Unit 18 Homework: Lets go Splunking!

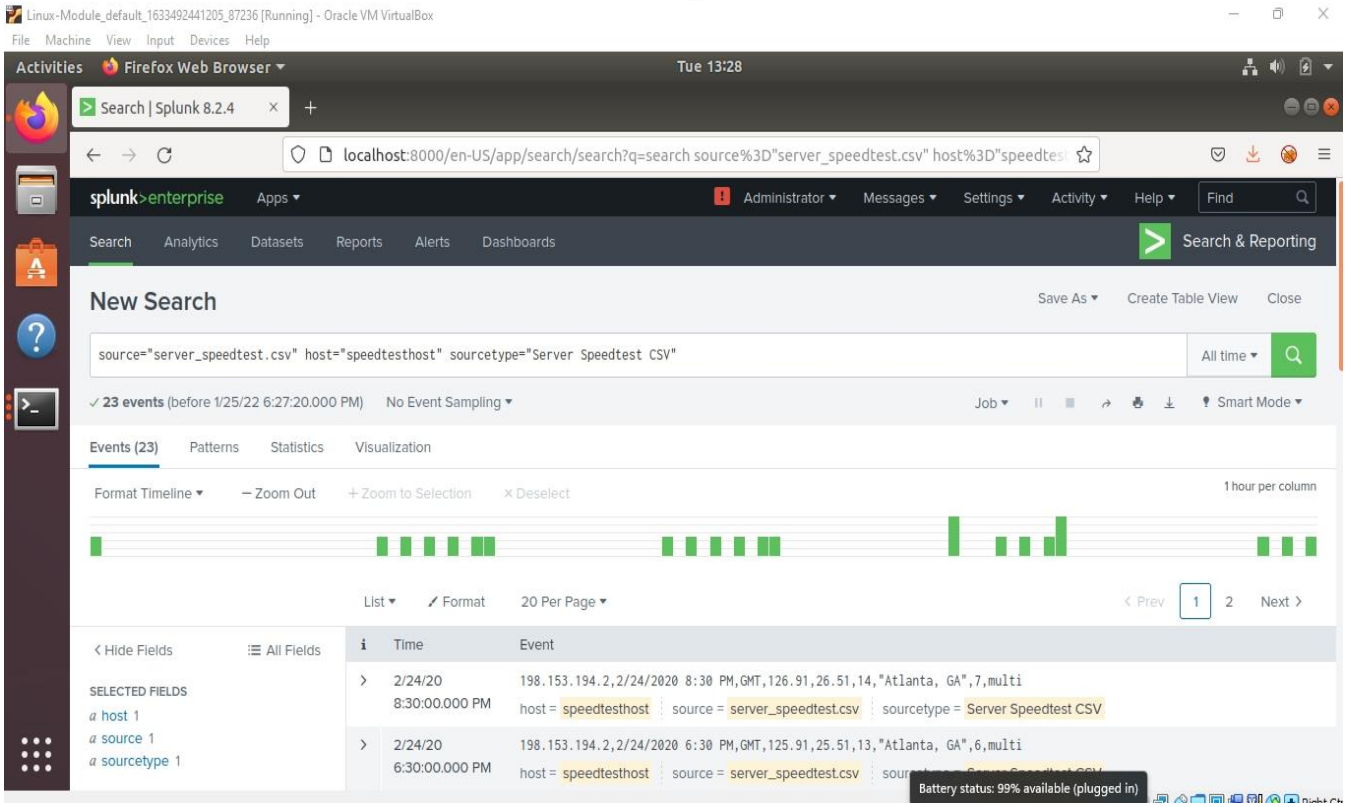
Vandalay Industries Monitoring Activity

Step 1: The Need for Speed

****Background**: As the worldwide leader of importing and exporting, Vandalay Industries has been the target of many adversaries attempting to disrupt their online business. Recently, Vandaly has been experiencing DDOS attacks against their web servers.**

Not only were web servers taken offline by a DDOS attack, but upload and download speed were also significantly impacted after the outage. Your networking team provided results of a network speed run around the time of the latest DDOS attack.

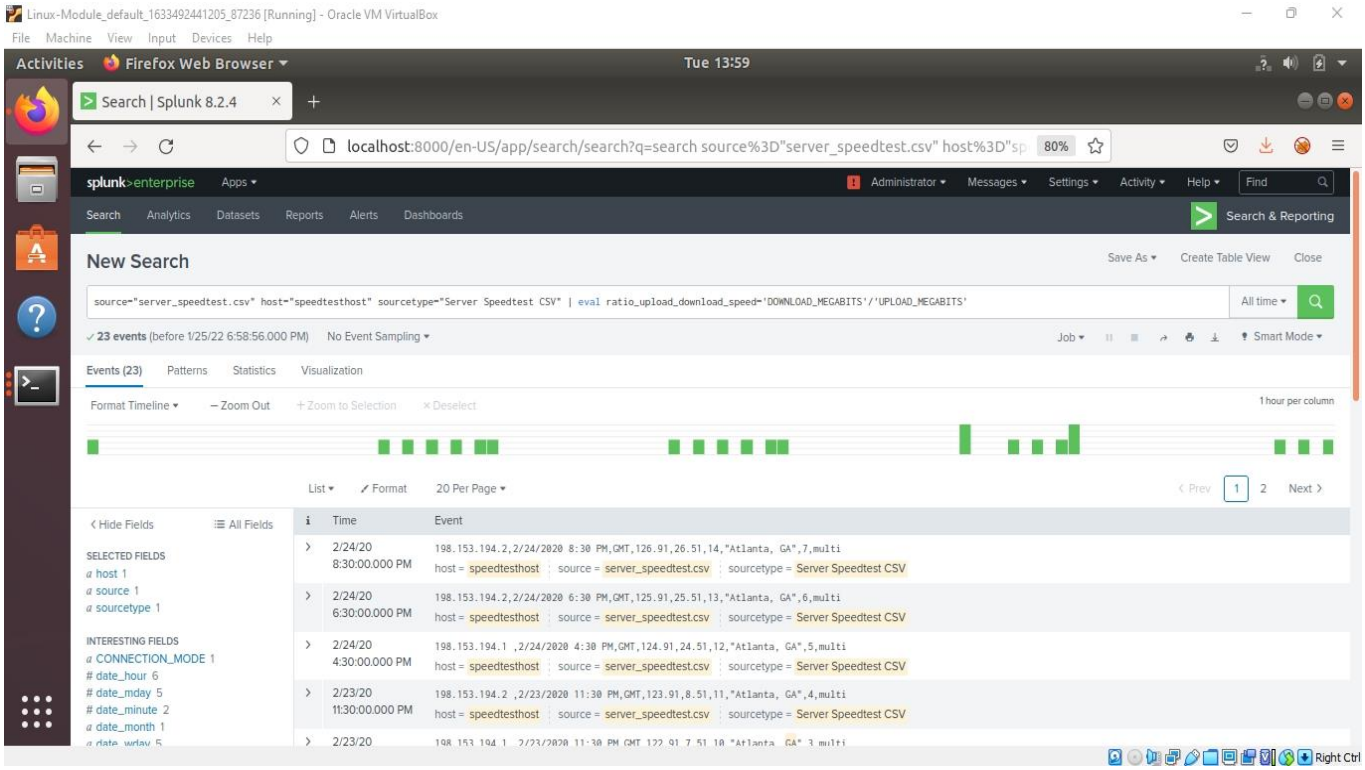
Below is a screenshot of the uploaded server_speedtest.csv file on SPLUNK,



