Step 1: The Need for Speed:

host=Server_speedtest | eval ratio = 'DOWNLOAD_MEGABITS' / 'UPLOAD_MEGABITS' | table _time IP_ADDRESS DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio

All time

✓ 23 events (before 3/17/22 3:40:16.000 AM) No Event Sampling

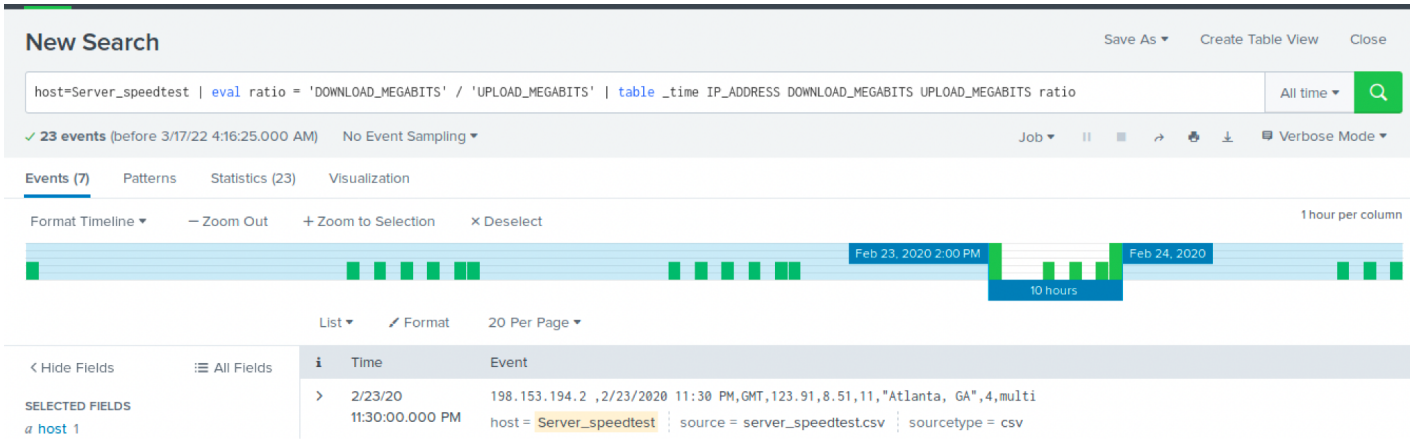
Job Verbose Mode

Events (23) Patterns Statistics (23) Visualization

20 Per Page Format Preview

Prev 1 2 Next

| _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 |
| 2020-02-22 23:30:00 | 198.153.194.2 | 109.16 | 9.51 | 11.5 |
| 2020-02-22 22:30:00 | 198.153.194.2 | 109.91 | 8.51 | 12.9 |
| 2020-02-22 20:30:00 | 198.153.194.2 | 108.91 | 7.51 | 14.5 |



New Search

Save As Create Table View Close

host=Server_speedtest | eval ratio = 'DOWNLOAD_MEGABITS' / 'UPLOAD_MEGABITS' | table _time IP_ADDRESS DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio

