

## Let's go Splunking:

### Step 1: Need for Speed

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

**source="statsreport.csv" | eval ratio = 'DOWNLOAD\_MEGABITS'/'UPLOAD\_MEGABITS'**

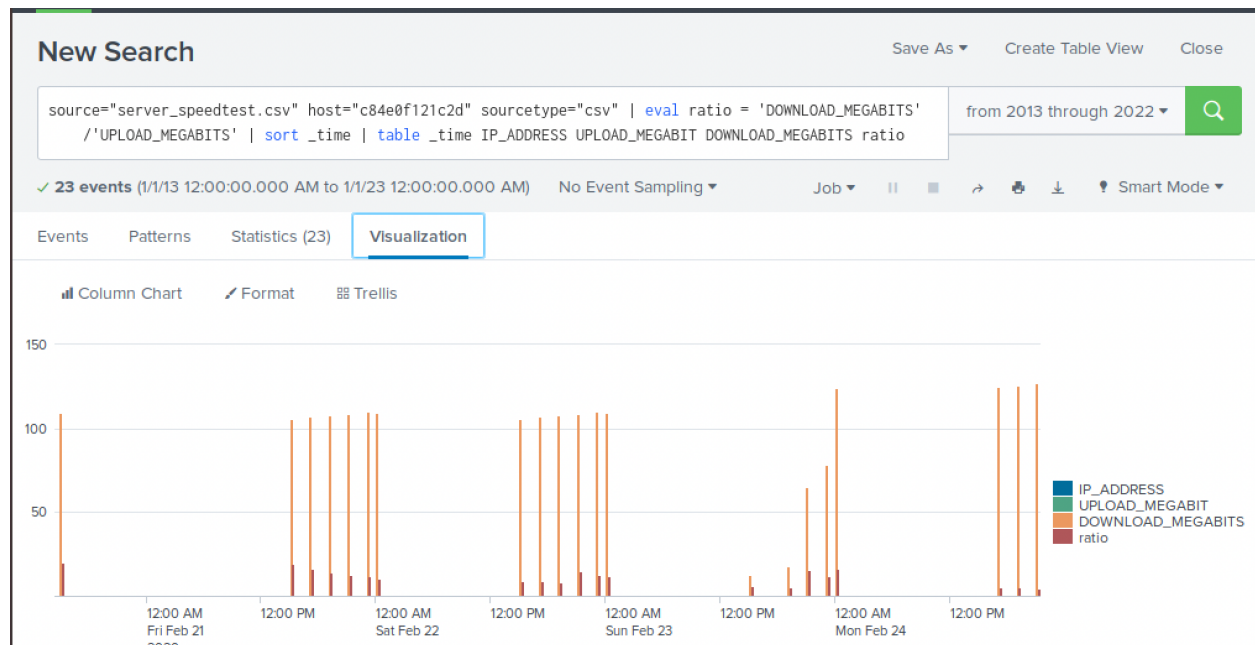
Create a report using the Splunk's table command to display the following fields in a statistics report:

**\_time**

**IP\_ADDRESS**

**DOWNLOAD\_MEGABITS**

**UPLOAD\_MEGABITS**



**source="statsreport.csv" | eval ratio = 'DOWNLOAD\_MEGABITS'/'UPLOAD\_MEGABITS' |  
sort \_time | table \_time IP\_ADDRESS UPLOAD\_MEGABITS DOWNLOAD\_MEGABITS ratio**

## Let's go Splunking:

2020-02-23 20:30:00	198.153.194.2	65.34	15.4
2020-02-23 23:30:00	198.153.194.2	123.91	14.6
2020-02-22 20:30:00	198.153.194.2	108.91	14.5
2020-02-21 18:30:00	198.153.194.2	107.91	14.4
2020-02-22 22:30:00	198.153.194.2	109.91	12.9
2020-02-21 20:30:00	198.153.194.1	108.91	12.8
2020-02-23 22:30:00	198.153.194.1	78.34	12.0
2020-02-21 22:30:00	198.153.194.1	109.91	11.6
2020-02-22 23:30:00	198.153.194.2	109.16	11.5
2020-02-21 23:30:00	198.153.194.1	109.16	10.39
2020-02-22 14:30:00	198.153.194.1	105.91	9.202
2020-02-22 16:30:00	198.153.194.2	106.91	8.546
2020-02-22 18:30:00	198.153.194.2	107.91	7.987
2020-02-23 14:30:00	198.153.194.2	12.76	5.83
2020-02-23 18:30:00	198.153.194.2	17.56	5.12
2020-02-24 16:30:00	198.153.194.1	124.91	5.096

