# 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

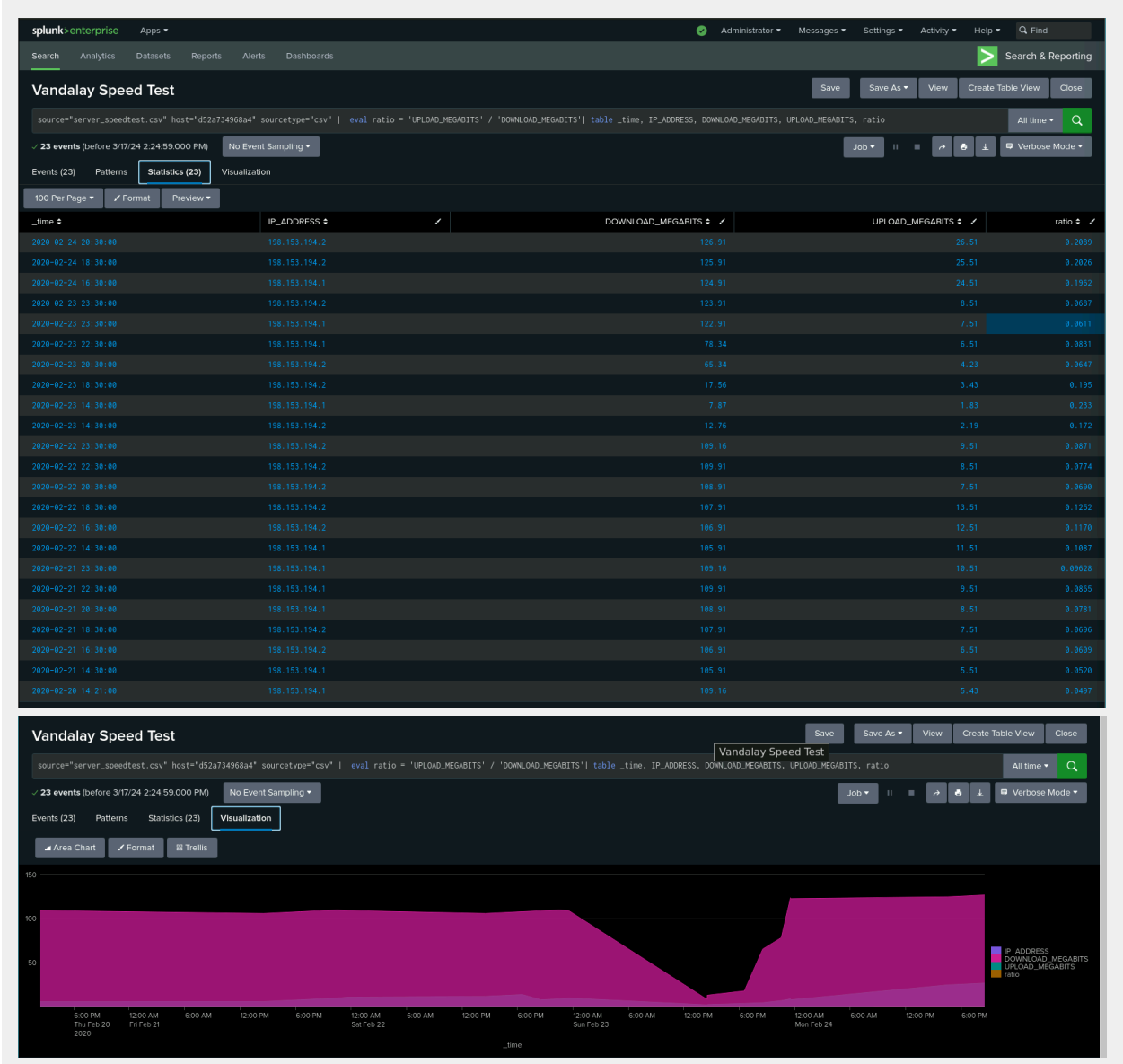
1. Based on the report you created, what is the approximate date and time of the attack?

```
Based on our report, Download speeds hit their maximum low at 2:30 p.m. on
February 23, 2020 but the attack appeared to start at 11:30 p.m. on February
22, 2020 and didn't end until February 23, at 11:30 p.m.
```

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

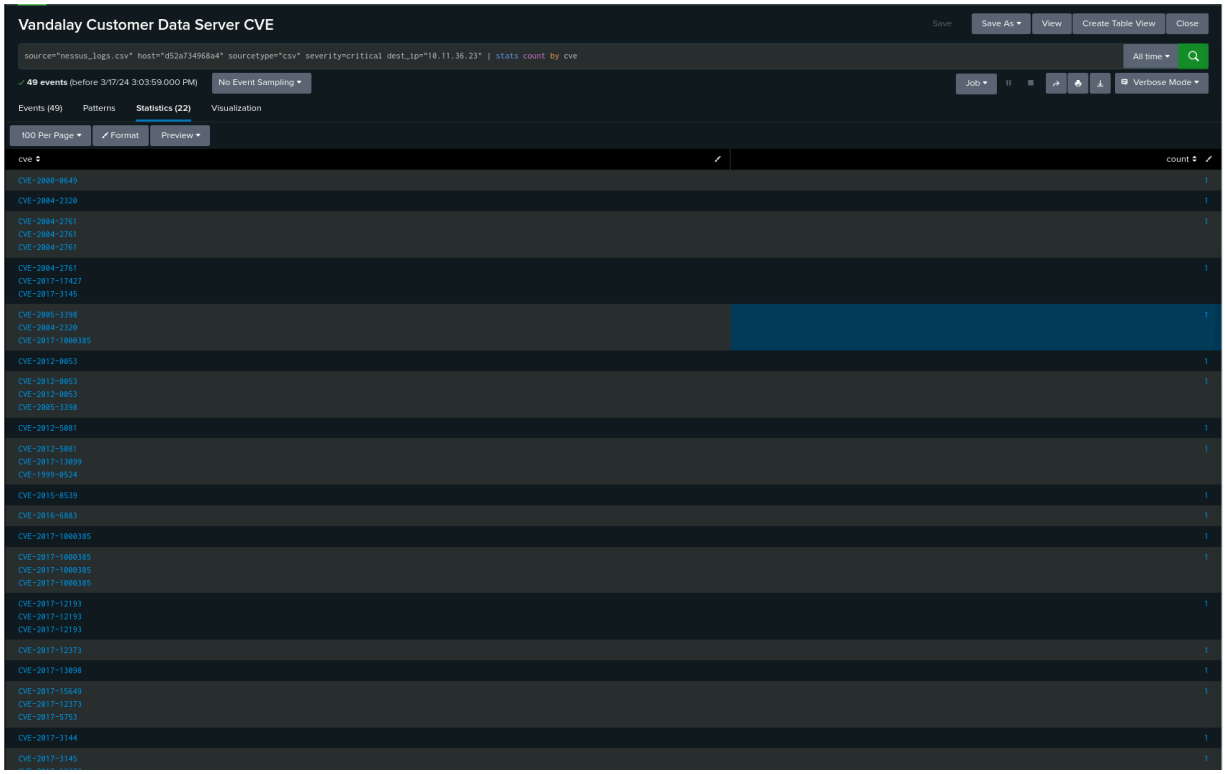
```
It took our systems 9 hours to recover from the maximum low point of
download speeds.
```

Provide a screenshot of your report:

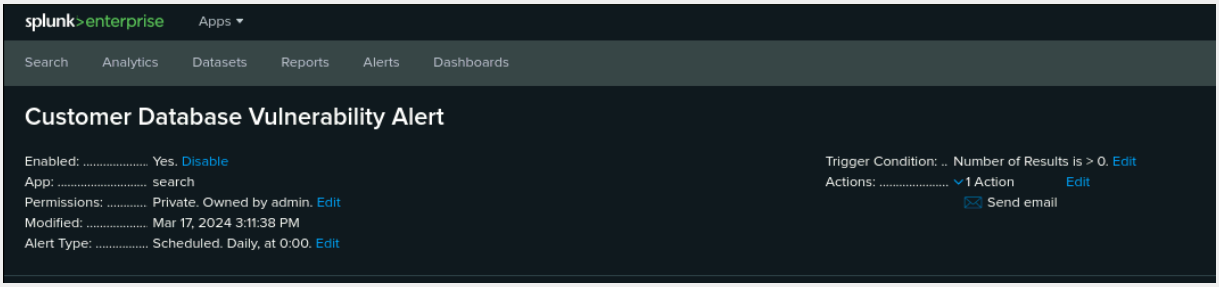



## Step 2: Are We Vulnerable?

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?

```
According to the logs, the largest amount of failed login attempts occurred at 4:00 a.m. on Friday, February 21, 2020. This would suggest that the brute force attack occurred at this time.
```

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

Over the course of 36 hours, there were 469 bag login attempts. If we exclude the hour of the attack, that comes out to 446 bad logins over the course of 35 hours. That averages out to about 13 bad logins per hour in each aforementioned case. Looking at days when there was no attack but the volume of bad logins was high, we see the numbers hit upwards of 20 events. Based on this information, we suggest a threshold of 16 bad logins per hour, the average of the normal amount of logins vs the highest number of normal logins.

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