All time

✓ 23 events (before 3/17/22 4:16:25.000 AM) No Event Sampling

Job Verbose Mode

Events (7) Patterns Statistics (23) Visualization

Format Timeline − Zoom Out + Zoom to Selection × Deselect 1 hour per column

Feb 23, 2020 2:00 PM Feb 24, 2020

10 hours

List Format 20 Per Page

Hide Fields All Fields

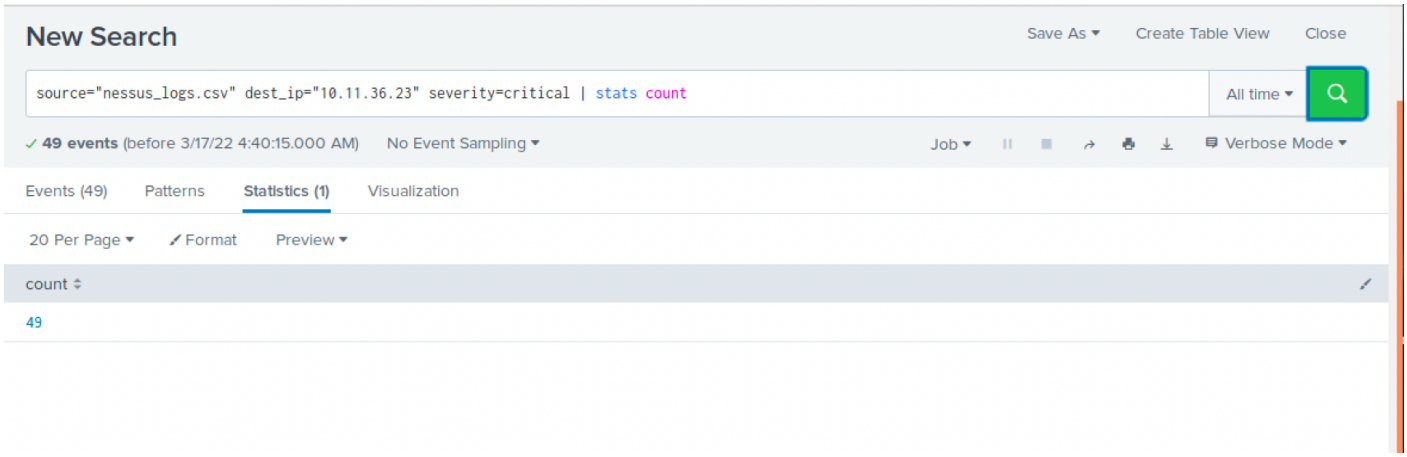
SELECTED FIELDS

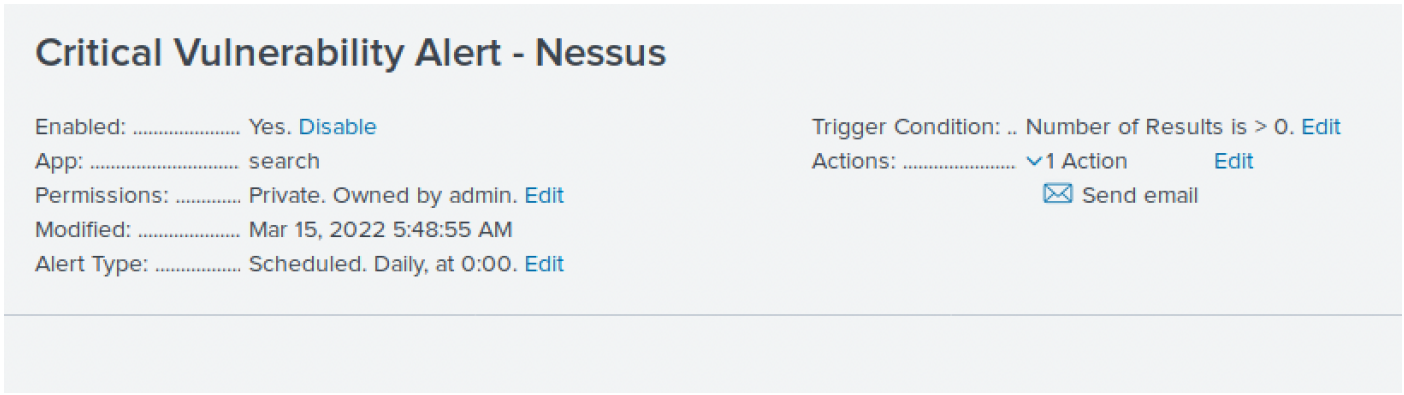
a host 1

| i | Time | Event |
|---|---|---|
| > | 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<br>host = Server_speedtest source = server_speedtest.csv sourcetype = csv |

- The attack approximately took place on February 23, 2020 from 2:30pm to 11:30pm. Taking roughly 8 hours for the system to recover.