Below is the search performed, using the `eval` command, to create a field called `ratio` that shows the ratio between the upload and download speeds.

```
source="server_speedtest.csv" host="speedtesthost" sourcetype="Server Speedtest CSV" | eval ratio_upload_download_speed='DOWNLOAD_MEGABITS'/'UPLOAD_MEGABITS'
```

Below is a screenshot of the above eval execution:



Create a report using the Splunk's `table` command to display the following fields in a statistics report:

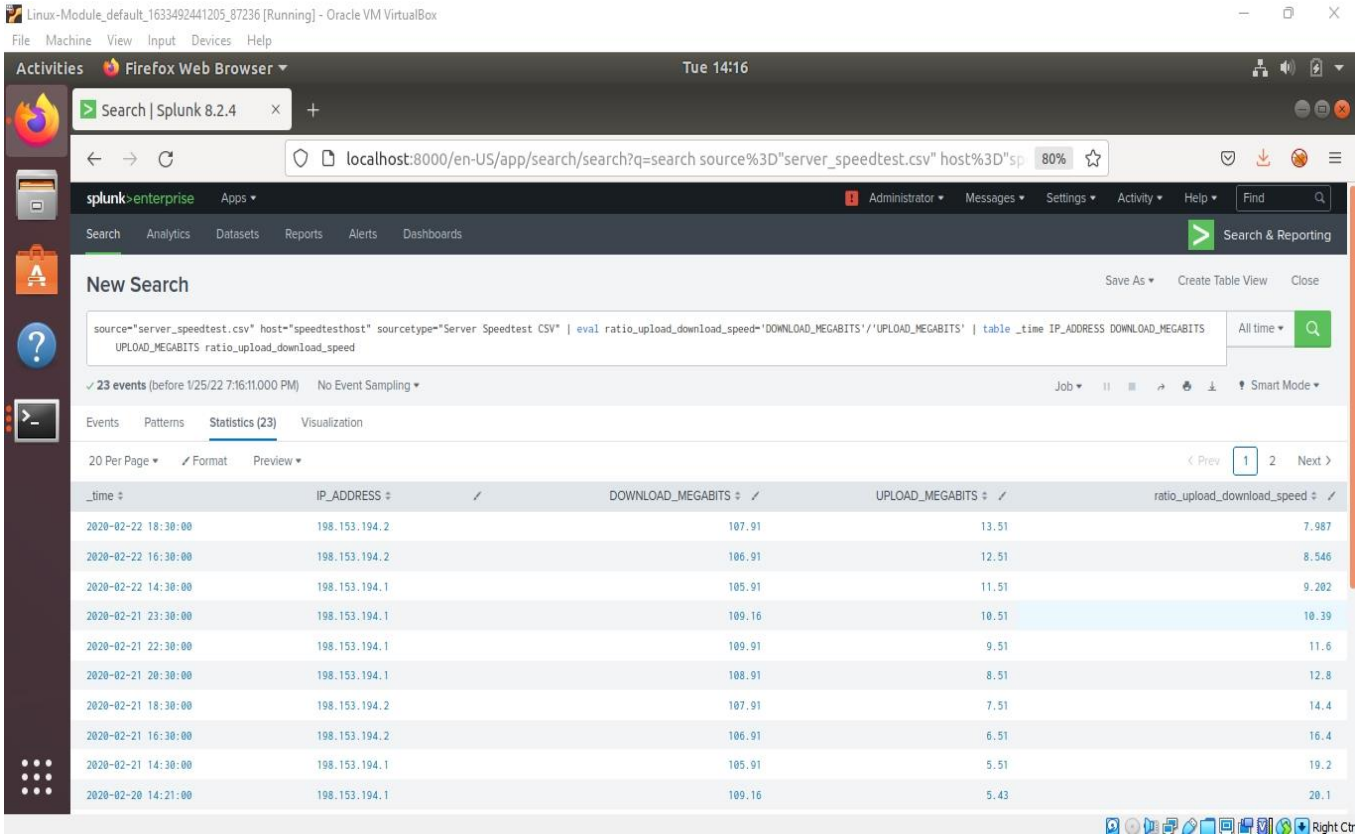
- `_time`
- `IP_ADDRESS`
- `DOWNLOAD_MEGABITS`
- `UPLOAD_MEGABITS`
- `ratio`

Ans: Below is the search entered to create the report. The output of the eval in the search is channeled to the create the statistical report.

