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?

```
Command: source="server_speedtest.csv" host="server-speed-test" | eval ratio
= 'UPLOAD_MEGABITS' / 'DOWNLOAD_MEGABITS' | table _time IP_ADDRESS
DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio

Based on the report the time of the attack was after 2020-02-22 at
approximately 23:30:00
```

Fig 1. The Download megabits value dips

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

```
About 15 hrs for the system to recover.
```

Fig 2. From 23:30:00 to 14:30:00

Provide a screenshot of your report:

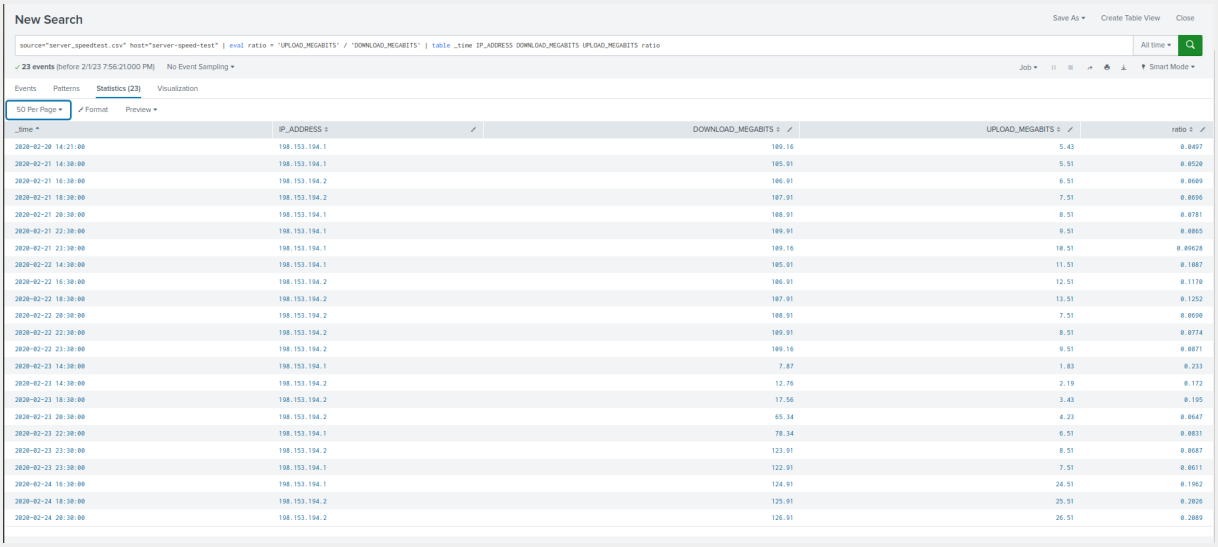

Fig 3.

Step 2: Are We Vulnerable?

Provide a screenshot of your report:

Command: **source="nessus_logs.csv" dest_ip="10.11.36.23" | stats count by severity**

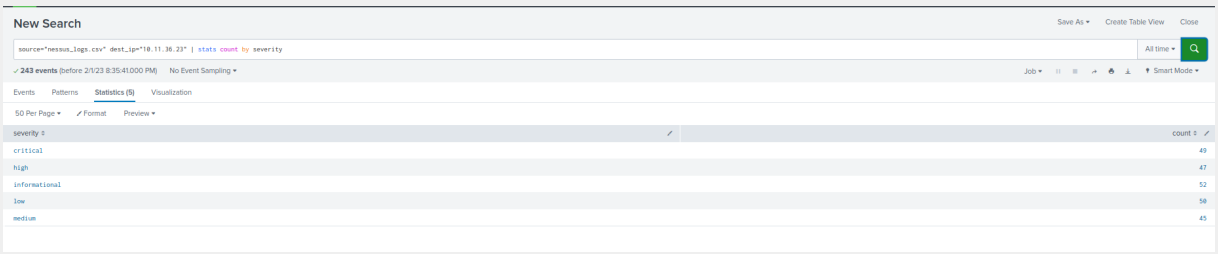

Fig 4. General Severity Sort

Command: **source="nessus_logs.csv" dest_ip="10.11.36.23" severity=critical | stats count by severity**

