

[Step 1: The Need for Speed](#)

[Questions](#)

[Step 2: Are We Vulnerable?](#)

[Step 3: Drawing the \(base\)line](#)

[The Baseline](#)

[The Alert](#)

Step 1: The Need for Speed

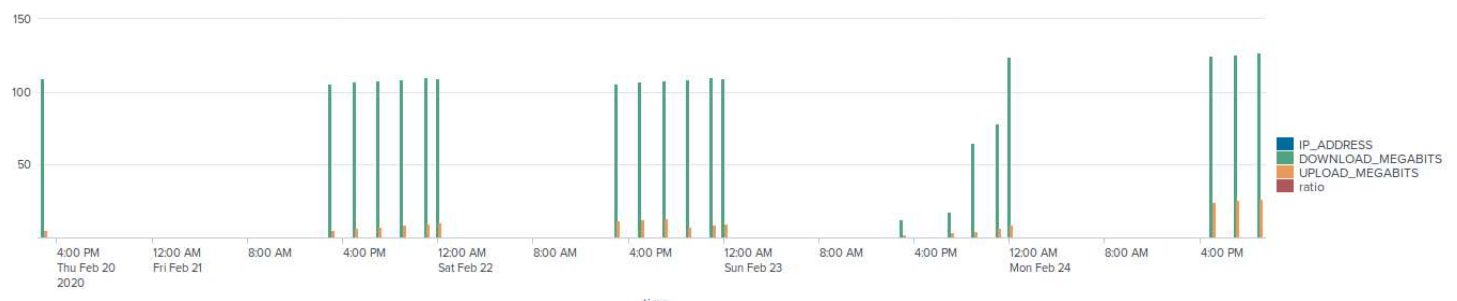
Here's the SPL search used to create the table:

```
source="server_speedtest.csv" | eval ratio = UPLOAD_MEGABITS / DOWNLOAD_MEGABITS | table [time IP_ADDRESS DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio]
```

Here is the table the above search created:

2020-02-22 14:30:00	198.153.194.1	105.91	11.51	0.1087
2020-02-21 23:30:00	198.153.194.1	109.16	10.51	0.09628
2020-02-21 22:30:00	198.153.194.1	109.91	9.51	0.0865
2020-02-21 20:30:00	198.153.194.1	108.91	8.51	0.0781
2020-02-21 18:30:00	198.153.194.2	107.91	7.51	0.0696
2020-02-21 16:30:00	198.153.194.2	106.91	6.51	0.0609
2020-02-21 14:30:00	198.153.194.1	105.91	5.51	0.0520
2020-02-20 14:21:00	198.153.194.1	109.16	5.43	0.0497
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	0.0687
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	0.0611
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	0.0831
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	0.0647
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	0.195
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	0.233
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	0.172
2020-02-22 23:30:00	198.153.194.2	109.16	9.51	0.0871
2020-02-22 22:30:00	198.153.194.2	109.91	8.51	0.0774
2020-02-22 20:30:00	198.153.194.2	108.91	7.51	0.0690
2020-02-24 18:30:00	198.153.194.2	125.91	25.51	0.2026
2020-02-24 16:30:00	198.153.194.1	124.91	24.51	0.1962
2020-02-24 20:30:00	198.153.194.2	126.91	26.51	0.2089

Here's a visualization of the data as well:



Questions

1. Based on the report created, what is the approximate date and time of the attack?
 - a. 2/23/2020 at 1430 (2:30 PM)
2. How long did it take your systems to recover?
 - a. The network didn't get back up to normal speeds until roughly nine hours later at 2330 (11:30 PM)

Step 2: Are We Vulnerable?