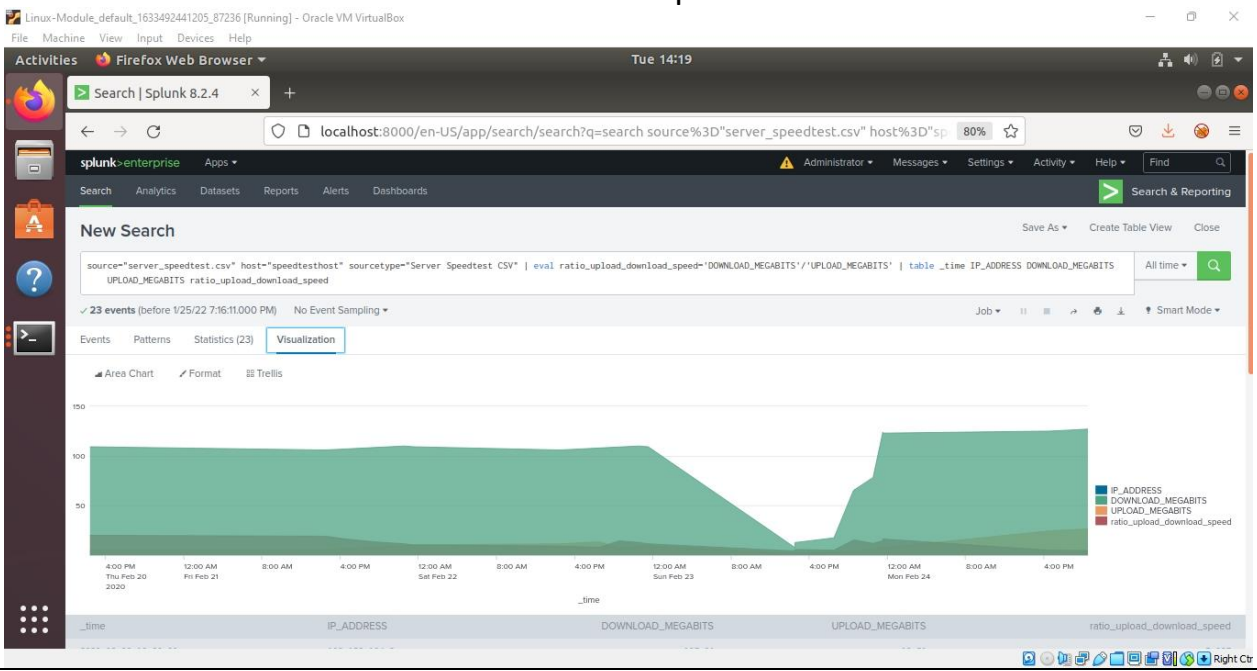
```
source="server_speedtest.csv" host="speedtesthost" sourcetype="Server Speedtest CSV" | eval ratio_upload_download_speed='DOWNLOAD_MEGABITS'/'UPLOAD_MEGABITS' |
```

table _time IP_ADDRESS DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio_upload_download_speed

Below is a screenshot of the above:



Below screenshot shows the visualization capture for the above:



Answer the following questions:

- Based on the report created, what is the approximate date and time of the attack?

Ans: The attack took place on 02/23/2020 at 14:30-the download speed dropped down very low to 7.87 Mbps.
This lasted till 02/23/2020 at 23:30, where the speed returned to over 122.91 Mbps.

- How long did it take your systems to recover?

Ans : It took the system a total of 9 hours to recover.

References:

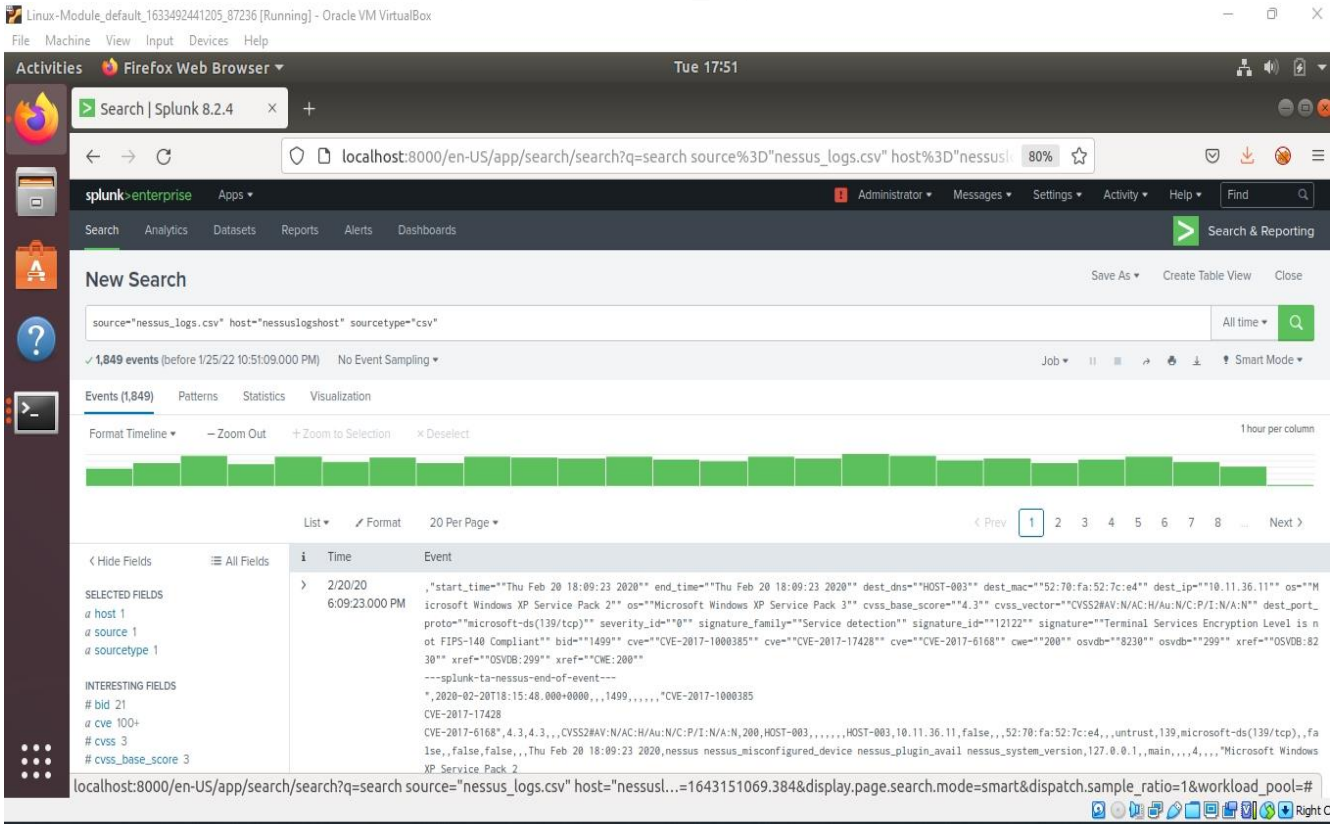
Evaluation functions - Splunk Documentation

Step 2: Are We Vulnerable?

