Lax Thomas \_Week\_ 18 Hw

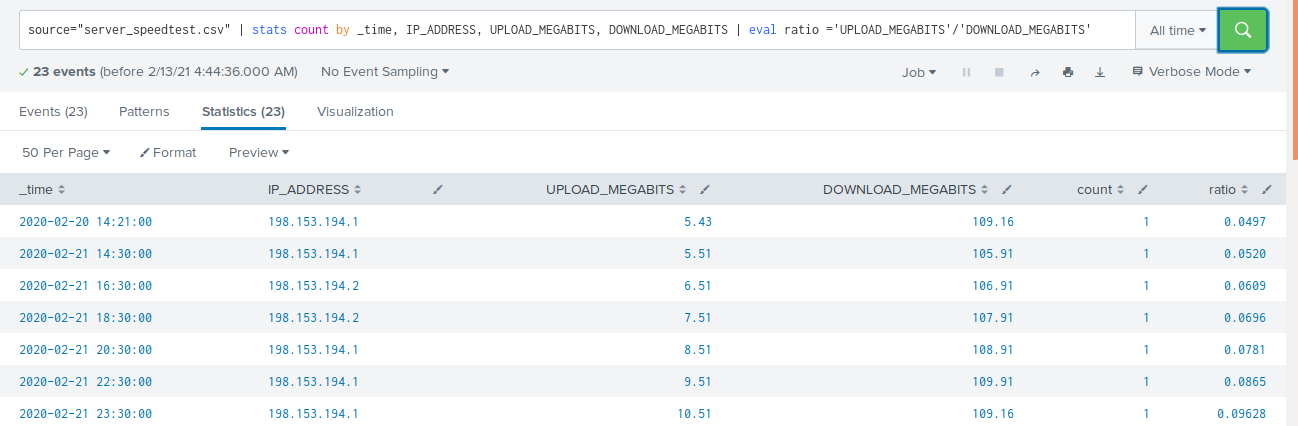
**Vandalay Industries Monitoring**

**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.

1. Upload the following file of the system speeds around the time of the attack.
   * [Speed Test File](https://utoronto.bootcampcontent.com/utoronto-bootcamp/utor-tor-cyber-pt-09-2020-u-c/-/blob/master/class_1/week_18/homework/resources/server_speedtest.csv)
2. Using the eval command, create a field called ratio that shows the ratio between the upload and download speeds.
   * Create field ratio:

source="server\_speedtest.csv" | eval ratio = 'UPLOAD\_MEGABITS'/'DOWNLOAD\_MEGABITS'

1. 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
2. Hint: Use the following format when for the table command: | table fieldA fieldB fieldC

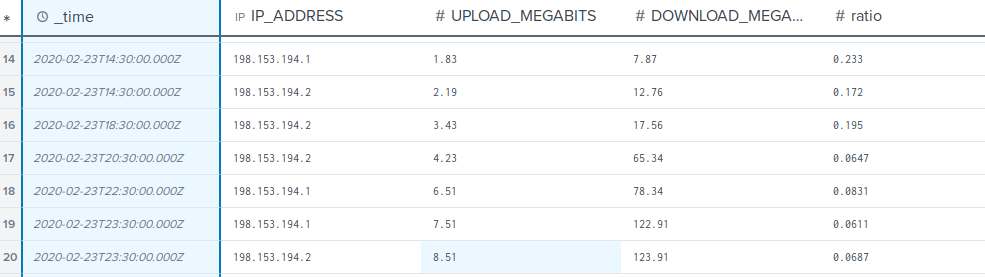
source="server\_speedtest.csv"| table\_time,IP\_ADDRESS,DOWNLOAD\_MEGABITS,UPLOAD\_MEGABITS |eval ratio ='UPLOAD\_MEGABITS'/'DOWNLOAD\_MEGABITS'

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

Ans: 23 Feb 2020 approx 1430 H till 1830H

* + How long did it take your systems to recover?

Ans: Around 2 hours from 1830 to 2030 H on 23 Feb 2020

Submit a screen shot of your report and the answer to the questions above.