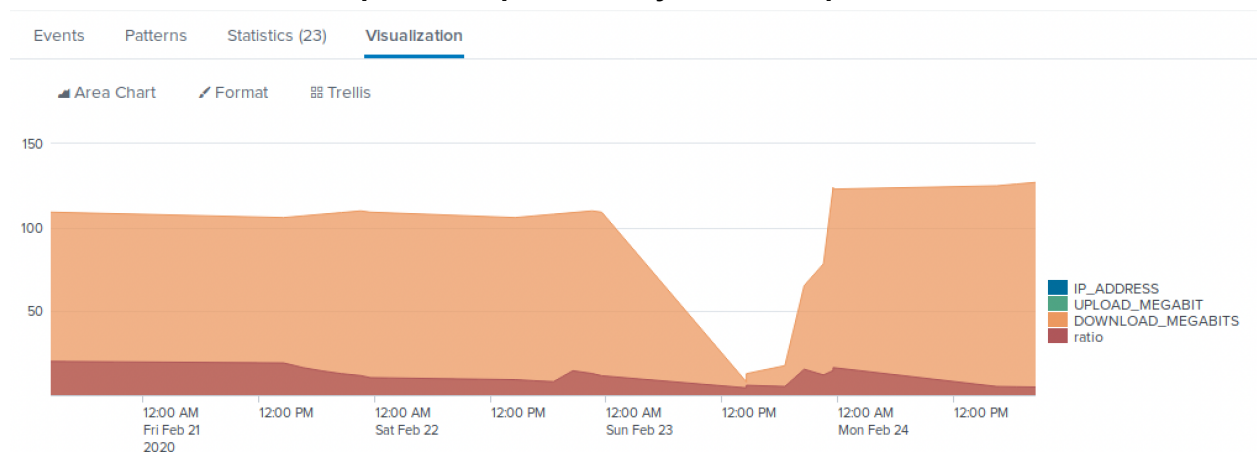
_time ↕	IP_ADDRESS ↕	UPLOAD_MEGABIT ↕	DOWNLOAD_MEGABITS ↕	ratio ↕
2020-02-24 18:30:00	198.153.194.2		125.91	4.936
2020-02-24 20:30:00	198.153.194.2		126.91	4.787
2020-02-23 14:30:00	198.153.194.1		7.87	4.30

Answer the following questions:

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

14:30 on 2/23/2020.

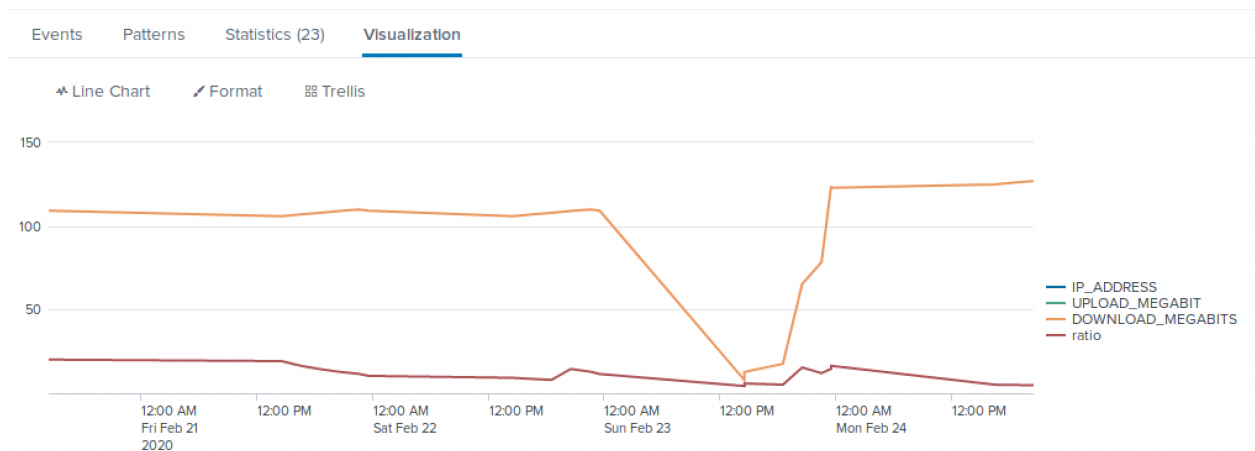
**Visual shows download speeds drop drastically to 7.87 mbps.**