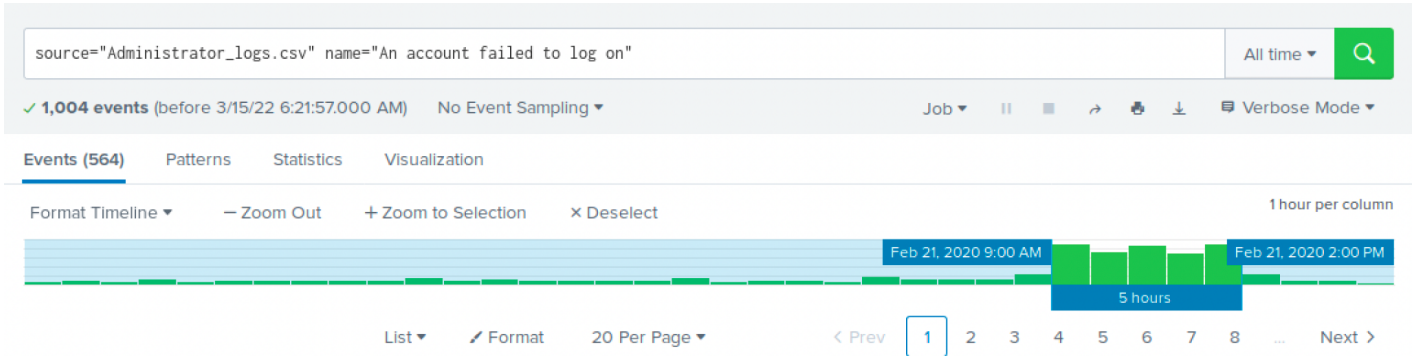
Step 2: Are We Vulnerable?

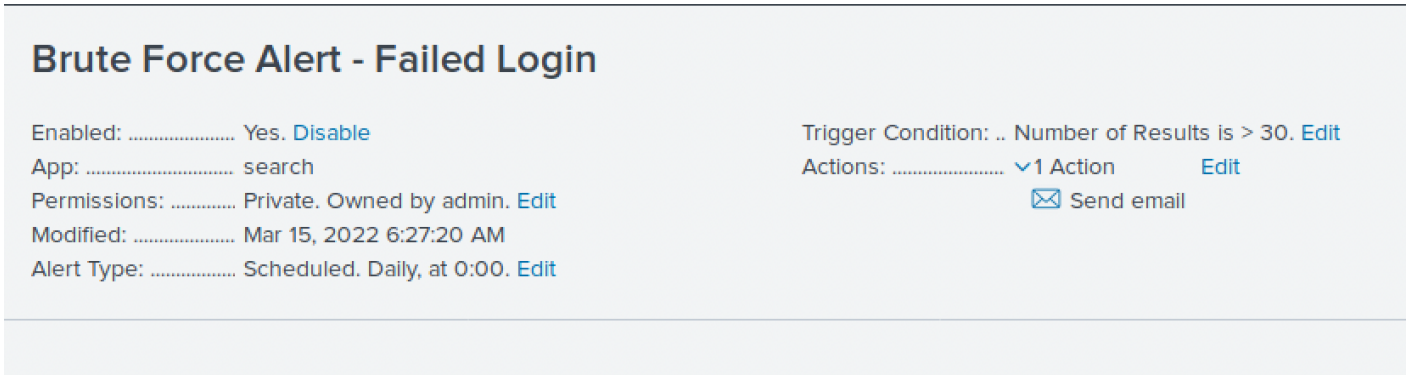



- Report shown above, reflecting count of critical vulnerabilities. Alert created to monitor daily, and to email soc@vandalay.com if vulnerability exists.

Step 3: Drawing the (base)line




- The brute force attack occurred on February 21, 2020 and lasted for 5 hours between 9:00 AM and 2:00 PM. The baseline of normal activity ranged from 15-25 failed logins, a good threshold to alert for a potential brute force attack would be 30 failed logins in one hour.