Vandalay Industries Monitoring Activity Instructions

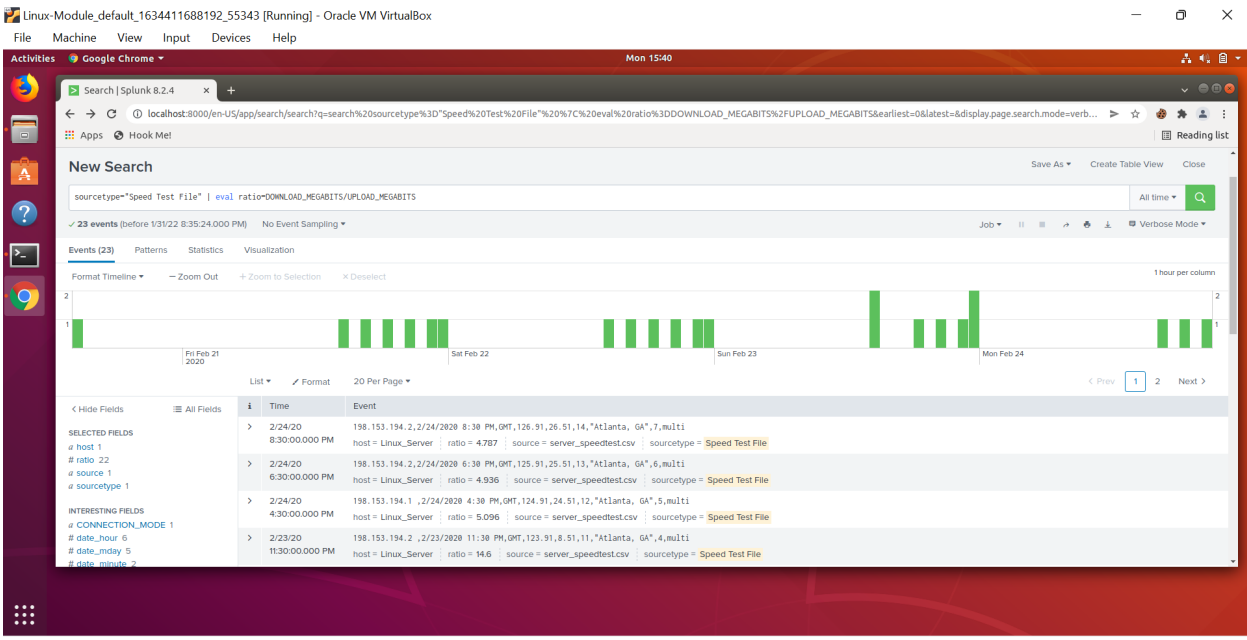
Step 1: The Need for Speed

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.

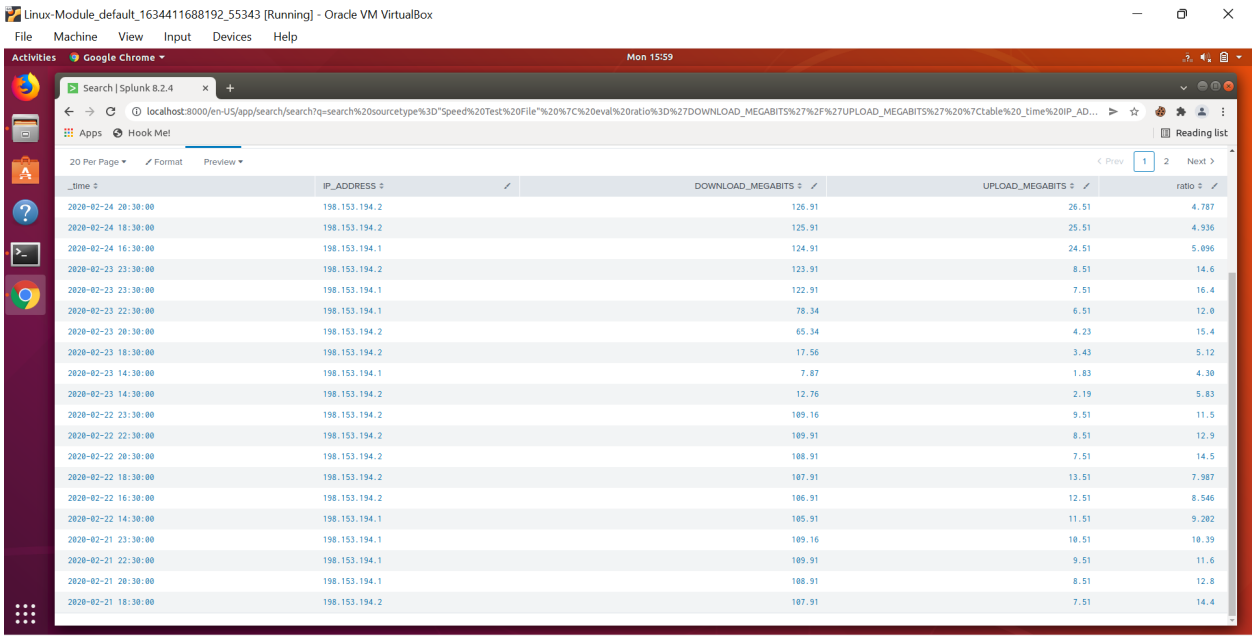
Task: Create a report to determine the impact that the DDOS attack had on download and upload speed. Additionally, create an additional field to calculate the ratio of the upload speed to the download speed.

