Week 16 Homework

SIEM Homework I

Billy Smith

[**Step 1: The Need for Speed**](#_q82nngq3aadu) **2**

[**Step 2: Are We Vulnerable?**](#_dhamd21u8zme) **3**

[**Step 3: Drawing the (base)line**](#_9xlqnl1lzseu) **6**

## Step 1: The Need for Speed

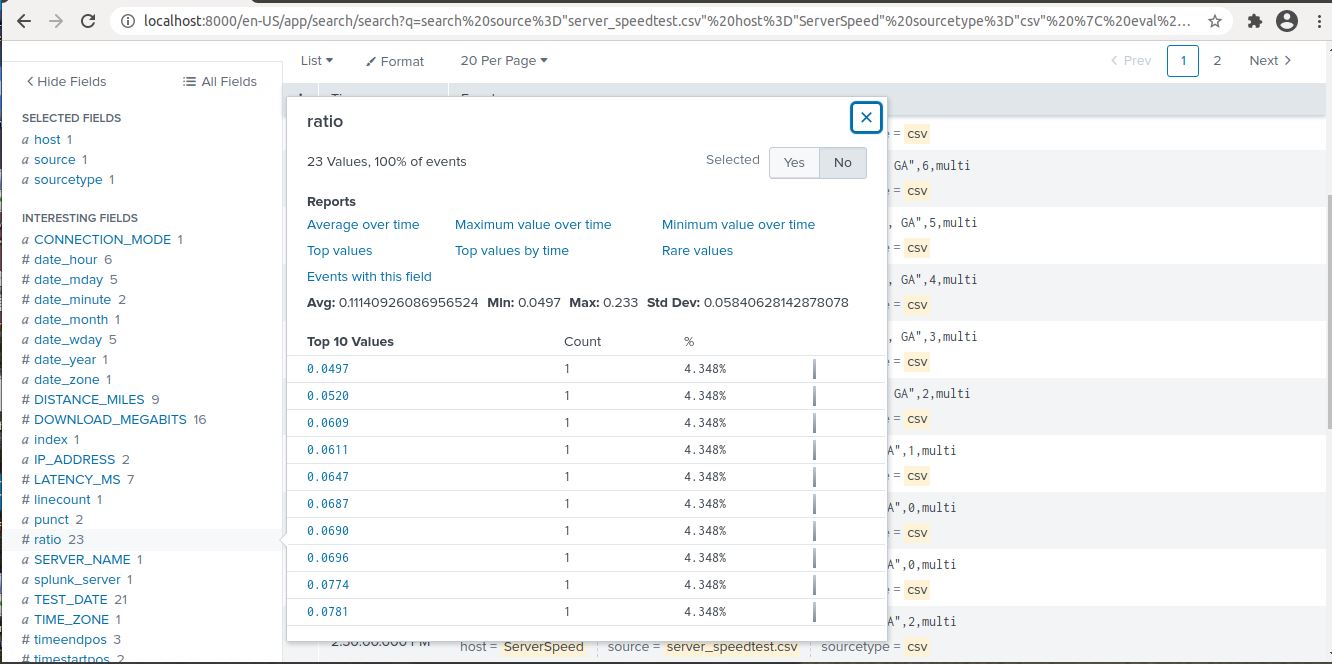
\*\*Background\*\*: As the worldwide leader of importing and exporting, Vandalay Industries has been the target of many adversaries attempting to disrupt their online business. Recently, Vandaly has been experiencing DDOS attacks against their web servers.

Not only were web servers taken offline by a DDOS attack, but upload and download speed were also significantly impacted after the outage. Your networking team provided results of a network speed run around the time of the latest DDOS attack.

\*\*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.

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

**source="server\_speedtest.csv" host="ServerSpeed" sourcetype="csv" | eval ratio = UPLOAD\_MEGABITS/DOWNLOAD\_MEGABITS**



