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

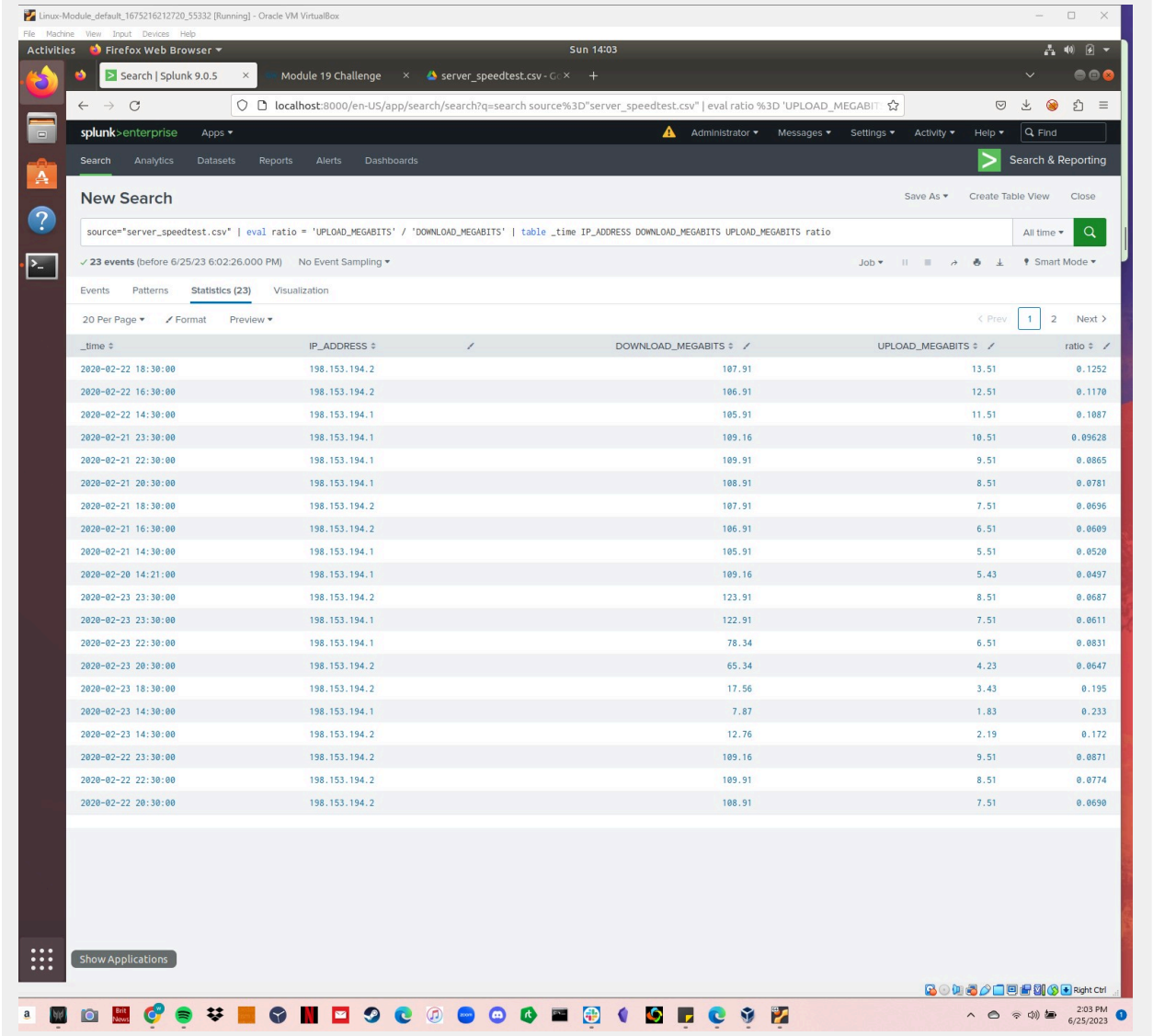
1. Based on the report you created, what is the approximate date and time of the attack?

```
02/23/2020 at 2:30pm
```