1. Upload the following file of the system speeds around the time of the attack.
    - Speed Test File
2. Using the eval command, create a field called ratio that shows the ratio between the upload and download speeds.
   |eval ratio='DOWNLOAD_MEGABITS'/'UPLOAD_MEGABITS'
    - Hint: The format for creating a ratio is: | eval new_field_name = 'fieldA' / 'fieldB'



3. 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
4. Hint: Use the following format when for the table command: | table fieldA fieldB fieldC



5. Answer the following questions:
    - Based on the report created, what is the approximate date and time of the attack? From the information provided we can see a clear and significant change in the Download and Upload speeds on 2020-02-23 at 14:30:00
    - How long did it take your systems to recover? This change in download and upload speeds lasted approximately 6 hrs lasting from 14:30 to 20:30.

Submit a screen shot of your report and the answer to the questions above.

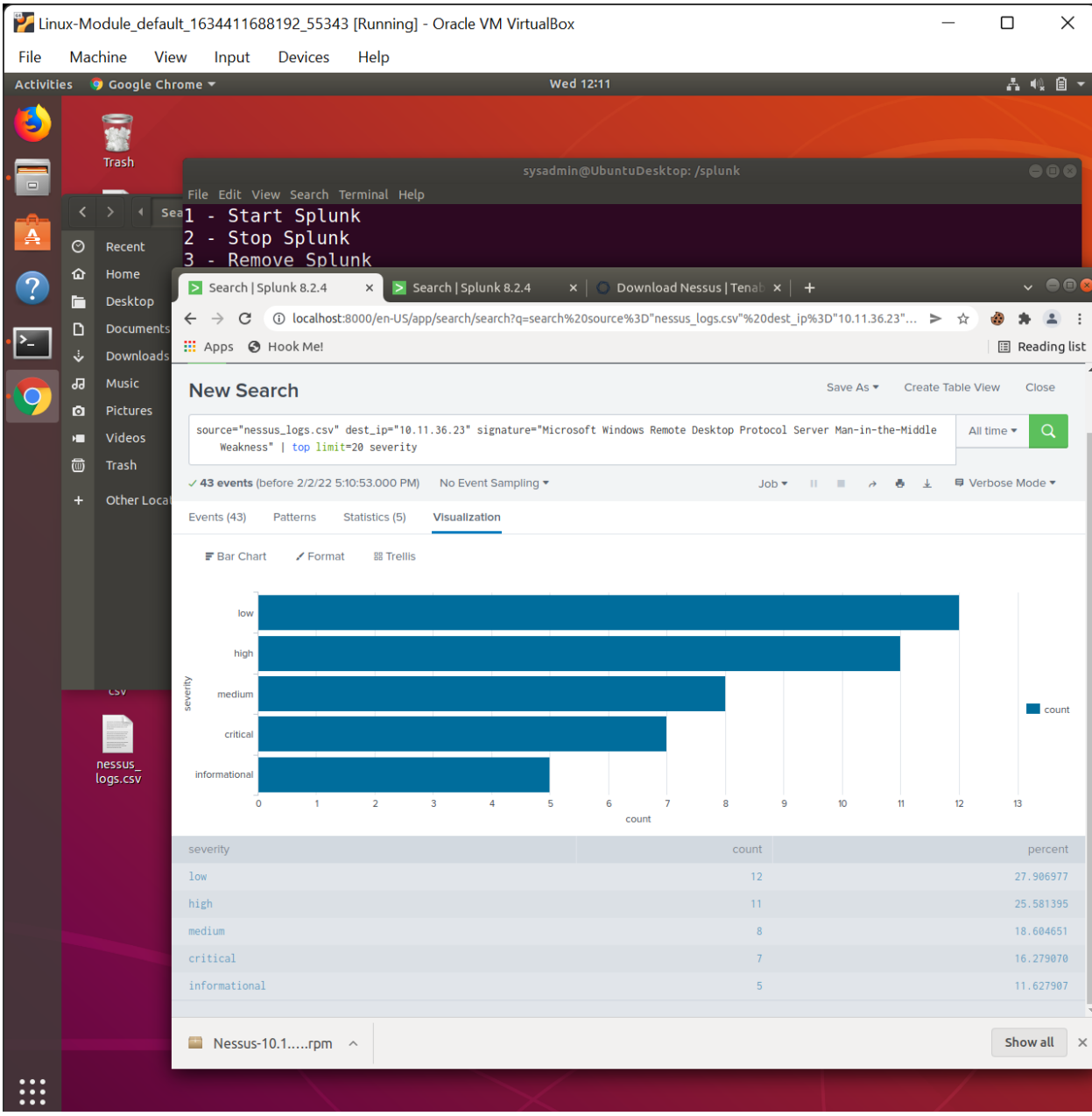
Step 2: Are We Vulnerable?

