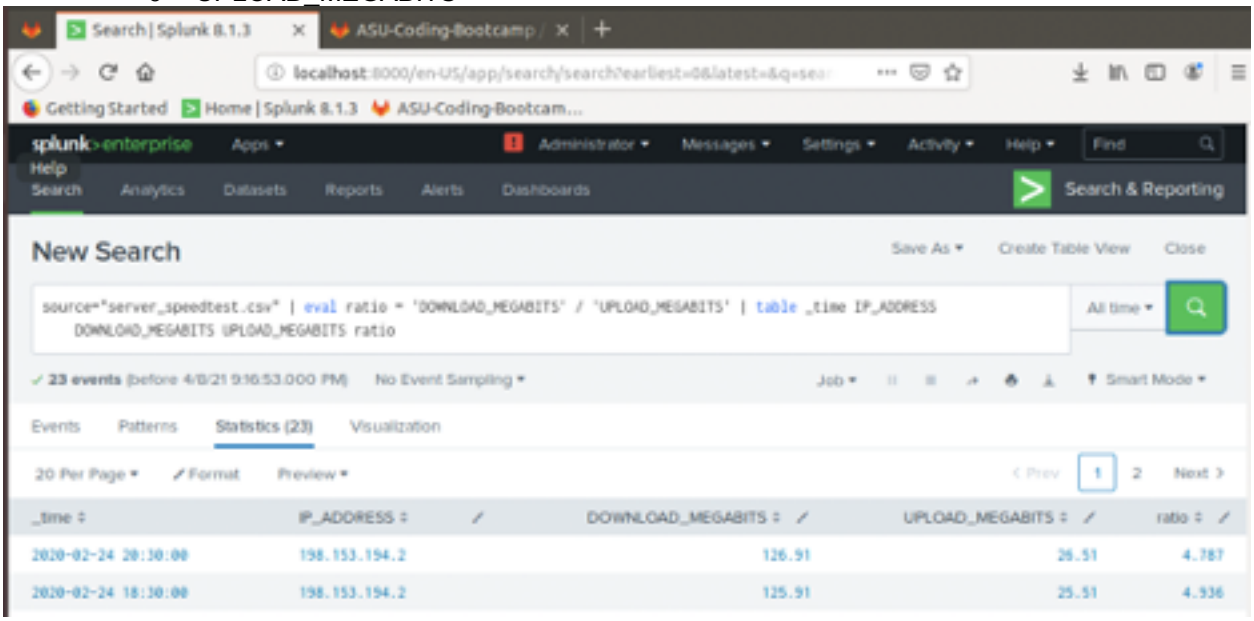
Week 18 Homework: SIEM I-Let's go Splunking

Step 1: The Need for Speed

1. Using the eval command, create a field called ratio that shows the ratio between the upload and download speeds.



2. 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

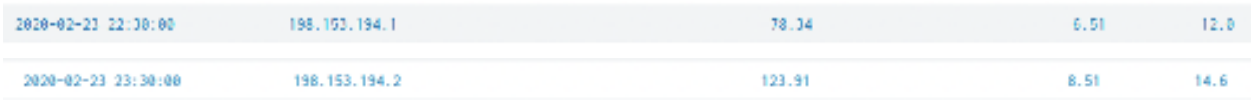


3. Based on the report created, what is the approximate date and time of the attack?

Answer: The approximate date and time was 2/23/20 at 2:30 p.m.

