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

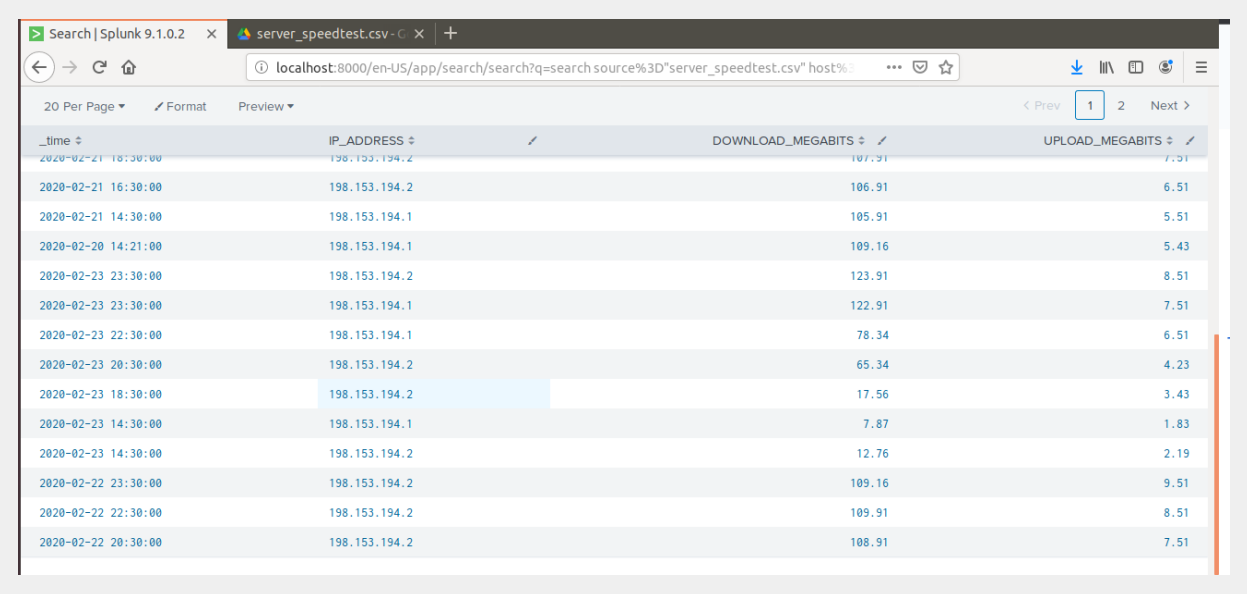
1. Based on the report you created, what is the approximate date and time of the attack?

```
2/23/2020 between 14:30 to 23:30
```

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

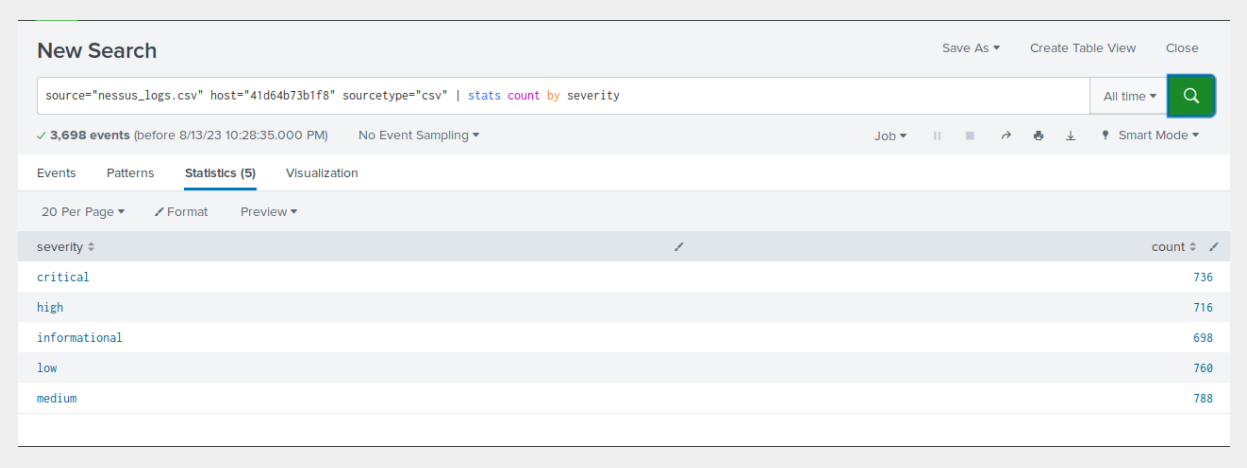
```
Nine hours
```

Provide a screenshot of your report:

