Cybersecurity

Module 19 Challenge Submission File

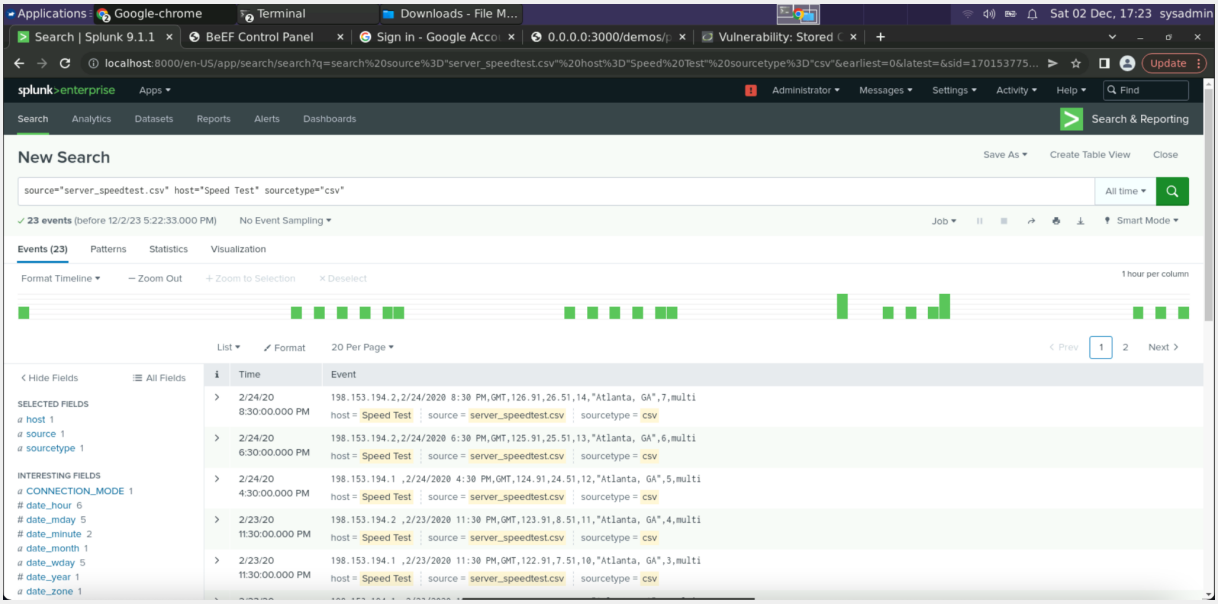
Let's Go Splunking!

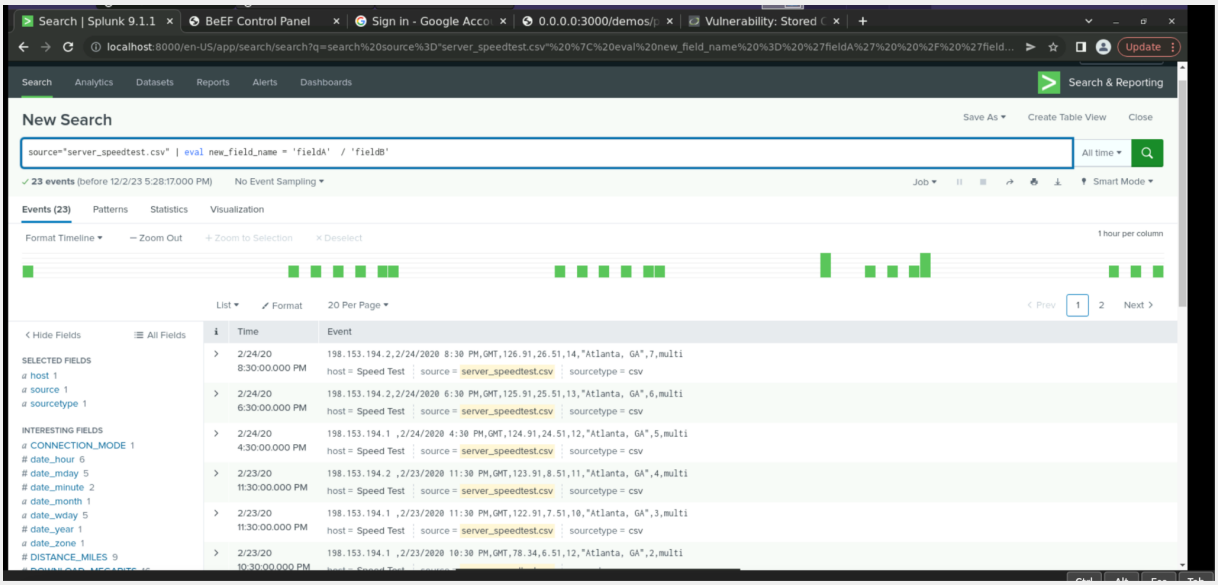
Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

