

Unit 18 Homework: Lets go Splunking!

Scenario

You have just been hired as an SOC Analyst by Vandalay Industries, an importing and exporting company.

- Vandalay Industries uses Splunk for their security monitoring and have been experiencing a variety of security issues against their online systems over the past few months.
- You are tasked with developing searches, custom reports and alerts to monitor Vandalay's security environment in order to protect them from future attacks.

System Requirements

You will be using the Splunk app located in the Ubuntu VM.

Your Objective

Utilize your Splunk skills to design a powerful monitoring solution to protect Vandalay from security attacks.

After you complete the assignment you are asked to provide the following:

- Screen shots where indicated.
- Custom report results where indicated.

Topics Covered in This Assignment

- Researching and adding new apps
- Installing new apps
- Uploading files
- Splunk searching
- Using fields
- Custom reports
- Custom alerts

Let's get started!

Vandalay Industries Monitoring Activity Instructions

Step 1: The Need for Speed

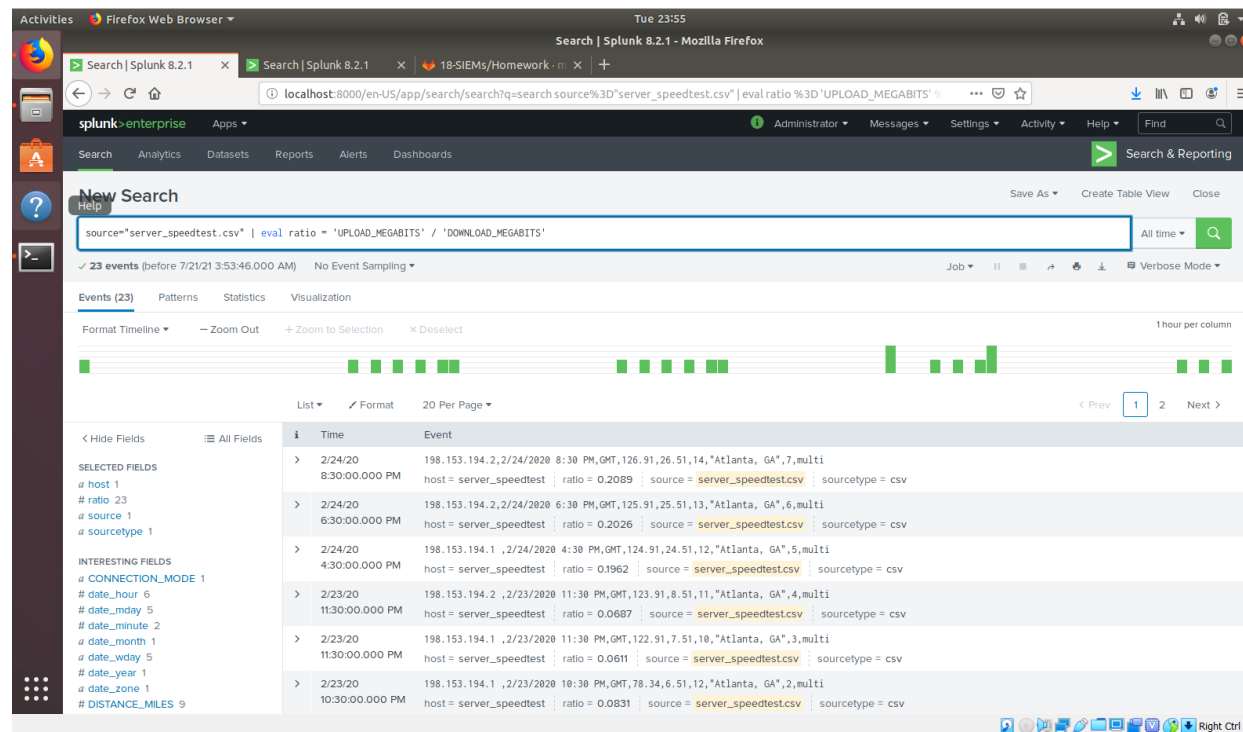
Background: As the worldwide leader of importing and exporting, Vandalay Industries has been the target of many adversaries attempting to disrupt their online business. Recently, Vandalay has been experiencing DDOS attacks against their web servers.