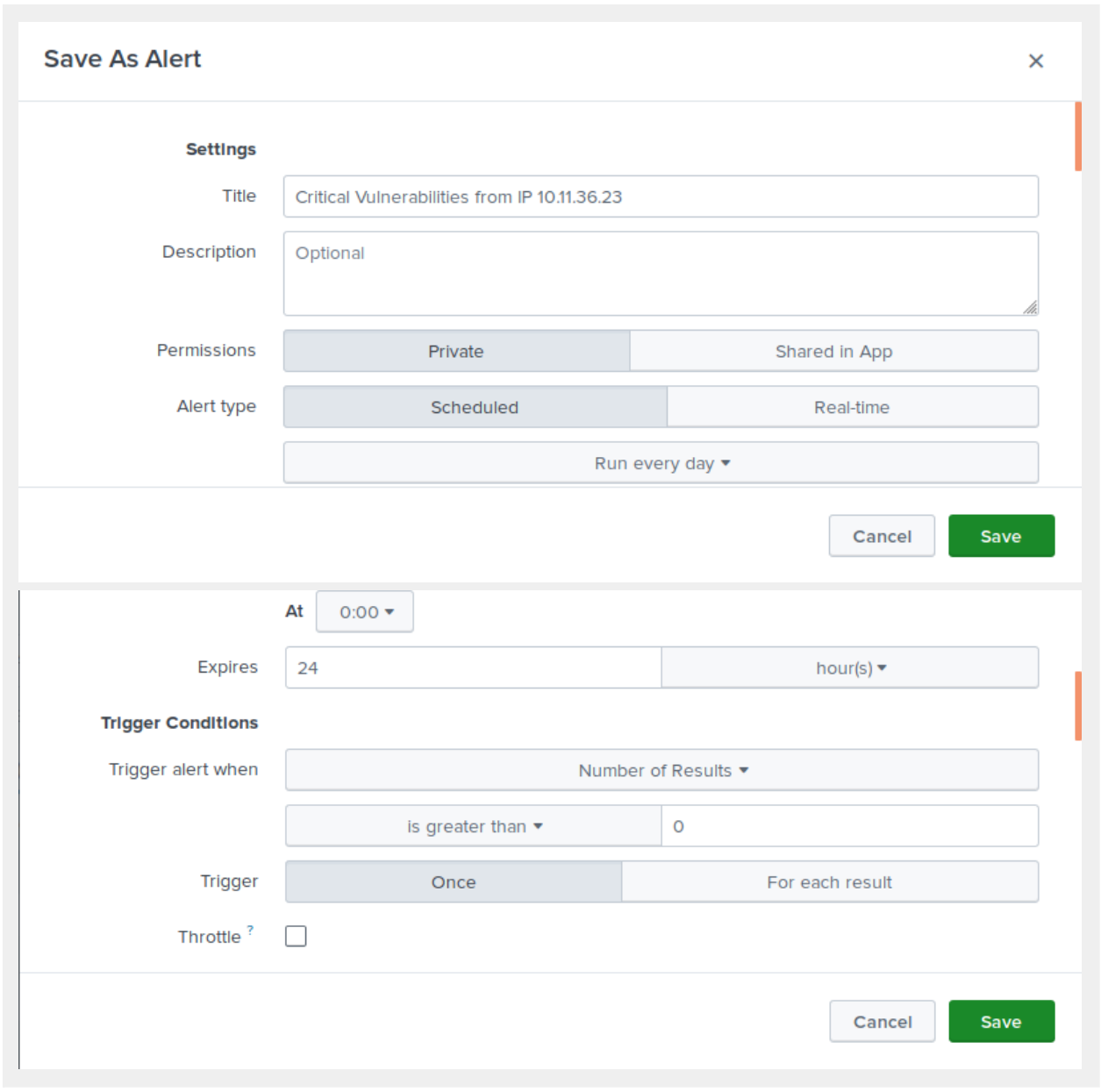


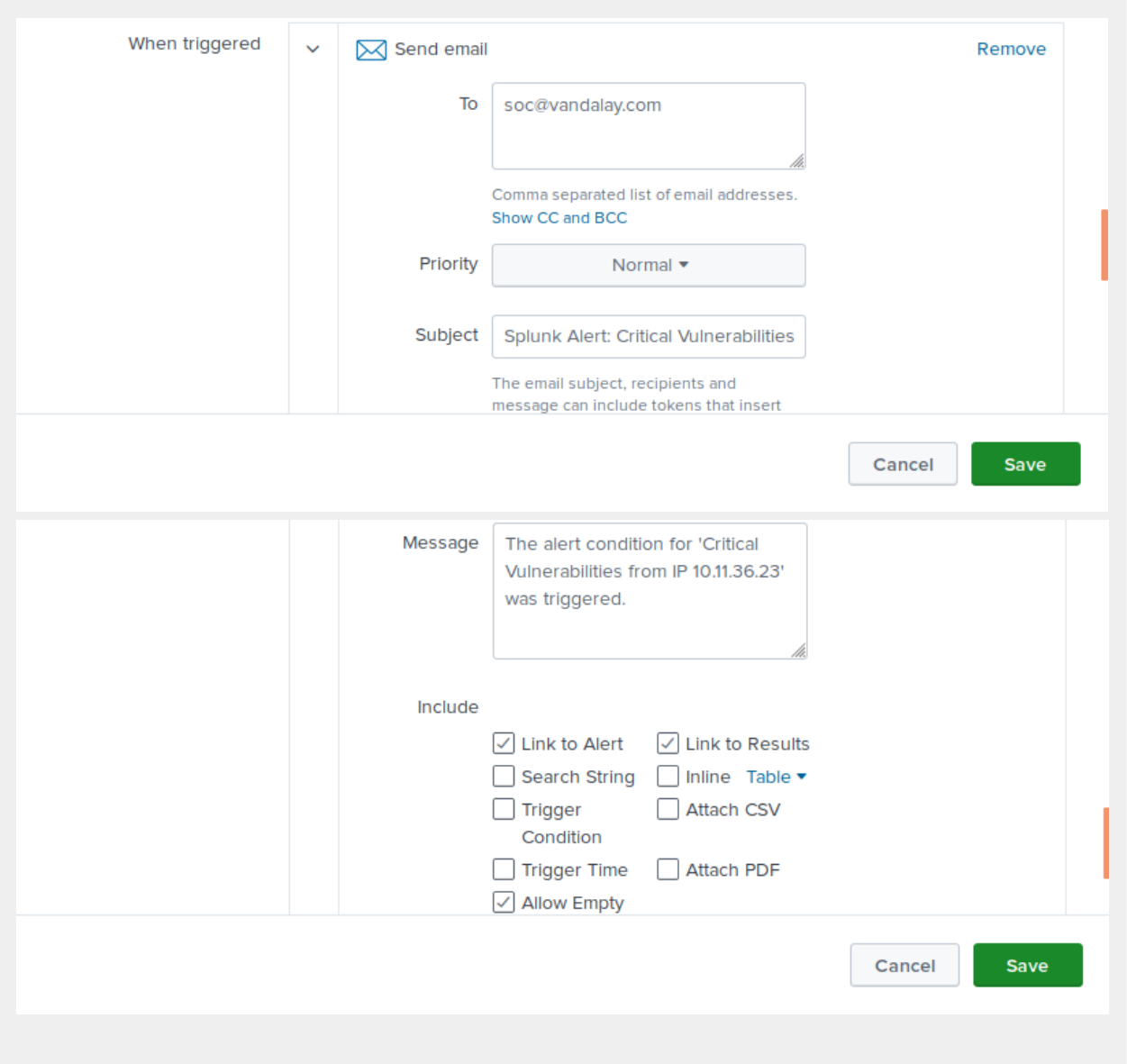
Step 2: Are We Vulnerable?

Provide a screenshot of your report:



Provide a screenshot showing that the alert has been created:


Save As Alert
Settings
Title
Critical Vulnerabilities from IP 10.11.36.23
Description
Optional
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every day
Cancel
Save
At
0:00
Expires
24
hour(s)
Trigger Conditions
Trigger alert when
Number of Results
is greater than
0
Trigger
Once
For each result
Throttle
Cancel
Save



Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

```
2/21/2020 from 9:00 to 14:00
```

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

```
My baseline is roughly 20 logins per hour and my threshold would be greater
than or equal to 30 attempts.
```

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