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

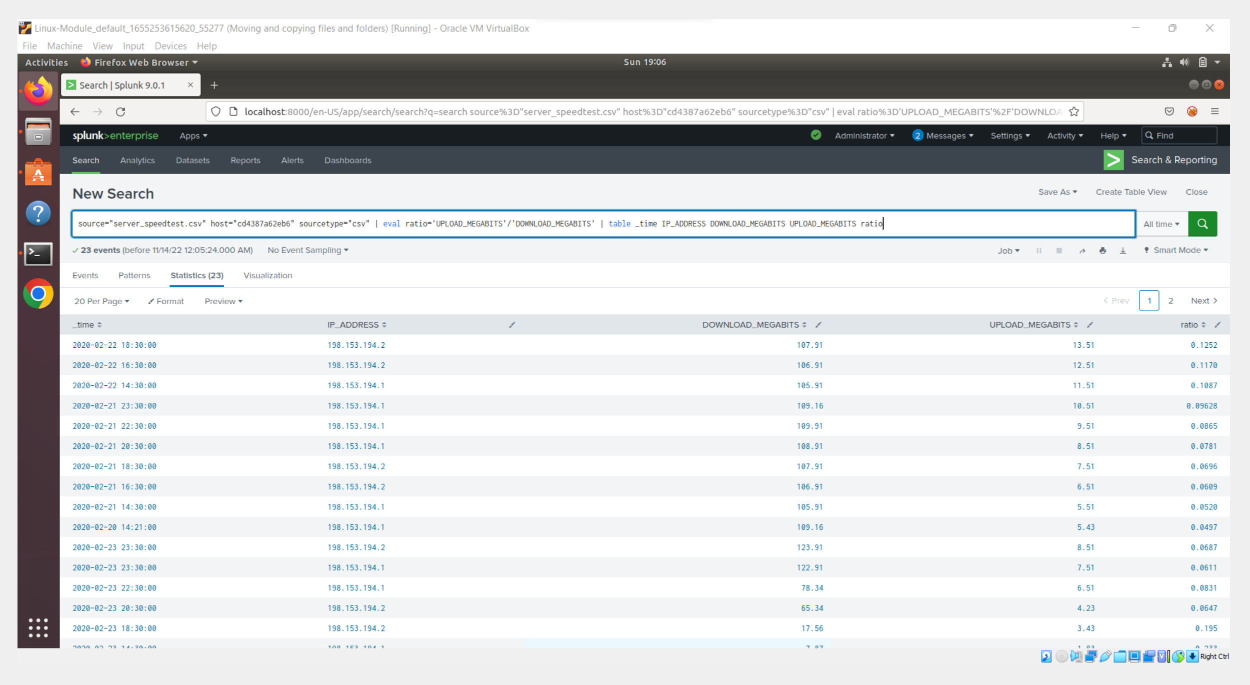
1. Based on the report you created, what is the approximate date and time of the attack?

```
Feb 22nd, 2022 at 18:30
```

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

```
Twenty hours
```

Provide a screenshot of your report:



Linux-Module_default_1655253615620_55277 (Moving and copying files and folders) [Running] - Oracle VM VirtualBox

New Search

```
source="server_speedtest.csv" host="cd4387a62eb6" sourcetype="csv" | eval ratio='UPLOAD_MEGABITS'/'DOWNLOAD_MEGABITS' | table _time IP_ADDRESS DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio
```

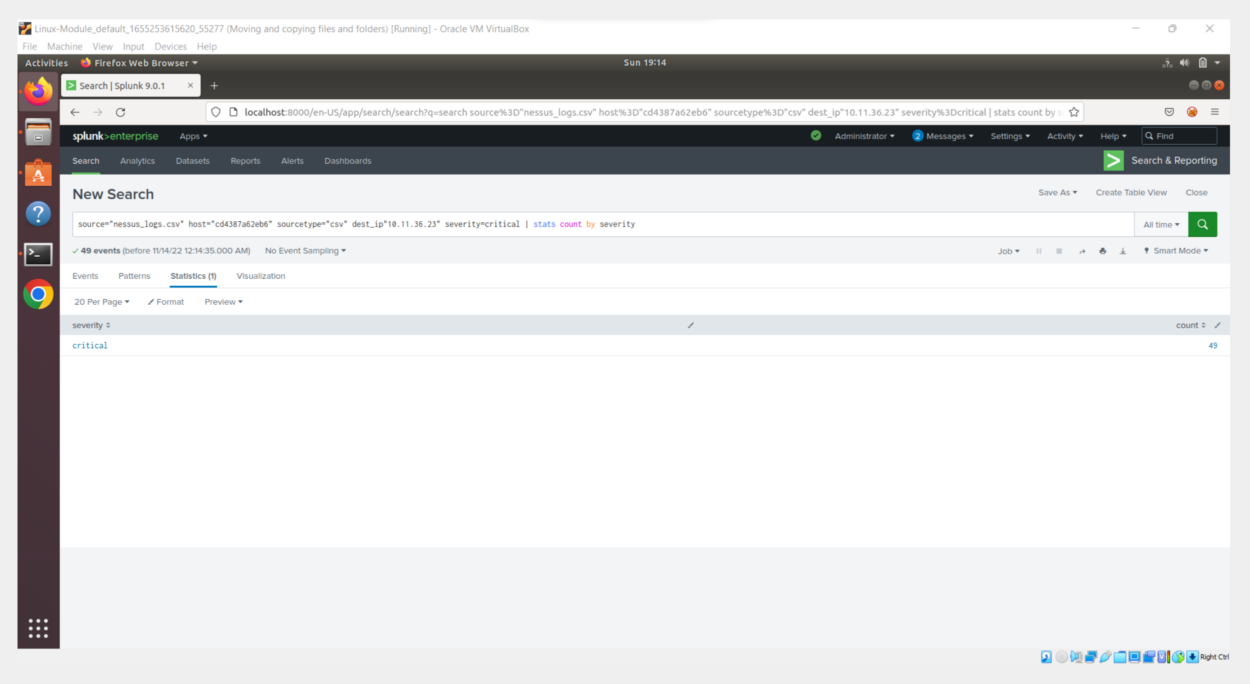
✓ 23 events (before 11/14/22 12:05:24.000 AM) No Event Sampling