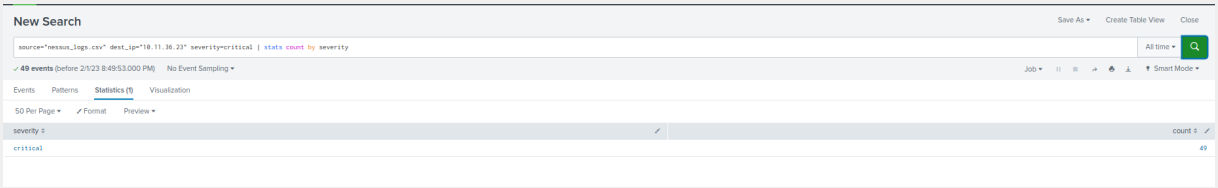

Fig 6. Filter Severity by Critical

Provide a screenshot showing that the alert has been created:

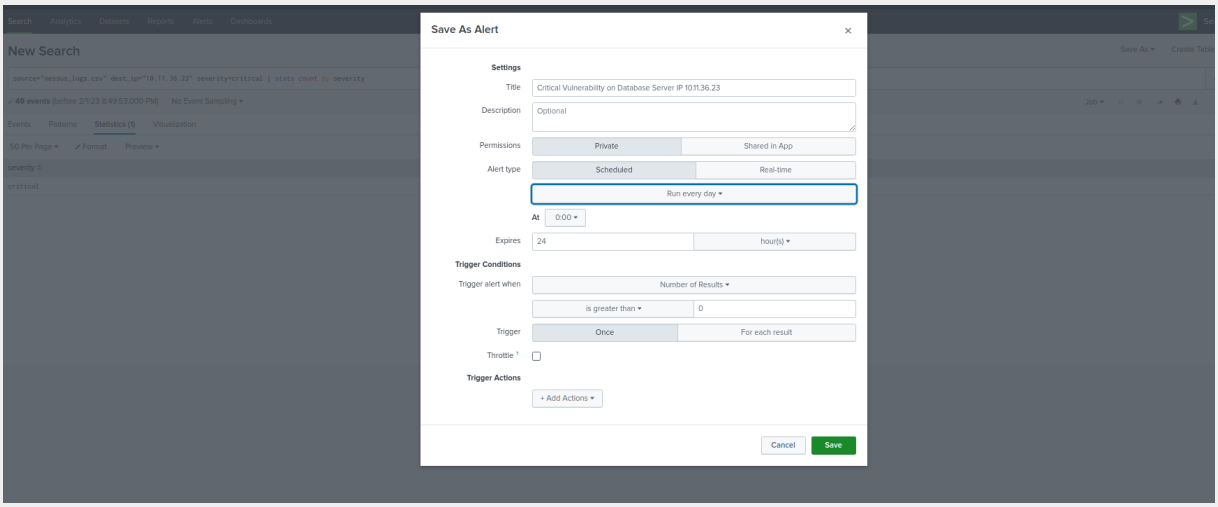

Fig 7. Naming alert and set Alert type

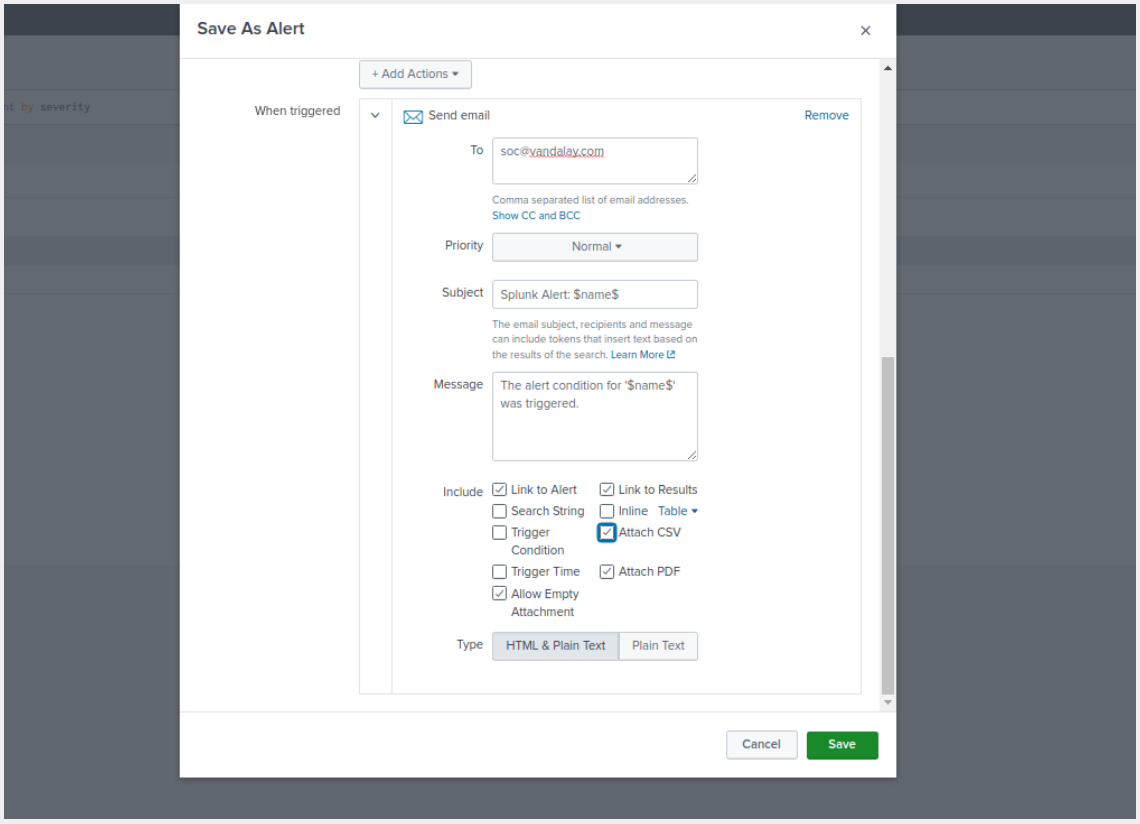

Fig 8. Setting email alert type

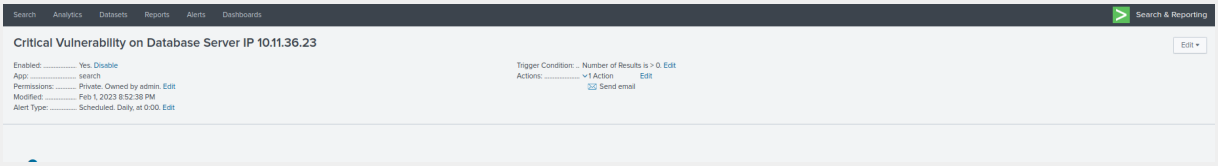

Fig 9. Result

Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