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

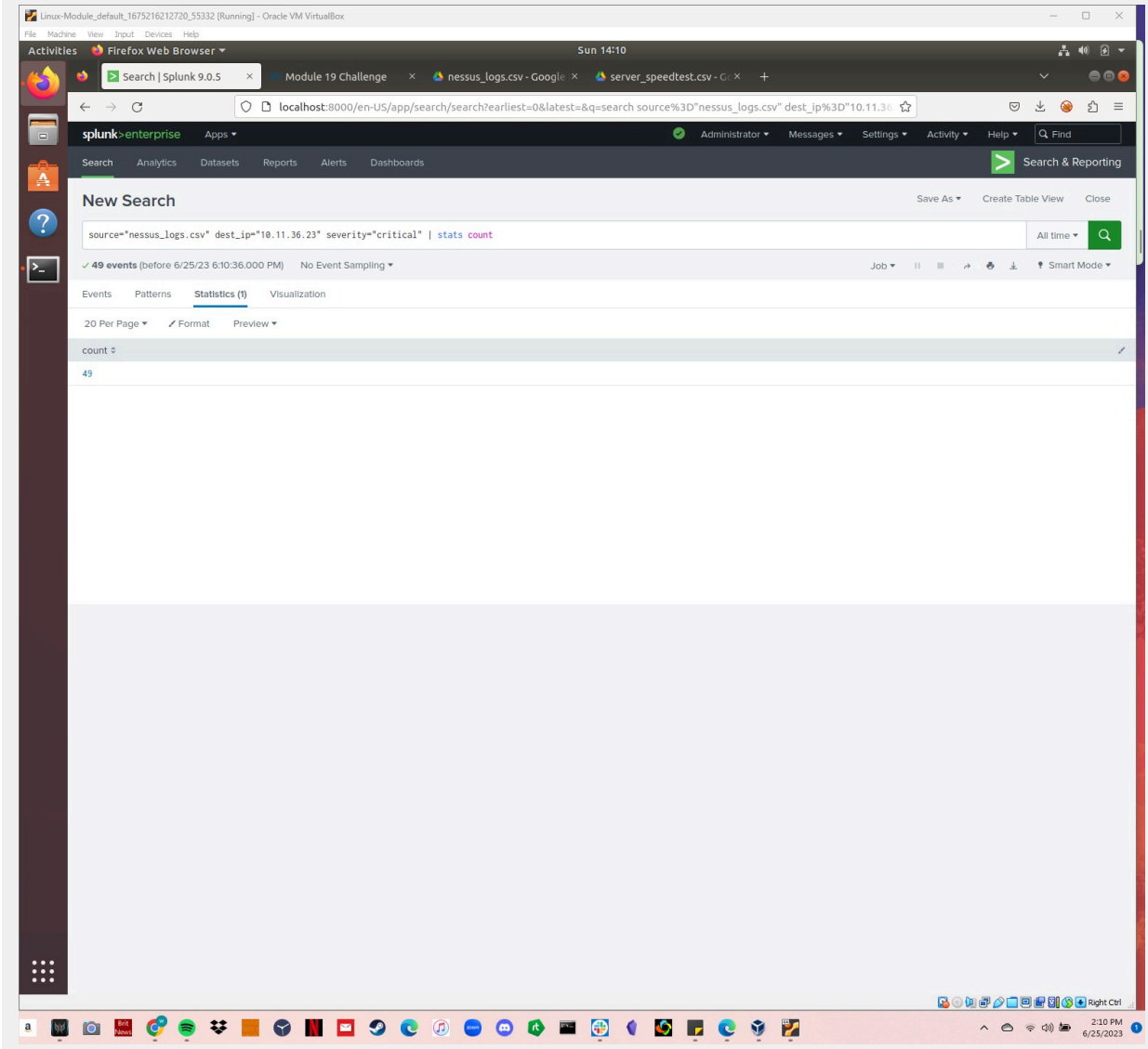