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.

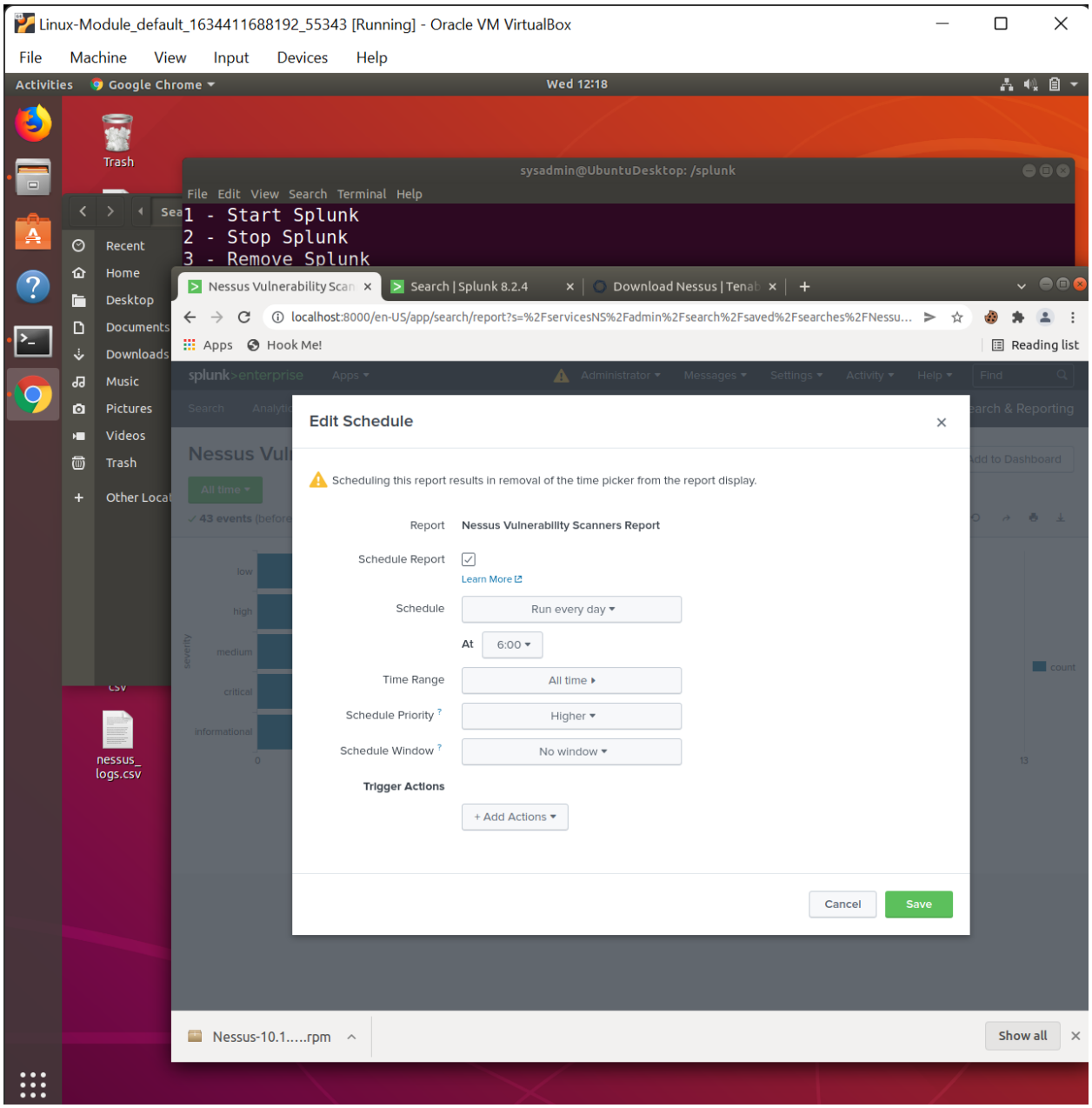
- For more information on Nessus, read the following link: https://www.tenable.com/products/nessus