### 

### 

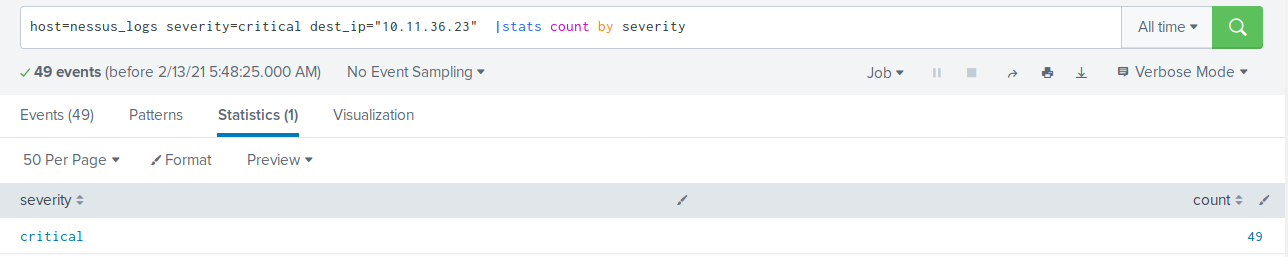
### 

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

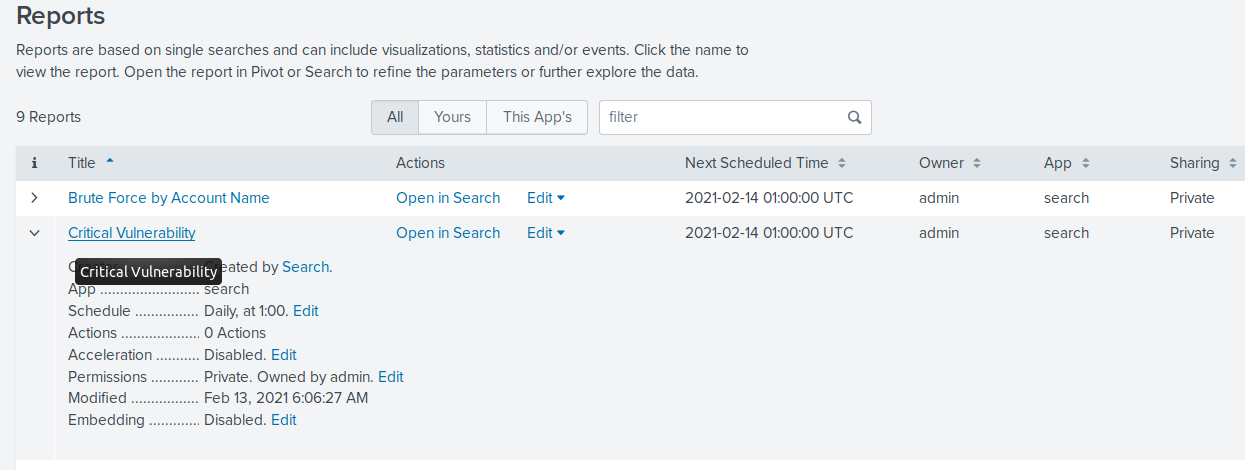
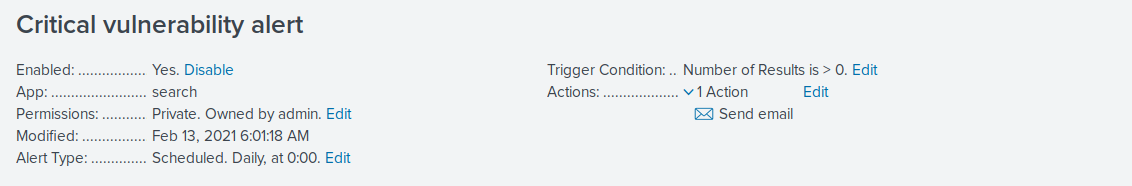
**Task:** Create a report determining how many critical vulnerabilities exist on the customer data server. Then, build an alert to notify your team if a critical vulnerability reappears on this server.

1. Upload the following file from the Nessus vulnerability scan.
   * [Nessus Scan Results](https://utoronto.bootcampcontent.com/utoronto-bootcamp/utor-tor-cyber-pt-09-2020-u-c/-/blob/master/class_1/week_18/homework/resources/nessus_logs.csv)
2. 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.

host=nessus\_logs severity=critical dest\_ip="10.11.36.23" |stats count by severity



1. 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.

Submit a screenshot of your report and a screenshot of proof that the alert has been created.

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

**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.

1. Upload the administrator login logs.
   * [Admin Logins](https://utoronto.bootcampcontent.com/utoronto-bootcamp/utor-tor-cyber-pt-09-2020-u-c/-/blob/master/class_1/week_18/homework/resources/Administrator_logs.csv)
2. When did the brute force attack occur?