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`

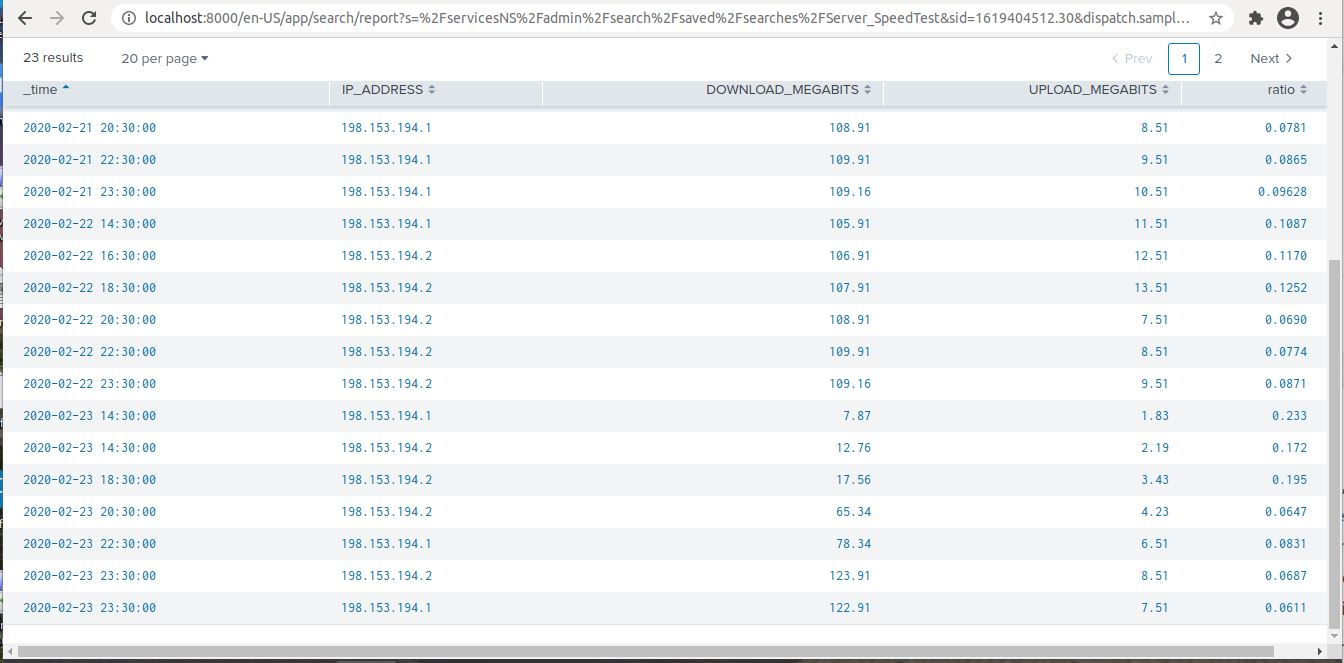
**source="server\_speedtest.csv" host="ServerSpeed" sourcetype="csv" | eval ratio = UPLOAD\_MEGABITS/DOWNLOAD\_MEGABITS | table \_time IP\_ADDRESS DOWNLOAD\_MEGABITS UPLOAD\_MEGABITS ratio**

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

**02/23/2020 @ 14:30:00**

- How long did it take your systems to recover?

**9 hours (02/23/2020 @ 23:30)**



## 

## 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.

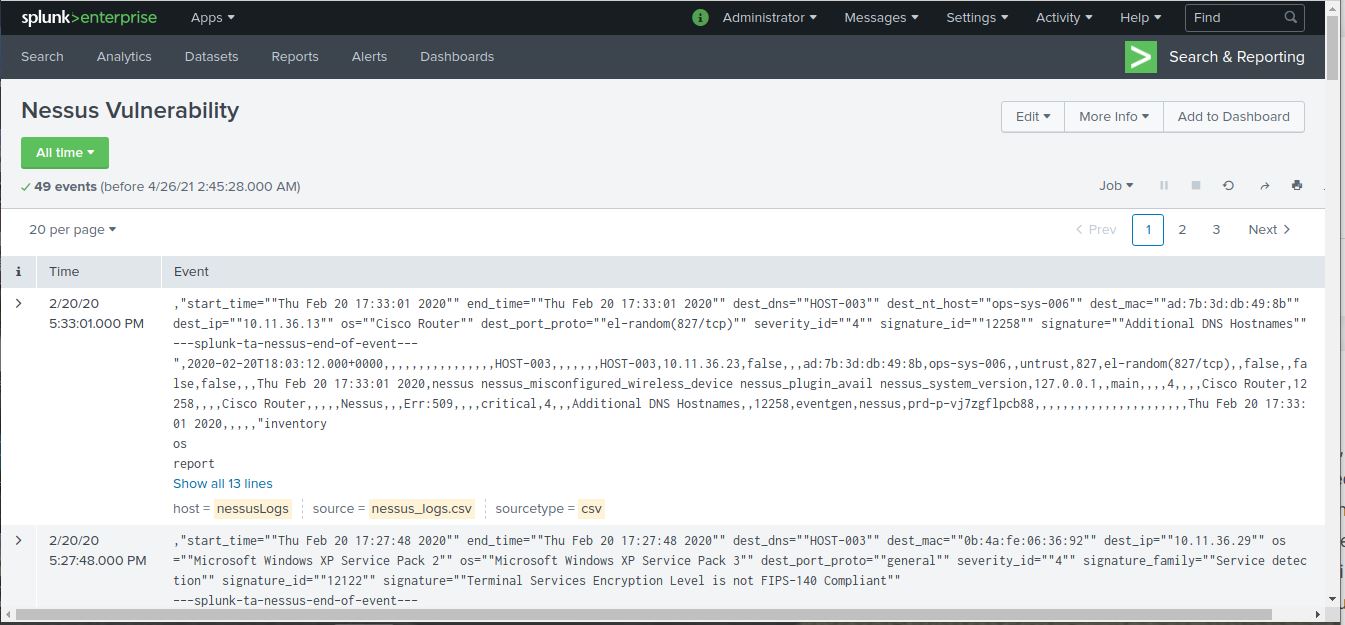
\*\*Task:\*\* Create a report determining how many critical vulnerabilities exist on the customer data server. Then, build an alert to notify your team if a critical vulnerability reappears on this server.