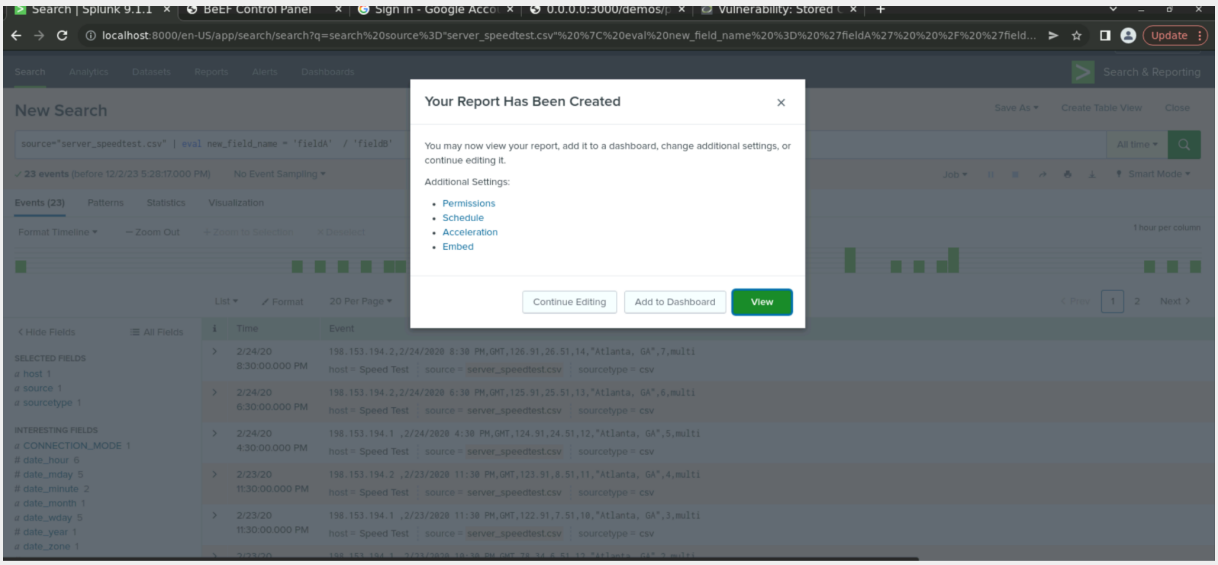
Step 1: The Need for Speed

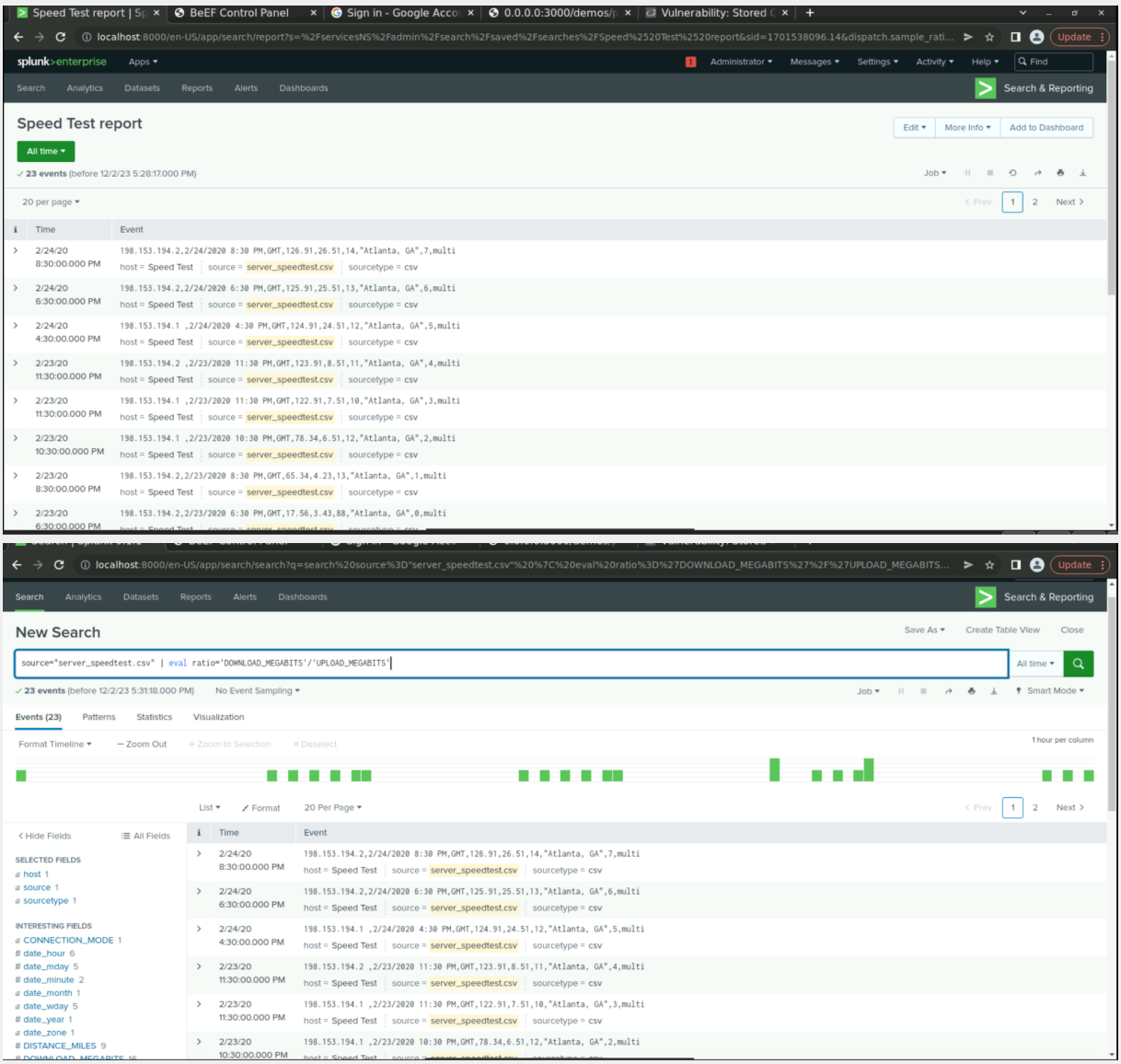
1. Based on the report you created, what is the approximate date and time of the attack?

```
The attack occurred on 02/22/2020 at 1130, where the download speed
decreased exponentially from 109.16 Mbps to 7.87 bps and it lasted till 2330
on 02/23/2020, when the speed reverted back to normal over 122.91 Mbps.
```