How long did it take your systems to recover?

**It did not recover until 23:30, making it 9 hours until full recovery.**

## Let's go Splunking:

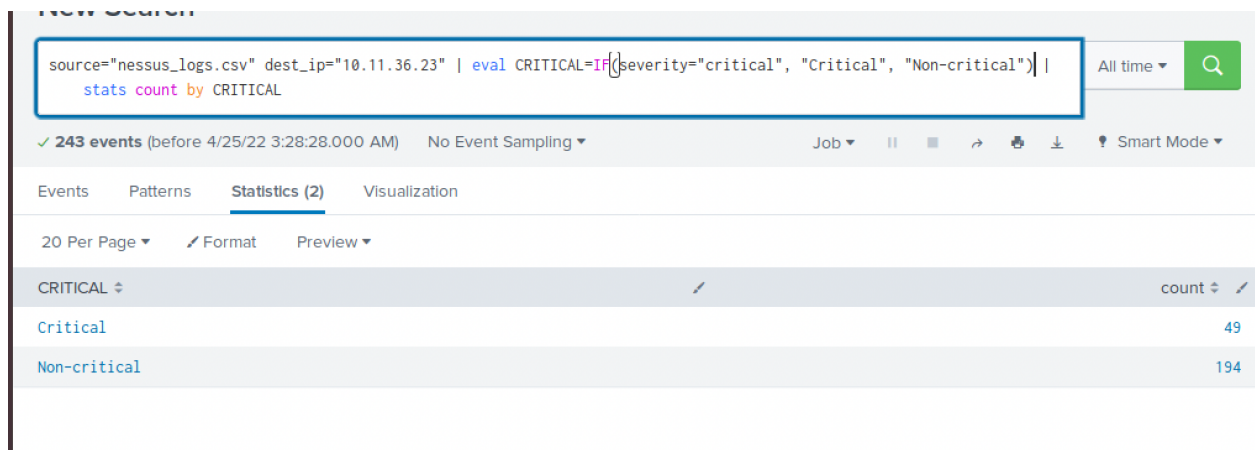


### Step 2: Are We Vulnerable?

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" dest\_ip="10.11.36.23" | eval CRITICAL=IF(severity="critical", "CRITICAL", "Non-critical") | stats count by 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).

Let's go Splunking:

Save As Alert

Settings

Title

Critical Vulnerabilities

Description

Optional

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Run every day ▾

At

0:00 ▾

Expires

24

hour(s) ▾

When triggered

✉ Send email

Remove

To

soc@vandalay.com

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

Priority

High ▾

Subject

CRITICAL database server Vulnera

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 CRITICAL

Critical Vulnerabilities

Enabled: ..... Yes. [Disable](#)

App: ..... search

Permissions: ..... Private. Owned by admin. [Edit](#)

Modified: ..... Apr 25, 2022 3:34:42 AM

Alert Type: ..... Scheduled. Daily, at 0:00. [Edit](#)

Trigger Condition: .. Number of Results is > 0. [Edit](#)

Actions: ..... ▾1 Action [Edit](#)