Background: Due to the frequency of attacks, your manager needs to be sure that sensitive customer data on their servers is not vulnerable. Since Vandalay uses Nessus vulnerability scanners, you have pulled the last 24 hours of scans to see if there are any critical vulnerabilities.

Task: Create a report determining how many critical vulnerabilities exist on the customer data server. Then, build an alert to notify your team if a critical vulnerability reappears on this server.

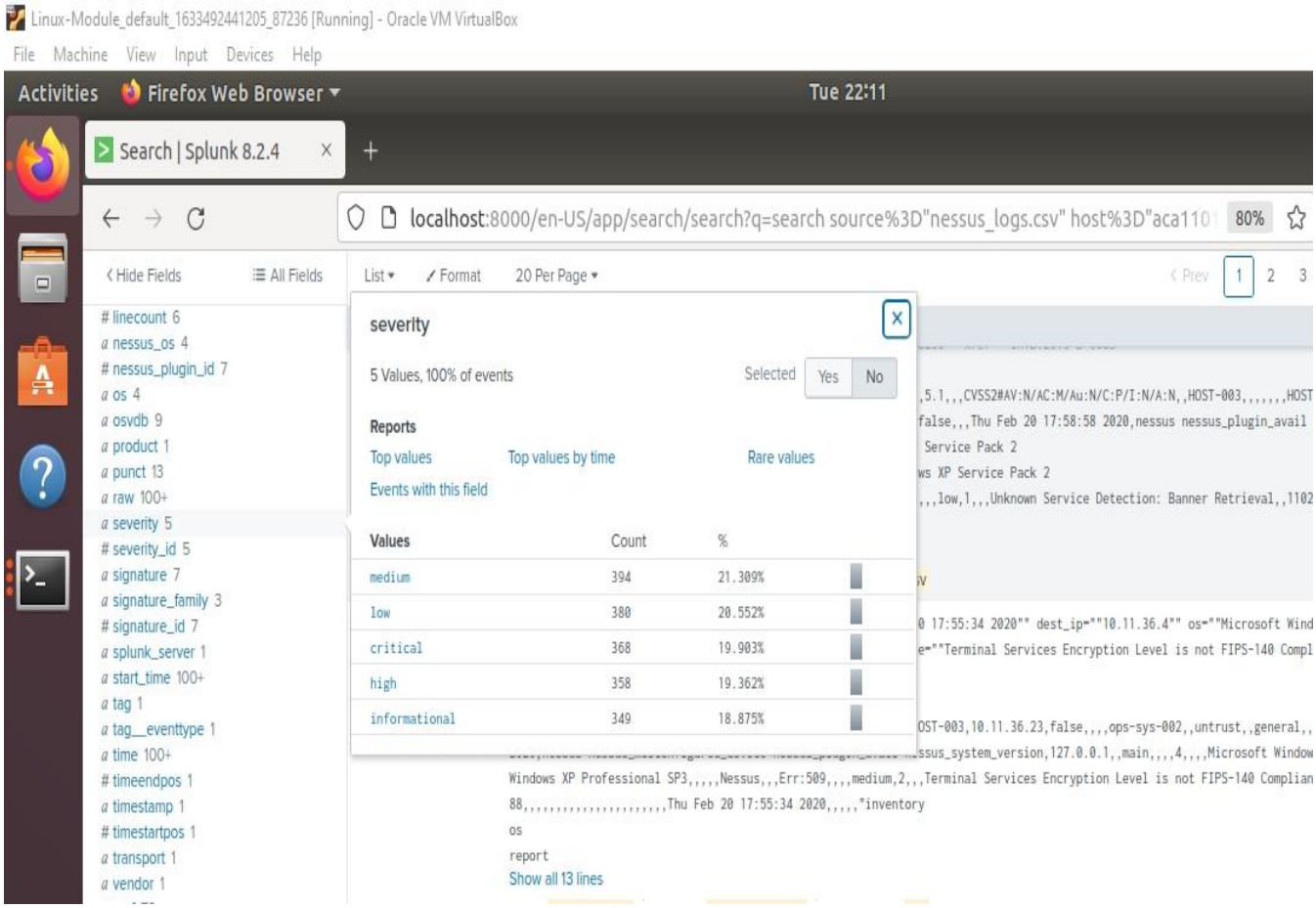
Below is a screenshot of the uploaded nessus_logs.csv file on SPLUNK,



Create a report that shows the `count` of critical vulnerabilities from the customer database server.

- The database server IP is `10.11.36.23`.
- The field that identifies the level of vulnerabilities is `severity`.

Ans: The severity Levels existing are indicated in below screenshot:

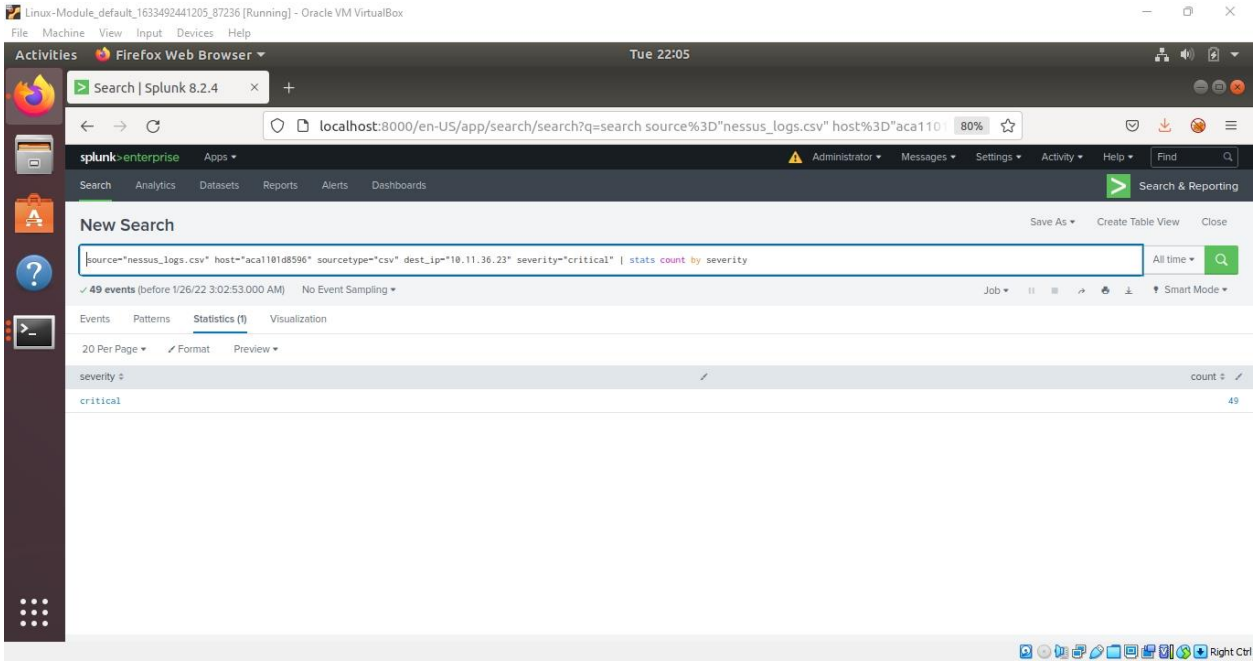


Below is the search entered to create the report.

```
source="nessus_logs.csv" host="aca1101d8596" sourcetype="csv" dest_ip="10.11.36.23" severity="critical" | stats count by severity
```

The above search returns that there are **49 critical vulnerabilities.**

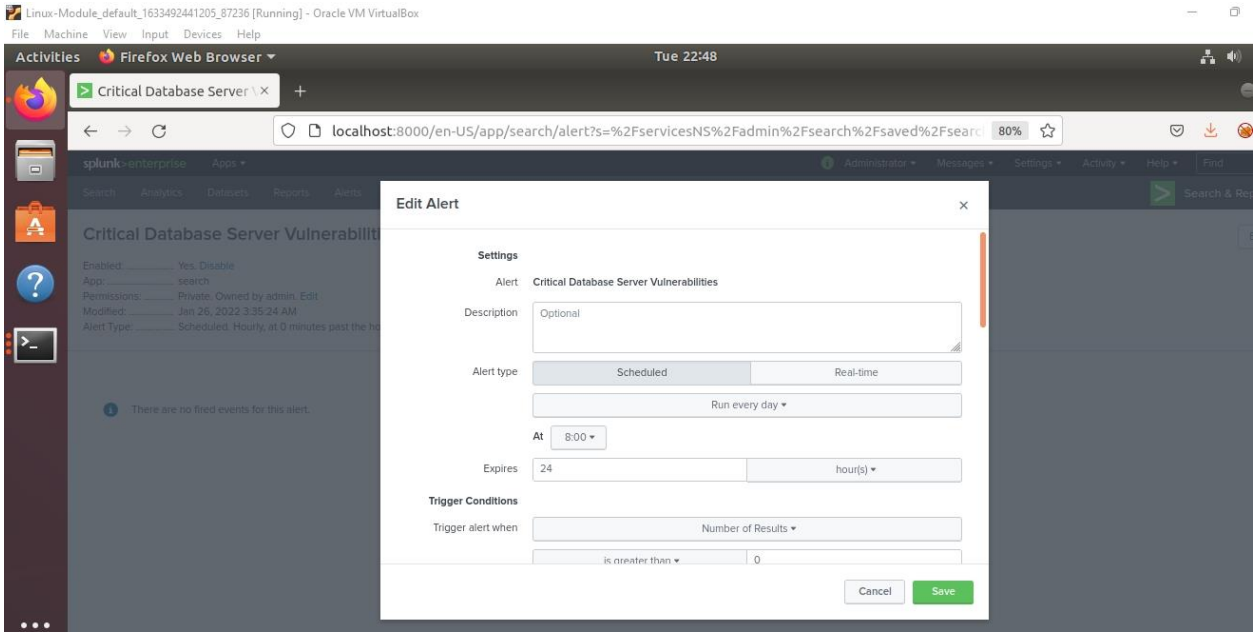
Below is a screenshot of the above search:

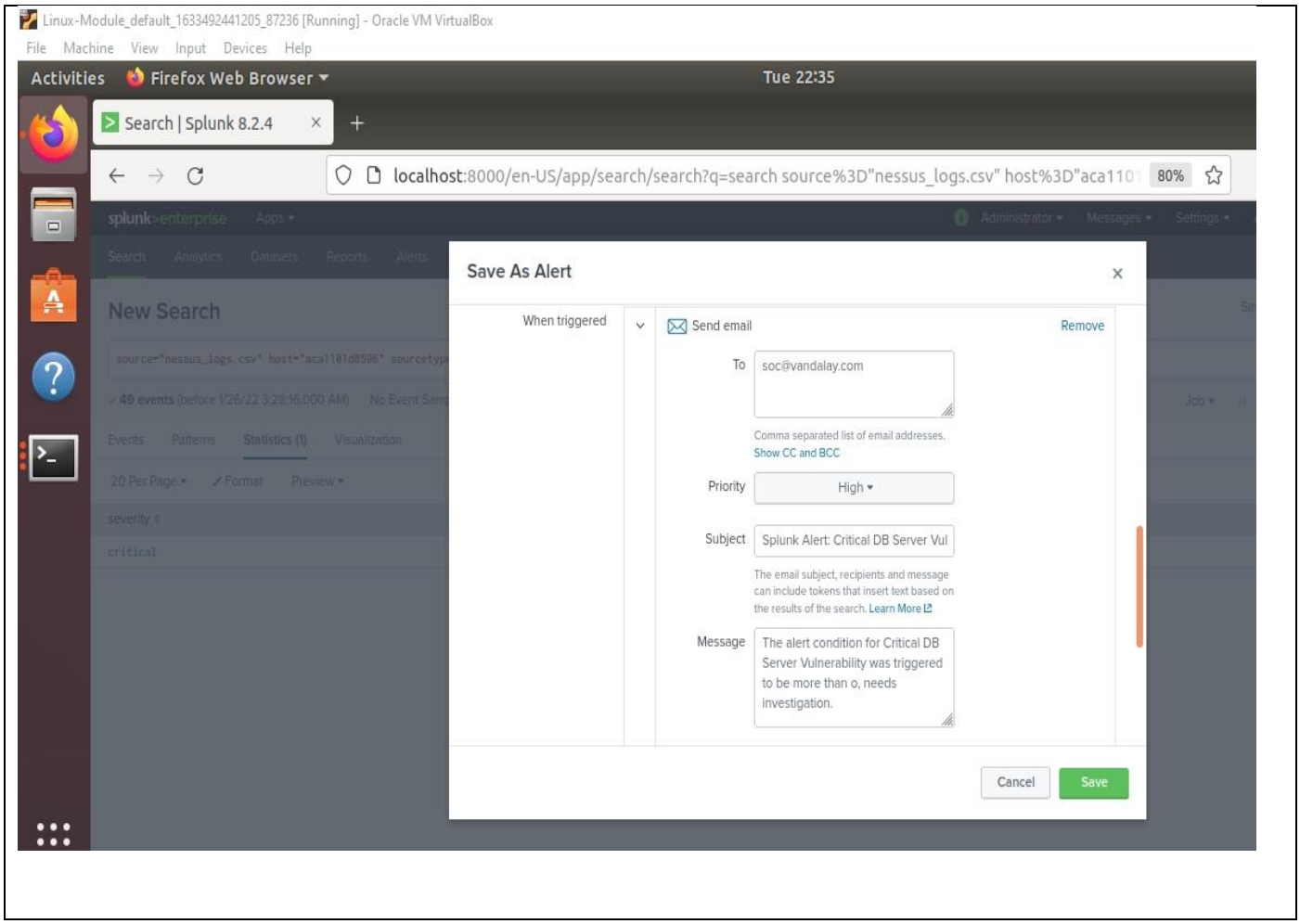


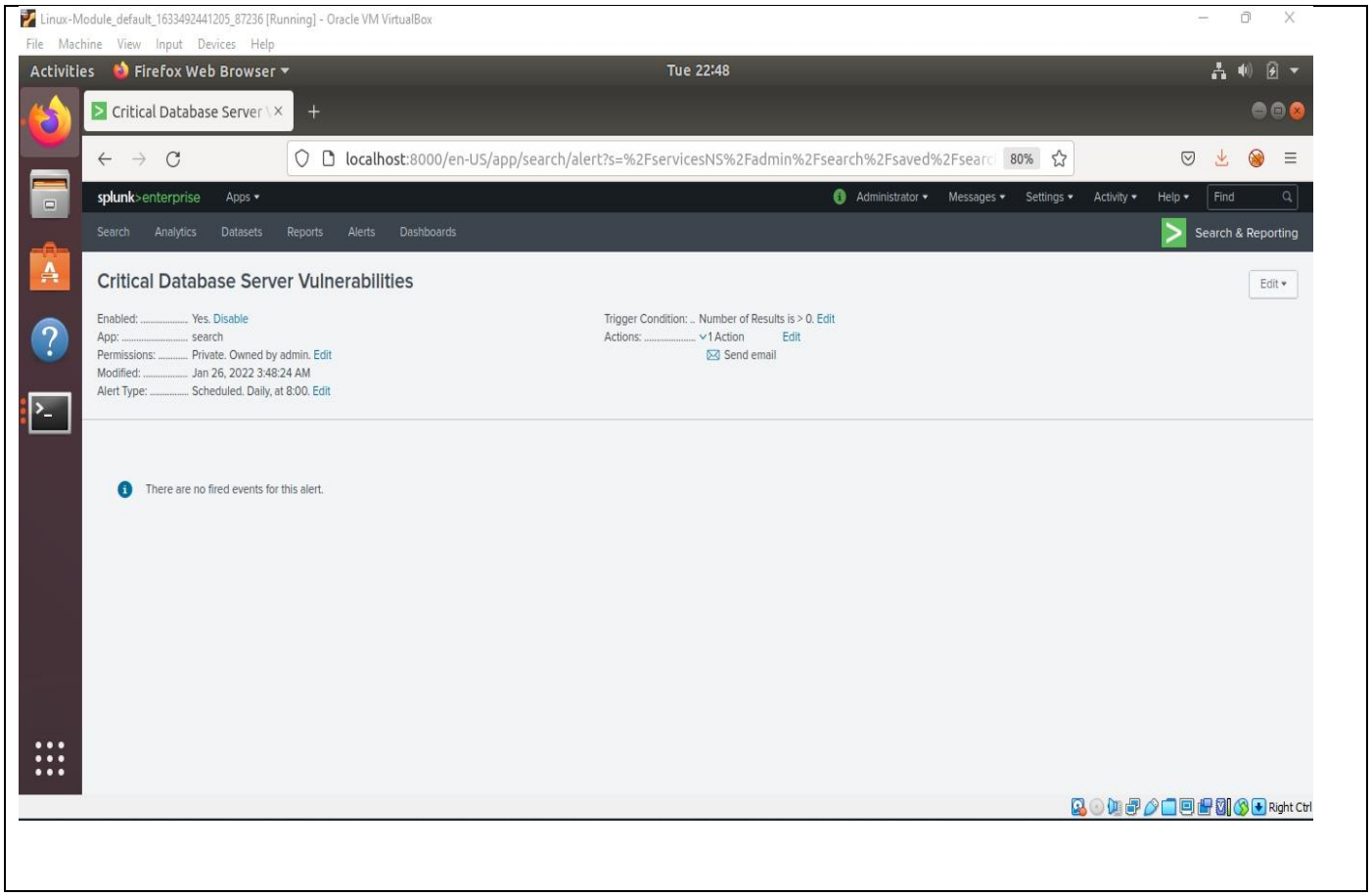
Build an alert that monitors every day to see if this server has any critical vulnerabilities. If a vulnerability exists, have an alert emailed to `soc@vandalay.com`.

Ans:

Below is a screenshot of the alert created:




Linux-Module_default_1633492441205_87236 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Tue 22:35
Search | Splunk 8.2.4
localhost:8000/en-US/app/search/search?q=search source%3D"nessus_logs.csv" host%3D"aca110
80%
splunk>enterprise
Apps
Administrator
Messages
Settings
Search
Analytics
Datasets
Reports
Alerts
New Search
49 events (before 1/26/22 3:28:16.000 AM)
Events
Patterns
Statistics (1)
Visualization
20 Per Page
Format
Preview
severity
critical
Save As Alert
When triggered
Send email
Remove
To
soc@vandalay.com
Comma separated list of email addresses.
Show CC and BCC
Priority
High
Subject
Splunk Alert: Critical DB Server Vul
The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More
Message
The alert condition for Critical DB Server Vulnerability was triggered to be more than 0, needs investigation.
Cancel
Save