Search | Splunk 9.1.1
BeEF Control Panel
Vulnerability: Stored
splunk>enterprise
Search & Reporting
New Search
source="server_speedtest.csv" host="Speed Test" sourcetype="csv"
23 events (before 12/2/23 5:22:33.000 PM)
Events (23)
Patterns
Statistics
Visualization
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
CONNECTION_MODE 1
date_hour 6
date_mday 5
date_minute 2
date_month 1
date_wday 5
date_year 1
date_zone 1
Time
Event
2/24/20 8:30:00.000 PM
198.153.194.2,2/24/2020 8:30 PM,GMT,126.91,26.51,14,"Atlanta, GA",7,multi
2/24/20 6:30:00.000 PM
198.153.194.2,2/24/2020 6:30 PM,GMT,125.91,25.51,13,"Atlanta, GA",6,multi
2/24/20 4:30:00.000 PM
198.153.194.1 ,2/24/2020 4:30 PM,GMT,124.91,24.51,12,"Atlanta, GA",5,multi
2/23/20 11:30:00.000 PM
198.153.194.2 ,2/23/2020 11:30 PM,GMT,123.91,8.51,11,"Atlanta, GA",4,multi
2/23/20 11:30:00.000 PM
198.153.194.1 ,2/23/2020 11:30 PM,GMT,122.91,7.51,10,"Atlanta, GA",3,multi


Search | Splunk 9.1.1
BeEF Control Panel
Vulnerability: Stored
Search & Reporting
New Search
source="server_speedtest.csv" | eval new_field_name = 'fieldA' / 'fieldB'
23 events (before 12/2/23 5:28:17.000 PM)
Events (23)
Patterns
Statistics
Visualization
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
CONNECTION_MODE 1
date_hour 6
date_mday 5
date_minute 2
date_month 1
date_wday 5
date_year 1
date_zone 1
DISTANCE_MILES 9
Time
Event
2/24/20 8:30:00.000 PM
198.153.194.2,2/24/2020 8:30 PM,GMT,126.91,26.51,14,"Atlanta, GA",7,multi
2/24/20 6:30:00.000 PM
198.153.194.2,2/24/2020 6:30 PM,GMT,125.91,25.51,13,"Atlanta, GA",6,multi
2/24/20 4:30:00.000 PM
198.153.194.1 ,2/24/2020 4:30 PM,GMT,124.91,24.51,12,"Atlanta, GA",5,multi
2/23/20 11:30:00.000 PM
198.153.194.2 ,2/23/2020 11:30 PM,GMT,123.91,8.51,11,"Atlanta, GA",4,multi
2/23/20 11:30:00.000 PM
198.153.194.1 ,2/23/2020 11:30 PM,GMT,122.91,7.51,10,"Atlanta, GA",3,multi
2/23/20
198.153.194.1 ,2/23/2020 10:30 PM,GMT,78.34,6.51,12,"Atlanta, GA",2,multi