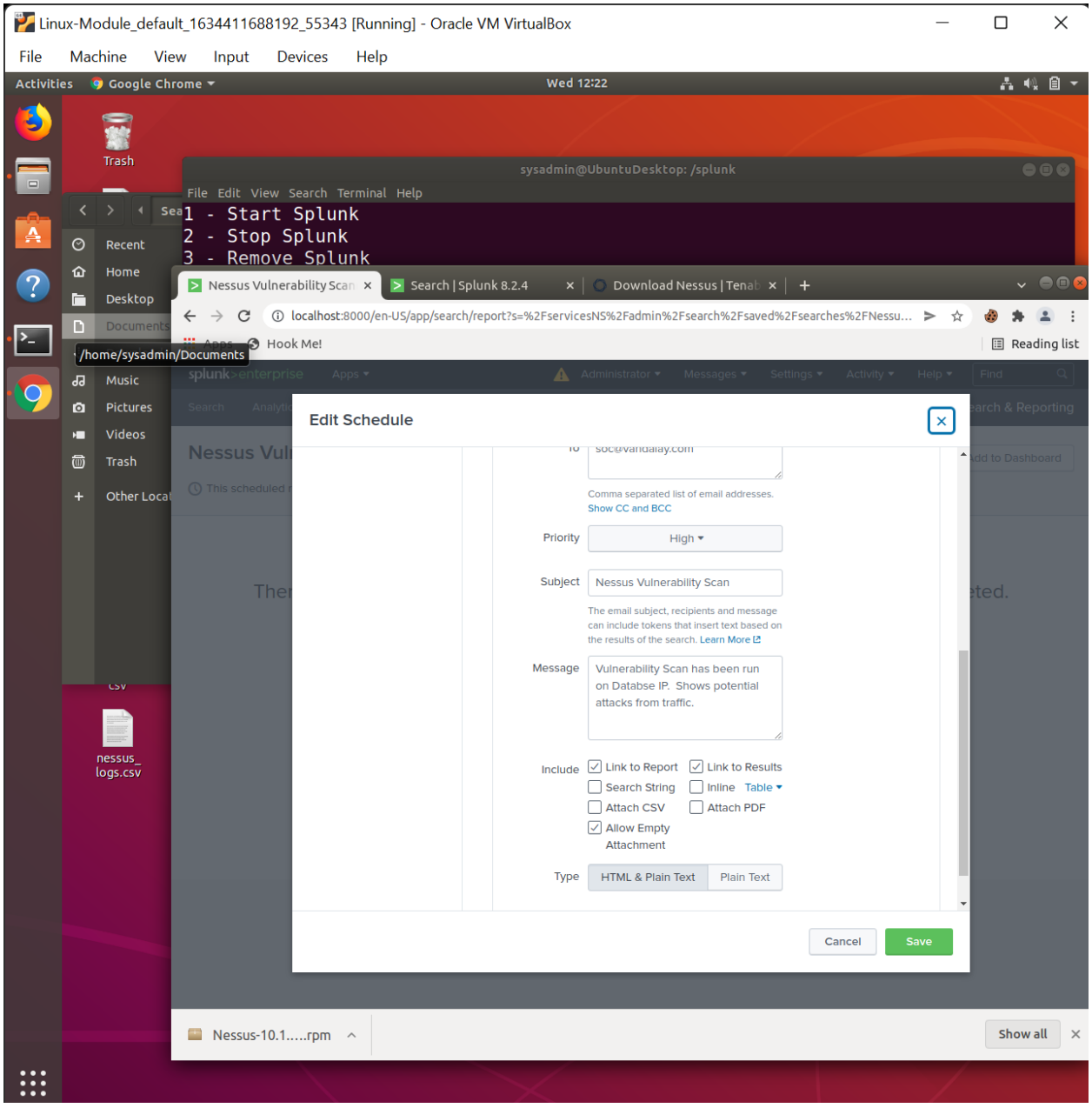
Task: Create a report determining how many critical vulnerabilities exist on the customer data server. Then, build an alert to notify your team if a critical vulnerability reappears on this server.

