



# 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 attack appears to have occurred/started at 2020-02-24 14:30:00  
Not only was the ratio high at this time, but the download and upload megabits are in excess of the average.  
While there is a high ratio on 2020-02-24 14:30:00, the downloaded and uploaded megabits are relatively low compared to the average during this time.

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

Approximately 5 hours. The high ratio and volume of downloaded and uploaded megabits continues through 2020-02-24 20:30:00. The report ends at this time, so it is difficult to say whether systems were impacted past this time.

Provide a screenshot of your report:

Search | Splunk 9.1.2

Search > Analytics > Datasets > Reports > Alerts > Dashboards

New Search

source='server\_speedtest.csv'  
| eval upload\_download\_ratio = 'UPLOAD\_MEGABITS' / 'DOWNLOAD\_MEGABITS'  
| table \_time IP\_ADDRESS DOWNLOAD\_MEGABITS UPLOAD\_MEGABITS upload\_download\_ratio

23 events (before 1/25/24 3:18:01.000 AM) No Event Sampling

Events Patterns Statistics (23) Visualization

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	upload_download_ratio
2020-02-23 14:39:00	198.153.194.1	7.87	1.83	0.233
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 18:30:00	198.153.194.2	17.56	3.43	0.195
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	0.172
2020-02-22 18:30:00	198.153.194.2	187.91	13.51	0.1252
2020-02-22 16:30:00	198.153.194.2	146.91	12.51	0.1178
2020-02-22 14:30:00	198.153.194.1	185.91	11.51	0.1667
2020-02-21 23:30:00	198.153.194.1	189.16	18.51	0.0928
2020-02-22 23:30:00	198.153.194.2	189.16	9.51	0.0871
2020-02-21 22:30:00	198.153.194.1	189.51	9.51	0.0865
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	0.0831
2020-02-21 20:30:00	198.153.194.1	188.91	8.51	0.0781

## Step 2: Are We Vulnerable?

Provide a screenshot of your report:

Search | Splunk 9.1.2

Search > Analytics > Datasets > Reports > Alerts > Dashboards

Critical Vulnerabilities from Customer Da...

source='nessus\_logs.csv' dest\_ip='10.11.36.23' severity='critical'  
| stats count as total

49 events (before 1/30/24 12:59:57.000 AM) No Event Sampling

Events Patterns Statistics (1) Visualization

total
49

Provide a screenshot showing that the alert has been created:

## Save As Alert



### Settings

Title Critical Vulnerability Detected from Customer Database Server

Description optional

Permissions Private

Shared in App

Alert type Scheduled

Real-time

Run every day ▼

At 0:00 ▼

Expires 24

hour(s) ▼

### Trigger Conditions

Trigger alert when Number of Results ▼

is greater than ▼

0

Trigger Once

For each result

Throttle ? ☐

Save As Alert

When triggered

Send email

To

soc@vandalay.com

Comma separated list of email addresses.  
[Show CC and BCC](#)

Priority

Normal

Subject

Critical Vulnerability Detected: Cus

The email subject, recipients and message can include tokens that insert text based on the results of the search. [Learn More](#)

Message

Critical Vulnerability detected from the customer database server

Include

☒ Link to Alert

☒ Link to Results

☐ Search String

☐ Inline [Table](#)

☐ Trigger Condition

☐ Attach CSV

☐ Trigger Time

☐ Attach PDF

Cancel

Save

### Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

February 21, 2020 9 AM - 2 PM (spike began in the 9-10 hour and continued through the 1-2 hour).

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

36 hours of data are in this file with 1,004 events, making the average 27.89 per hour. Outside the attack range, the events appear to range from 6

to 34, and during the attack, range from 95-124. Therefore, I would set the alert threshold at 40. This value should prevent many false positives without actual attack indicators slipping through the cracks.

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

The screenshot shows a 'Save As Alert' dialog box with the following configuration:

- Title:** Brute Force Attack Indicated
- Description:** Optional
- Permissions:** Private
- Alert type:** Scheduled
- Frequency:** Run every hour
- At:** 0 minutes past the hour
- Expires:** 30 day(s)
- Trigger Conditions:**
  - Trigger alert when:** Number of Results
  - Operator:** is greater than
  - Value:** 39
- Trigger:** Once
- Throttle:** (checkbox) [unchecked]

Save As Alert

+ Add Actions ▾

When triggered ▾

✉ Send email

Remove

To

soc@vandalay.com

Comma separated list of email addresses.  
[Show CC and BCC](#)

Priority

Normal ▾

Subject

Brute Force Attack Indicated

The email subject, recipients and message can include tokens that insert text based on the results of the search. [Learn More](#)

Message

Failed login attempts in the last hour have exceeded 39, indicating a possible brute force attack.

Include

☒ Link to Alert

☒ Link to Results

☐ Search String

☐ Inline [Table ▾](#)

☐ Trigger

☐ Attach CSV

Cancel

Save