Coursework

Unit 18 Homework: Lets go Splunking!

Submitted By
Shaerul Haque Joarder

Vandalay Industries Monitoring Activity Instructions

Step 1: The Need for Speed

Background: As the worldwide leader of importing and exporting, Vandalay Industries has been the target of many adversaries attempting to disrupt their online business. Recently, Vandaly has been experiencing DDOS attacks against their web servers.

Not only were web servers taken offline by a DDOS attack, but upload and download speed were also significantly impacted after the outage. Your networking team provided results of a network speed run around the time of the latest DDOS attack.

Task: Create a report to determine the impact that the DDOS attack had on download and upload speed. Additionally, create an additional field to calculate the ratio of the upload speed to the download speed.

1. Upload the following file of the system speeds around the time of the attack.
    - Speed Test File
2. Using the eval command, create a field called ratio that shows the ratio between the upload and download speeds.
    - Hint: The format for creating a ratio is: | eval new_field_name = 'fieldA' / 'fieldB'

    Answer:

    ```
    eval DownToUpRatio = 'DOWNLOAD_MEGABITS'/'UPLOAD_MEGABITS'
    ```

3. Create a report using the Splunk's table command to display the following fields in a statistics report:
    - _time
    - IP_ADDRESS
    - DOWNLOAD_MEGABITS
    - UPLOAD_MEGABITS
    - Ratio

    Hint: Use the following format when for the table command: | table fieldA field fieldC

    Answer:

    SPL

    ```
    source="server_speedtest.csv" | eval DownToUpRatio =
    'DOWNLOAD_MEGABITS'/'UPLOAD_MEGABITS' | table _time
    DOWNLOAD_MEGABITS UPLOAD_MEGABITS DownToUpRatio
    ```

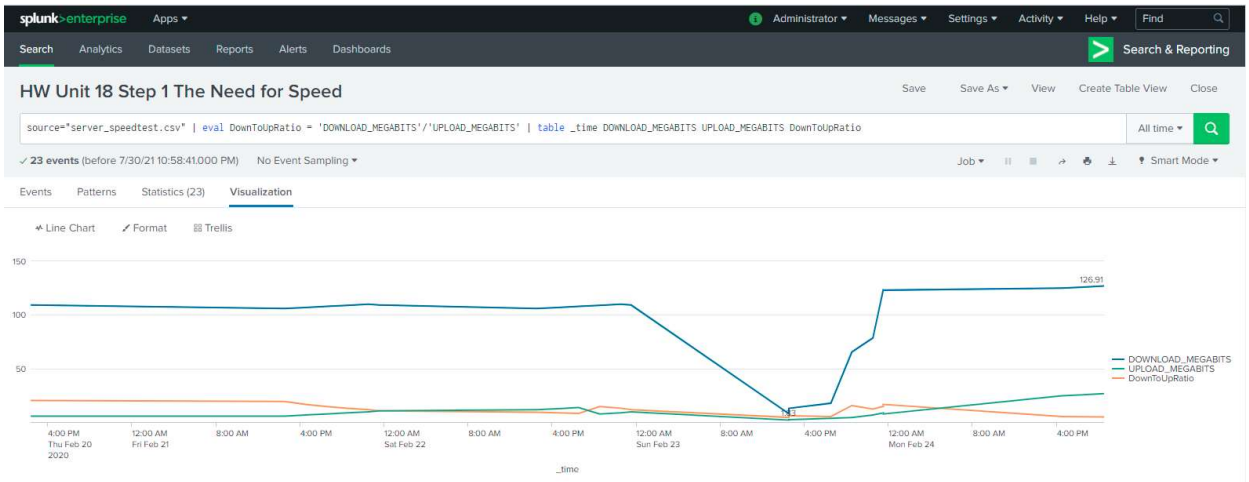
Statistical Output in Splunk:

Events Patterns **Statistics (23)** Visualization

20 Per Page ▾ Format Preview ▾ < Prev 1 2 Next >

_time	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	DownToUpRatio
2020-02-21 18:30:00	107.91	7.51	14.4
2020-02-21 16:30:00	106.91	6.51	16.4
2020-02-21 14:30:00	105.91	5.51	19.2
2020-02-20 14:21:00	109.16	5.43	20.1
2020-02-22 14:30:00	105.91	11.51	9.202
2020-02-21 23:30:00	109.16	10.51	10.39
2020-02-21 22:30:00	109.91	9.51	11.6
2020-02-21 20:30:00	108.91	8.51	12.8
2020-02-22 22:30:00	109.91	8.51	12.9
2020-02-22 20:30:00	108.91	7.51	14.5
2020-02-22 18:30:00	107.91	13.51	7.987
2020-02-22 16:30:00	106.91	12.51	8.546
2020-02-23 18:30:00	17.56	3.43	5.12
2020-02-23 14:30:00	7.87	1.83	4.30
2020-02-23 14:30:00	12.76	2.19	5.83
2020-02-22 23:30:00	109.16	9.51	11.5
2020-02-23 23:30:00	123.91	8.51	14.6
2020-02-23 23:30:00	122.91	7.51	16.4
2020-02-23 22:30:00	78.34	6.51	12.0
2020-02-23 20:30:00	65.34	4.23	15.4

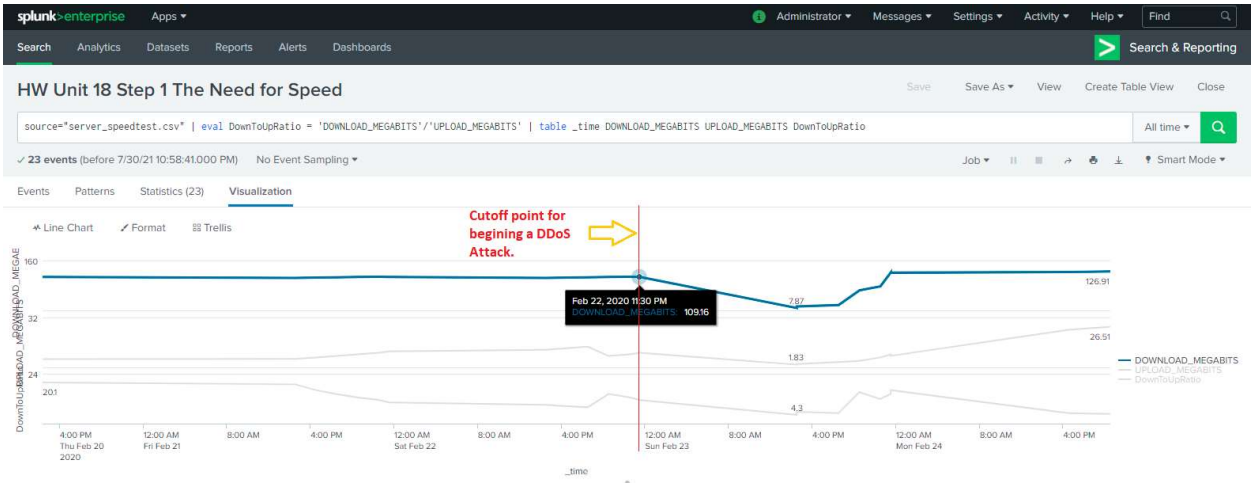
Visualized Output in Splunk:



4. Answer the following questions:

   - Based on the report created, what is the approximate date and time of the attack?

     Answer: The beginning of sharp decline witnesses the beginning of attack which was approximately on **Feb 22, 2020** at **11:30 PM** as per the time series visual.