Statistics (23)

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-22 18:30:00	198.153.194.2	107.91	13.51	0.1252
2020-02-22 16:30:00	198.153.194.2	106.91	12.51	0.1170
2020-02-22 14:30:00	198.153.194.1	105.91	11.51	0.1087
2020-02-21 23:30:00	198.153.194.1	109.16	10.51	0.09628
2020-02-21 22:30:00	198.153.194.1	109.91	9.51	0.0865
2020-02-21 20:30:00	198.153.194.1	108.91	8.51	0.0781
2020-02-21 18:30:00	198.153.194.2	107.91	7.51	0.0696
2020-02-21 16:30:00	198.153.194.2	106.91	6.51	0.0609
2020-02-21 14:30:00	198.153.194.1	105.91	5.51	0.0520
2020-02-20 14:21:00	198.153.194.1	109.16	5.43	0.0497
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	0.0687
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	0.0611
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	0.0831
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	0.0647
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	0.195

Step 2: Are We Vulnerable?

Provide a screenshot of your report:



Linux-Module_default_1655253615620_55277 (Moving and copying files and folders) [Running] - Oracle VM VirtualBox

New Search

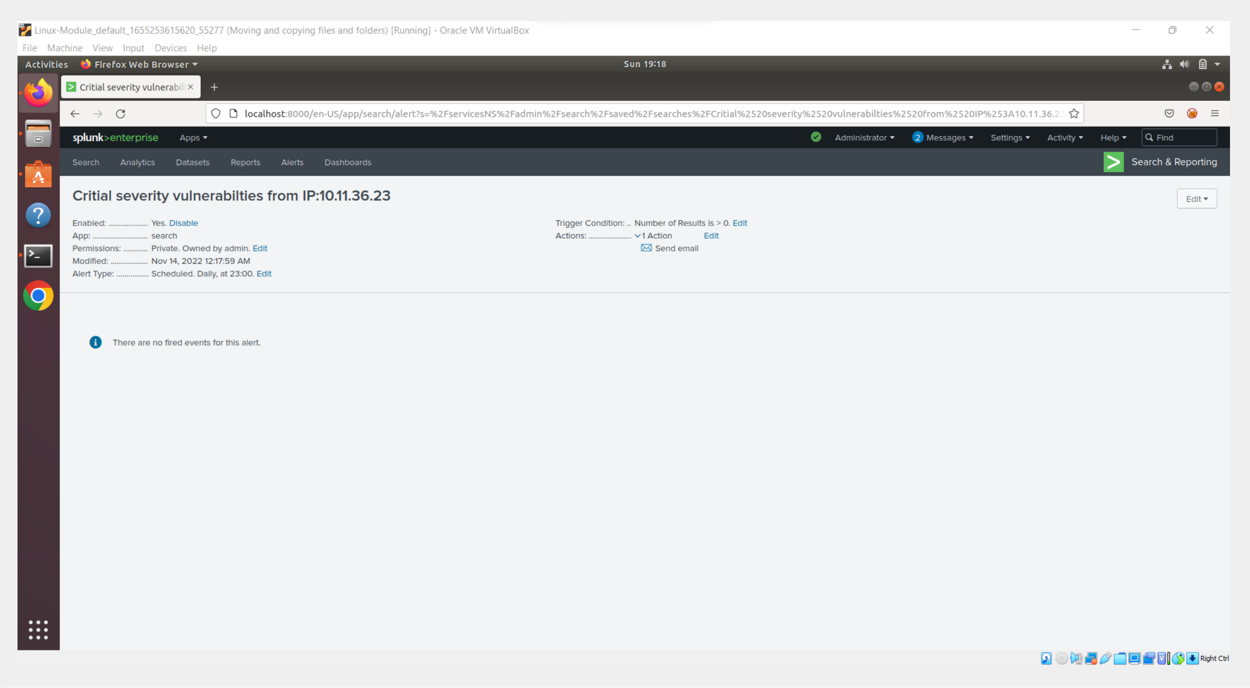
```
source="nessus_logs.csv" host="cd4387a62eb6" sourcetype="csv" dest_ip"10.11.36.23" severity=critical | stats count by severity
```