Command: **source="Administrator_logs.csv" name="An account failed to log on"**

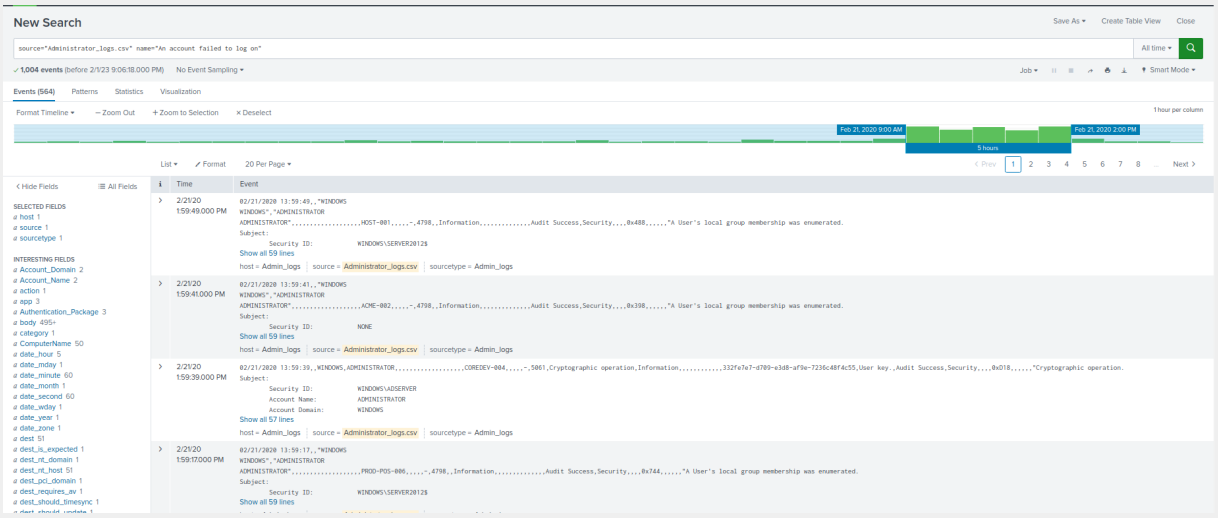

Fig 10.

The brute force attack occurred between Feb 21, 2020 9:00 am to Feb 21, 2020 2:00 pm for a time of 5 hrs

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

```
Normal activity: 20 logins
Brute Force attack: 25 logins
```