1. Upload the following file from the Nessus vulnerability scan.
    - Nessus Scan Results
2. 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.

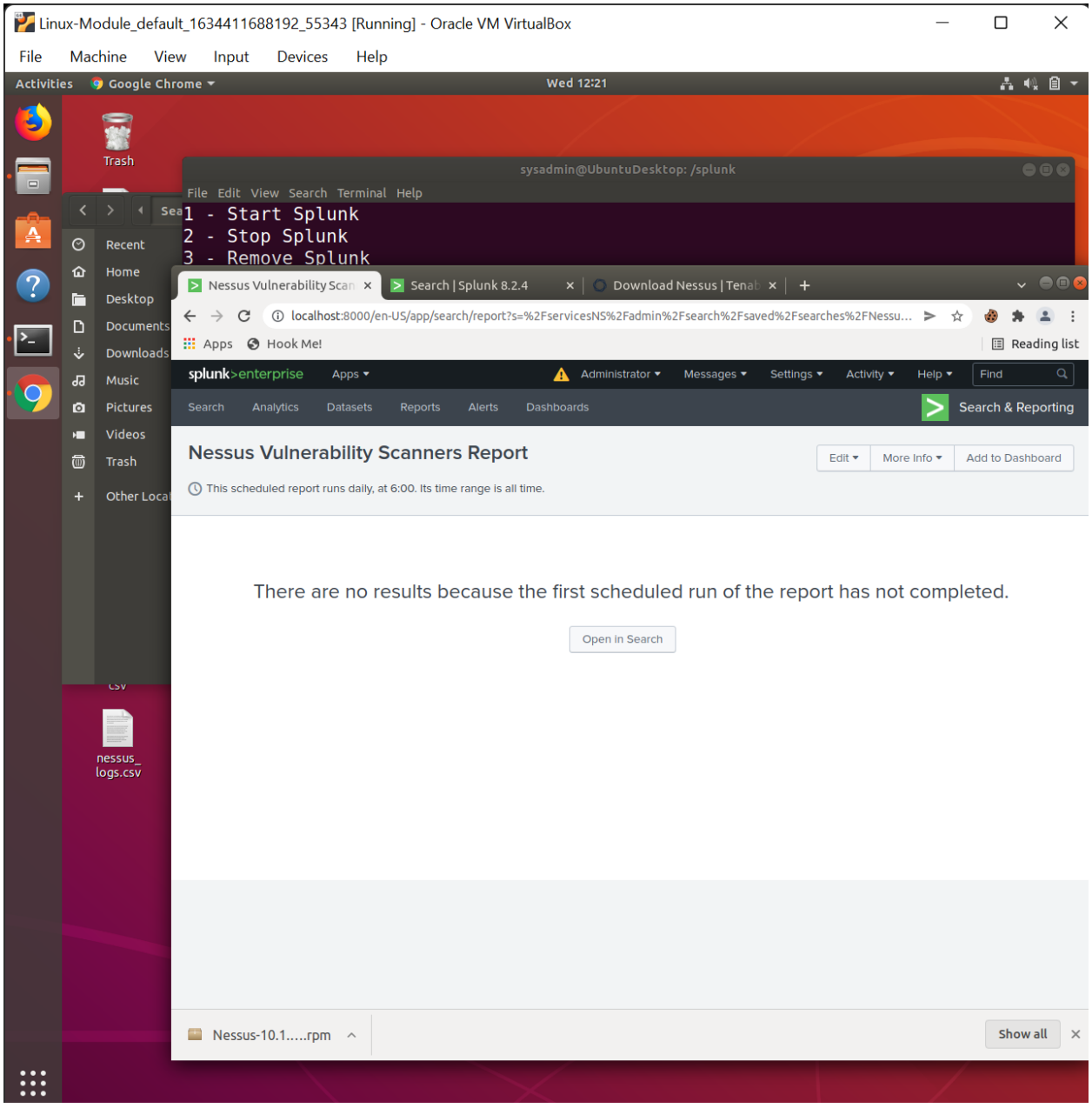


3. Build an alert that monitors every day to see if this server has any critical vulnerabilities. If a vulnerability exists, have an alert emailed to soc@vandalay.com.