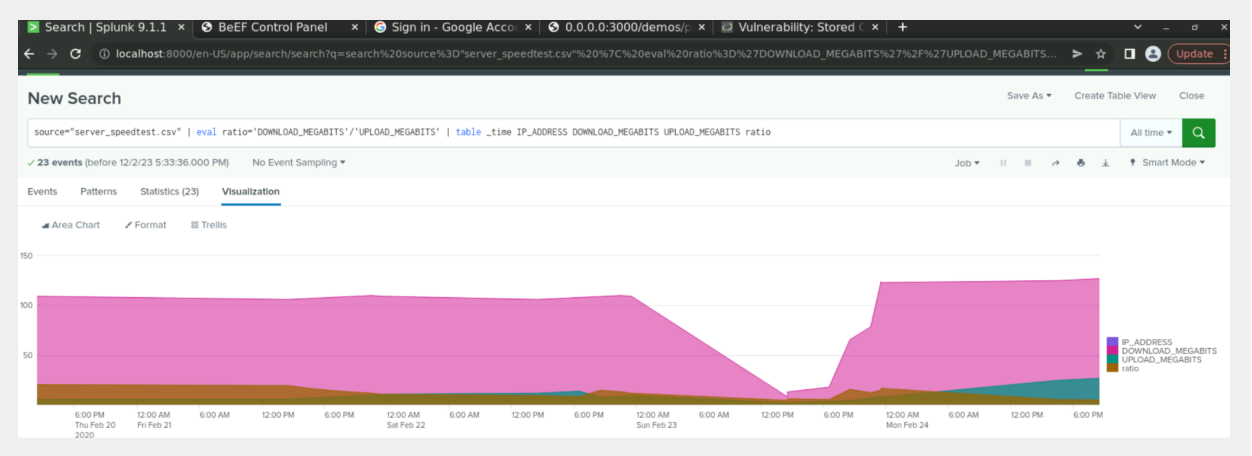

Your Report Has Been Created
You may now view your report, add it to a dashboard, change additional settings, or continue editing it.
Additional Settings:
Permissions
Schedule
Acceleration
Embed
Continue Editing
Add to Dashboard
View
New Search