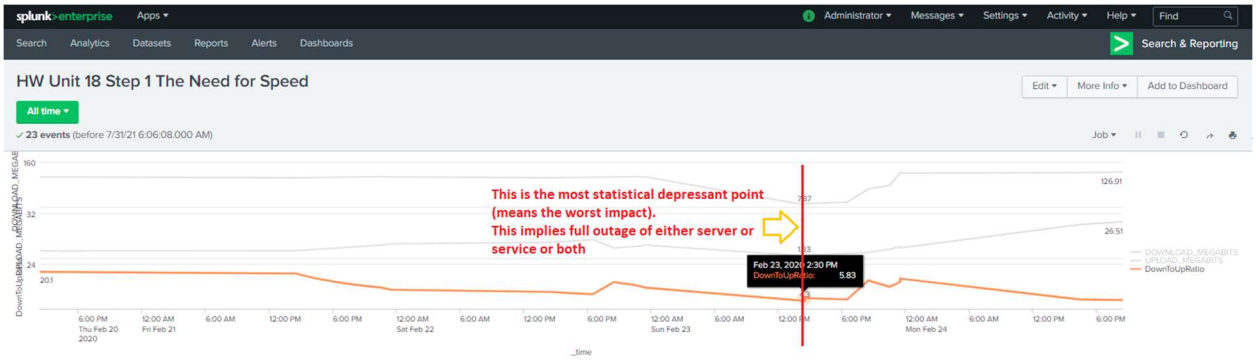


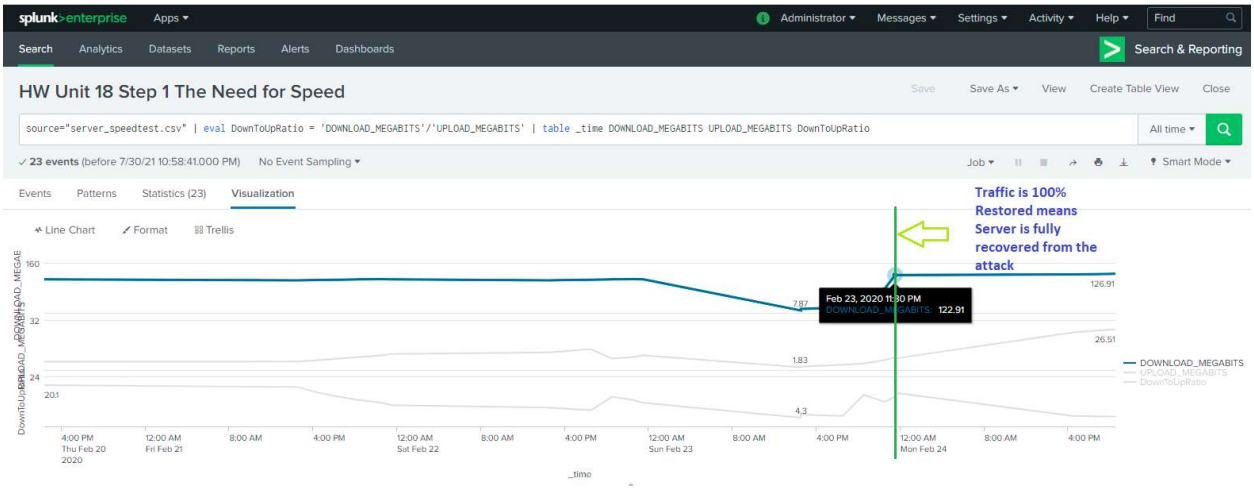
- How long did it take your systems to recover?

Submit a screen shot of your report and the answer to the questions above.

Answer:

The worst impact or server down occurred on **Feb 23, 2020** at **02:30 PM**





100% traffic restoration as per the visuals were around **Feb 23, 2020** at **11:30 PM** as per the time series visual.

The duration between the start of DDoS attack and Full recovery was 12 Hours. **Meantime to Repair (MTTR) 9 Hours [Feb 23, 2020** at **02:30 PM - 11:30 PM]**

Step 2: Are We Vulnerable?

Background: Due to the frequency of attacks, your manager needs to be sure that sensitive customer data on their servers is not vulnerable. Since Vandalay uses Nessus vulnerability scanners, you have pulled the last 24 hours of scans to see if there are any critical vulnerabilities.

