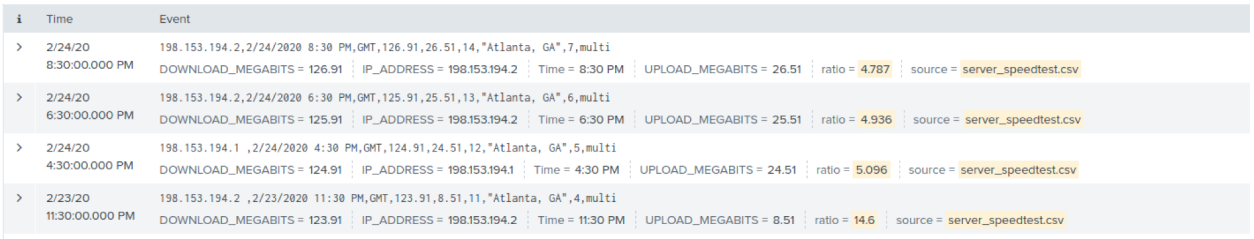
Cameron Wright

Splunk Project Part 1

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.

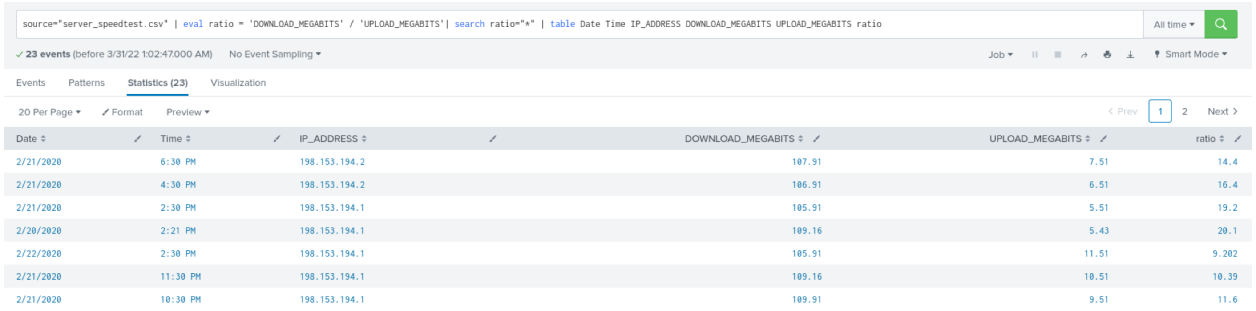
Using the eval command, create a field called ratio that shows the ratio between the upload and download speeds.



i	Time	Event
>	2/24/20 8:30:00.000 PM	198.153.194.2,2/24/2020 8:30 PM,GMT,126.91,26.51,14,"Atlanta, GA",7,multi DOWNLOAD_MEGABITS = 126.91 | IP_ADDRESS = 198.153.194.2 | Time = 8:30 PM | UPLOAD_MEGABITS = 26.51 | ratio = 4.787 | source = server_speedtest.csv
>	2/24/20 6:30:00.000 PM	198.153.194.2,2/24/2020 6:30 PM,GMT,125.91,25.51,13,"Atlanta, GA",6,multi DOWNLOAD_MEGABITS = 125.91 | IP_ADDRESS = 198.153.194.2 | Time = 6:30 PM | UPLOAD_MEGABITS = 25.51 | ratio = 4.936 | source = server_speedtest.csv
>	2/24/20 4:30:00.000 PM	198.153.194.1 ,2/24/2020 4:30 PM,GMT,124.91,24.51,12,"Atlanta, GA",5,multi DOWNLOAD_MEGABITS = 124.91 | IP_ADDRESS = 198.153.194.1 | Time = 4:30 PM | UPLOAD_MEGABITS = 24.51 | ratio = 5.096 | source = server_speedtest.csv
>	2/23/20 11:30:00.000 PM	198.153.194.2 ,2/23/2020 11:30 PM,GMT,123.91,8.51,11,"Atlanta, GA",4,multi DOWNLOAD_MEGABITS = 123.91 | IP_ADDRESS = 198.153.194.2 | Time = 11:30 PM | UPLOAD_MEGABITS = 8.51 | ratio = 14.6 | source = server_speedtest.csv

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



Date	Time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2/21/2020	6:30 PM	198.153.194.2	107.91	7.51	14.4
2/21/2020	4:30 PM	198.153.194.2	106.91	6.51	16.4
2/21/2020	2:30 PM	198.153.194.1	105.91	5.51	19.2
2/20/2020	2:21 PM	198.153.194.1	109.16	5.43	20.1
2/22/2020	2:30 PM	198.153.194.1	105.91	11.51	9.202
2/21/2020	11:30 PM	198.153.194.1	109.16	10.51	10.39
2/21/2020	10:30 PM	198.153.194.1	109.91	9.51	11.6

Answer the following questions:

Based on the report created, what is the approximate date and time of the attack?
How long did it take your systems to recover?