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

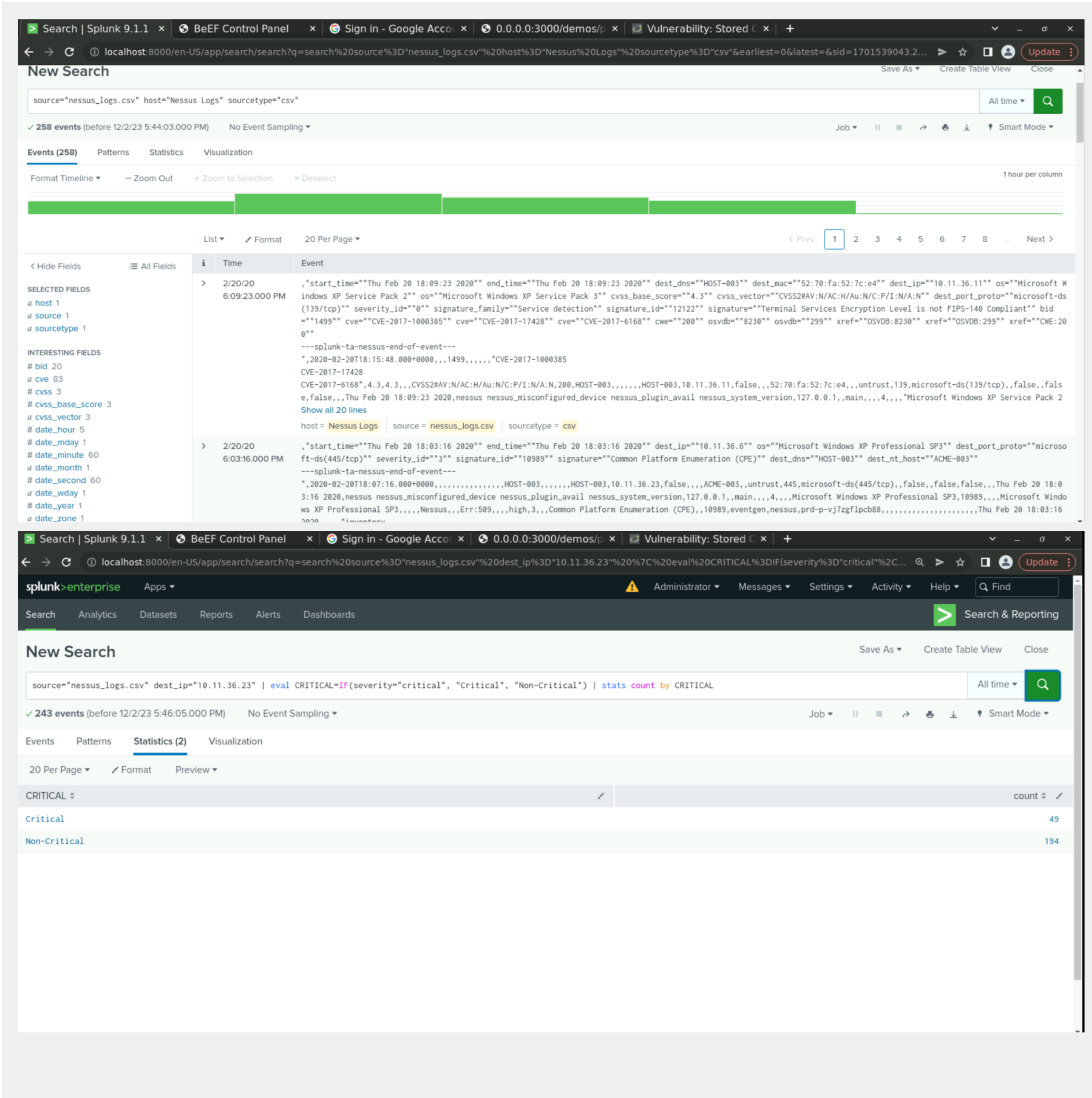
```
It took 24 hours to recover.
```

Provide a screenshot of your report:

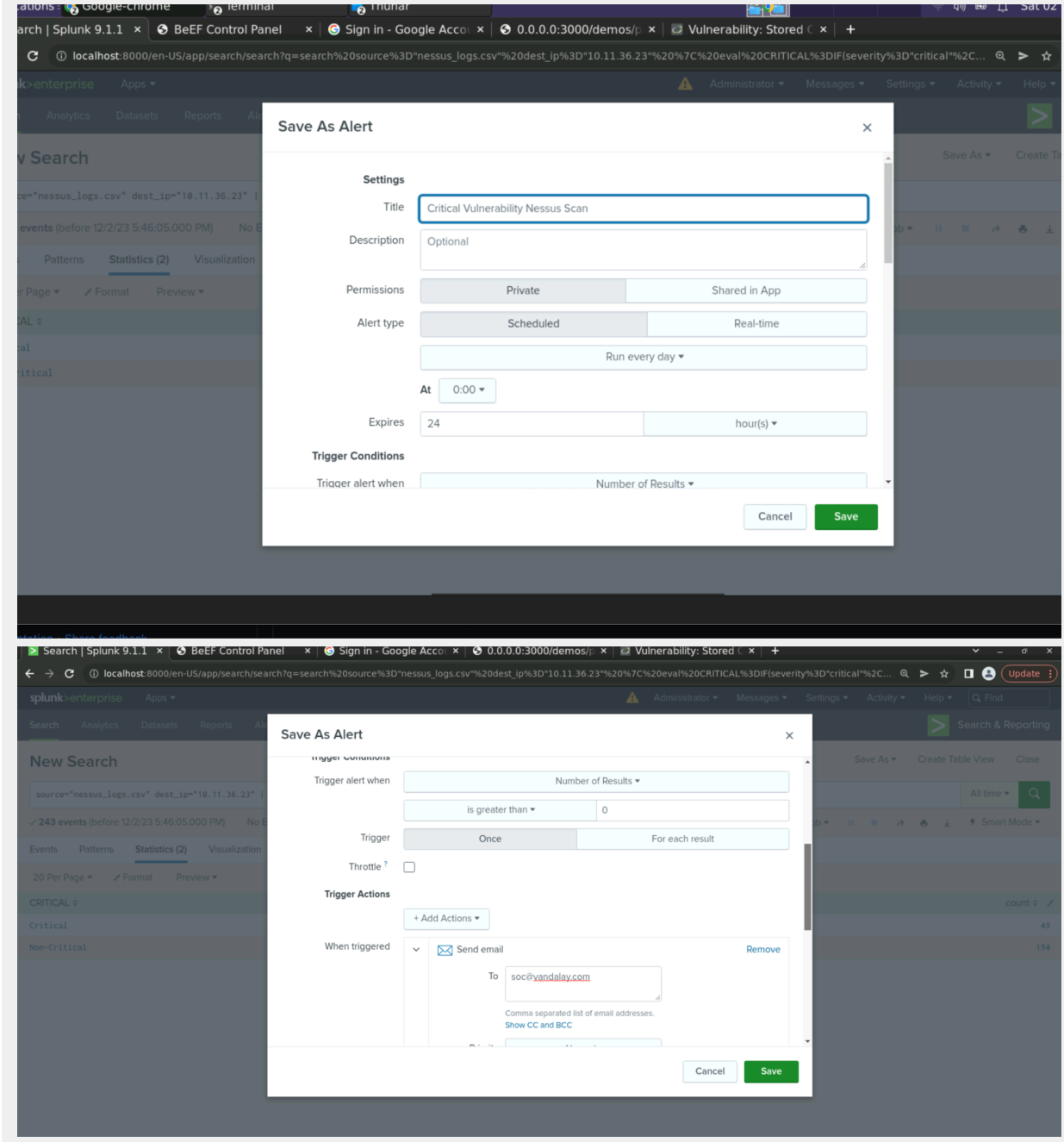


Step 2: Are We Vulnerable?