Submit a screenshot of your report and a screenshot of proof that the alert has been created.

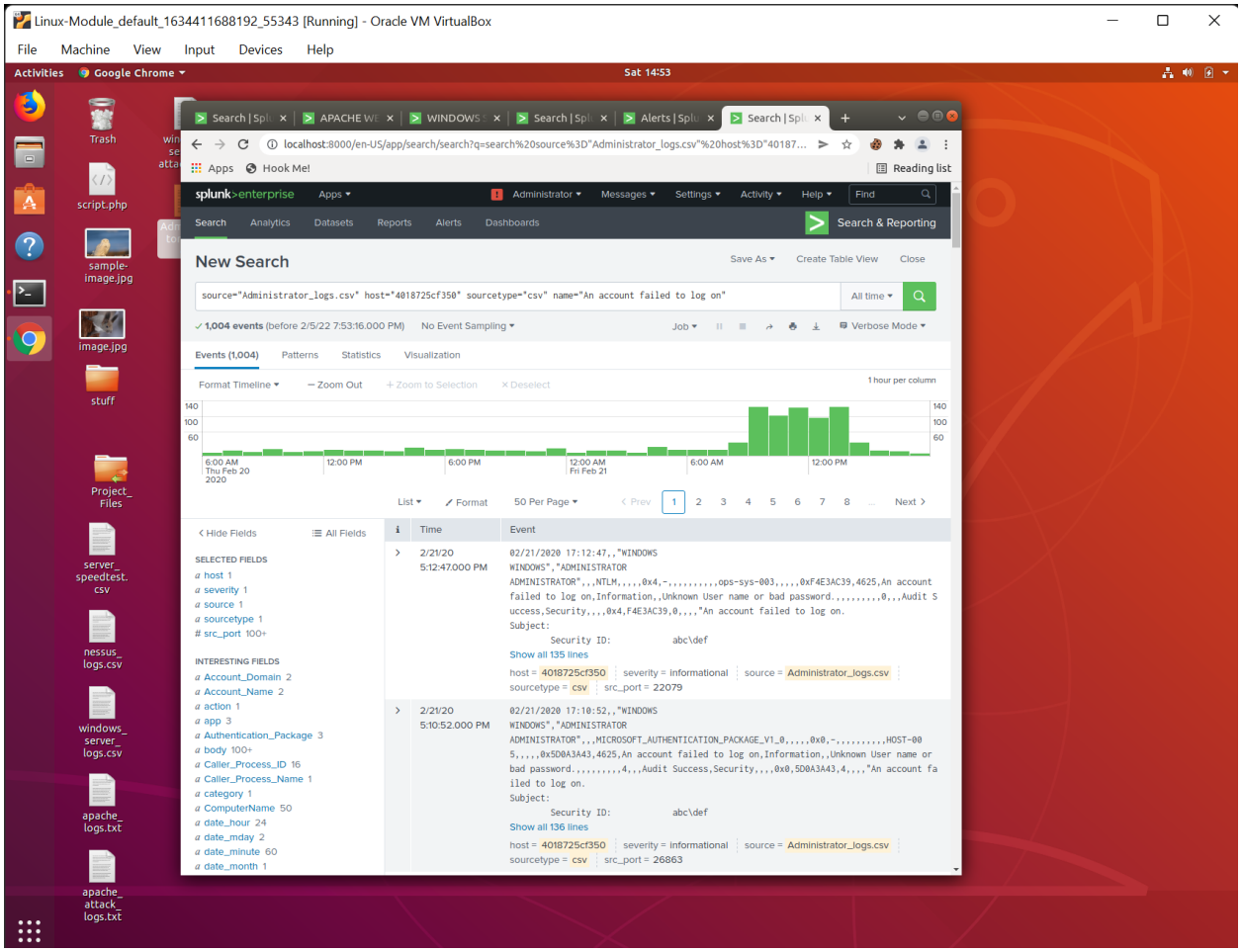


Step 3: Drawing the (base)line

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.