Linux-Module_default_1633492441205_87236 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Tue 22:48
Critical Database Server
localhost:8000/en-US/app/search/alert?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearc
80%
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Critical Database Server Vulnerabilities
Edit
Enabled: Yes. Disable
App: search
Permissions: Private. Owned by admin. Edit
Modified: Jan 26, 2022 3:48:24 AM
Alert Type: Scheduled. Daily, at 8:00. Edit
Trigger Condition: Number of Results is > 0. Edit
Actions: 1 Action Edit
Send email
There are no fired events for this alert.
Right Ctrl

Step 3: Drawing the (base)line

****Background:** A Vandaly server is also experiencing brute force attacks into their administrator account. Management would like you to set up monitoring to notify the SOC team if a brute force attack occurs again.**

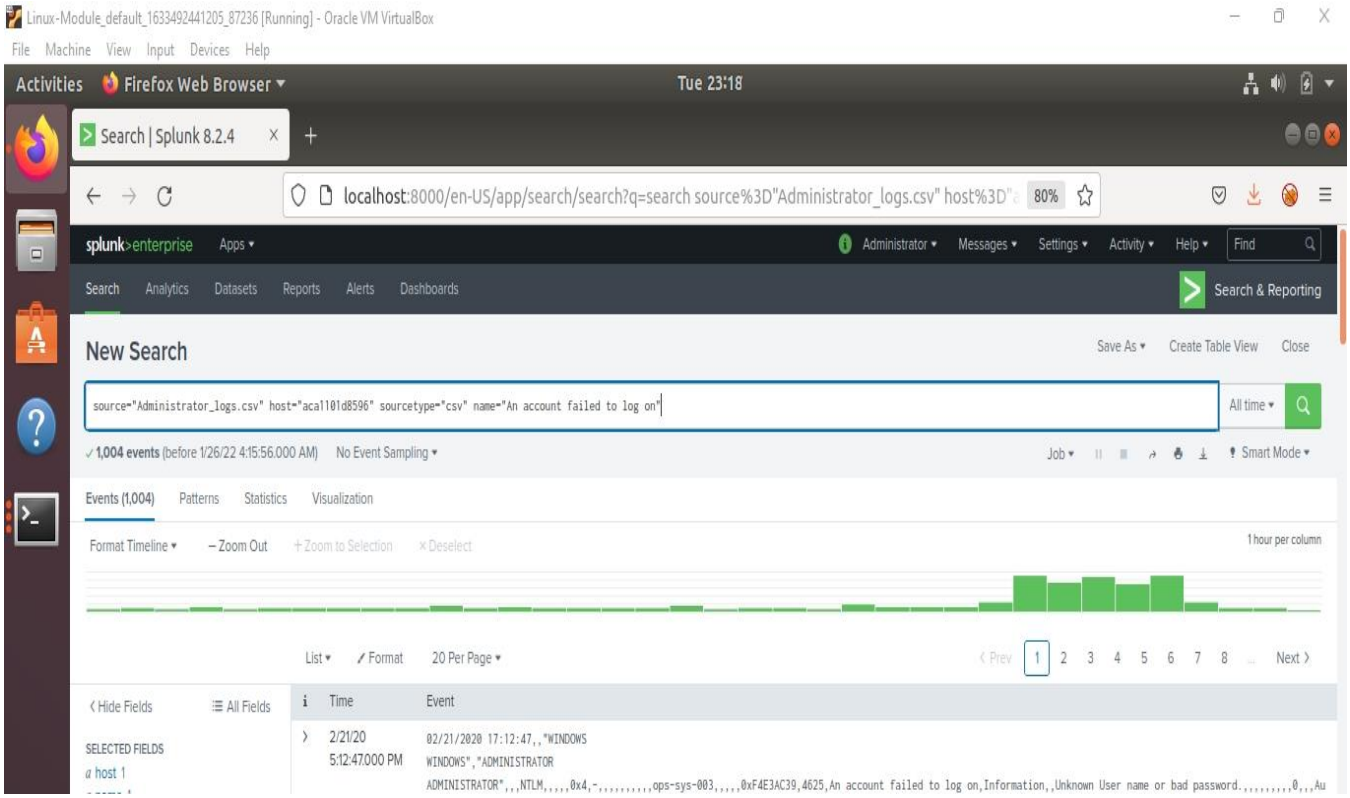
****Task:** Analyze administrator logs that document a brute force attack. Then, create a baseline of the ordinary amount of administrator bad logins and determine a threshold to indicate if a brute force attack is occurring.**

Ans:

I used the below search to recognize when the brute force attack started.

source="Administrator_logs.csv" host="aca1101d8596" sourcetype="csv" name="An account failed to log on"