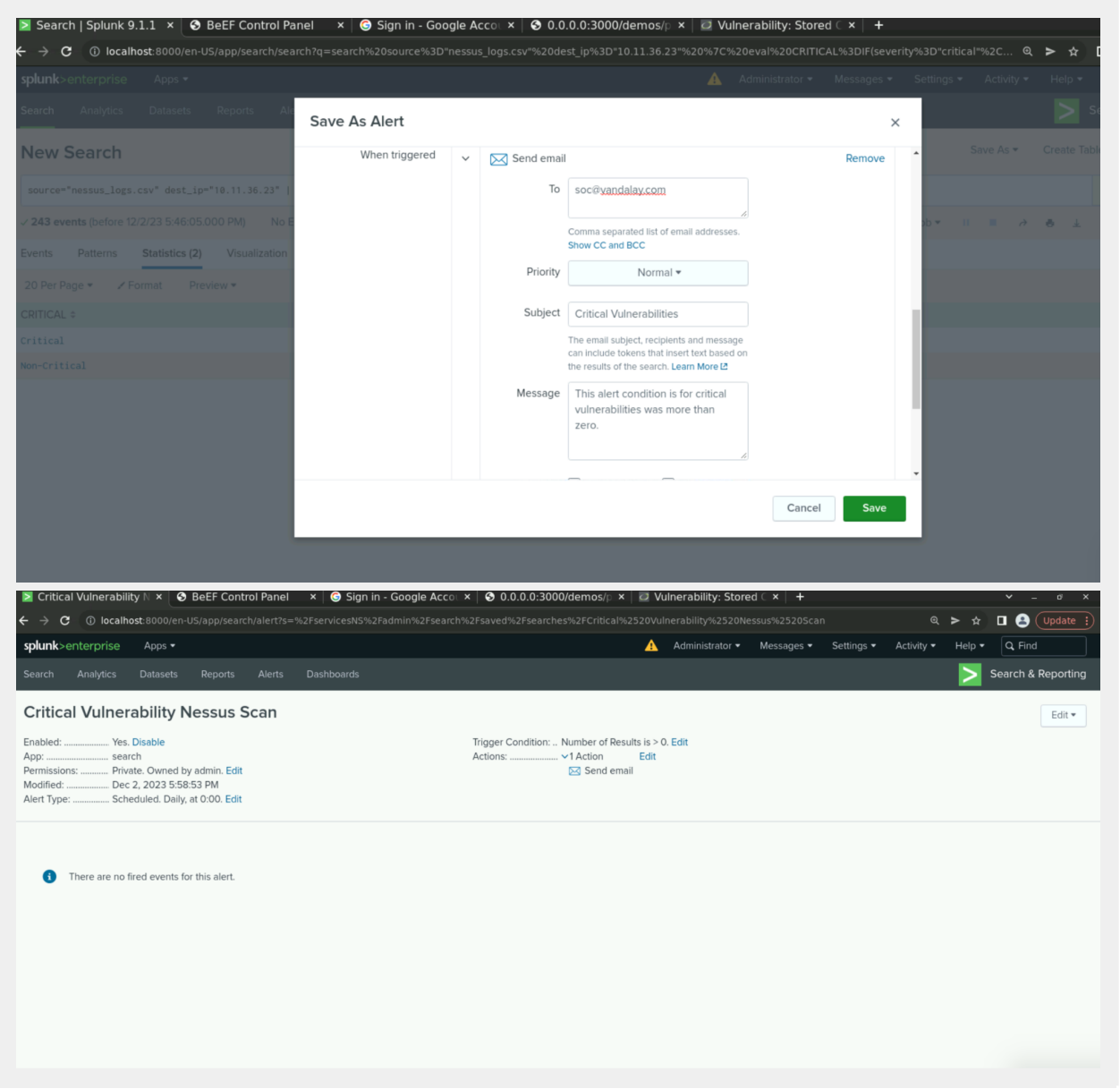
Provide a screenshot of your report:



