



# 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?

02/23/2020 at 2:30pm

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

6hrs to recover  
9hrs from 2:30pm - 10:30pm

Provide a screenshot of your report:

**New Search** Save As Create Table View Close

source="server\_speedtest.csv" | cve() | rex | "DOWNLOADED" | "UPLOADED" | 1000 | size IP\_ADDRESS DOWNLOADED.MEGABITS UPLOADED.MEGABITS | rex

23 events (before 2/15/23 8:47:45.000 PM) Alt time Smart mode

Events Fields Statistics (23) Visualization

20 Per Page Format Preview

_time	IP_ADDRESS	DOWNLOADED.MEGABITS	UPLOADED.MEGABITS	Index
2020-02-20 14:21:00	100.102.104.1	100.10	5.43	28.1
2020-02-21 14:10:00	100.102.104.1	100.91	5.51	29.2
2020-02-21 16:10:00	100.102.104.2	100.91	6.51	
2020-02-21 18:10:00	100.102.104.2	100.91	7.51	
2020-02-21 20:10:00	100.102.104.1	100.91	8.51	12.8
2020-02-21 22:10:00	100.102.104.1	100.91	9.51	11.6
2020-02-21 23:10:00	100.102.104.1	100.10	10.51	10.39
2020-02-22 14:10:00	100.102.104.1	100.91	11.51	9.202
2020-02-22 16:10:00	100.102.104.2	100.91	12.51	6.546
2020-02-22 18:10:00	100.102.104.2	100.91	13.51	7.987
2020-02-22 20:10:00	100.102.104.2	100.91	14.51	
2020-02-22 22:10:00	100.102.104.2	100.91	15.51	12.9
2020-02-22 23:10:00	100.102.104.2	100.10	16.51	11.5
2020-02-23 14:10:00	100.102.104.1	7.87	1.82	4.38
2020-02-23 16:10:00	100.102.104.2	12.76	2.19	5.83
2020-02-23 18:10:00	100.102.104.2	17.50	3.43	5.12
2020-02-23 20:10:00	100.102.104.2	65.34	4.23	15.4
2020-02-23 22:10:00	100.102.104.1	79.34	6.51	12.8
2020-02-23 23:10:00	100.102.104.2	122.91	8.51	18.6
2020-02-23 23:10:00	100.102.104.1	122.91	7.51	18.4

## Step 2: Are We Vulnerable?

Provide a screenshot of your report:

**Critical Vulnerabilities** Edit More info Add to Dashboard

count of critical vulnerabilities in the customer database server

Alt time

40 events (before 2/15/23 9:07:06.000 PM) Alt time Smart mode

Fields 20 per page

Severity	Count
critical	40

Provide a screenshot showing that the alert has been created:

**Critical Vulnerability**

critical vulnerability detected in customer database

Enabled: Yes, Disabled

App: search

Permissions: Private, Owned by admin, Edit

Modified: Feb 13, 2023 9:12:43 PM

Alert Type: Scheduled, Daily, at 9:00, Edit

Trigger Condition: Number of Results is > 0, Edit

Action: T Action, Edit

Send email

There are no feed events for this alert.

## Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

02/21 4am - 2pm

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

The baseline is 25 or more log in attempts per hour is the baseline to determine brute force attacks.

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