Below is a screenshot of the search and the timeline-

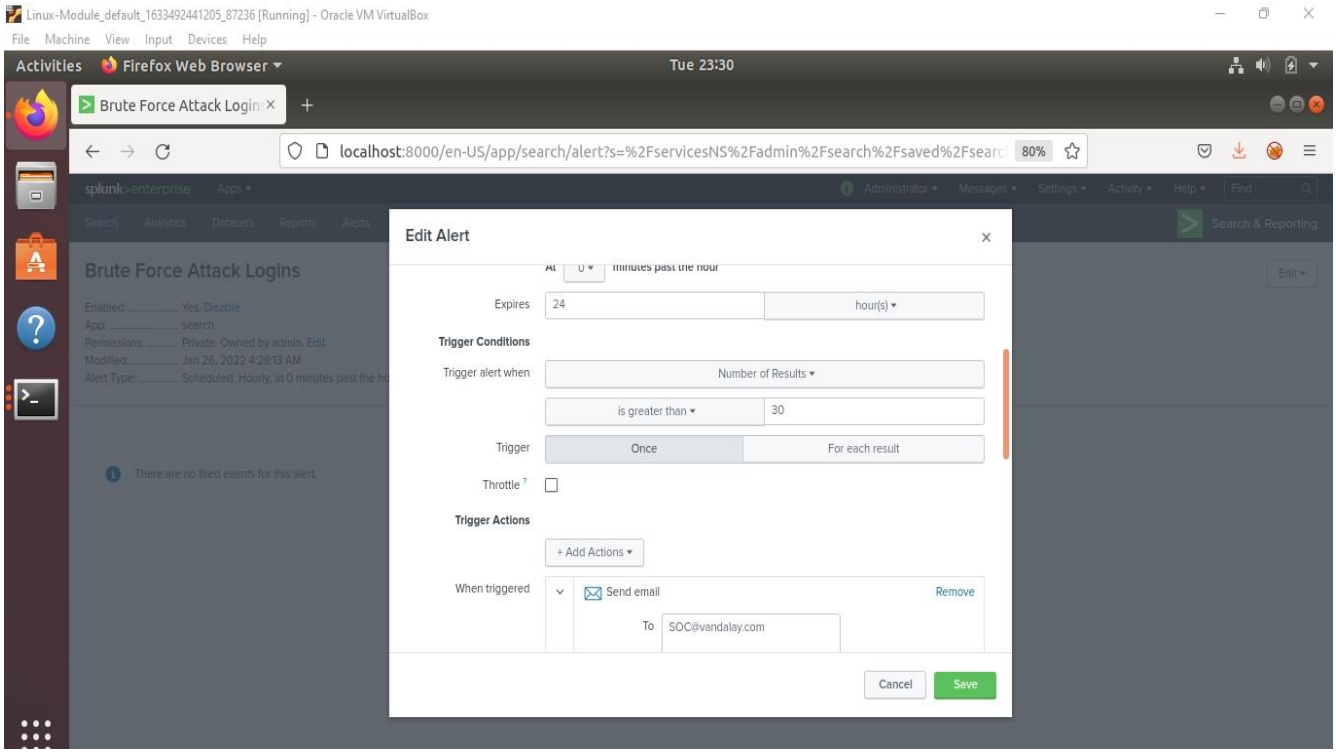


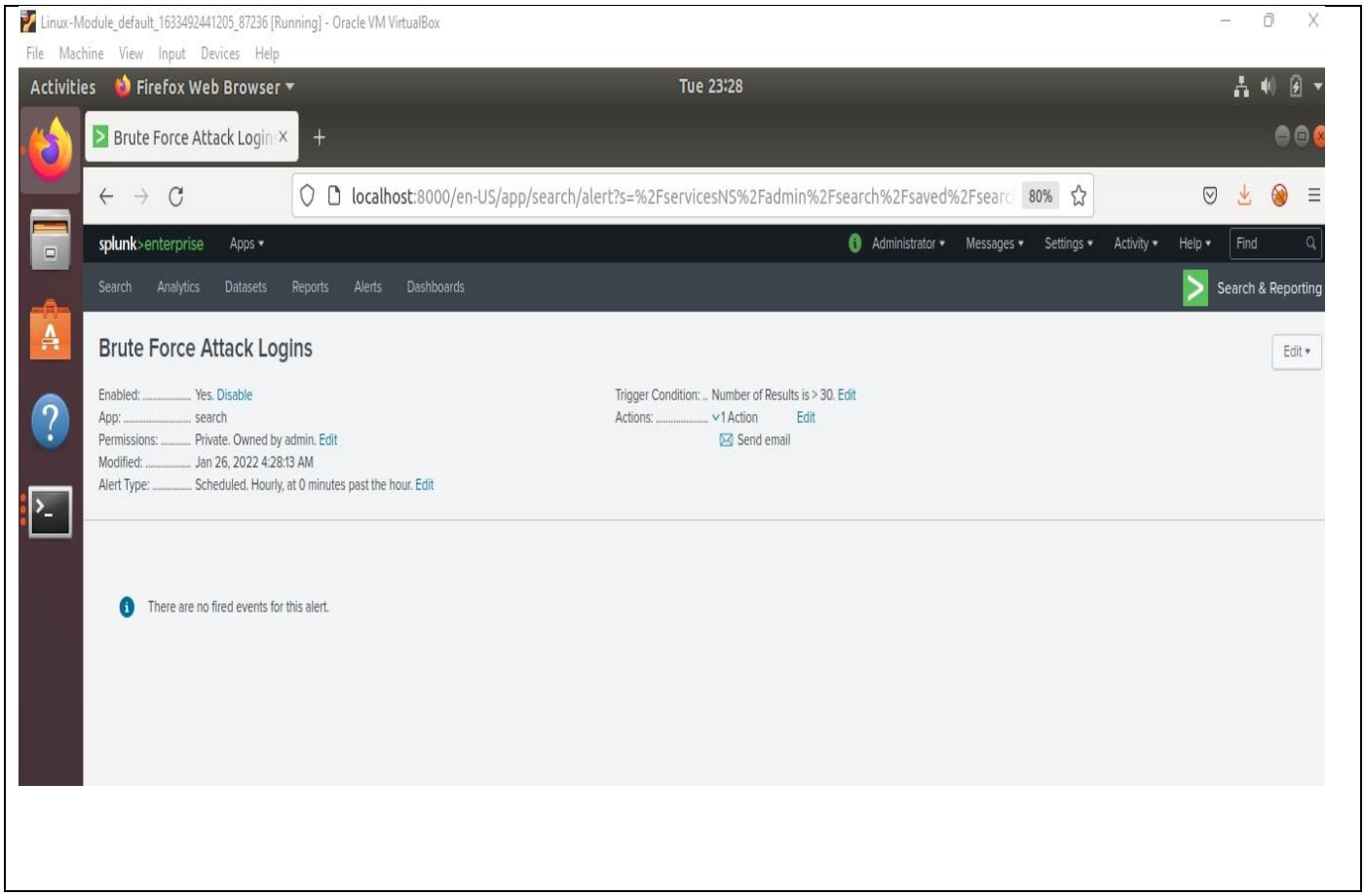
When did the brute force attack occur?
The attack started at 8AM on Feb 21 2020.

Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring.
Since the average failed logins attempts is around 6 to 23, I set the baseline at that. I put the alert trigger at 30 or higher within an hour span, which is the threshold.

Design an alert to check the threshold every hour and email the SOC team at SOC@vandalay.com if triggered.

Below is the alert created :




Linux-Module_default_1633492441205_87236 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Tue 23:28
Brute Force Attack Login
localhost:8000/en-US/app/search/alert?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearc
80%
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Brute Force Attack Logins
Edit
Enabled: Yes. Disable
App: search
Permissions: Private. Owned by admin. Edit
Modified: Jan 26, 2022 4:28:13 AM
Alert Type: Scheduled. Hourly, at 0 minutes past the hour. Edit
Trigger Condition: Number of Results is > 30. Edit
Actions: 1 Action Edit
Send email
There are no fired events for this alert.