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'`

`| eval ratio = 'UPLOAD_MEGABITS' / 'DOWNLOAD_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 fieldB fieldC`

`| table _time IP_ADDRESS DOWNLOAD_MEGABITS
UPLOAD_MEGABITS ratio`

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-24 20:30:00	198.153.194.2	126.91	26.51	
2020-02-24 18:30:00	198.153.194.2	125.91	25.51	
2020-02-24 16:30:00	198.153.194.1	124.91	24.51	
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	
2020-02-22 23:30:00	198.153.194.2	109.16	9.51	
2020-02-22 22:30:00	198.153.194.2	109.91	8.51	
2020-02-22 20:30:00	198.153.194.2	108.91	7.51	
2020-02-22 18:30:00	198.153.194.2	107.91	13.51	
2020-02-22 16:30:00	198.153.194.2	106.91	12.51	

4. Answer the following questions:

- Based on the report created, what is the approximate date and time of the attack? **2020-02-23 14:30:00**
- How long did it take your systems to recover? **Full recovery took approximately 9 hours**

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

The screenshot shows the Splunk 8.2.1 interface. The search bar contains the query: `source="server_speedtest.csv" | eval ratio = 'UPLOAD_MEGABITS' / 'DOWNLOAD_MEGABITS' | table _time IP_ADDRESS DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio`. The results are displayed in a table with 5 columns: `_time`, `IP_ADDRESS`, `DOWNLOAD_MEGABITS`, `UPLOAD_MEGABITS`, and `ratio`. The table shows 23 events from 2020-02-21 to 2020-02-24.

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-24 20:30:00	198.153.194.2	126.91	26.51	0.2089
2020-02-24 18:30:00	198.153.194.2	125.91	25.51	0.2026
2020-02-24 16:30:00	198.153.194.1	124.91	24.51	0.1962
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
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	0.233
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	0.172
2020-02-22 23:30:00	198.153.194.2	109.16	9.51	0.0871
2020-02-22 22:30:00	198.153.194.2	109.91	8.51	0.0774
2020-02-22 20:30:00	198.153.194.2	108.91	7.51	0.0698
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

Step 2: Are We Vulnerable?

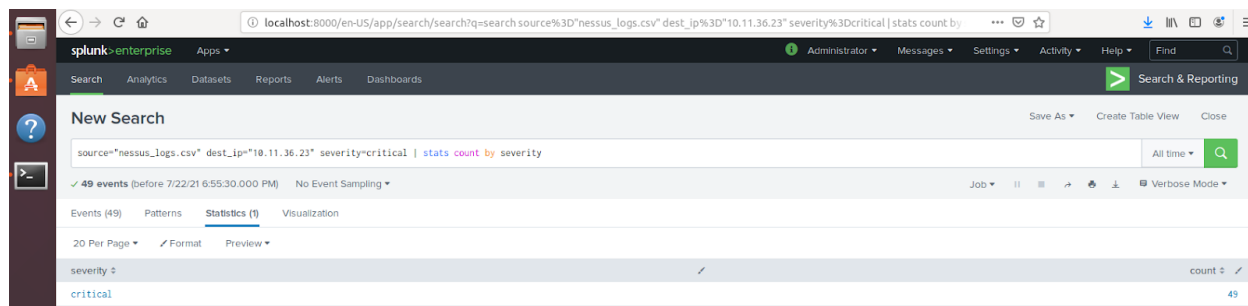
Background: Due to the frequency of attacks, your manager needs to be sure that sensitive customer data on their servers is not vulnerable. Since Vandalay uses Nessus vulnerability scanners, you have pulled the last 24 hours of scans to see if there are any critical vulnerabilities.

- 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.

- Upload the following file from the Nessus vulnerability scan.
 - Nessus Scan Results
- Create a report that shows the count of critical vulnerabilities from the customer database server.

- The database server IP is 10.11.36.23.



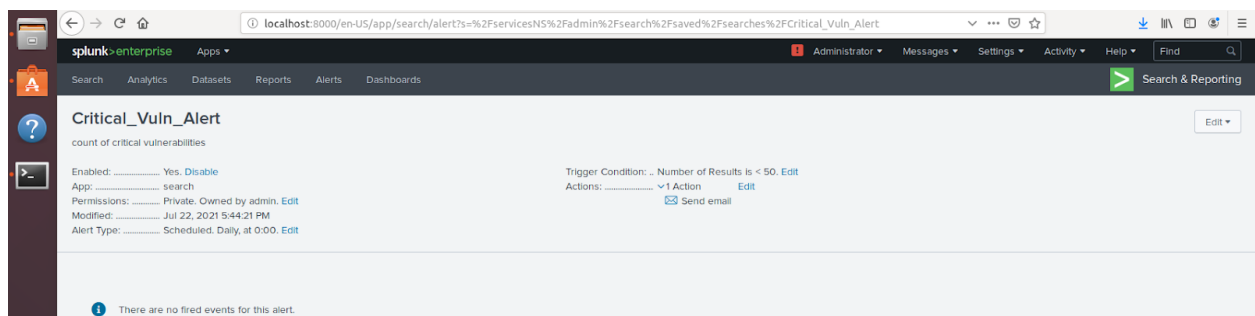
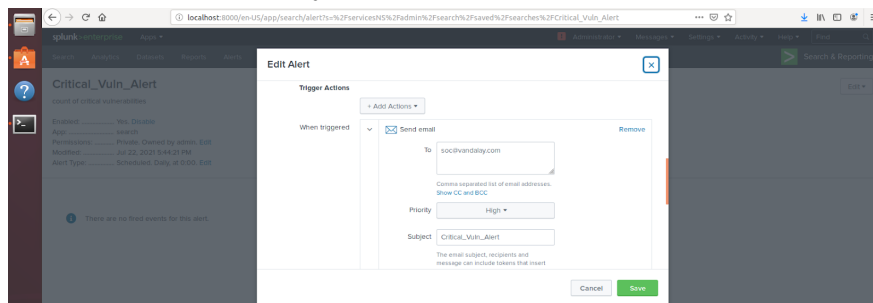
- The field that identifies the level of vulnerabilities is severity.

