

## Cameron Wright

### Splunk Project Part 1

#### 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.

Using the eval command, create a field called ratio that shows the ratio between the upload and download speeds.

i	Time	Event
>	2/24/20 8:30:00.000 PM	198.153.194.2,2/24/2020 8:30 PM,GMT,126.91,26.51,14,"Atlanta, GA",7,multi DOWNLOAD_MEGABITS = 126.91   IP_ADDRESS = 198.153.194.2   Time = 8:30 PM   UPLOAD_MEGABITS = 26.51   ratio = 4.787   source = server_speedtest.csv
>	2/24/20 6:30:00.000 PM	198.153.194.2,2/24/2020 6:30 PM,GMT,125.91,25.51,13,"Atlanta, GA",6,multi DOWNLOAD_MEGABITS = 125.91   IP_ADDRESS = 198.153.194.2   Time = 6:30 PM   UPLOAD_MEGABITS = 25.51   ratio = 4.936   source = server_speedtest.csv
>	2/24/20 4:30:00.000 PM	198.153.194.1,2/24/2020 4:30 PM,GMT,124.91,24.51,12,"Atlanta, GA",5,multi DOWNLOAD_MEGABITS = 124.91   IP_ADDRESS = 198.153.194.1   Time = 4:30 PM   UPLOAD_MEGABITS = 24.51   ratio = 5.096   source = server_speedtest.csv
>	2/23/20 11:30:00.000 PM	198.153.194.2,2/23/2020 11:30 PM,GMT,123.91,8.51,11,"Atlanta, GA",4,multi DOWNLOAD_MEGABITS = 123.91   IP_ADDRESS = 198.153.194.2   Time = 11:30 PM   UPLOAD_MEGABITS = 8.51   ratio = 14.6   source = server_speedtest.csv

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

source="server_speedtest.csv"   eval ratio = 'DOWNLOAD_MEGABITS' / 'UPLOAD_MEGABITS'   search ratio="*"   table Date Time IP_ADDRESS DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio									
✓ 23 events (before 3/31/22 1:02:47:000 AM) No Event Sampling									
Events Patterns Statistics (23) Visualization									
20 Per Page Format Preview < Prev 1 2 Next >									
Date	Time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio				
2/21/2020	6:30 PM	198.153.194.2	107.91	7.51	14.4				
2/21/2020	4:30 PM	198.153.194.2	106.91	6.51	16.4				
2/21/2020	2:30 PM	198.153.194.1	105.91	5.51	19.2				
2/20/2020	2:21 PM	198.153.194.1	109.16	5.43	20.1				
2/22/2020	2:30 PM	198.153.194.1	105.91	11.51	9.202				
2/21/2020	11:30 PM	198.153.194.1	109.16	10.51	10.39				
2/21/2020	10:30 PM	198.153.194.1	109.91	9.51	11.6				

Answer the following questions:

Based on the report created, what is the approximate date and time of the attack?  
 How long did it take your systems to recover?

On the 2/23/2020 at 2:30pm The attack was causing the most significant impact, until around 8:30pm the same day the web servers were seeing half of their normal speeds regain. It was until 11:30pm that night that speeds were back around normal levels, The whole attack lasting for approximately 9 hours before the systems recovered.

2/22/2020	4:30 PM	198.153.194.2	106.91	12.51	8.546
2/22/2020	11:30 PM	198.153.194.2	109.16	9.51	11.5
2/23/2020	6:30 PM	198.153.194.2	17.56	3.43	5.12
2/23/2020	2:30 PM	198.153.194.1	7.87	1.83	4.30
2/23/2020	2:30 PM	198.153.194.2	12.76	2.19	5.83
2/23/2020	11:30 PM	198.153.194.2	123.91	8.51	14.6
2/23/2020	11:30 PM	198.153.194.1	122.91	7.51	16.4
2/23/2020	10:30 PM	198.153.194.1	78.34	6.51	12.0
2/23/2020	8:30 PM	198.153.194.2	65.34	4.23	15.4

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.
 table

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.

source="nessus\_logs.csv" host="nessus" sourcetype="nessus\_logs.csv" time=\* dest\_ip="10.11.36.23" dest\_port=\* os=\* signature=\* severity="critical" cve=\* | table time dest\_ip dest\_port os signature severity cve

19 events (before 3/31/22 1:46:25.000 AM) No Event Sampling

Events Patterns Statistics (19) Visualization

20 Per Page Format Preview

time	dest_ip	dest_port	os	signature	severity	cve
2020-02-28T14:55:45.000+0000	10.11.36.23	0	Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3	Nessus Scan Information	critical	CVE-2004-2761 CVE-2004-2761 CVE-2004-2761
2020-02-28T14:56:13.000+0000	10.11.36.23	139	Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3	Unknown Service Detection: Banner Retrieval	critical	CVE-2004-2761 CVE-2017-17427 CVE-2017-3145
2020-02-28T15:01:27.000+0000	10.11.36.23	2204	Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3	Nessus Scan Information	critical	CVE-2017-3144
2020-02-28T15:21:22.000+0000	10.11.36.23	1820	Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3	Terminal Services Encryption Level is not FIPS-140 Compliant	critical	CVE-2012-5081
2020-02-28T15:33:36.000+0000	10.11.36.23	139	Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3	Terminal Services Encryption Level is not FIPS-140 Compliant	critical	CVE-2015-8539
2020-02-28T15:39:01.000+0000	10.11.36.23	2204	Microsoft Windows XP Service Pack 2 Microsoft Windows XP Service Pack 3	Additional DNS Hostnames	critical	CVE-2004-2320

source="nessus\_logs.csv" host="nessus" sourcetype="nessus\_logs.csv" time=\* dest\_ip="10.11.36.23" dest\_port=\* os=\* signature=\* severity="critical" cve=\* | stats count by severity

19 events (before 3/31/22 1:48:32.000 AM) No Event Sampling

Events Patterns Statistics (1) Visualization

20 Per Page Format Preview

severity	count
critical	19

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.

**Nessus Critical Vulnerabilities**

Daily alert to show critical vulnerability warnings against the customer database

Enabled: ..... Yes. [Disable](#)

App: ..... search

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

Modified: ..... Mar 31, 2022 1:54:04 AM

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

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

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

[Send email](#)

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 Vandalay 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.

Upload the administrator login logs.

### Admin Logins

When did the brute force attack occur?  
09:00 21/2/2020 untill 13:00 21/2/2020

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

Normal activity would be in the range of 0 to 15 failed login attempts per hour from the logs supplied. At certain times there was a failed login amount seen to be closer to 30 per hour, where during the attack the number was on average 120 attempts per hour. Factoring in all of the information I believe that a baseline of 30 would be the most suitable for an hourly alert threshold to minimize the chances of the SOC team being overwhelmed with unnecessary alerts being triggered.

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

