



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

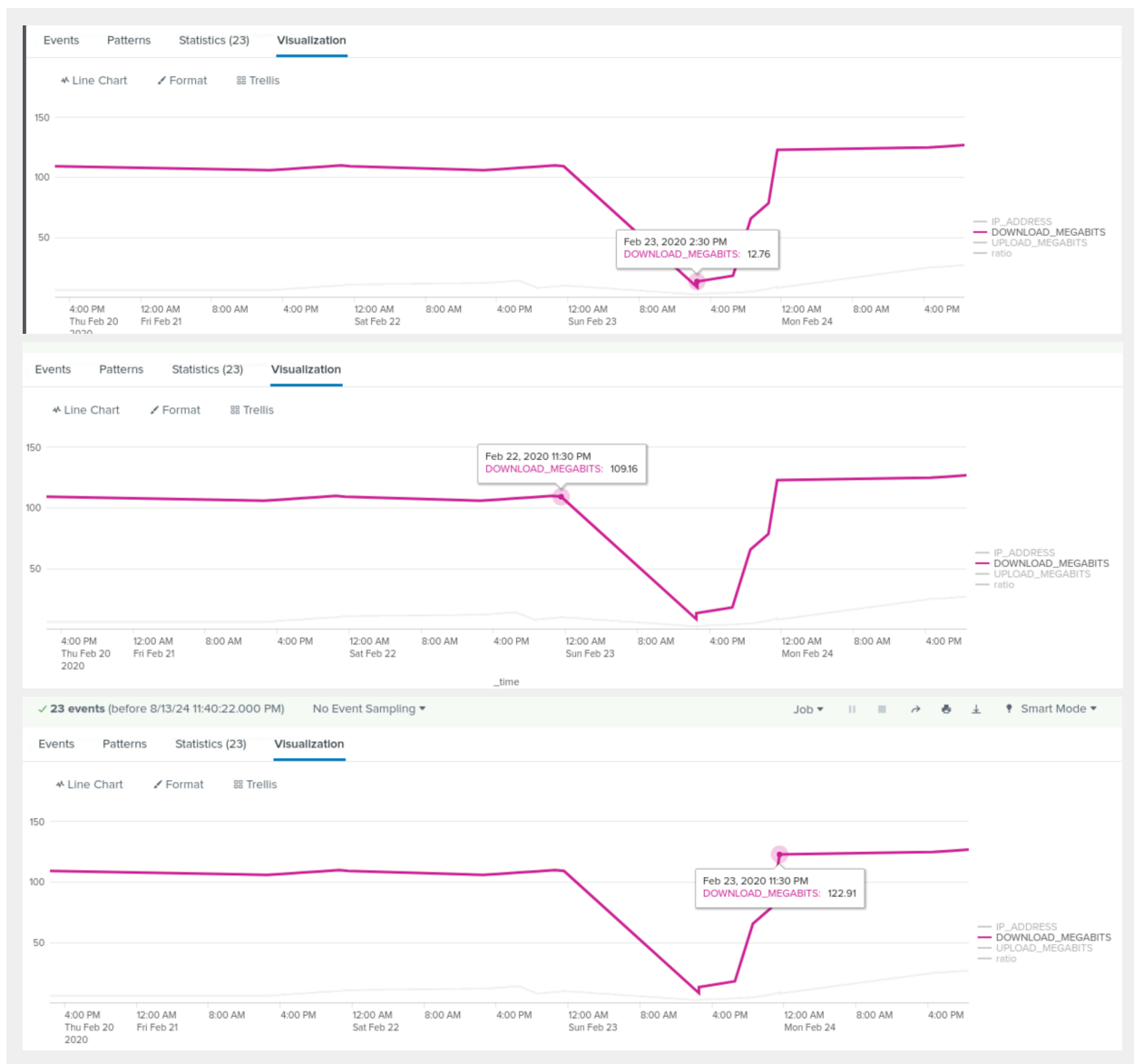
1. Based on the report you created, what is the approximate date and time of the attack?

The approximate date and time is between February 22/2020 at 11:30pm, February 23/2020 at 2:30pm.

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

It took 9 hour to recover

Provide a screenshot of your report:

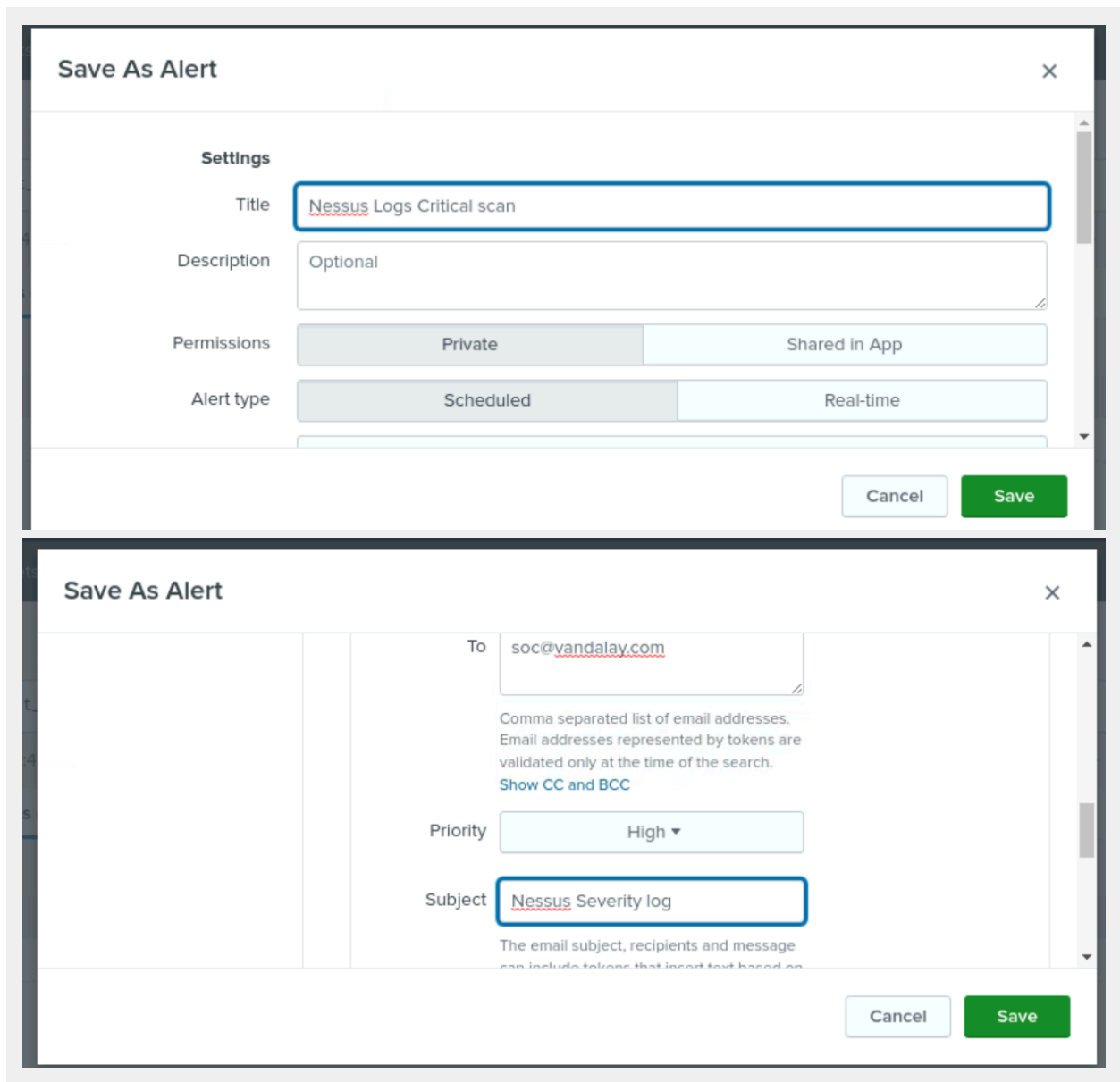


Step 2: Are We Vulnerable?

Provide a screenshot of your report:



Provide a screenshot showing that the alert has been created:



Save As Alert

Message

The Nessus alert is ready to check with a critical severity level

Include

☒ Link to Alert
☐ Link to Results
☐ Search String
☐ Trigger Condition
☐ Trigger Time
☐ Allow Empty
☐ Attach CSV
☐ Attach PDF

Cancel

Save

Search Analytics Datasets Reports Alerts Dashboards

Nessus Logs Critical scan

Enabled: Yes. [Disable](#)

App: search

Permissions: Private. Owned by admin. [Edit](#)

Modified: Aug 14, 2024 12:09:35 AM

Alert Type: Scheduled. Daily, at 0:00. [Edit](#)

Trigger Condition: .. Number of Results is > 0. [Edit](#)

Actions: [1 Action](#) [Edit](#)

[Send email](#)

Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

The attack occur on February/21(friday)/2020 at 9:00am

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

The attack has between 130 and 142 failed log on, a normal activity for the system is about 10 to 18.

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

Save As Alert



Settings

Title Failed log on critical

Description Optional

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Run every hour

Cancel

Save

Save As Alert



When triggered



Send email

Remove

To SOC@vandalay.com

Comma separated list of email addresses.
Email addresses represented by tokens are
validated only at the time of the search.

[Show CC and BCC](#)

Priority

High

Subject failed log on alert

Cancel

Save

Save As Alert

the results of the search: [Learn more](#)

Message

The log on alert has been created and is ready to investigate a Brute Force Attack.

Include

☒ Link to Alert

☐ Link to Results

☐ Search String

☐ Inline [Table](#)

☐ Trigger Condition

☐ Attach CSV

☐ Trigger Time

☐ Attach PDF

Cancel

Save

SearchAnalyticsDatasetsReportsAlertsDashboards

Failed log on critical

Enabled: Yes. [Disable](#)

App: search

Permissions: Private. Owned by admin. [Edit](#)

Modified: Aug 14, 2024 4:25:33 AM

Alert Type: Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)

Trigger Condition: .. Number of Results is > 0. [Edit](#)

Actions: [1 Action](#) [Edit](#)

☒ Send email

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.