



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 2:30pm - 8:30pm

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

6 hours

Provide a screenshot of your report:

DOWNLOAD_MEGABITS ↕ ✓	UPLOAD_MEGABITS ↕ ✓	_time ↕	ratio ↕ ✓	IP_ADDRESS ↕ ✓
107.91	13.51	2020-02-22 18:30:00	7.987	198.153.194.2
106.91	12.51	2020-02-22 16:30:00	8.546	198.153.194.2
105.91	11.51	2020-02-22 14:30:00	9.202	198.153.194.1
109.16	10.51	2020-02-21 23:30:00	10.39	198.153.194.1
109.91	9.51	2020-02-21 22:30:00	11.6	198.153.194.1
108.91	8.51	2020-02-21 20:30:00	12.8	198.153.194.1
107.91	7.51	2020-02-21 18:30:00	14.4	198.153.194.2
106.91	6.51	2020-02-21 16:30:00	16.4	198.153.194.2
105.91	5.51	2020-02-21 14:30:00	19.2	198.153.194.1
109.16	5.43	2020-02-20 14:21:00	20.1	198.153.194.1
123.91	8.51	2020-02-23 23:30:00	14.6	198.153.194.2
122.91	7.51	2020-02-23 23:30:00	16.4	198.153.194.1
78.34	6.51	2020-02-23 22:30:00	12.0	198.153.194.1
65.34	4.23	2020-02-23 20:30:00	15.4	198.153.194.2
17.56	3.43	2020-02-23 18:30:00	5.12	198.153.194.2
7.87	1.83	2020-02-23 14:30:00	4.30	198.153.194.1
12.76	2.19	2020-02-23 14:30:00	5.83	198.153.194.2
109.16	9.51	2020-02-22 23:30:00	11.5	198.153.194.2
109.91	8.51	2020-02-22 22:30:00	12.9	198.153.194.2
108.91	7.51	2020-02-22 20:30:00	14.5	198.153.194.2

Step 2: Are We Vulnerable?

Provide a screenshot of your report:

severity ↕ ✓	count(severity) ↕ ✓
critical	368
high	358
informational	349
low	380
medium	394

Provide a screenshot showing that the alert has been created:

Save As Alert

!

Enable at least one action.

Settings

Title

Nessus Vuln

Description

Optional

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Run every hour ▾

At

0 ▾

 minutes past the hour

Expires

24

hour(s) ▾

Trigger Conditions

Trigger alert when

Number of Results ▾

is greater than ▾

0

Trigger

Once

For each result

Throttle ?

☐

Trigger Actions

+ Add Actions ▾

When triggered

>

✉ Send email

Remove

Cancel

Save

Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

Feb 21 2020 2am

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

15> baseline, 23 threshold ($x \times 2 - \frac{1}{2}$)

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

The screenshot shows a 'Save As Alert' configuration window with the following settings:

- Settings**
 - Title: FailedAdminLogon
 - Description: Optional
 - Permissions: Private (selected), Shared in App
 - Alert type: Scheduled (selected), Real-time
 - Run every hour ▼
 - At: 0 ▼ minutes past the hour
 - Expires: 24 hour(s) ▼
- Trigger Conditions**
 - Trigger alert when: Number of Results ▼
 - is greater than ▼ 23
 - Trigger: Once (selected), For each result
 - Throttle ? ☐
- Trigger Actions**
 - + Add Actions ▼
 - When triggered: > Send email Remove

Buttons: Cancel, Save

