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

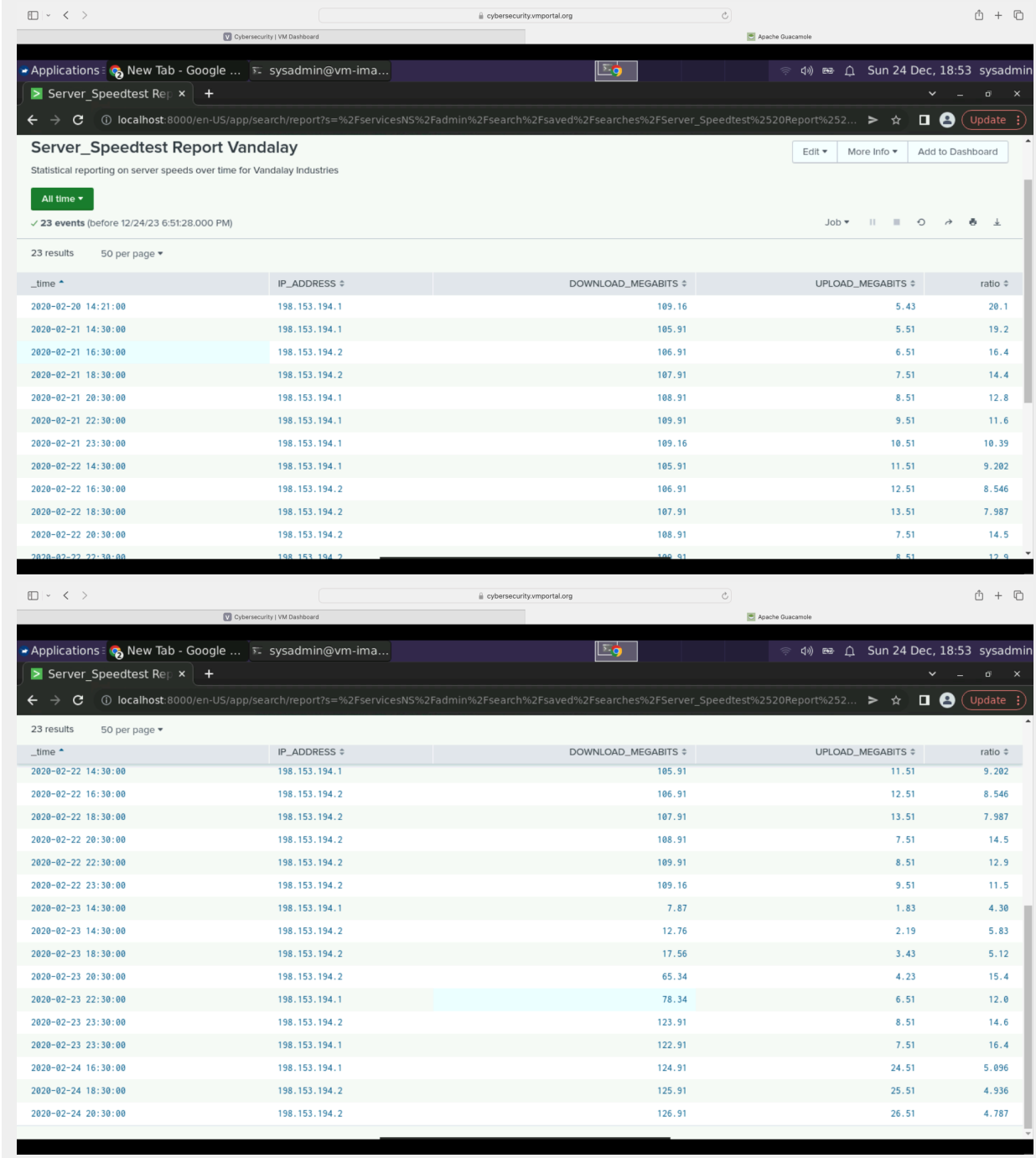
1. Based on the report you created, what is the approximate date and time of the attack?

```
The attack commenced on 02/22/2020, at 11:30 pm. The download speed began
drastically dropping from 109.16 Mbps to 7.87 Mbps
```