On the 2/23/2020 at 2:30pm The attack was causing the most significant impact, until around 8:30pm the same day the webservers were seeing half of their normal speeds regain. It was until 11:30pm that night that speeds were back around normal levels, The whole attack lasting for approximately 9 hours before the systems recovered.

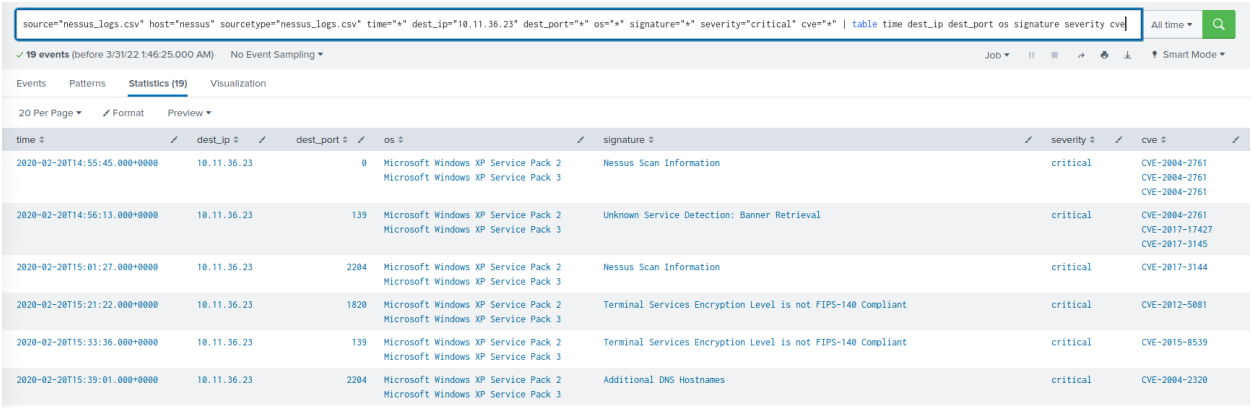
2/22/2020	4:30 PM	198.153.194.2	106.91	12.51	8.546
2/22/2020	11:30 PM	198.153.194.2	109.16	9.51	11.5
2/23/2020	6:30 PM	198.153.194.2	17.56	3.43	5.12
2/23/2020	2:30 PM	198.153.194.1	7.87	1.83	4.30
2/23/2020	2:30 PM	198.153.194.2	12.76	2.19	5.83
2/23/2020	11:30 PM	198.153.194.2	123.91	8.51	14.6
2/23/2020	11:30 PM	198.153.194.1	122.91	7.51	16.4
2/23/2020	10:30 PM	198.153.194.1	78.34	6.51	12.0
2/23/2020	8:30 PM	198.153.194.2	65.34	4.23	15.4

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.
table

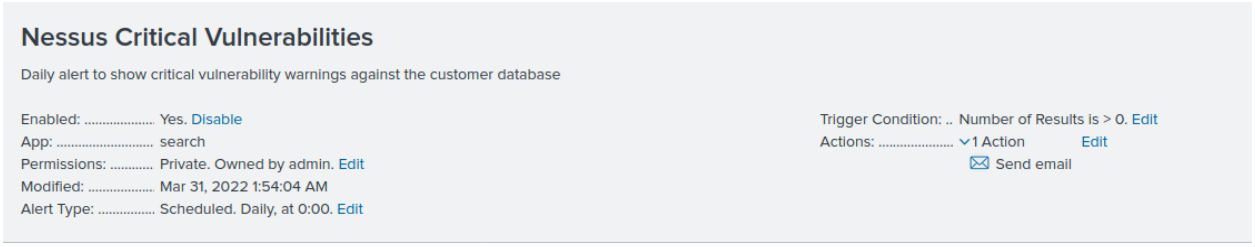
Create a report that shows the count of critical vulnerabilities from the customer database server.

The database server IP is 10.11.36.23.

The field that identifies the level of vulnerabilities is severity.



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
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.

Upload the administrator login logs.

Admin Logins

When did the brute force attack occur?
09:00 21/2/2020 untill 13:00 21/2/2020

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

Normal activity would be in the range of 0 to 15 failed login attempts per hour from the logs supplied. At certain times there was a failed login amount seen to be closer to 30 per hour, where during the attack the number was on average 120 attempts per hour. Factoring in all of the information I believe that a baseline of 30 would be the most suitable for an hourly alert threshold to minimize the chances of the SOC team being overwhelmed with unnecessary alerts being triggered.

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