✓ 49 events (before 11/14/22 12:14:35.000 AM) No Event Sampling

Statistics (1)

severity	count
critical	49

Provide a screenshot showing that the alert has been created:


Linux-Module_default_1655253615620_55277 (Moving and copying files and folders) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Sun 19:18
Critial severity vulnerabil
localhost:8000/en-US/app/search/alert?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2FCritial%2520severity%2520vulnerabilties%2520from%2520IP%253A10.11.36.2
splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit
Right Ctrl

Critial severity vulnerabilties from IP:10.11.36.23

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Nov 14, 2022 12:17:59 AM
Alert Type: .... Scheduled. Daily, at 23:00. Edit

Trigger Condition: .. Number of Results is > 0. Edit
Actions: .... 1 Action Edit
Send email

There are no fired events for this alert.

Step 3: Drawing the (Base)line

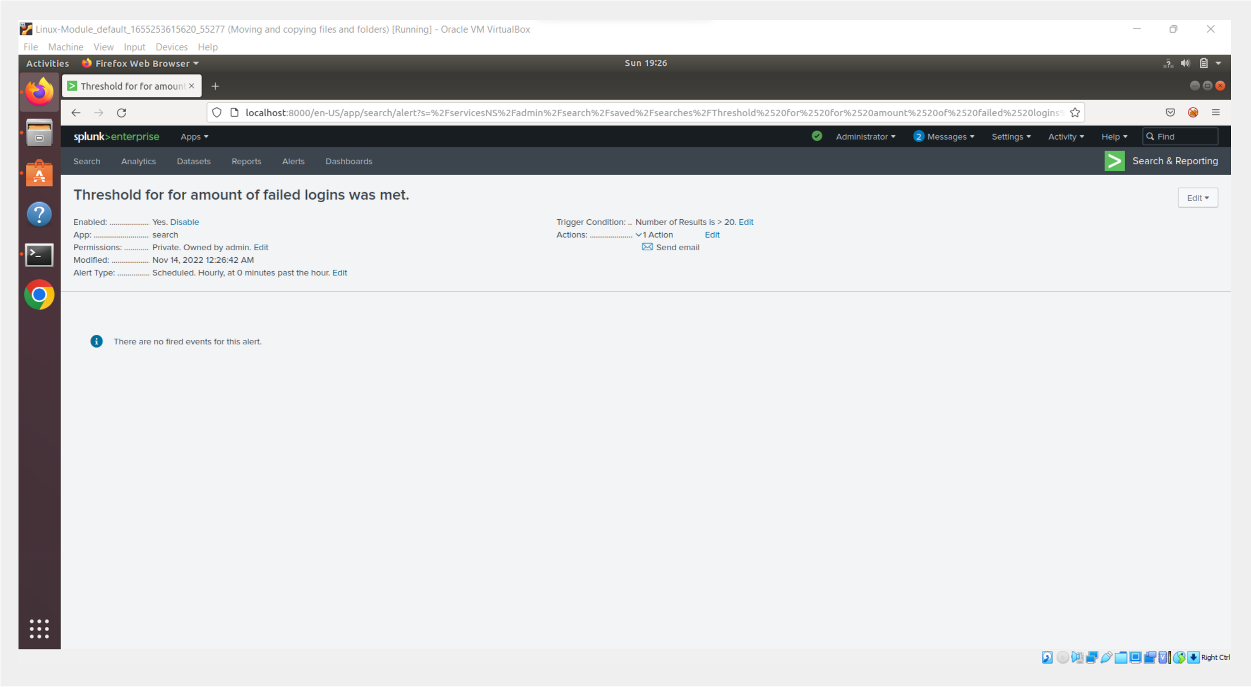
1. When did the brute force attack occur?

```
Feb 21st, at 9:00am
```

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

```
My baseline is 15 an hour and 20 or more is an attack
```

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



Linux-Module_default_1655253615620_55277 (Moving and copying files and folders) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Sun 19:26
Threshold for for amount
localhost:8000/en-US/app/search/alert?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2FThreshold%2520for%2520for%2520amount%2520of%2520failed%2520logins
splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit
Right Ctrl

Threshold for for amount of failed logins was met.

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by admin. Edit
Modified: .... Nov 14, 2022 12:26:42 AM
Alert Type: .... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 20. Edit
Actions: .... 1 Action Edit
Send email

There are no fired events for this alert.