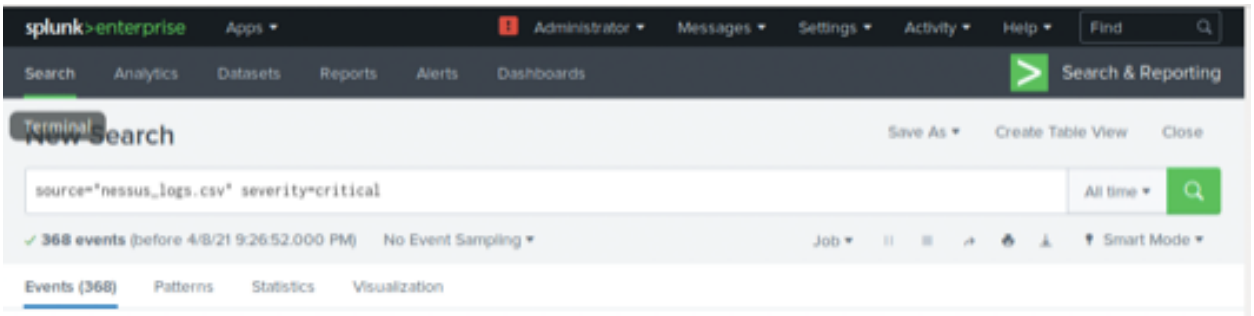
4. How long did it take your systems to recover?

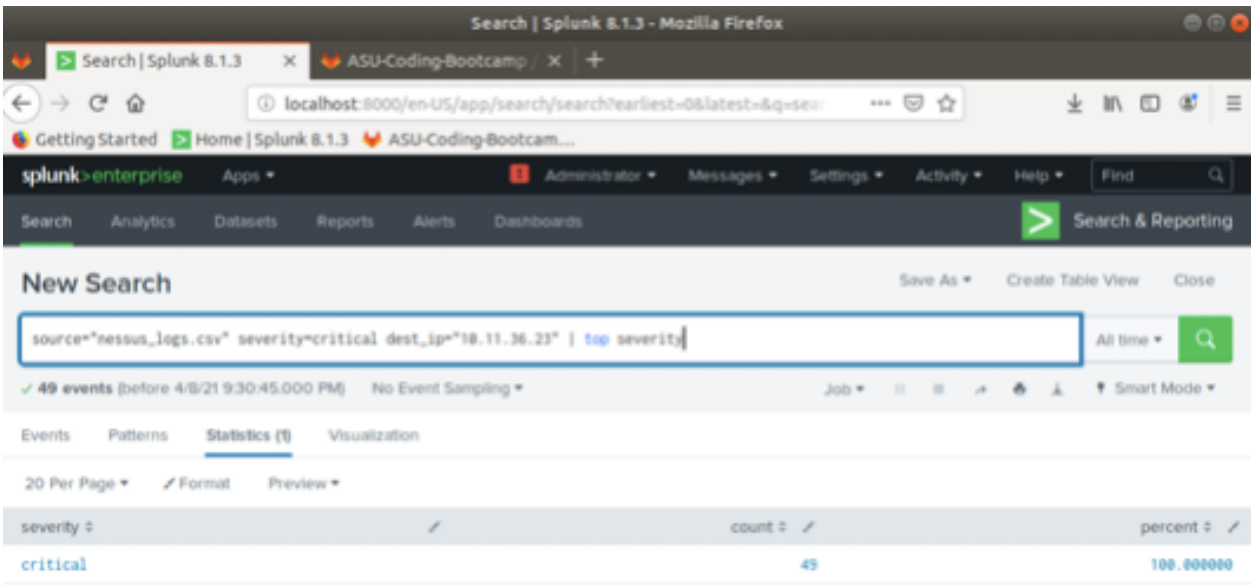
Answer: Recovery started at 10:30 p.m. and full recovery by 11:30 p.m.