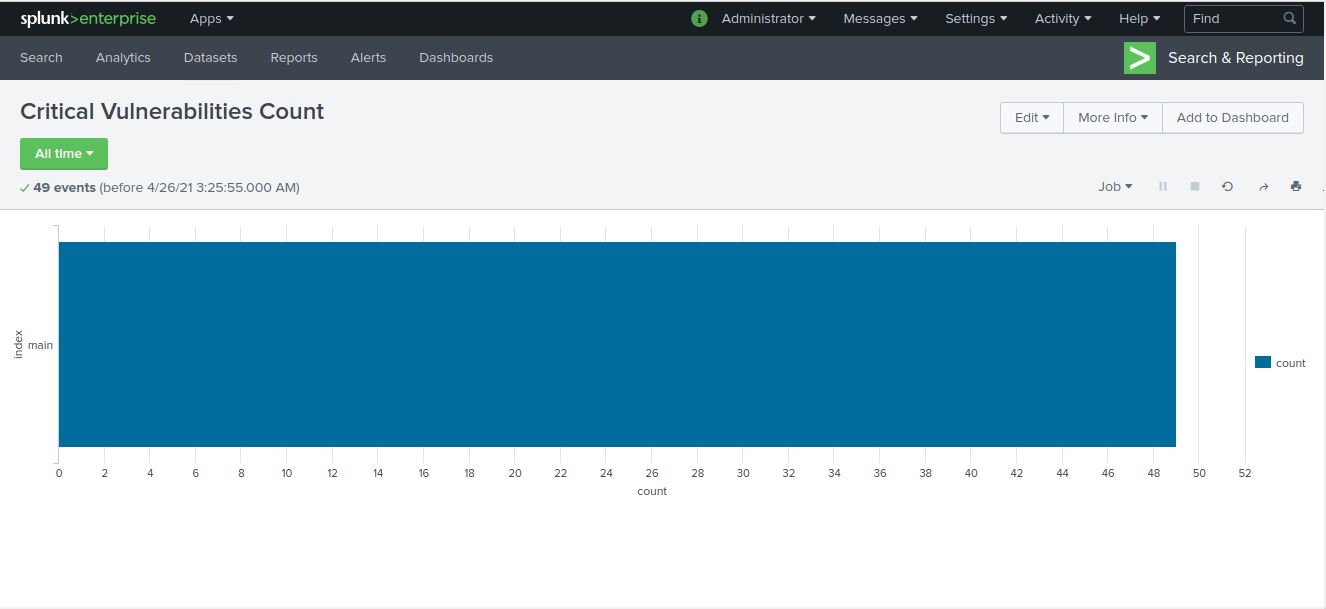
Create a report that shows the `count` of critical vulnerabilities from the customer database server.

- The database server IP is `10.11.36.23`.