```
9 hours
```

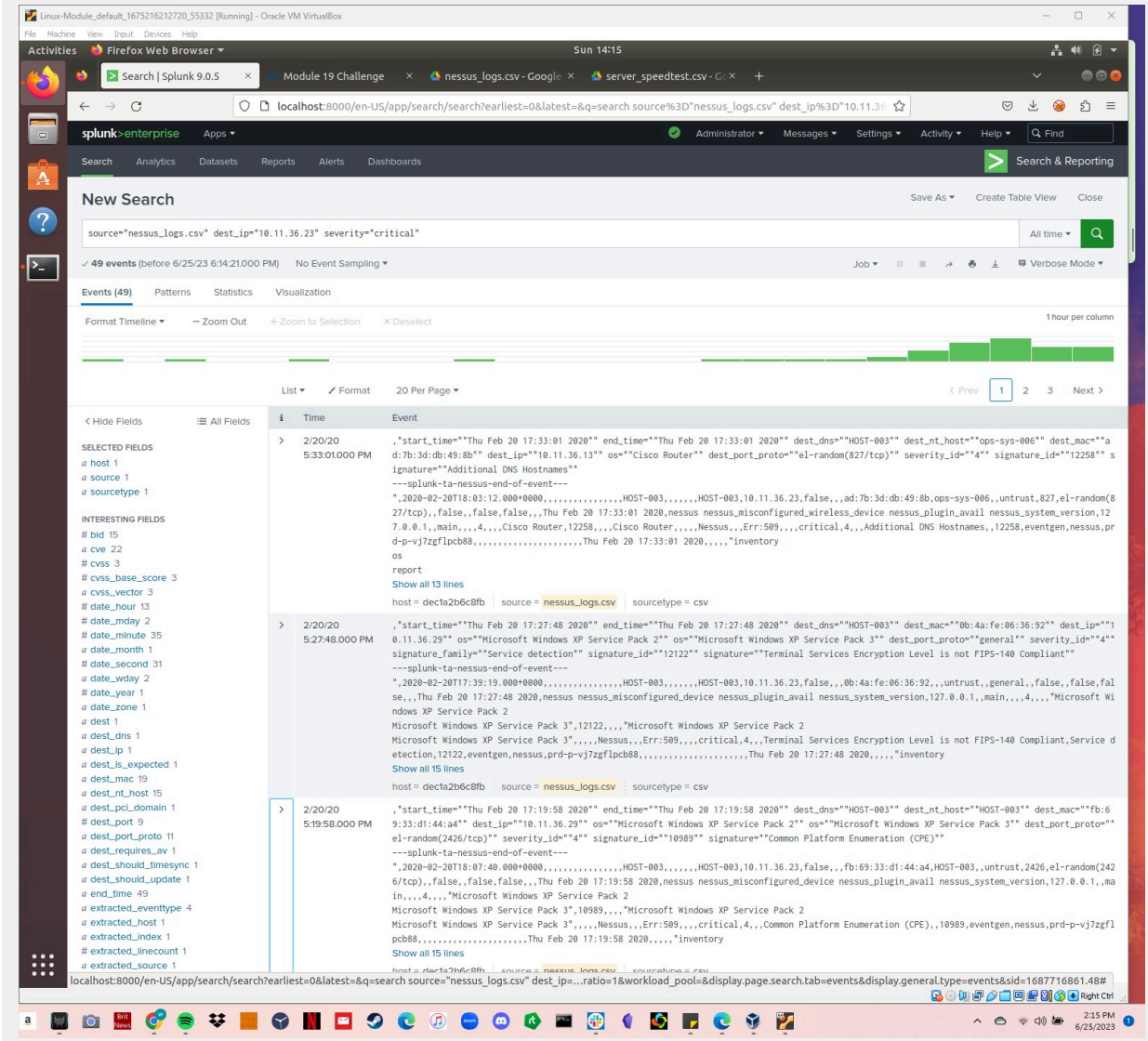
Provide a screenshot of your report:



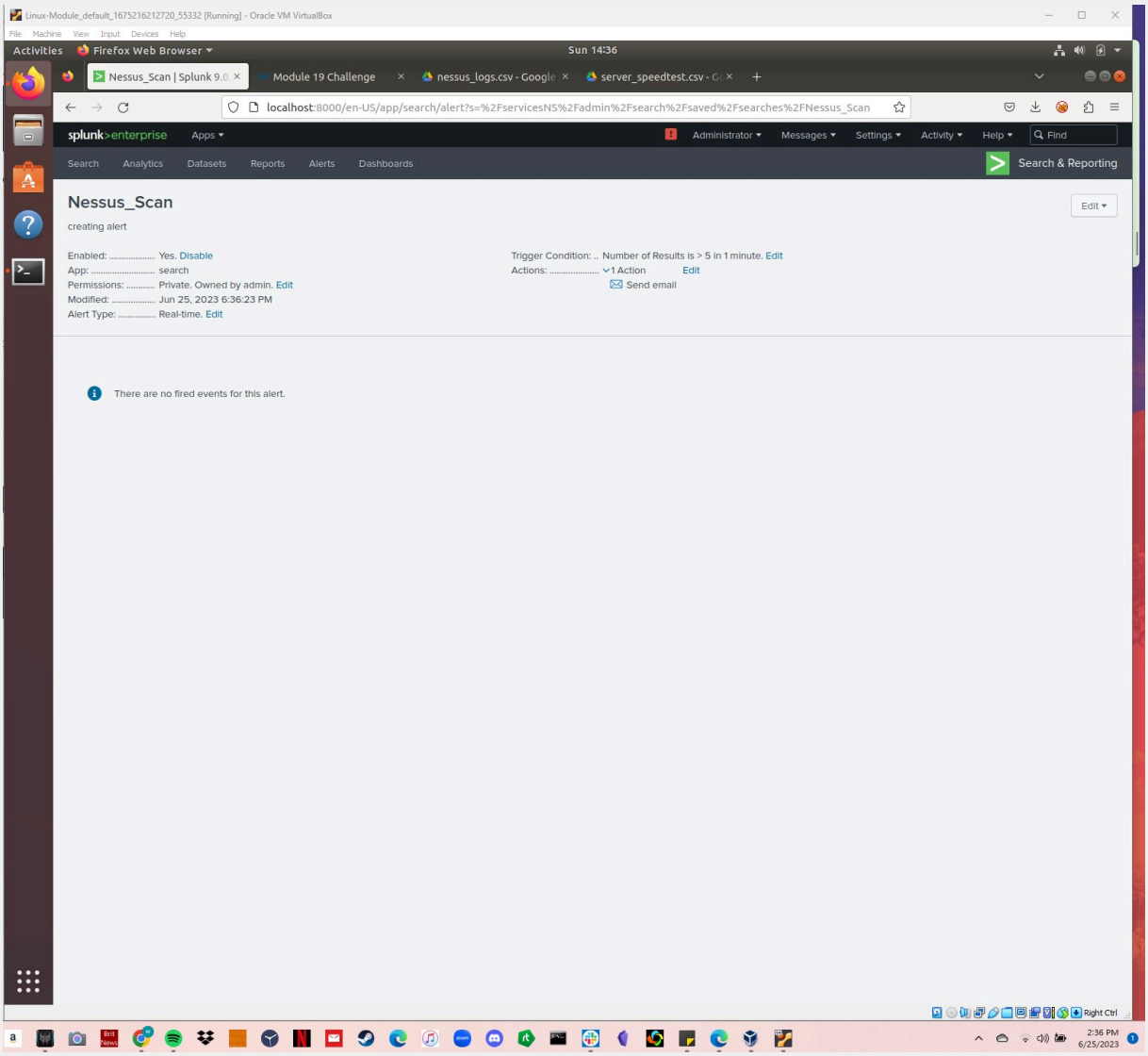
Step 2: Are We Vulnerable?