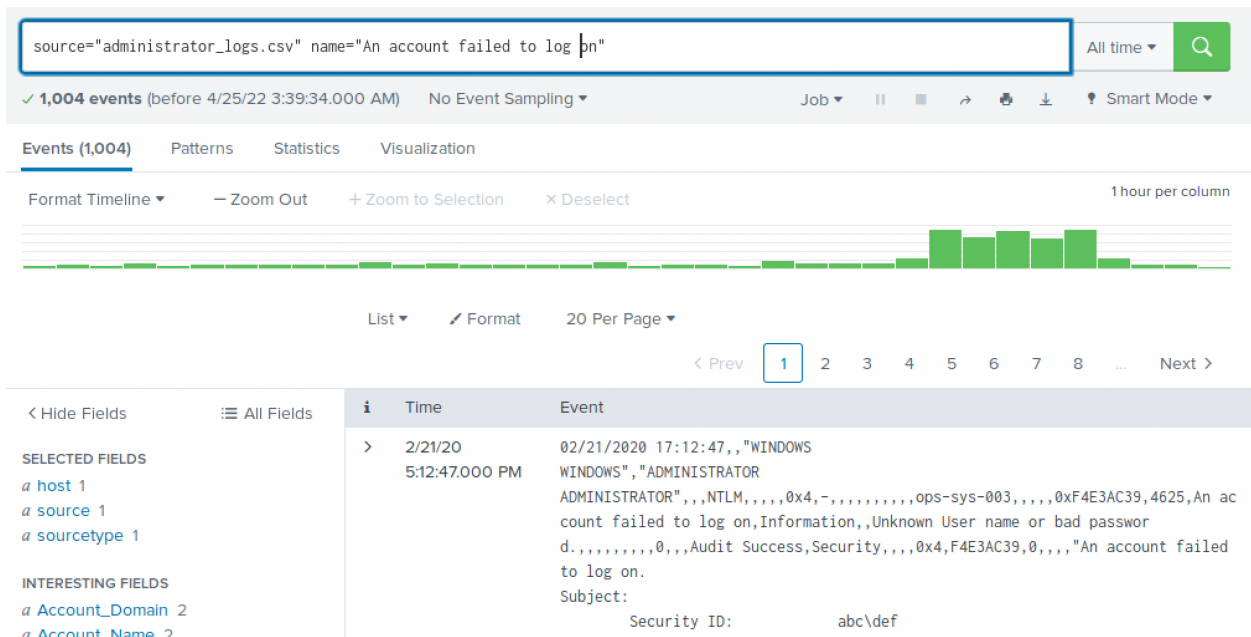
✉ Send email

Let's go Splunking:

Step 3: Drawing the (base)line

When did the brute force attack occur?

source="administrator\_logs.csv" name="An account failed to log on"



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

The attack occurred from 9AM - 2 PM on 2/21/2020. The normal baseline ranges from 6 - 34. We can set a safe baseline above 40 failed login attempts as "Brute Force" attempt/attack.

source="administrator\_logs.csv" | stats count by name | sort -count | eval Bruteforce=if(count>40, "Potential Brute Force", "Not Brute Force")

3,742 events (before 4/25/22 3:48:00.000 AM) No Event Sampling

Events Patterns Statistics (7) Visualization

20 Per Page Format Preview

name	count	Bruteforce
An account failed to log on	1004	Potential Brute Force
An account was logged off	417	Not Brute Force
Special privileges assigned to new logon	414	Not Brute Force
A logon was attempted using explicit credentials	399	Not Brute Force
Key file operation	382	Not Brute Force
Cryptographic operation	369	Not Brute Force
An account was successfully logged on	365	Not Brute Force

## Let's go Splunking:

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

Save As Alert

×

Settings

Title

Brute Force Attempt

Description

Optional

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Run every hour ▼

At

0 ▼

minutes past the hour

Expires

24

hour(s) ▼

When triggered

▼

✉ Send email

Remove

To

SOC@vandalay.com

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

Priority

Normal ▼

Subject

Brute Force Attempt Alert

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

Message

Alert for possible Brute Force Attempt. Please verify and check.

Cancel

Save



## Let's go Splunking:

### Brute Force Attempt

Enabled: ..... Yes. [Disable](#)

App: ..... search

Permissions: ..... Private. Owned by admin. [Edit](#)

Modified: ..... Apr 25, 2022 3:51:38 AM

Alert Type: ..... Scheduled. Hourly, at 0 minutes past the hour.  
[Edit](#)

Trigger Condition: .. Number of Results is > 0. [Edit](#)

Actions: ..... [▼](#) 1 Action [Edit](#)

 Send email