- For more information on Nessus, read the following link: https://www.tenable.com/products/nessus

Task: Create a report determining how many critical vulnerabilities exist on the customer data server. Then, build an alert to notify your team if a critical vulnerability reappears on this server.

1. Upload the following file from the Nessus vulnerability scan.
    - Nessus Scan Results
2. Create a report that shows the count of critical vulnerabilities from the customer database server.
    - The database server IP is 10.11.36.23.
    - The field that identifies the level of vulnerabilities is severity.
3. Build an alert that monitors every day to see if this server has any critical vulnerabilities. If a vulnerability exists, have an alert emailed to soc@vandalay.com.

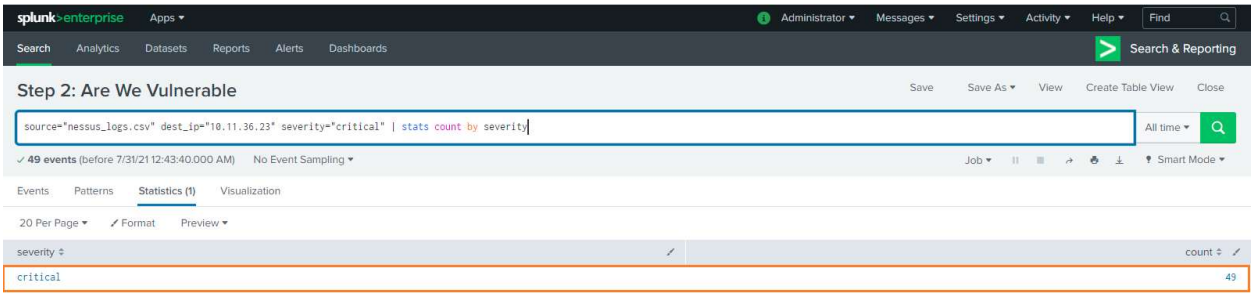
Submit a screenshot of your report and a screenshot of proof that the alert has been created.

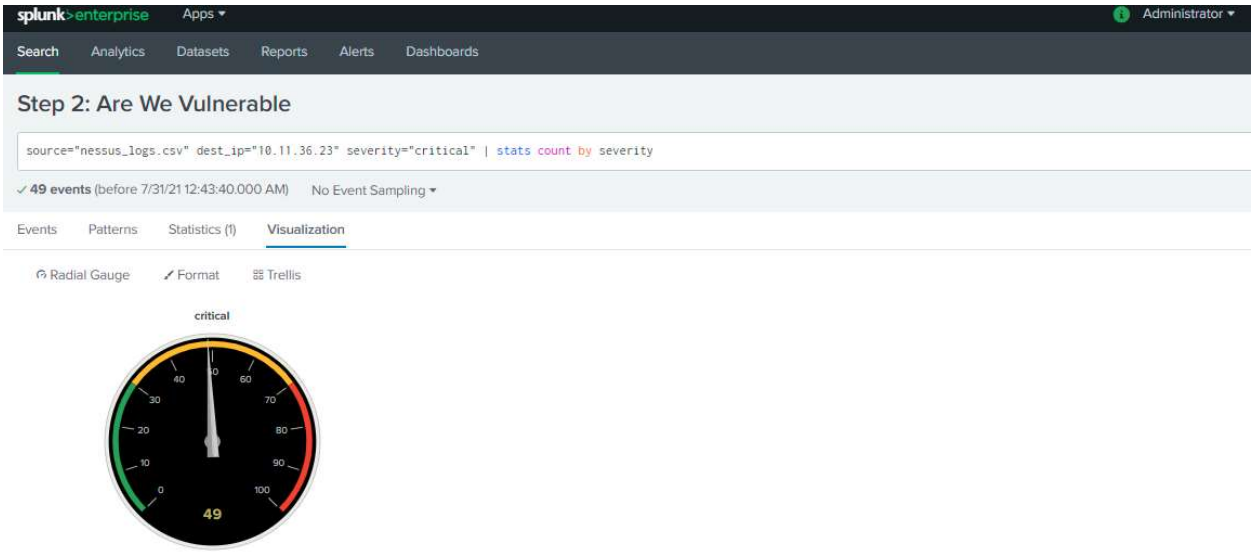
Answer:

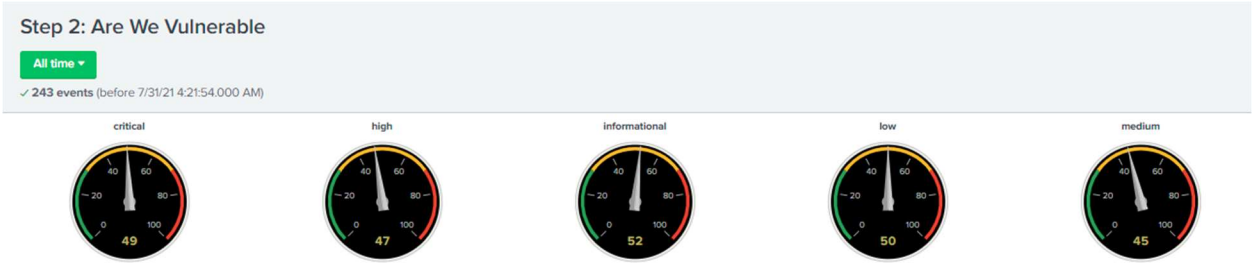
SPL:

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

Narrowing down and Identifying the Critical Logs using SPL

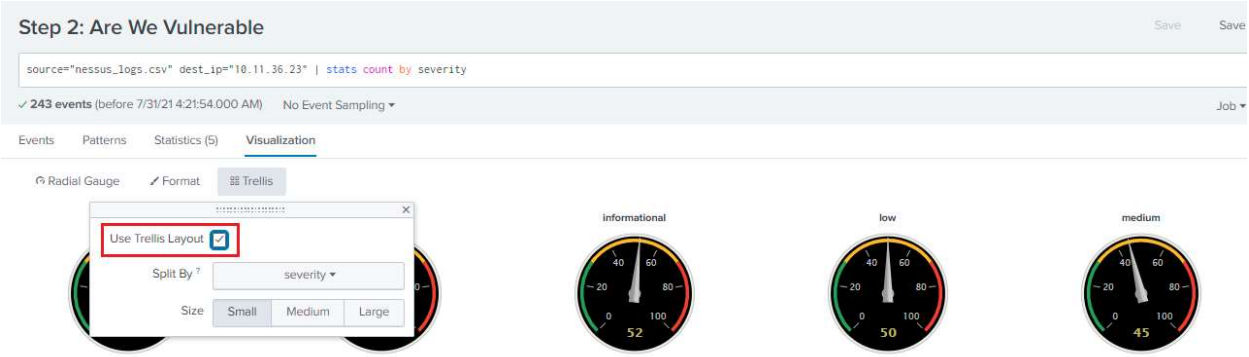




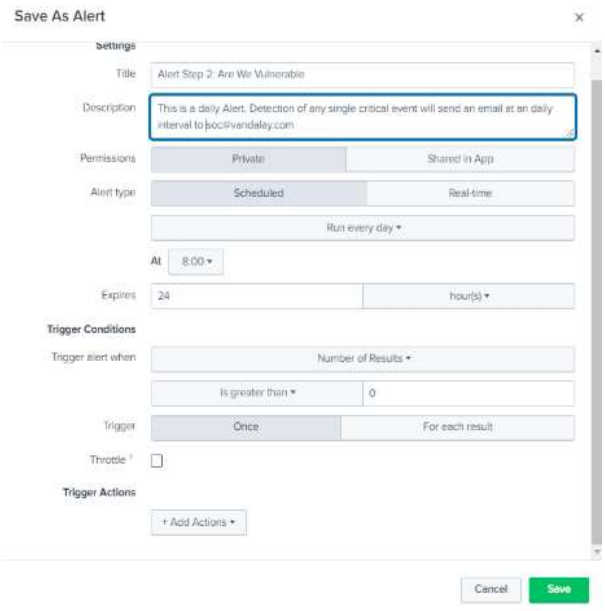


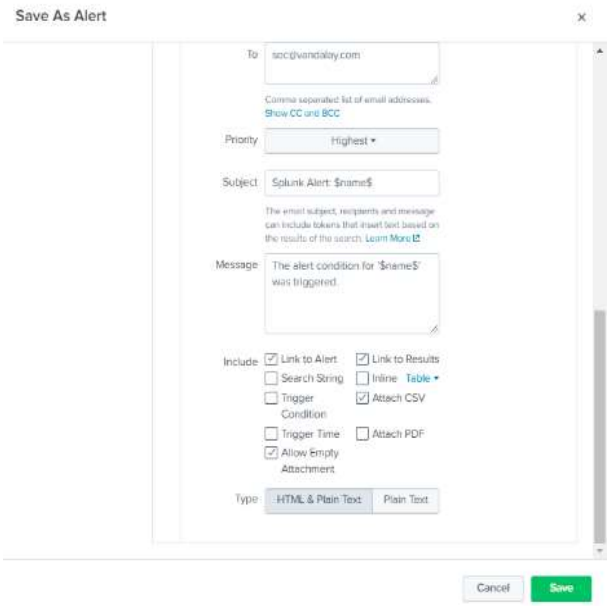
[SPL for to bring all severity: `source="nessus_logs.csv" dest_ip="10.11.36.23" | stats count by severity]`

Then



Generating Alert:





Step 3: Drawing the (base)line

Background: A Vandaly server is also experiencing brute force attacks into their administrator account. Management would like you to set up monitoring to notify the SOC team if a brute force attack occurs again.

Task: Analyze administrator logs that document a brute force attack. Then, create a baseline of the ordinary amount of administrator bad logins and determine a threshold to indicate if a brute force attack is occurring.

1. Upload the administrator login logs.