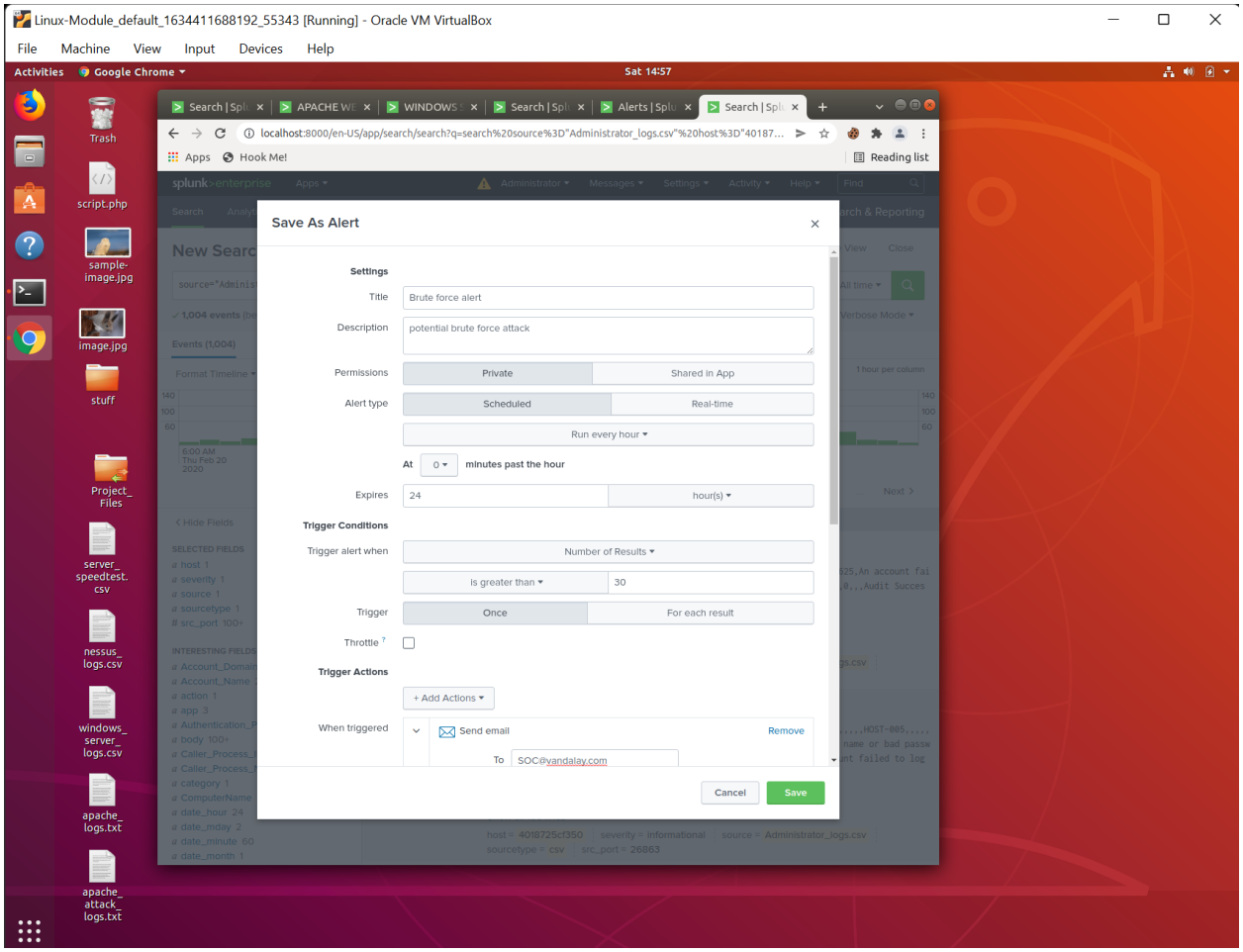
Task: Analyze administrator logs that document a brute force attack. Then, create a baseline of the ordinary amount of administrator bad logins and determine a threshold to indicate if a brute force attack is occurring.