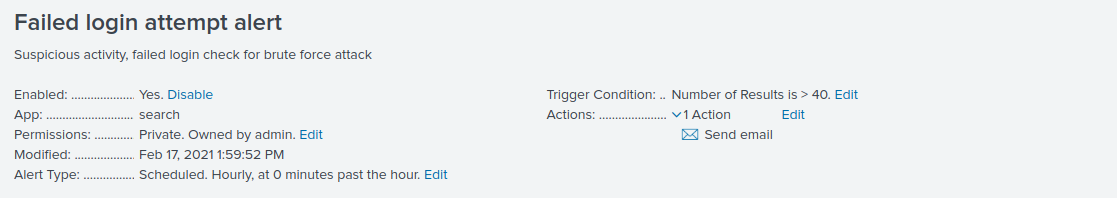
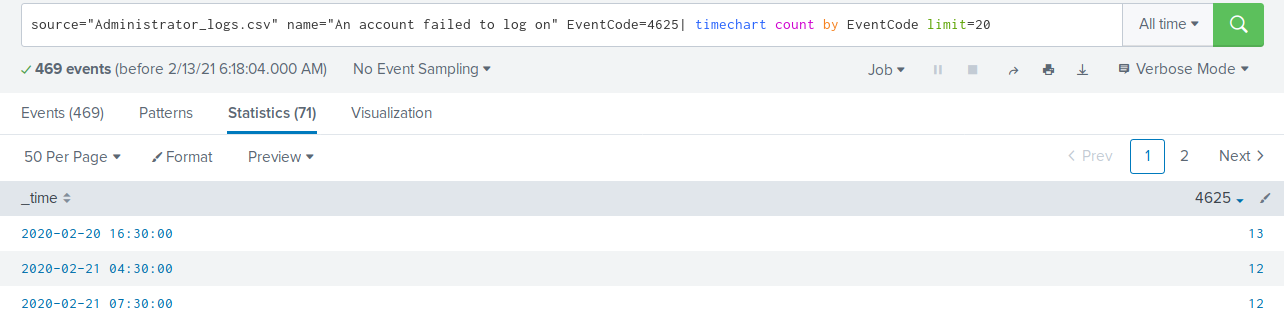
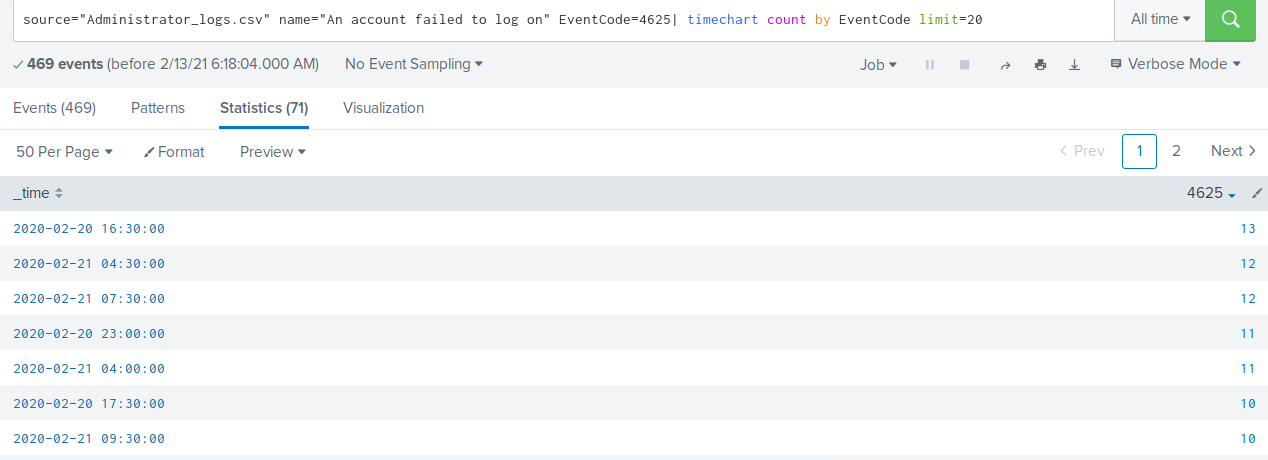
Ans: 21 feb 2020at 8am . there were 34 failed login events.

source="Administrator\_logs.csv" name="An account failed to log on" EventCode=4625| timechart count by EventCode limit=20

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

If the failed logon attempts are more than 40 an alert is triggered.

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

Submit the answers to the questions about the brute force timing, baseline and threshold. Additionally, provide a screenshot as proof that the alert has been created.