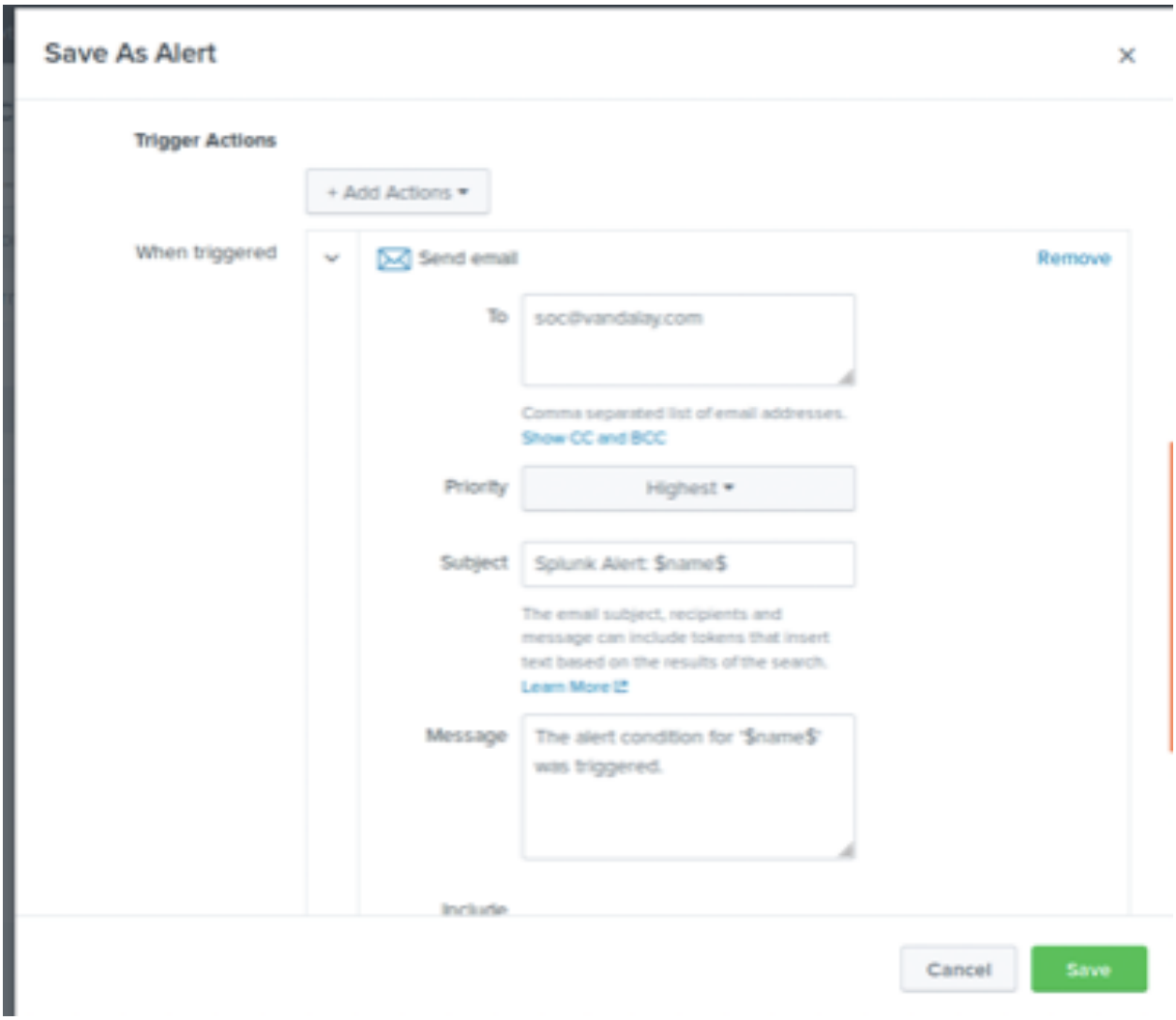
Step 2: Are We Vulnerable?