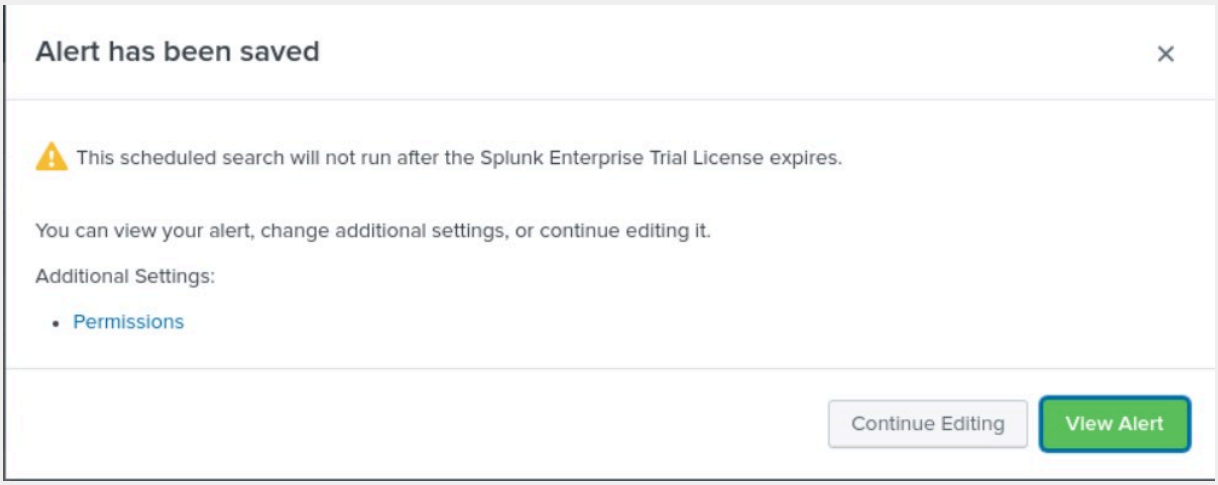
Provide a screenshot of your report:


Linux-Module_default_1675216212720_55332 [Running] - Oracle VM VirtualBox
Activities
Firefox Web Browser
Sun 14:10
Search | Splunk 9.0.5
Module 19 Challenge
nessus_logs.csv - Google
server_speedtest.csv - G
localhost:8000/en-US/app/search/search?earliest=0&latest=&q=search source%3D"nessus_logs.csv" dest_ip%3D"10.11.3
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="nessus_logs.csv" dest_ip="10.11.36.23" severity="critical" | stats count
All time
✓ 49 events (before 6/25/23 6:10:36.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (1)
Visualization
20 Per Page
Format
Preview
count
49
Right Ctrl
2:10 PM
6/25/2023



Provide a screenshot showing that the alert has been created:


Linux-Module_default_1675216212720_55332 [Running] - Oracle VM VirtualBox
Activities
Firefox Web Browser
Sun 14:36
Nessus_Scan | Splunk 9.0
Module 19 Challenge
nessus_logs.csv - Google
server_speedtest.csv
localhost:8000/en-US/app/search/alert?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2FNessus_Scan
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Nessus_Scan
Edit
creating alert
Enabled: Yes. Disable
App: search
Permissions: Private. Owned by admin. Edit
Modified: Jun 25, 2023 6:36:23 PM
Alert Type: Real-time. Edit
Trigger Condition: Number of Results is > 5 in 1 minute. Edit
Actions: 1 Action Edit
Send email
There are no fired events for this alert.
Right Ctrl
2:36 PM
6/25/2023


Alert has been saved
This scheduled search will not run after the Splunk Enterprise Trial License expires.
You can view your alert, change additional settings, or continue editing it.
Additional Settings:
Permissions
Continue Editing
View Alert