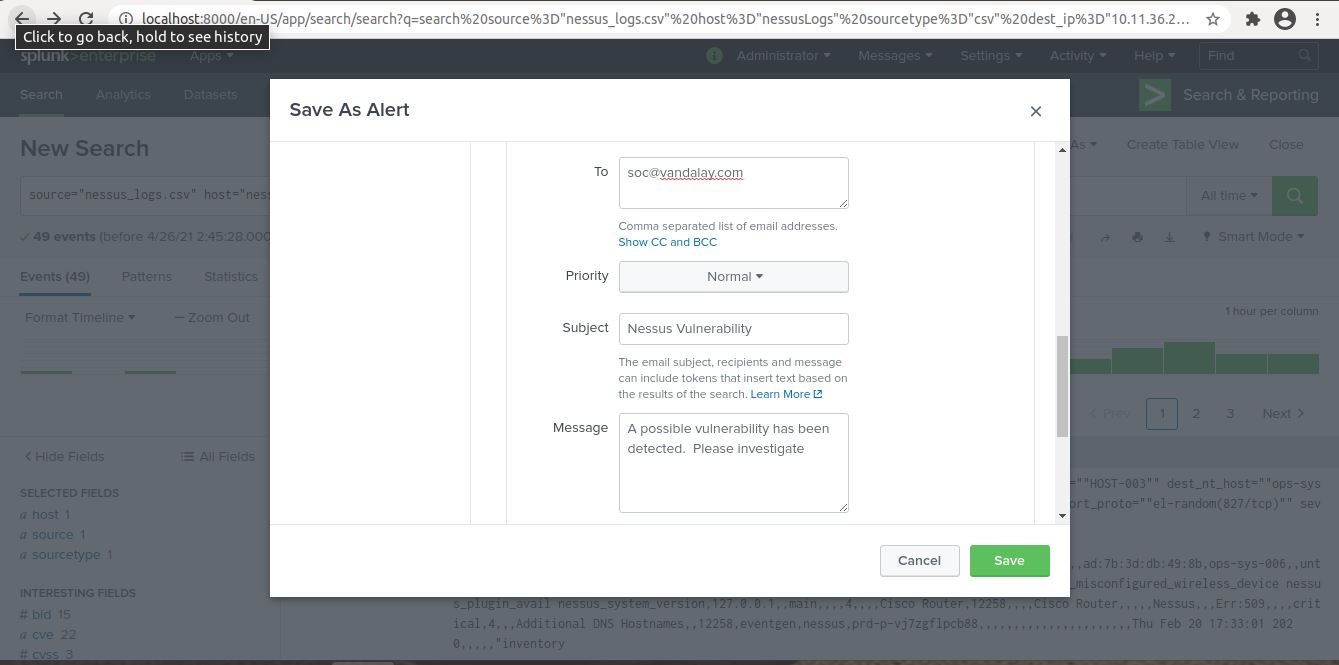
- The field that identifies the level of vulnerabilities is `severity`.

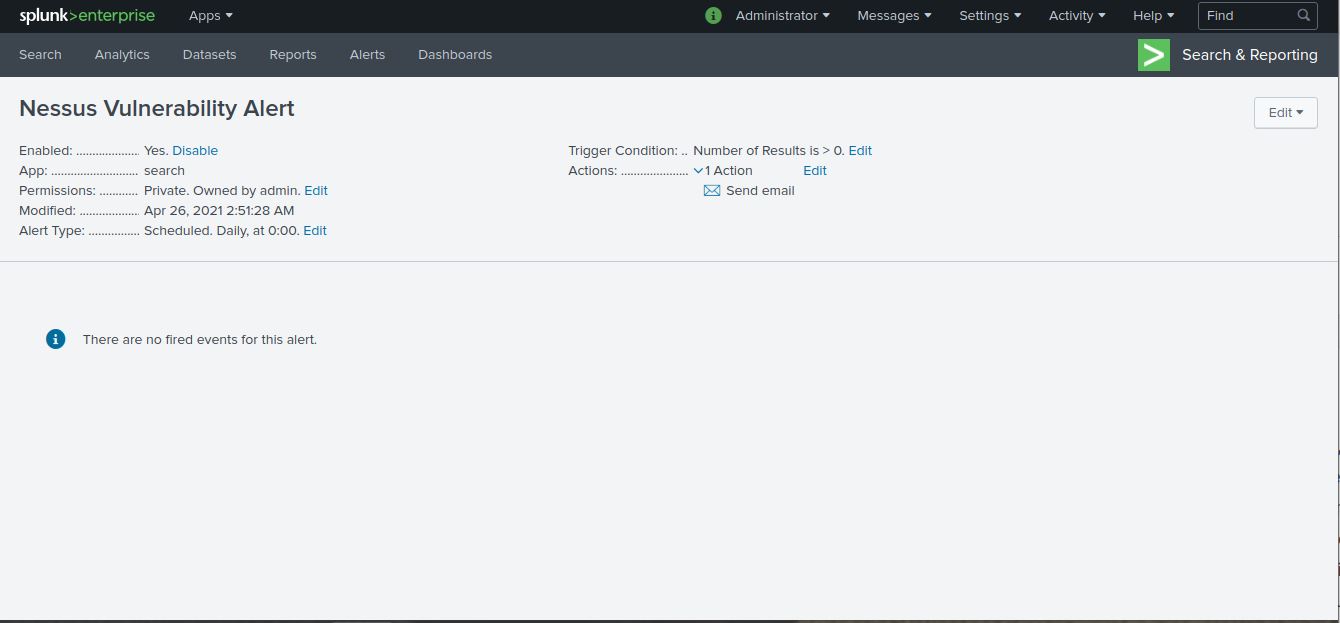
**source="nessus\_logs.csv" host="nessusLogs" sourcetype="csv" dest\_ip="10.11.36.23" severity=critical**





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.

When did the brute force attack occur?

**source="Administrator\_logs.csv" host="AdministratorLogin" sourcetype="csv" name="An account failed to log on"**

**Possibly started at 8am Friday Feb. 21, 2020 as the abnormal increase of failed logins started at that time**

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

**Baseline of normal activity is between 6 and 25 events, I would set a threshold of 30 events**

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