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

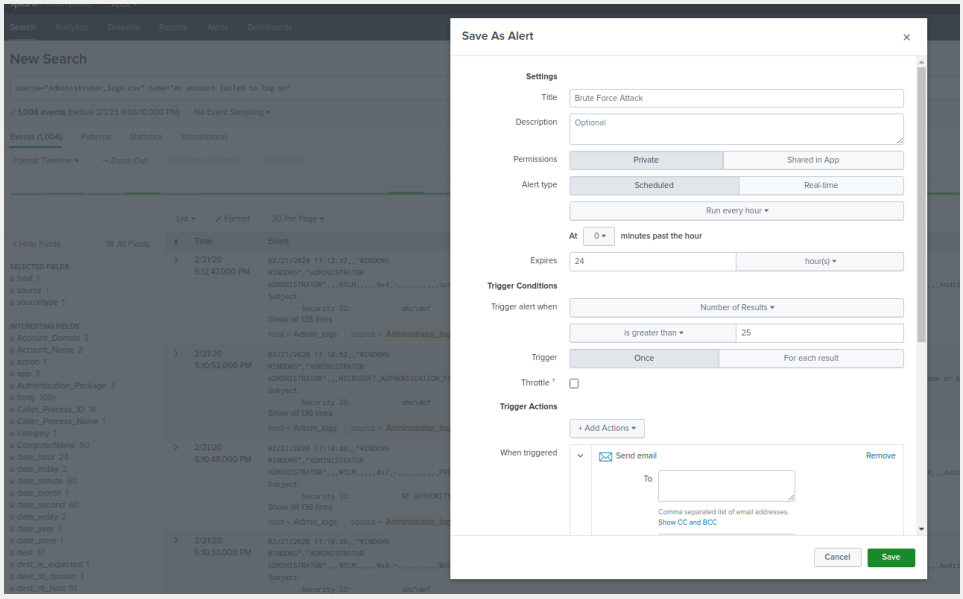

Fig 11. Setting alert every hour