Step 3: Drawing the (Base)line

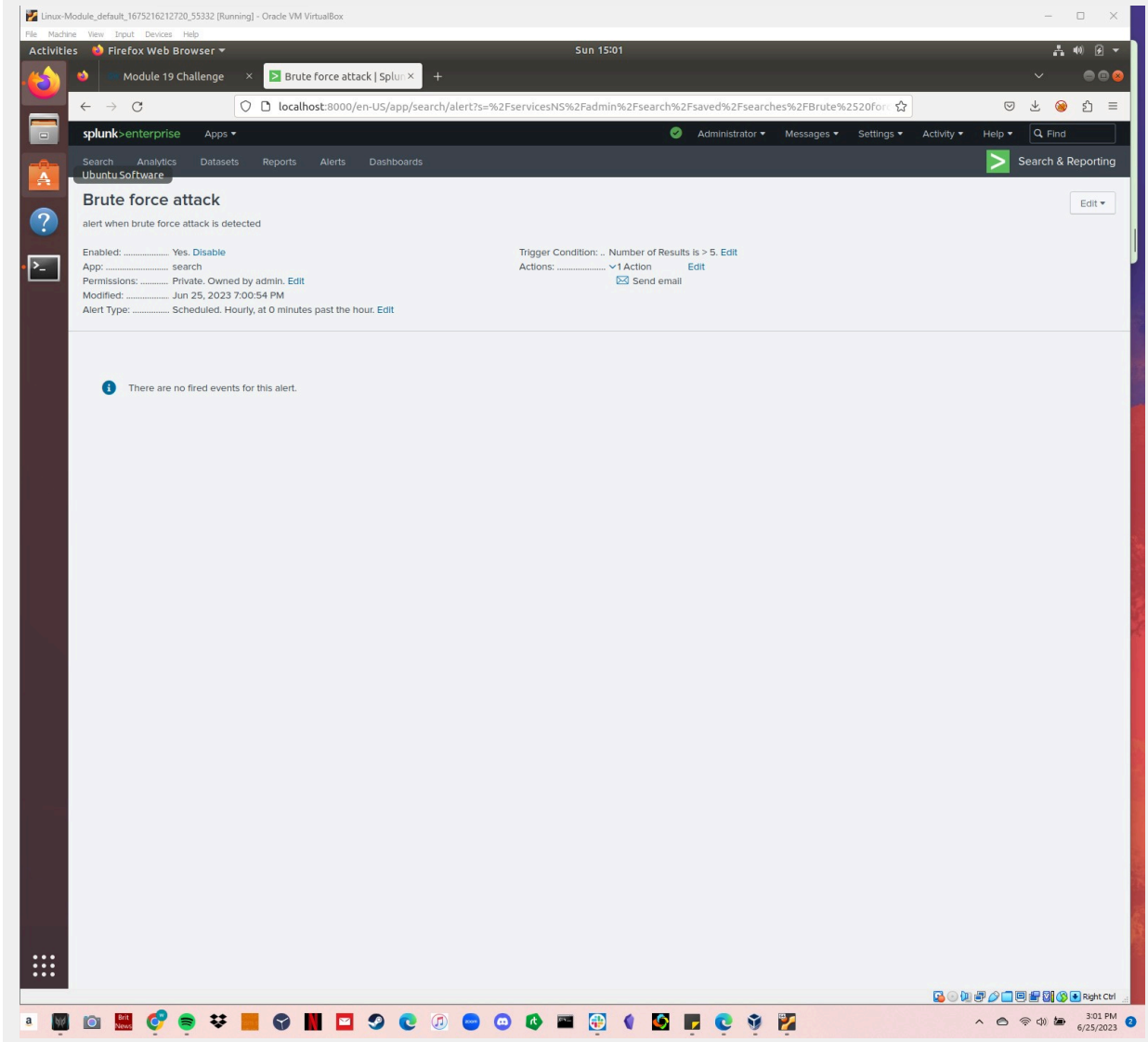
1. When did the brute force attack occur?

```
02/21/2020 9:00am - 1:00pm
```

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

```
My baseline for normal activity is 4 failed logins in an hour, my threshold
to alert a brute force will be 5 failed logins in an hour
```

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


Linux-Module_default_1675216212720_55332 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Sun 15:01
Module 19 Challenge
Brute force attack | Splun
localhost:8000/en-US/app/search/alert?s=%2FservicesNS%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2FBrute%2520for
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Ubuntu Software
Brute force attack
Edit
alert when brute force attack is detected
Enabled: Yes. Disable
App: search
Permissions: Private. Owned by admin. Edit
Modified: Jun 25, 2023 7:00:54 PM
Alert Type: Scheduled. Hourly, at 0 minutes past the hour. Edit
Trigger Condition: Number of Results is > 5. Edit
Actions: 1 Action Edit
Send email
There are no fired events for this alert.
Right Ctrl
3:01 PM
6/25/2023