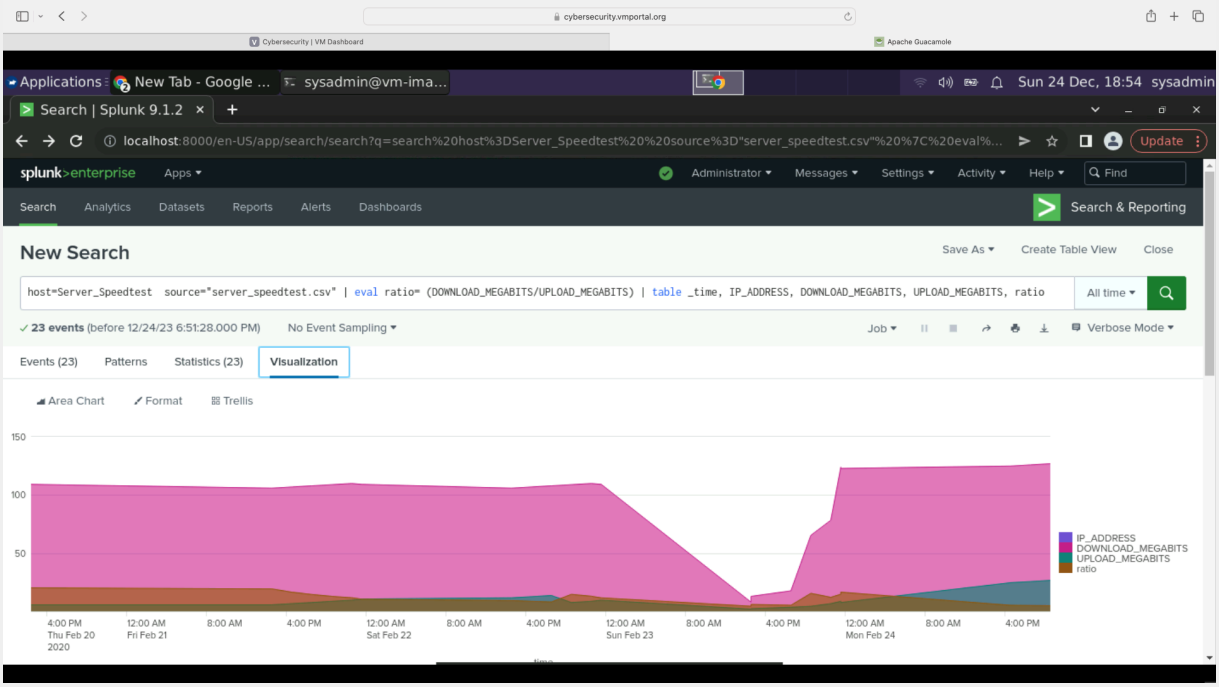
2. How long did it take your systems to recover?

```
24 hours for the systems to fully recover.
```

Provide a screenshot of your report:


cybersecurity.vmportal.org
Cybersecurity | VM Dashboard
Apache Guacamole
Applications
New Tab - Google ...
sysadmin@vm-ima...
Sun 24 Dec, 18:53 sysadmin
Server_Speedtest Rep
localhost:8000/en-US/app/search/report?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2FServer_Speedtest%2520Report%252...
Update
Server_Speedtest Report Vandalay
Edit
More Info
Add to Dashboard
Statistical reporting on server speeds over time for Vandalay Industries
All time
23 events (before 12/24/23 6:51:28.000 PM)
Job
23 results
50 per page
_time
IP_ADDRESS
DOWNLOAD_MEGABITS
UPLOAD_MEGABITS
ratio
2020-02-20 14:21:00 198.153.194.1 109.16 5.43 20.1
2020-02-21 14:30:00 198.153.194.1 105.91 5.51 19.2
2020-02-21 16:30:00 198.153.194.2 106.91 6.51 16.4
2020-02-21 18:30:00 198.153.194.2 107.91 7.51 14.4
2020-02-21 20:30:00 198.153.194.1 108.91 8.51 12.8
2020-02-21 22:30:00 198.153.194.1 109.91 9.51 11.6
2020-02-21 23:30:00 198.153.194.1 109.16 10.51 10.39
2020-02-22 14:30:00 198.153.194.1 105.91 11.51 9.202
2020-02-22 16:30:00 198.153.194.2 106.91 12.51 8.546
2020-02-22 18:30:00 198.153.194.2 107.91 13.51 7.987
2020-02-22 20:30:00 198.153.194.2 108.91 7.51 14.5

cybersecurity.vmportal.org
Cybersecurity | VM Dashboard
Apache Guacamole
Applications
New Tab - Google ...
sysadmin@vm-ima...
Sun 24 Dec, 18:53 sysadmin
Server_Speedtest Rep
localhost:8000/en-US/app/search/report?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2FServer_Speedtest%2520Report%252...
Update
23 results
50 per page
_time
IP_ADDRESS
DOWNLOAD_MEGABITS
UPLOAD_MEGABITS
ratio
2020-02-22 14:30:00 198.153.194.1 105.91 11.51 9.202
2020-02-22 16:30:00 198.153.194.2 106.91 12.51 8.546
2020-02-22 18:30:00 198.153.194.2 107.91 13.51 7.987
2020-02-22 20:30:00 198.153.194.2 108.91 7.51 14.5
2020-02-22 22:30:00 198.153.194.2 109.91 8.51 12.9
2020-02-22 23:30:00 198.153.194.2 109.16 9.51 11.5
2020-02-23 14:30:00 198.153.194.1 7.87 1.83 4.30
2020-02-23 14:30:00 198.153.194.2 12.76 2.19 5.83
2020-02-23 18:30:00 198.153.194.2 17.56 3.43 5.12
2020-02-23 20:30:00 198.153.194.2 65.34 4.23 15.4
2020-02-23 22:30:00 198.153.194.1 78.34 6.51 12.0
2020-02-23 23:30:00 198.153.194.2 123.91 8.51 14.6
2020-02-23 23:30:00 198.153.194.1 122.91 7.51 16.4
2020-02-24 16:30:00 198.153.194.1 124.91 24.51 5.096
2020-02-24 18:30:00 198.153.194.2 125.91 25.51 4.936
2020-02-24 20:30:00 198.153.194.2 126.91 26.51 4.787