Here's the report of critical vulnerabilities for the "10.11.36.23" server which includes the "stats" search that compiled it:

```
source="nessus_logs.csv" | stats count(eval((dest_ip == "10.11.36.23") and (severity == "critical"))) as crit_vulns
```

✓ 1,849 events (before 1/31/22 4:30:38.000 AM) No Event Sampling ▼

Events Patterns **Statistics (1)** Visualization

50 Per Page ▼ ✎ Format Preview ▼

crit_vulns ▼

49

Also, I simply listed out the 49 critical vulnerabilities with the following:

```
source="nessus_logs.csv" | where [(dest_ip == "10.11.36.23") and (severity == "critical")]
```

And I used the above "where" search to create the following alert:

Critical Vulnerability on Database 10.11.36.23

Enabled: Yes. [Disable](#)

App: search

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

Modified: Jan 31, 2022 4:45:48 AM

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

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

Actions: ▼ 1 Action [Edit](#)

✉ Send email

Step 3: Drawing the (base)line

I used the following search to determine the number of failed login attempts by hour for the entire event file:

```

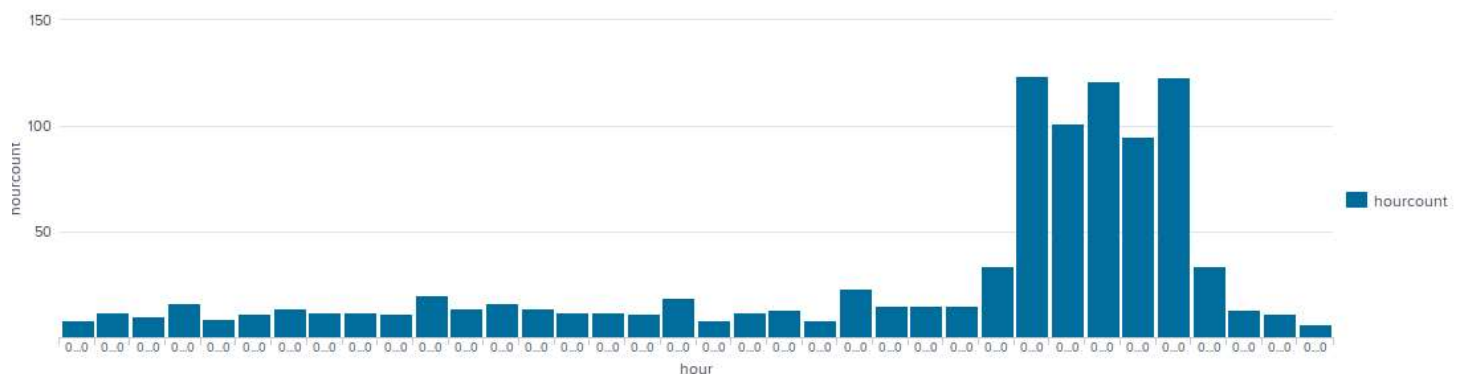
source="Administrator_logs.csv"
| where name == "An account failed to log on"
| bin _time as hour span=1h
| eval hour=strftime(hour,"%m-%dT%H:%M")
| stats count as hourcount by hour

```

The following subsection of the report shows the counts for a time range that seems most likely to be when the attack occurred:

02-21T 05:00	15
02-21T 06:00	15
02-21T 07:00	15
02-21T 08:00	34
02-21T 09:00	124
02-21T 10:00	101
02-21T 11:00	121
02-21T 12:00	95
02-21T 13:00	123
02-21T 14:00	34
02-21T 15:00	13
02-21T 16:00	11
02-21T 17:00	6

A visualization makes it even more clear:



So, the attack most likely occurred between a little before 2/21 9:00 AM until a little after 2/21 2:00 PM.

The Baseline

I think a number that errs on the safe side is thirty instances of a “An account failed to log on” event.

The Alert

Here is the search I used for the alert:

```
source="Administrator_logs.csv"
| where name == "An account failed to log on"
```

Here is the alert:

Possible Brute Force Login Attack

Enabled: Yes. [Disable](#)

App: search


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

Modified: Jan 31, 2022 5:36:39 AM

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

Trigger Condition: .. Number of Results is > 29. [Edit](#)

Actions: [▼](#) 1 Action [Edit](#)

 Send email