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

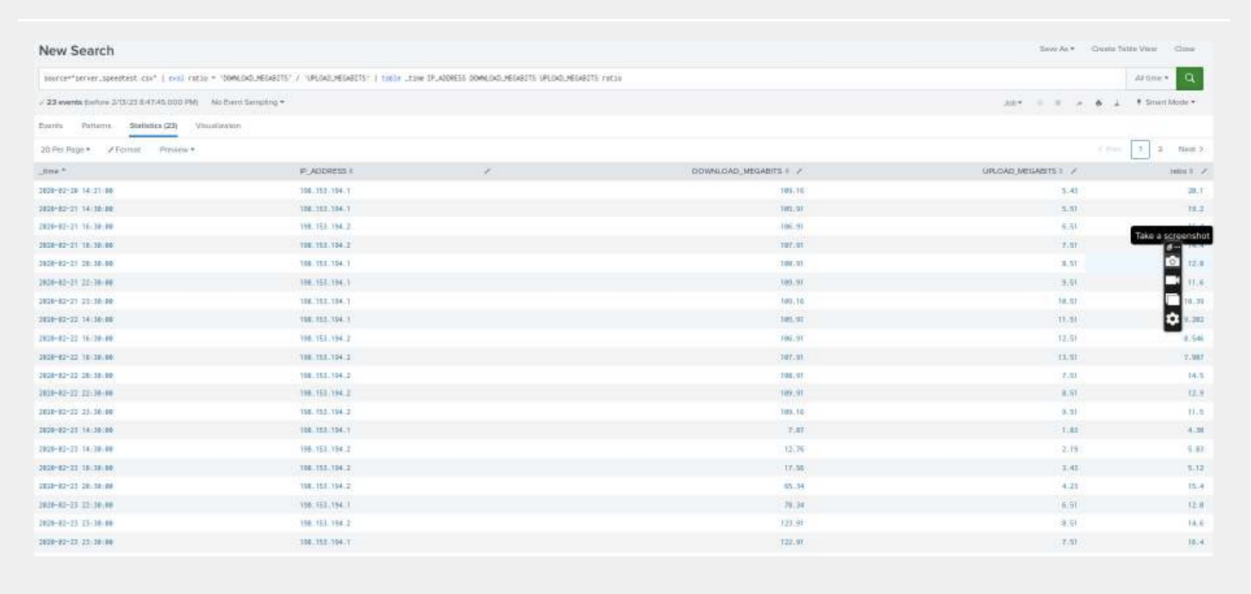
1. Based on the report you created, what is the approximate date and time of the attack?

```
02/23/2020 at 2:30pm
```

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

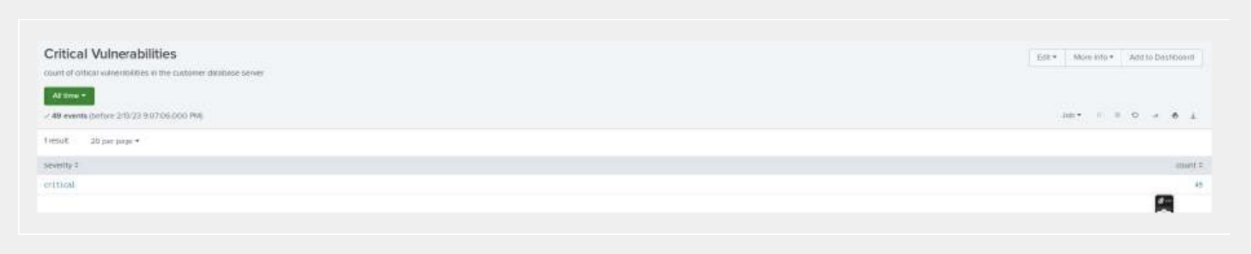
```
6hrs to recover
9hrs from 2:30pm - 10:30pm
```

Provide a screenshot of your report:

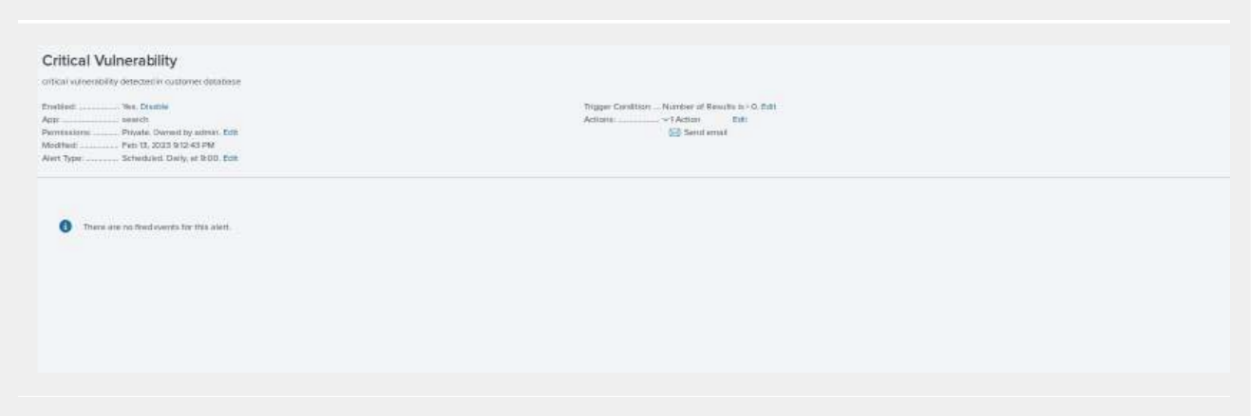


Step 2: Are We Vulnerable?

Provide a screenshot of your report:



Provide a screenshot showing that the alert has been created:



Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

```
02/21 4am - 2pm
```

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

```
The baseline is 25 or more log in attempts per hour is the baseline to
determine brute force attacks.
```

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