    - Admin Logins
2. When did the brute force attack occur?
    - Hints:
        - Look for the name field to find failed logins.
        - Note the attack lasted several hours.

    Answer:

    SPL

    ```
    source="Administrator_logs.csv" name="An account failed to log on" | bin _time span=60m | stats count by _time | sort - count
    ```

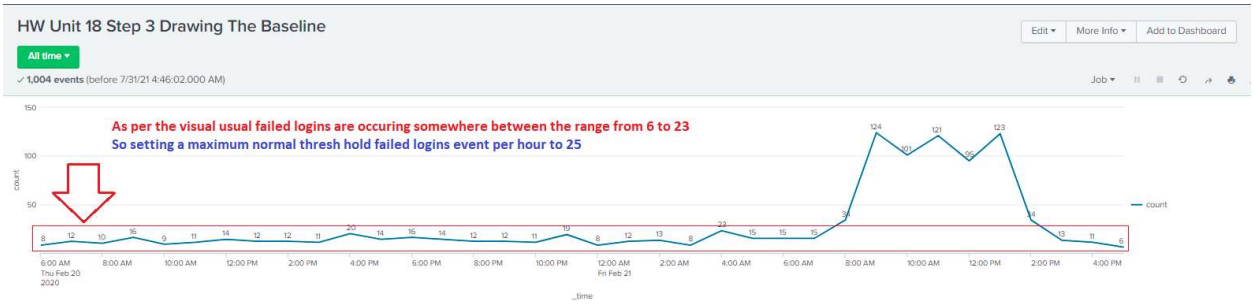
    The beginning of attack seemed to be started around on **Feb 21, 2020** at **8:00 AM** reached to the peak at around **9:00PM**

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

    Answer:

As per the generated visual from logs below,

Usual failed logins are occurring at an hourly rate between 6 to 23
So picking up a baseline normal **statistical thresh hold value of 25 failed logins per hour**



4. Design an alert to check the threshold every hour and email the SOC team at SOC@vandalay.com if triggered.