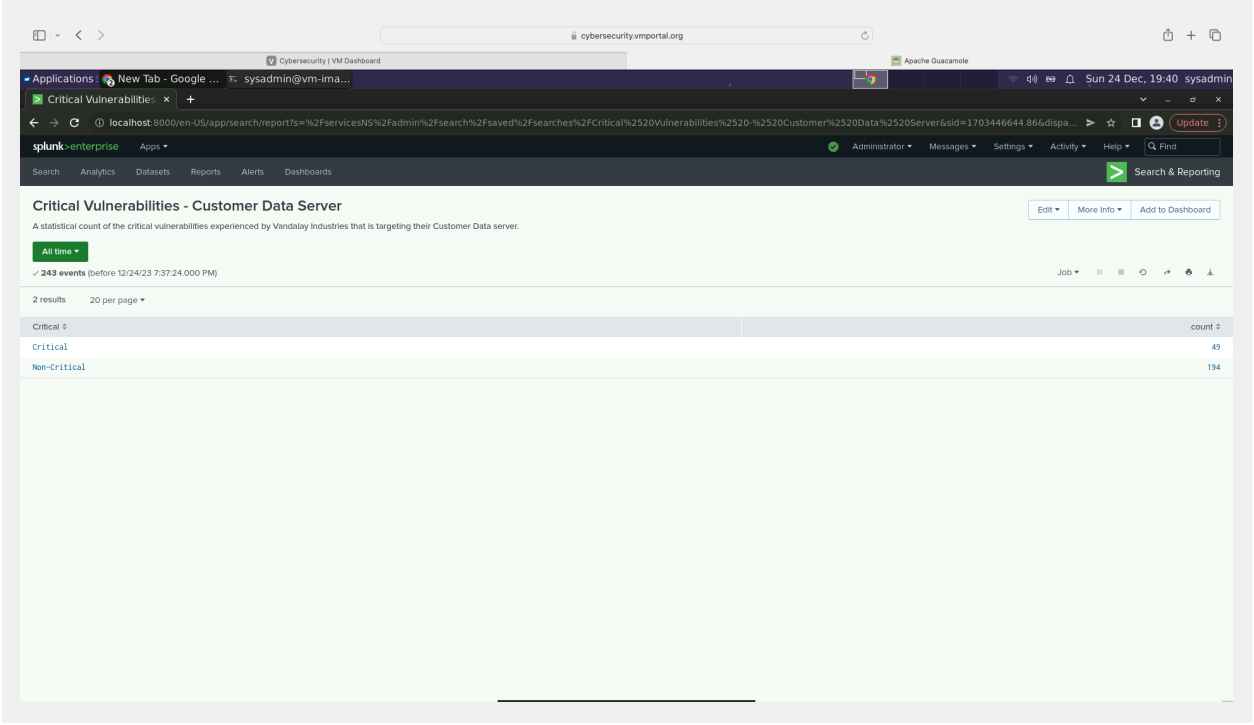


Step 2: Are We Vulnerable?

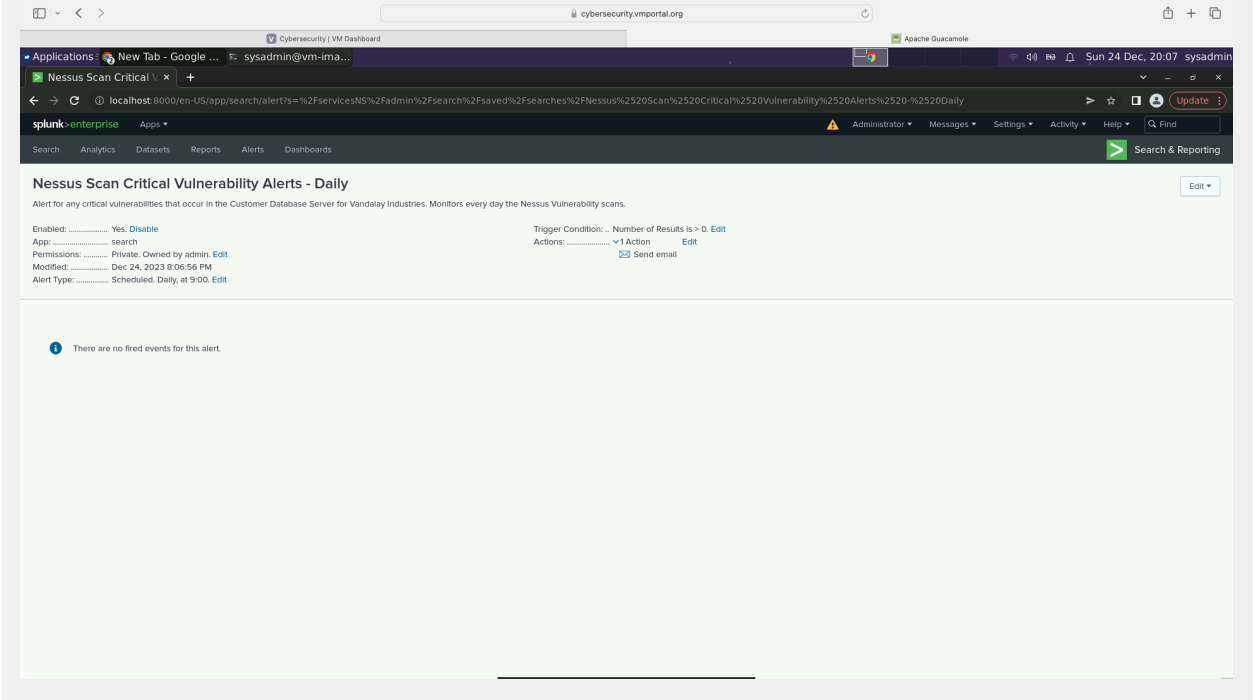
Provide a screenshot of your report:

To create the statistical report, the following query was input into the Splunk search field:

source="nessus_logs.csv" dest_ip="10.11.36.23" | eval Critical=IF(severity="critical", "Critical", "Non-Critical") | stats count by Critical



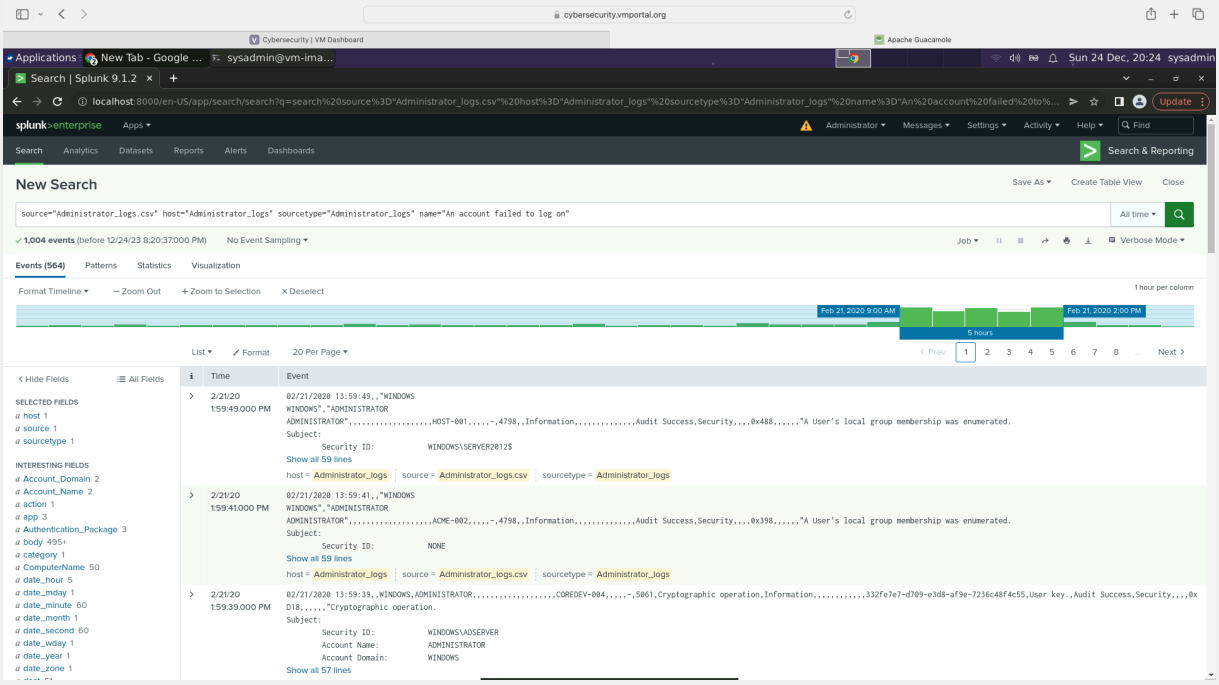
Provide a screenshot showing that the alert has been created:



Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

Brute force attack commenced at: 9:00 am on 02/21/2020.
It lasted for 5 hours, until 2:00 pm.