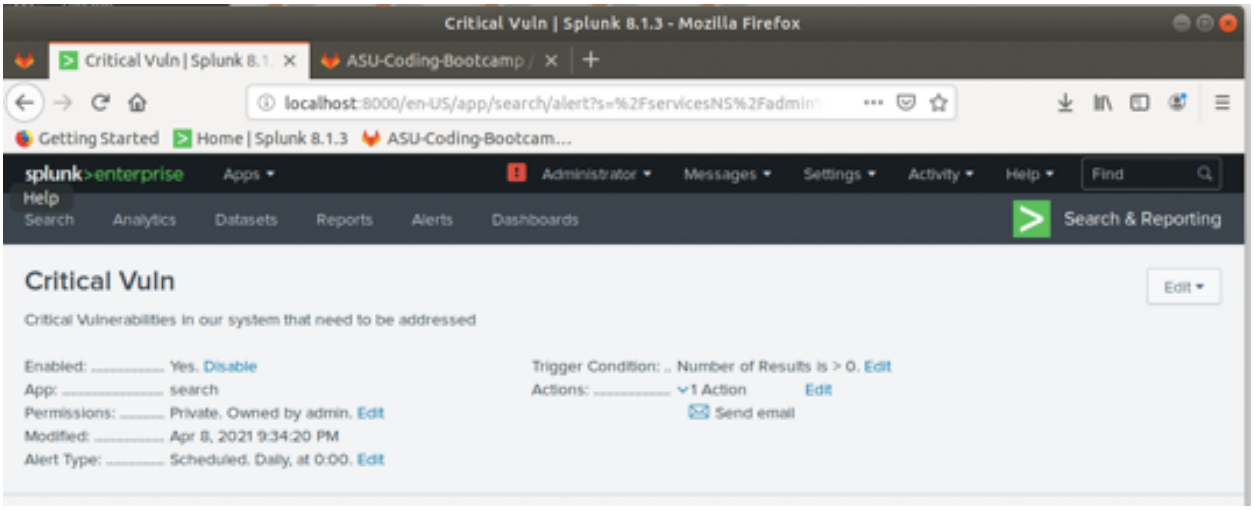
1. Create a report that shows the count of critical vulnerabilities from the customer database server.
    - The database server IP is 10.11.36.23.
    - The field that identifies the level of vulnerabilities is severity.





2. 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.





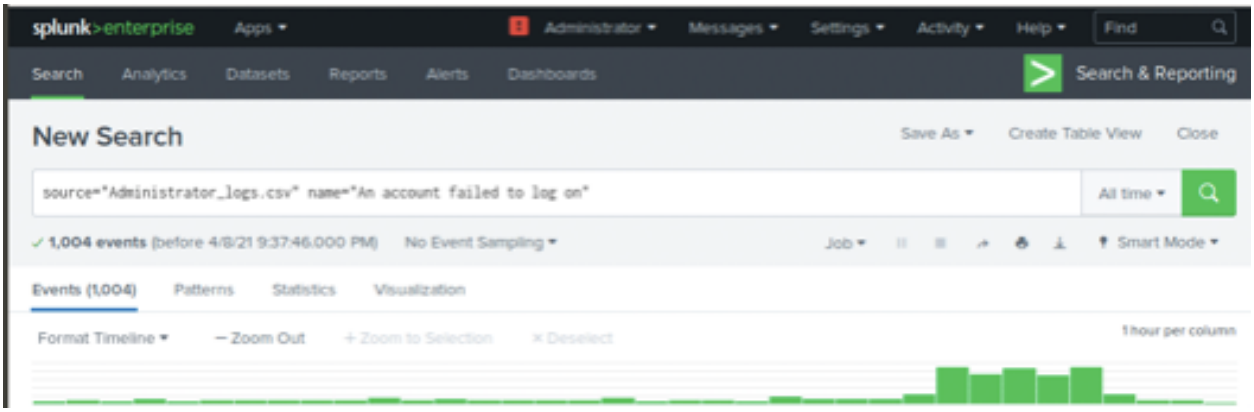
Step 3: Drawing the (base)line

1. When did the brute force attack occur?

Answer: The Brute Force Attack occurred at 9 a.m. on 2/21/20 with 124 events.

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

Answer: I would set the baseline at 30 which is slightly higher than average.



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