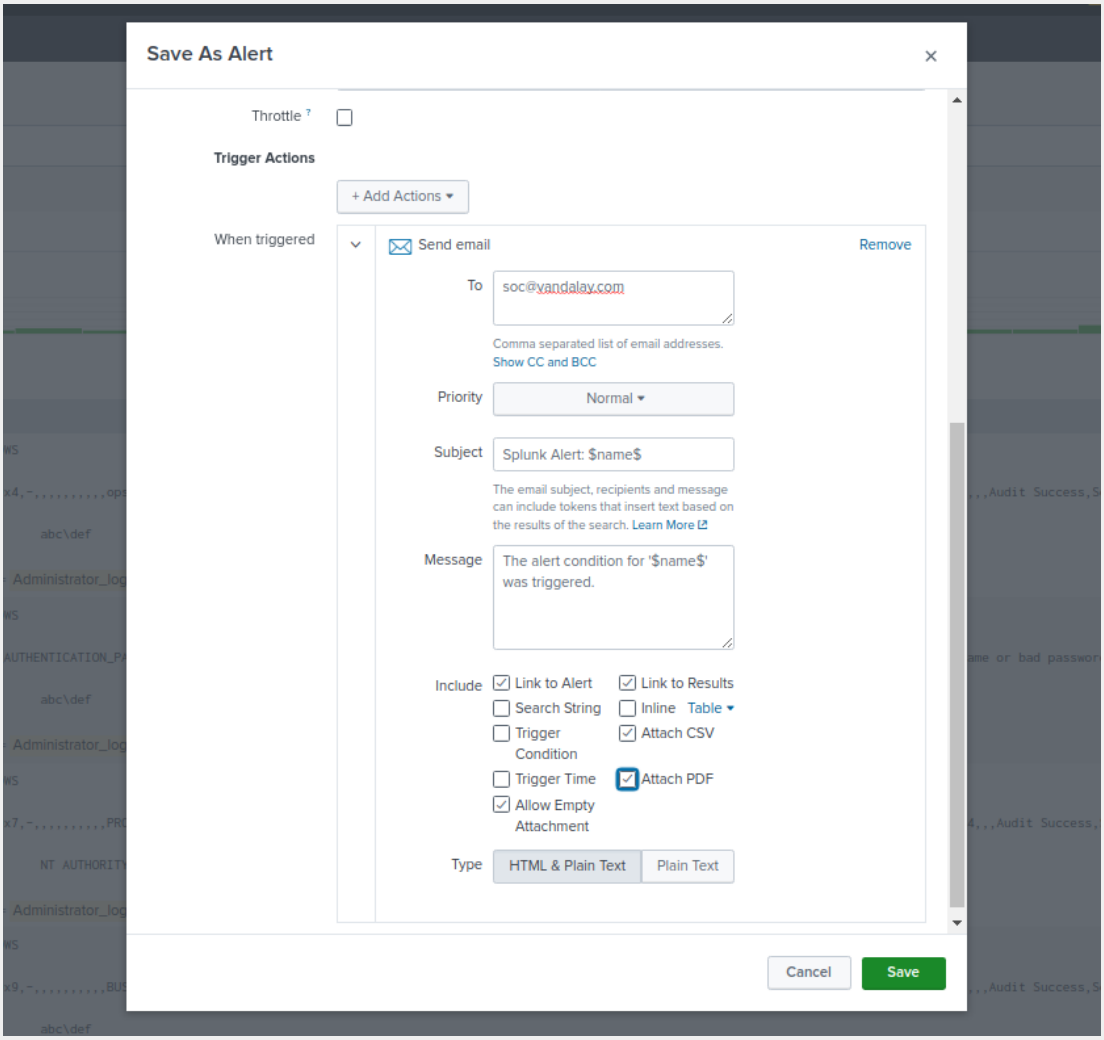

Fig 12.

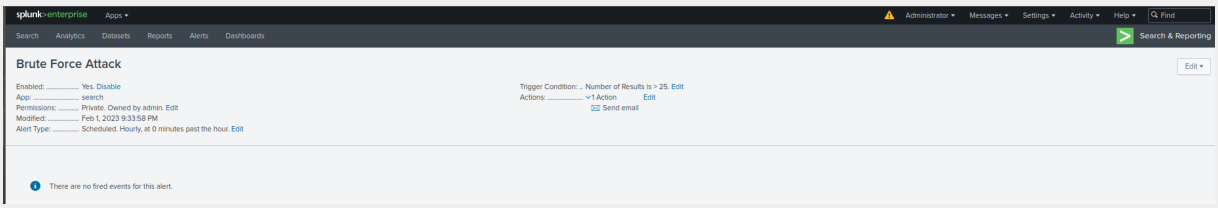

Fig 13. Result of creating alert