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

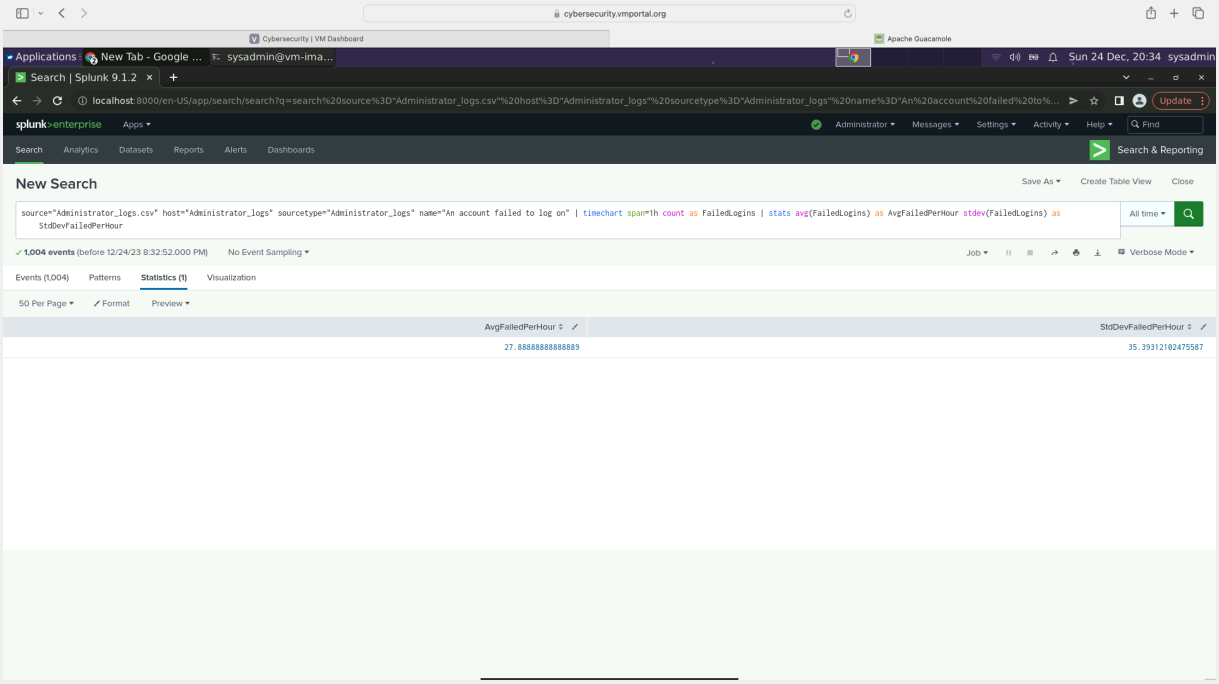
When removing the 5 hours during which a Brute Force Attack was taking place, the range of failed logins is between 6 to 34 failed logins per hour, which is the Baseline.

The lowest number of failed logins during the 5 hours of the Brute Force Attack is 95 events, which is almost triple the amount of the top of the baseline number of failed logins (34).

My recommendation for the Threshold would be set at 40 events per hour. Since 34 events itself seems like an outlier when looking at the other hours (excluding the 5 hours during Brute Force Attack), I wouldn't want the threshold that much higher. 40 allows a little bit of leeway with the purpose of not inducing Alert Fatigue. Should there be a lot of false alerts going forward, I would then raise the threshold to 50.

Note: if the sample size was much larger, I would likely determine my threshold by adding the average number of failed logins per hour to about

1-2 standard deviations, and use that number as my threshold. In this example, even one standard deviation from the average is approximately 63.28 events per hour, which in my opinion is too far away from the top of the baseline, thus risking that potential future Brute Force Attacks might go unnoticed.



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