Cybersecurity

Module 19 Challenge Submission File

Let's Go Splunking!

Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

Step 1: The Need for Speed

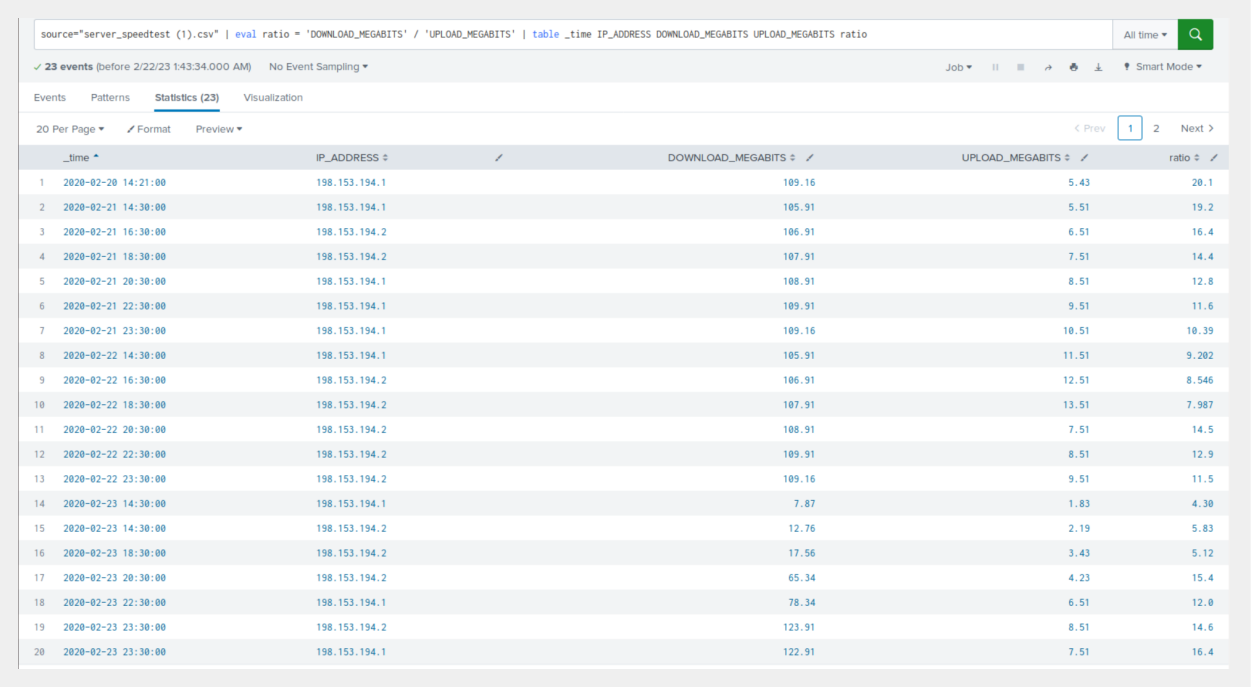
1. Based on the report you created, what is the approximate date and time of the attack?

```
The attack began on 2020-02-23 at 14:30:00, the download speeds dropped from
around 100 to ~7 and the Upload went from around 10 to ~1.
```

2. How long did it take your systems to recover?

```
It seems that the systems had recovered by 23:30:00 on the same day.
```

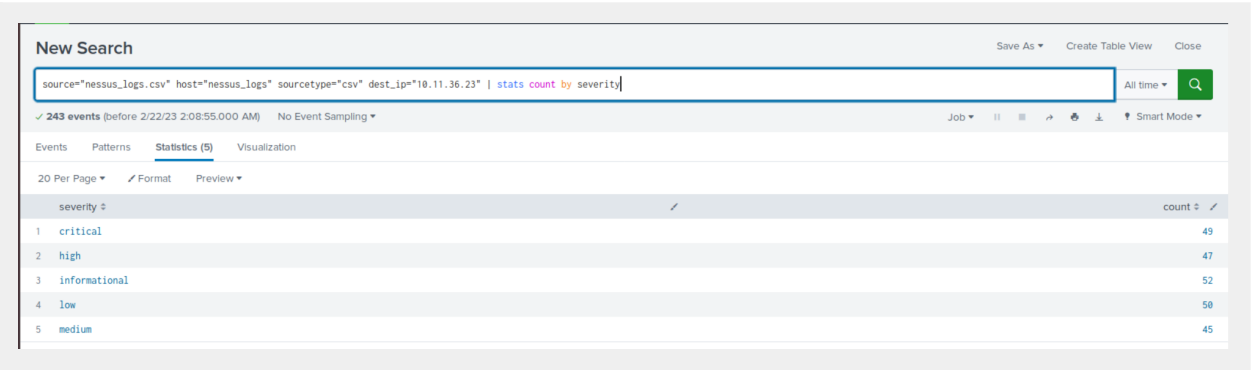
Provide a screenshot of your report:



