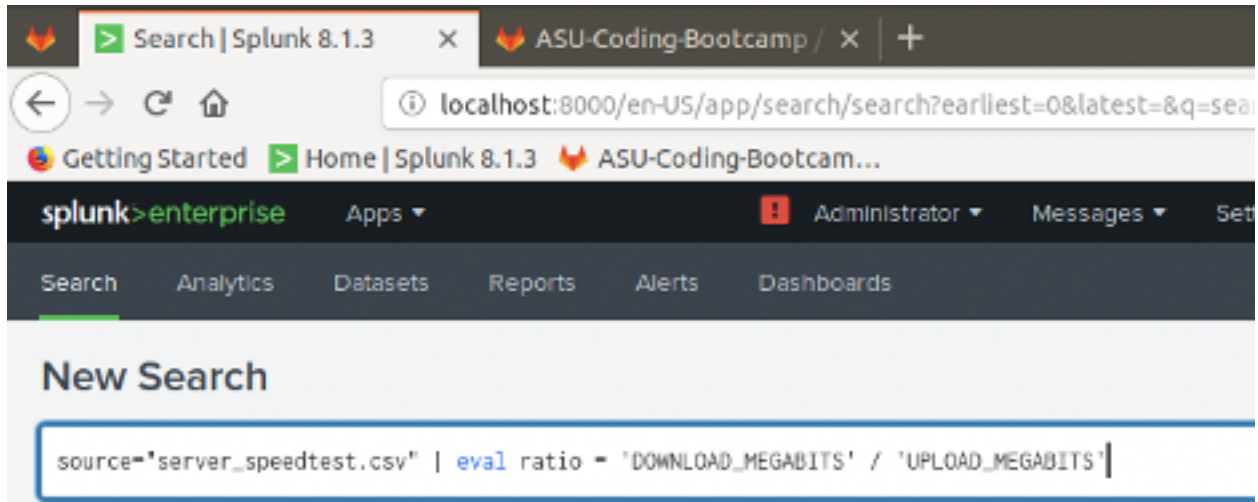


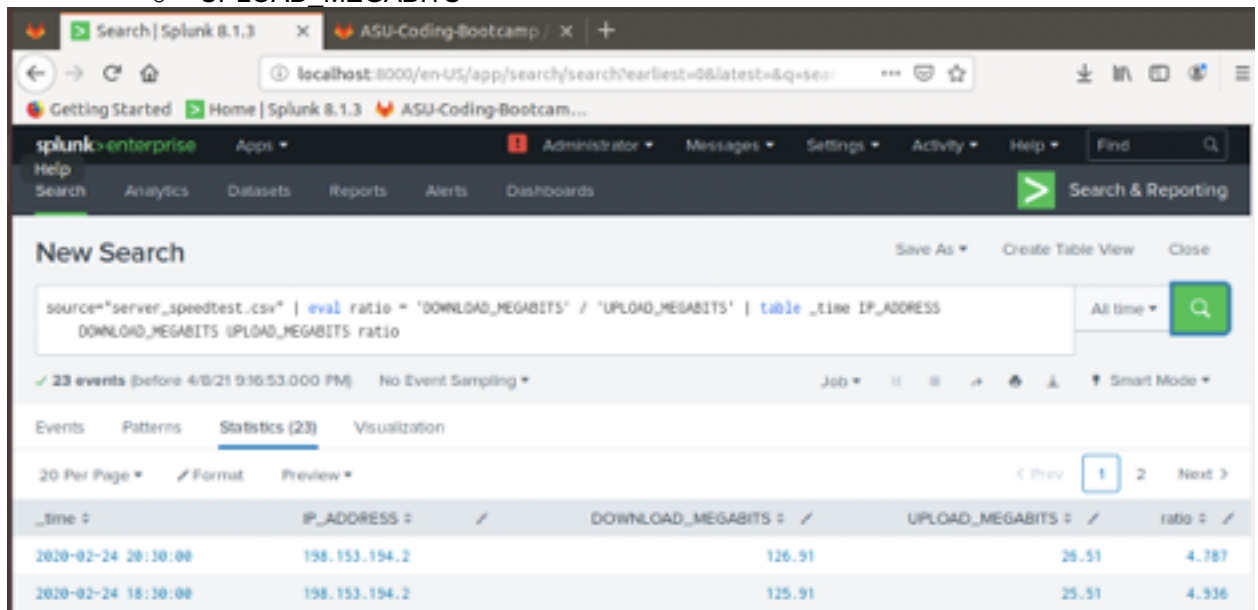
Week 18 Homework: SIEM I-Let's go Splunking

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:
 - o `_time`
 - o `IP_ADDRESS`
 - o `DOWNLOAD_MEGABITS`
 - o `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.

2020-02-23 22:30:00	198.153.194.1	78.34	6.51	12.0
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	14.6

Step 2: Are We Vulnerable?

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

The screenshot shows the Splunk search interface. The search bar contains the query: `source="nessus_logs.csv" severity=critical`. The results show 368 events. The interface includes a top navigation bar with links like Search, Analytics, Datasets, Reports, Alerts, and Dashboards. A 'New Search' button is visible.

The screenshot shows the Splunk search interface with a more refined search query: `source="nessus_logs.csv" severity=critical dest_ip="10.11.36.23" | top severity`. The results show 49 events. The 'Statistics' tab is selected, displaying a table with the following data:

severity	count	percent
critical	49	100.000000

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.

Save As Alert

Trigger Actions

+ Add Actions

When triggered

Send email

Remove

To

soc@vandalay.com

Comma separated list of email addresses.
[Show CC and BCC](#)

Priority

Highest

Subject

Splunk Alert: \$name\$

The email subject, recipients and message can include tokens that insert text based on the results of the search.
[Learn More](#)

Message

The alert condition for "\$name\$" was triggered.

Include

Cancel Save

Critical Vuln | Splunk 8.1.3 - Mozilla Firefox

Critical Vuln | Splunk 8.1.3 ASU-Coding-Bootcamp

localhost:8000/en-US/app/search/alert?<div>Getting Started Home | Splunk 8.1.3 ASU-Coding-Bootcamp...</div><div>splunk>enterprise</div>Help<div>Search Analytics Datasets Reports Alerts Dashboards</div><div>Search & Reporting</div><div><div>Critical Vuln</div><div>Critical Vulnerabilities in our system that need to be addressed</div><div><div>Enabled: Yes, Disable</div><div>App: search</div><div>Permissions: Private, Owned by admin, Edit</div><div>Modified: Apr 8, 2021 9:34:20 PM</div><div>Alert Type: Scheduled, Daily, at 0:00, Edit</div><div>Trigger Condition: .. Number of Results is > 0, Edit</div><div>Actions: 1 Action Edit</div><div>Send email</div></div></div>

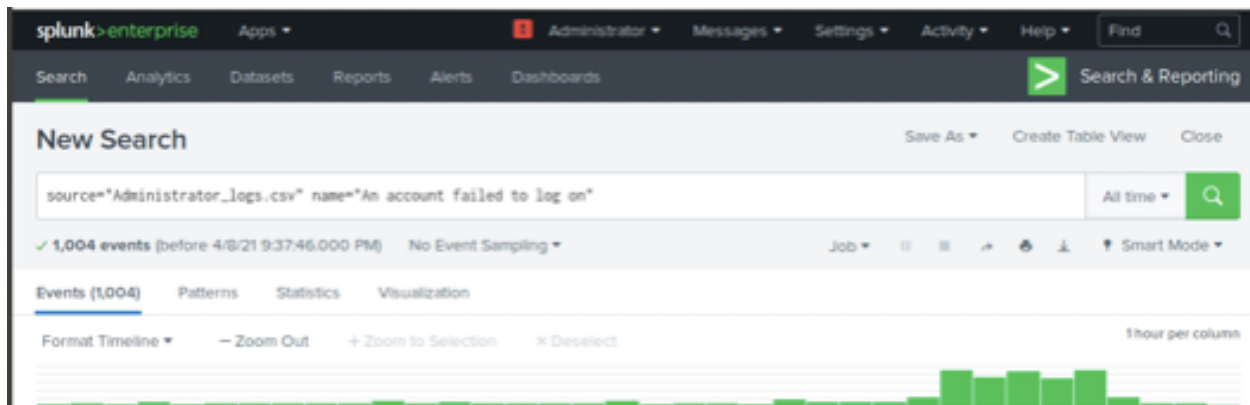
Step 3: Drawing the (base)line

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.

