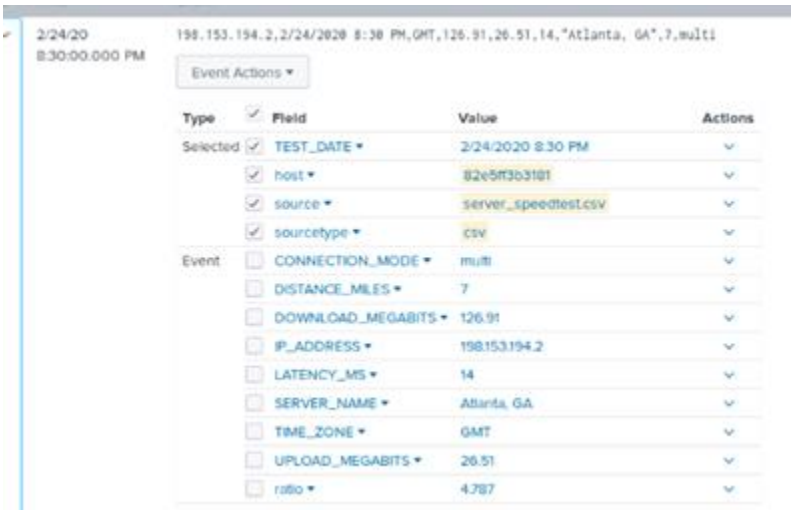
Step 1: The Need for Speed

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

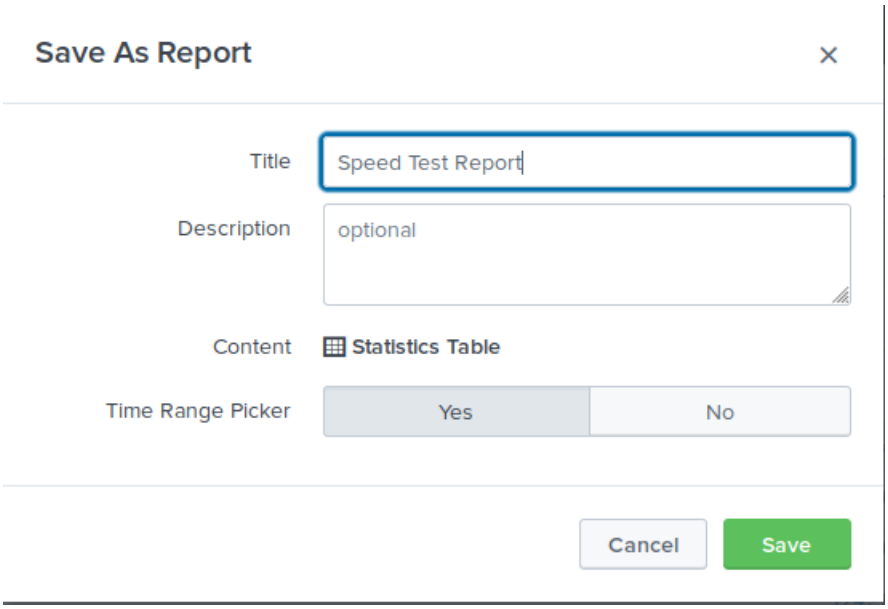
Source="server_speedtest.csv" sourcetype="csv" | eval ratio = 'DOWNLOAD_MEGABITS' / 'UPLOAD_MEGABITS'



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

Source="server_speedtest.csv" sourcetype="csv" | table _time IP_ADDRESS DOWNLOAD_MEGABITS UPLOAD MEGABITS | eval ratio = 'DOWNLOAD_MEGABITS' / 'UPLOAD_MEGABITS'

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-24 20:30:00	198.153.194.2	126.91	26.51	4.787
2020-02-24 18:30:00	198.153.194.2	125.91	25.51	4.936
2020-02-24 16:30:00	198.153.194.1	124.91	24.51	5.096
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	14.6
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	16.4
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	12.0
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	15.4
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	5.12
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	4.30
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	5.83



Answer the following questions:

Based on the report created, what is the approximate date and time of the attack?
2020-02-23 14:30:00pm

How long did it take your systems to recover?
Systems recovered at 2020-02-23 22:30:00pm. 8 hours total

Step 2: Are We Vulnerable?