	_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
1	2020-02-20 14:21:00	198.153.194.1	109.16	5.43	20.1
2	2020-02-21 14:30:00	198.153.194.1	105.91	5.51	19.2
3	2020-02-21 16:30:00	198.153.194.2	106.91	6.51	16.4
4	2020-02-21 18:30:00	198.153.194.2	107.91	7.51	14.4
5	2020-02-21 20:30:00	198.153.194.1	108.91	8.51	12.8
6	2020-02-21 22:30:00	198.153.194.1	109.91	9.51	11.6
7	2020-02-21 23:30:00	198.153.194.1	109.16	10.51	10.39
8	2020-02-22 14:30:00	198.153.194.1	105.91	11.51	9.202
9	2020-02-22 16:30:00	198.153.194.2	106.91	12.51	8.546
10	2020-02-22 18:30:00	198.153.194.2	107.91	13.51	7.987
11	2020-02-22 20:30:00	198.153.194.2	108.91	7.51	14.5
12	2020-02-22 22:30:00	198.153.194.2	109.91	8.51	12.9
13	2020-02-22 23:30:00	198.153.194.2	109.16	9.51	11.5
14	2020-02-23 14:30:00	198.153.194.1	7.87	1.83	4.30
15	2020-02-23 14:30:00	198.153.194.2	12.76	2.19	5.83
16	2020-02-23 18:30:00	198.153.194.2	17.56	3.43	5.12
17	2020-02-23 20:30:00	198.153.194.2	65.34	4.23	15.4
18	2020-02-23 22:30:00	198.153.194.1	78.34	6.51	12.0
19	2020-02-23 23:30:00	198.153.194.2	123.91	8.51	14.6
20	2020-02-23 23:30:00	198.153.194.1	122.91	7.51	16.4

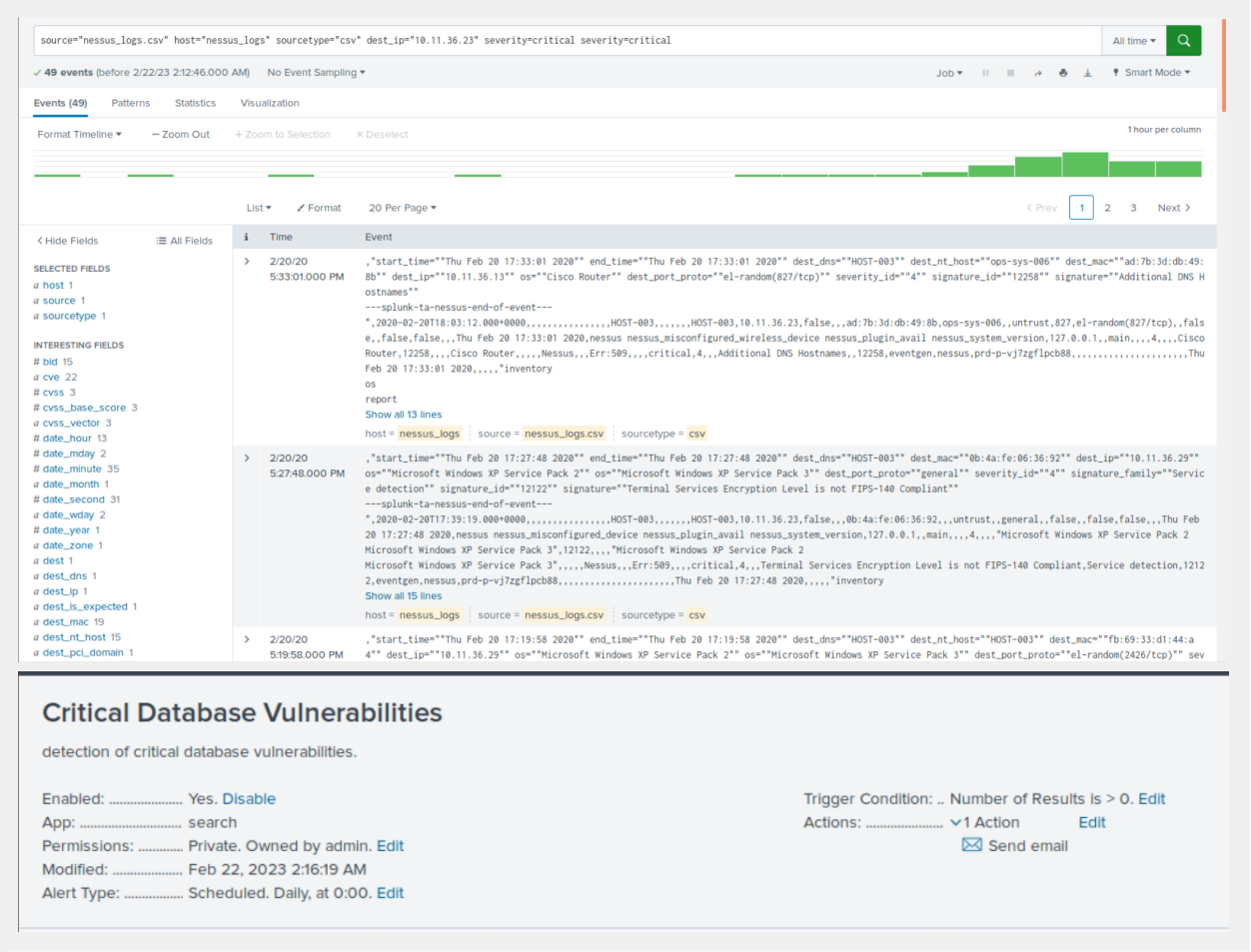
Step 2: Are We Vulnerable?

Provide a screenshot of your report:



	severity	count
1	critical	49
2	high	47
3	informational	52
4	low	50
5	medium	45

Provide a screenshot showing that the alert has been created:



Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

```
The brute force attack started at 8am on Feb 21st 2020 and ended around 2pm
on the same day.
```

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

```
The baseline of activity would be from 5-28 failed login attempts, and the
threshold would be 35 failed login attempts
```

3. Provide a screenshot showing that the alert has been created: