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

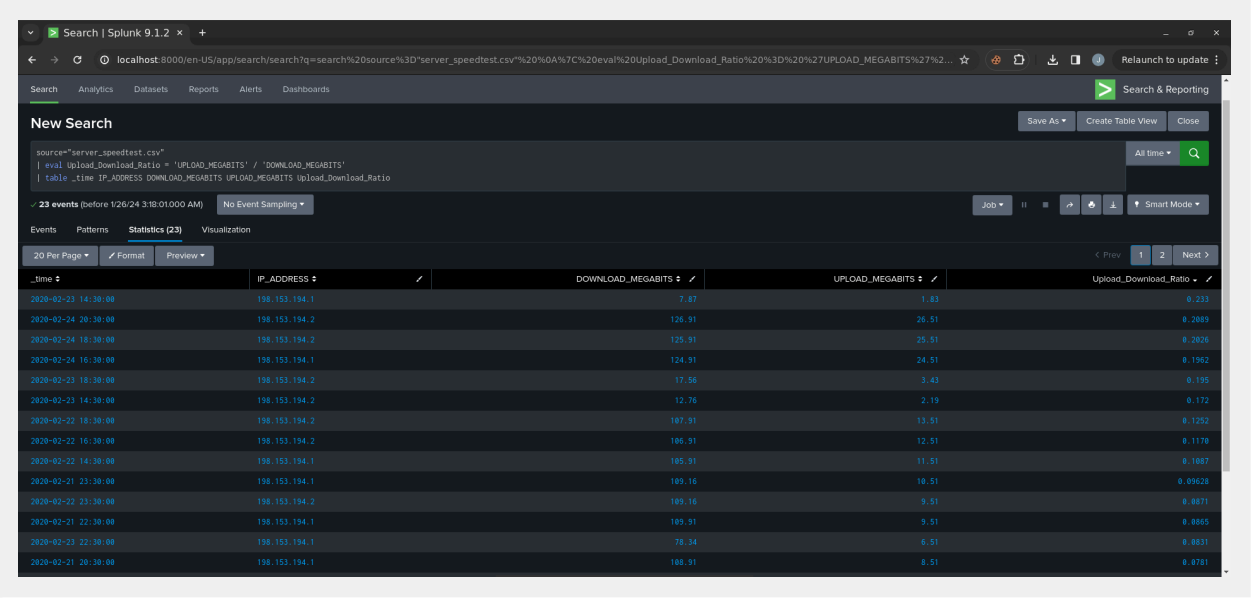
1. Based on the report you created, what is the approximate date and time of the attack?

```
The attack appears to have occurred/started at 2020-02-24 14:30:00
Not only was the ratio high at this time, but the download and upload
megabits are in excess of the average.
While there is a high ratio on 2020-02-24 14:30:00, the downloaded and
uploaded megabits are relatively low compared to the average during this
time.
```

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

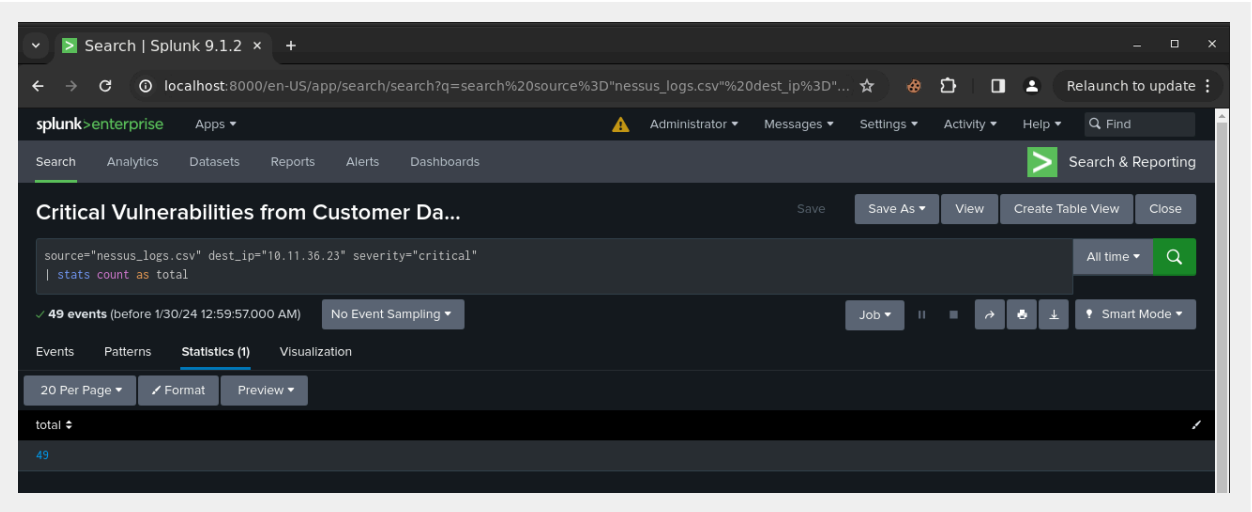
```
Approximately 5 hours. The high ratio and volume of downloaded and uploaded
megabits continues through 2020-02-24 20:30:00. The report ends at this
time, so it is difficult to say whether systems were impacted past this
time.
```

Provide a screenshot of your report:

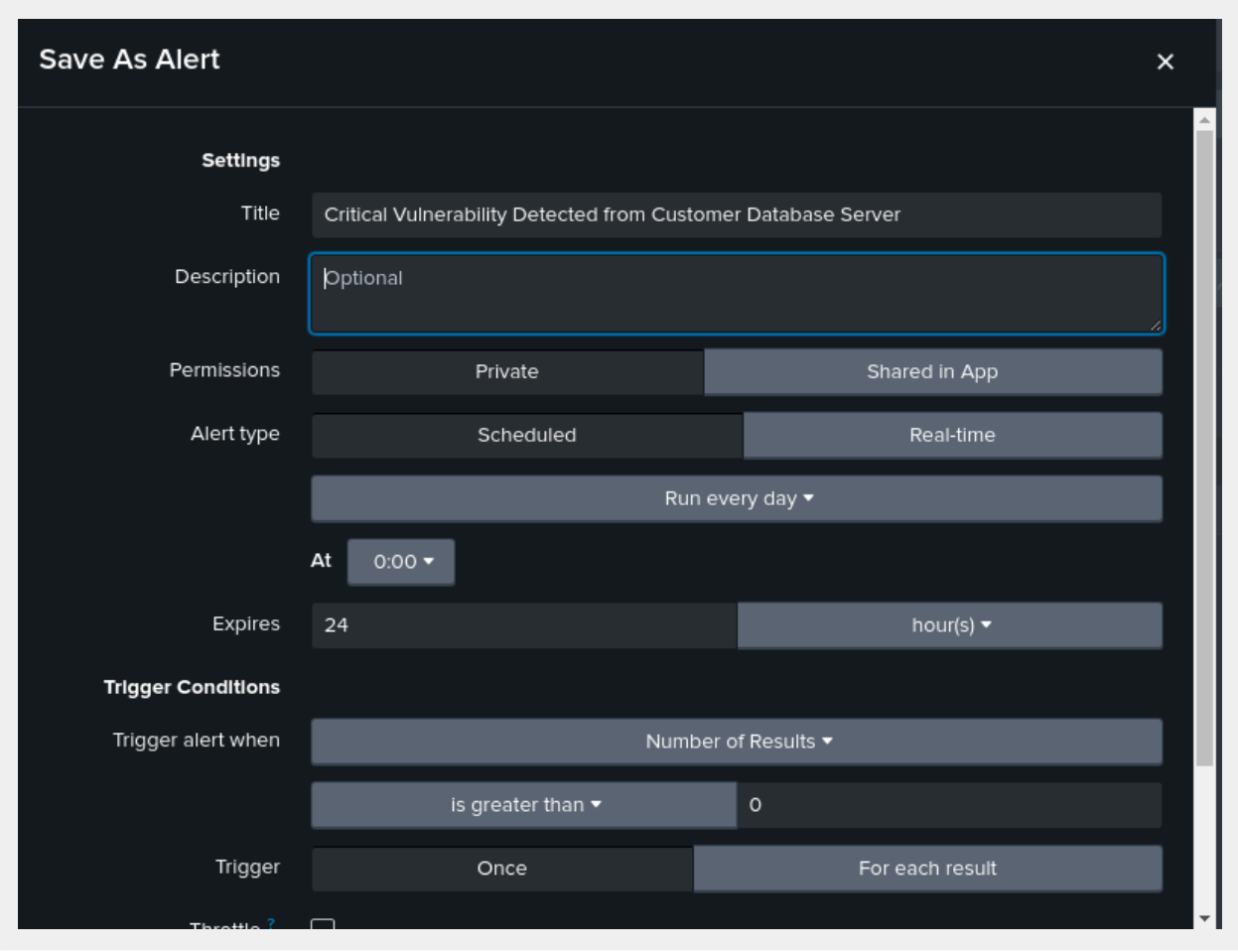


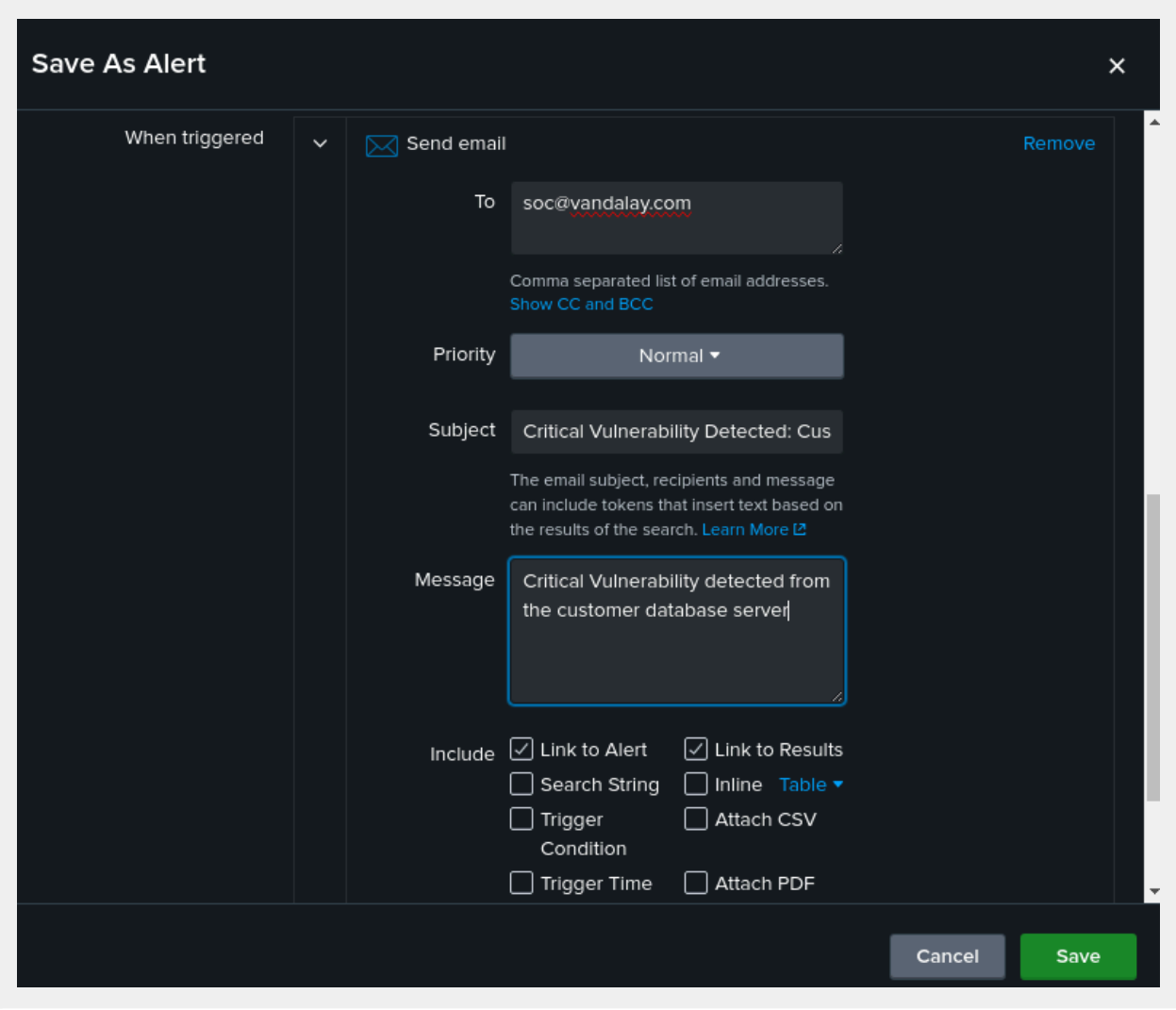
Step 2: Are We Vulnerable?

Provide a screenshot of your report:



Provide a screenshot showing that the alert has been created:


Save As Alert
Settings
Title
Critical Vulnerability Detected from Customer Database Server
Description
Optional
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every day
At
0:00
Expires
24
hour(s)
Trigger Conditions
Trigger alert when
Number of Results
is greater than
0
Trigger
Once
For each result



Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

```
February 21, 2020 9 AM - 2 PM (spike began in the 9-10 hour and continued
through the 1-2 hour).
```

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

```
36 hours of data are in this file with 1,004 events, making the average
27.89 per hour. Outside the attack range, the events appear to range from 6
```

to 34, and during the attack, range from 95-124. Therefore, I would set the alert threshold at 40.
This value should prevent many false positives without actual attack indicators slipping through the cracks.

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