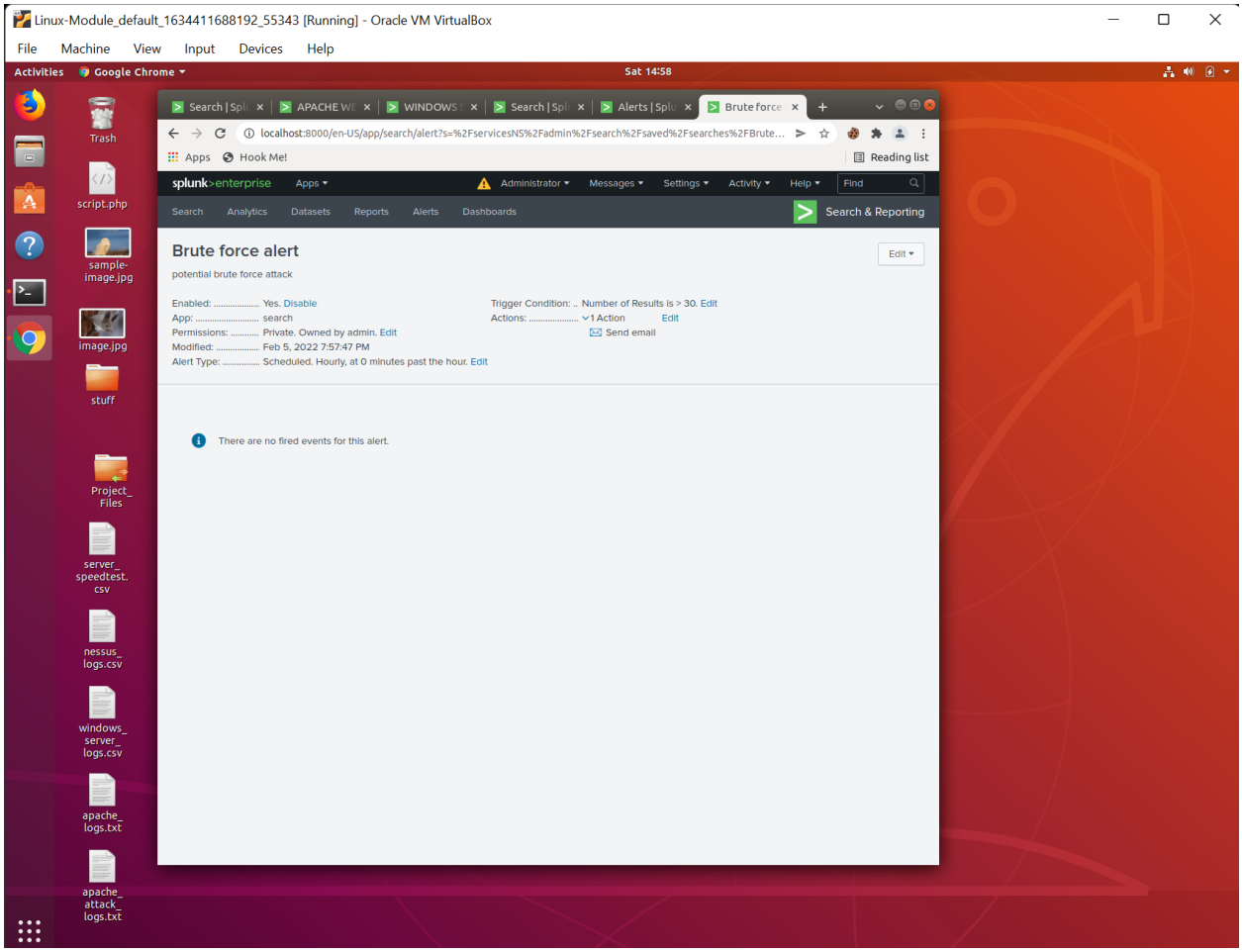
1. Upload the administrator login logs.
    - Admin Logins
2. When did the brute force attack occur?



The brute force attack occurred on February 21st, 2020 and lasted until 2pm (9am-2pm)

    - Hints:
        - Look for the name field to find failed logins.
        - Note the attack lasted several hours.
3. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring.
   Baseline of normal activity was set at 20 logins per hour; the threshold is set at 30 logins per hour.
4. Design an alert to check the threshold every hour and email the SOC team at SOC@vandalay.com if triggered.


Linux-Module_default_1634411688192_55343 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Google Chrome Sat 14:57
Trash
script.php
sample-image.jpg
image.jpg
stuff
Project_Files
server_speedtest.csv
nessus_logs.csv
windows_server_logs.csv
apache_logs.txt
apache_attack_logs.txt
Save As Alert
Settings
Title
Brute force alert
Description
potential brute force attack
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every hour
At 0 minutes past the hour
Expires
24
hour(s)
Trigger Conditions
Trigger alert when
Number of Results
is greater than
30
Trigger
Once
For each result
Throttle
Trigger Actions
+ Add Actions
When triggered
Send email
Remove
To
SOC@vandalay.com
Cancel
Save



Submit the answers to the questions about the brute force timing, baseline and threshold. Additionally, provide a screenshot as proof that the alert has been created.

Your Submission

In a word document, provide the following:

- Answers to all questions where indicated.
- Screenshots where indicated.