Provide a screenshot showing that the alert has been created:


Save As Alert
Settings
Title
Critical Vulnerability Nessus Scan
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
Cancel
Save

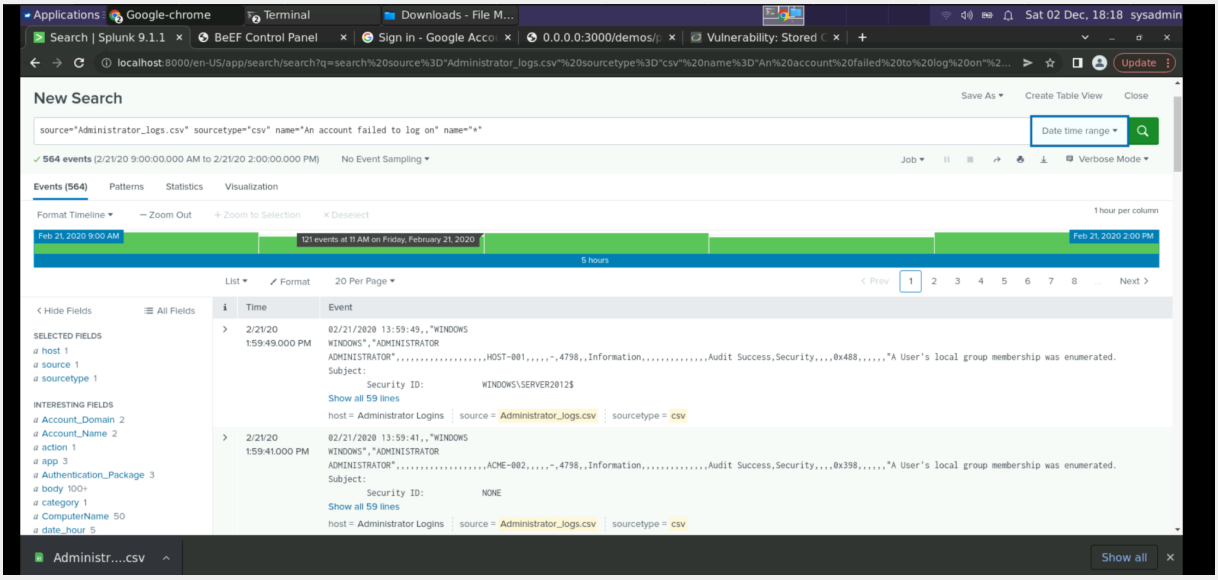
Save As Alert
Trigger alert when
Number of Results
is greater than
0
Trigger
Once
For each result
Throttle
Trigger Actions
+ Add Actions
When triggered
Send email
Remove
To
soc@yandalay.com
Comma separated list of email addresses.
Show CC and BCC
Cancel
Save



Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

The brute force attack occurred 0900 until 1400 on 2/21/2020 for 5 hours.



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

According to the logs, the baseline is 5-35 logs per hour. Therefore the threshold should be set at 40 or higher login attempts each hour and the alert will be emailed to SOC@vandalay.com when it's triggered.

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