The screenshot shows the 'count of critical vulnerabilities' report. The table displays the following data:

severity	count	percent
informational	52	21.399177
low	58	28.576132
critical	49	28.164689
high	47	19.341564
medium	45	18.518519

- 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.



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?

Start Time 2020-02-21 09:51:10

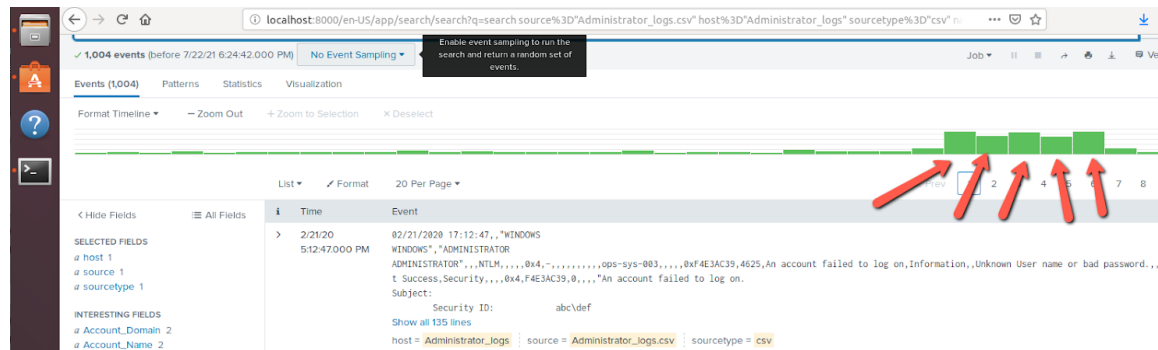
End Time 2020-02-21 17:12:47

- Hints:
 - Look for the name field to find failed logins.

The screenshot shows a Splunk search interface. The search bar contains the query: `search source="Administrator_logs.csv" host="Administrator_logs" sourcetype="csv"`. The results are displayed in a table with columns for Time and Event. A field summary for the 'name' field is shown, indicating 7 values and 89.524% of events. The summary table lists the following values and their counts:

Values	Count	%
An account failed to log on	1,084	29.97%
An account was logged off	417	12.448%
Special privileges assigned to new logon	414	12.358%
A logon was attempted using explicit credentials	399	11.91%
Key file operation	382	11.483%
Cryptographic operation	369	11.015%
An account was successfully logged on	365	10.896%

- Note the attack lasted several hours.



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

New Search

source=Administrator_logs.csv host=Administrator_logs sourcetype=csv | stats count by name | eval bruteForce= if (name = "An account failed to log on" And count > 20,"Potential BruteForce", "Not BruteForce")

3,742 events (before 7/22/21 6:11:28.000 PM) No Event Sampling

Events (3,742) Patterns Statistics (7) Visualization

20 Per Page Format Preview

name	count	bruteForce
A logon was attempted using explicit credentials	399	Not BruteForce
An account failed to log on	1004	Potential BruteForce
An account was logged off	417	Not BruteForce
An account was successfully logged on	365	Not BruteForce
Cryptographic operation	369	Not BruteForce
Key file operation	382	Not BruteForce
Special privileges assigned to new logon	414	Not BruteForce

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

Bruteforce_Alert

Brute force_Alert

Enabled: Yes, Disable

App: search

Permissions: Private, Owned by admin, Edit

Modified: Jul 22, 2021 6:18:14 PM

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

There are no fired events for this alert.

Submit the answers to the questions about the brute force timing, baseline and threshold. Additionally, provide a screenshot as proof that the alert has been created.

Your Submission

In a word document, provide the following:

- Answers to all questions where indicated.
- Screenshots where indicated.

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.