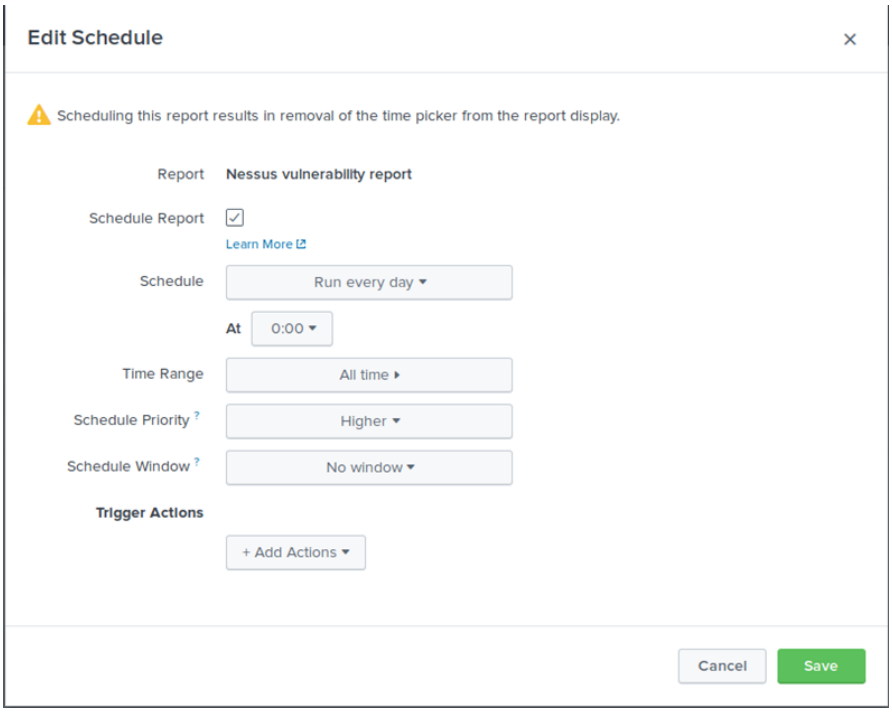
Create a report that shows the count of critical vulnerabilities from the customer database server.

The database server IP is 10.11.36.23.

The field that identifies the level of vulnerabilities is severity.

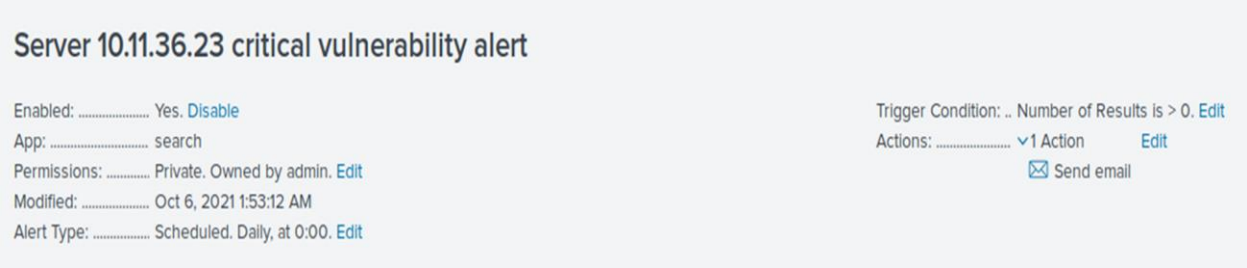
source="nessus_logs.csv" sourcetype="csv" dest_ip="10.11.36.23" | stats count by severity

severity	count
critical	49
high	47
informational	52
low	50
medium	45



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.

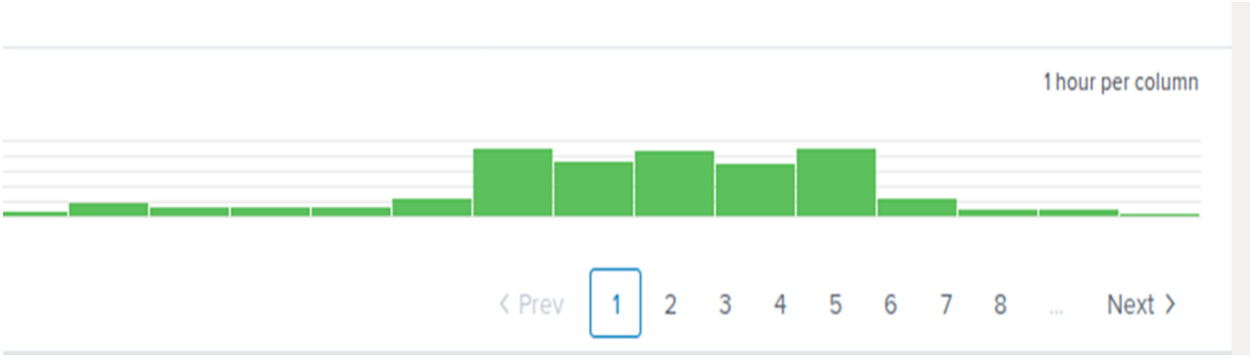
source="nessus_logs.csv" sourcetype="csv" dest_ip="10.11.36.23" severity=critical



Step 3: Drawing the (base)line

When did the brute force attack occur?

source="Administrator_logs.csv" sourcetype="csv" name="An account failed to log in"



The attack started at 8AM on Feb 21 2020

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

Since the average failed logins attempts is around 6 to 23. I put the alert trigger at 30 or higher within an hour span.

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

Possible brute force attack

Enabled: ..... Yes. Disable
App: ..... search
Permissions: ..... Private. Owned by admin. Edit
Modified: ..... Oct 6, 2021 2:18:10 AM
Alert Type: ..... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 30. Edit
Actions: ..... 1 Action Edit
Send email