



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 approximate date and time of attack was 02/23/2020 at 2:30pm until about 02/23/2020 at 8:30pm.

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

It took the systems about 6 hours to recover.

Provide a screenshot of your report:

Linux-Module_default_1678841110859_23677 Clone 1 (Snapshot 1) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Firefox Web Browser

Table | Splunk 9.1.0.1 - Mozilla Firefox

localhost:8000/en-US/app/search/table?bs=source%3D%27server_speedtest.csv%27 | eval ratio%3D(UPLOAD_MEGABITS)%2F(DOWNLOAD_MEGABITS)&dataset...

Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

Create Table View

source="server_speedtest.csv" | eval ratio=(UPLOAD_MEGABITS)/(DOWNLOAD_MEGABITS)

Previewing 23 events (1/28/20 100:48:00 PM to 8/1/23 8:44:52:000 PM) Sample: Latest

Select existing fields

Filter existing fields

ip Add X

☐ all fields
☒ _time
☒ _raw
☒ CONNECTION_MODE
data_hour
data_mday
data_minute
data_month
data_wday
data_year
data_zone
DISTANCE_MILES
☒ DOWNLOAD_MEGABITS
host
index
☒ IP_ADDRESS
LATENCY_MS
linecount
punct
☒ ratio
SERVER_NAME
☒ _source

Done

#	_time	DOWNLOAD_MEGA...	IP	IP_ADDRESS	# ratio	# source	UPLOAD_MEGABITS	> _raw
1	2020-02-24T20:30:00.000Z	126.91		198.153.194.2	0.2089	server_speedtest.csv	26.51	198.153.19
2	2020-02-24T18:30:00.000Z	125.91		198.153.194.2	0.2026	server_speedtest.csv	25.51	198.153.19
3	2020-02-24T16:30:00.000Z	124.91		198.153.194.1	0.1962	server_speedtest.csv	24.51	198.153.19
4	2020-02-23T23:30:00.000Z	123.91		198.153.194.2	0.0687	server_speedtest.csv	8.51	198.153.19
5	2020-02-23T23:30:00.000Z	122.91		198.153.194.1	0.0611	server_speedtest.csv	7.51	198.153.19
6	2020-02-23T22:30:00.000Z	78.34		198.153.194.1	0.0831	server_speedtest.csv	6.51	198.153.19
7	2020-02-23T20:30:00.000Z	65.34		198.153.194.2	0.0647	server_speedtest.csv	4.23	198.153.19
8	2020-02-23T18:30:00.000Z	17.56		198.153.194.2	0.195	server_speedtest.csv	3.43	198.153.19
9	2020-02-23T14:30:00.000Z	7.87		198.153.194.1	0.233	server_speedtest.csv	1.83	198.153.19
10	2020-02-23T14:30:00.000Z	12.76		198.153.194.2	0.172	server_speedtest.csv	2.19	198.153.19
11	2020-02-23T23:30:00.000Z	189.16		198.153.194.2	0.0871	server_speedtest.csv	9.51	198.153.19
12	2020-02-23T22:30:00.000Z	189.91		198.153.194.2	0.0774	server_speedtest.csv	8.51	198.153.19
13	2020-02-22T20:30:00.000Z	188.91		198.153.194.2	0.0698	server_speedtest.csv	7.51	198.153.19
14	2020-02-22T18:30:00.000Z	187.91		198.153.194.2	0.1252	server_speedtest.csv	13.51	198.153.19
15	2020-02-22T16:30:00.000Z	186.91		198.153.194.2	0.1178	server_speedtest.csv	12.51	198.153.19
16	2020-02-22T14:30:00.000Z	185.91		198.153.194.1	0.1087	server_speedtest.csv	11.51	198.153.19
17	2020-02-21T23:30:00.000Z	189.16		198.153.194.1	0.09628	server_speedtest.csv	10.51	198.153.19
18	2020-02-21T22:30:00.000Z	189.91		198.153.194.1	0.0885	server_speedtest.csv	9.51	198.153.19
19	2020-02-21T20:30:00.000Z	188.91		198.153.194.1	0.0781	server_speedtest.csv	8.51	198.153.19

Linux-Module_default_1678841110859_23677 Clone 1 (Snapshot 1) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Activities Firefox Web Browser

Table | Splunk 9.1.0.1 - Mozilla Firefox

localhost:8000/en-US/app/search/table?bs=source%3D%27server_speedtest.csv%27 | eval ratio%3D(UPLOAD_MEGABITS)%2F(DOWNLOAD_MEGABITS)&dataset...

Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

Create Table View

source="server_speedtest.csv" | eval ratio=(UPLOAD_MEGABITS)/(DOWNLOAD_MEGABITS)

Previewing 23 events (1/28/20 100:48:00 PM to 8/1/23 8:44:52:000 PM) Sample: Latest

Select existing fields

Filter existing fields

ip Add X

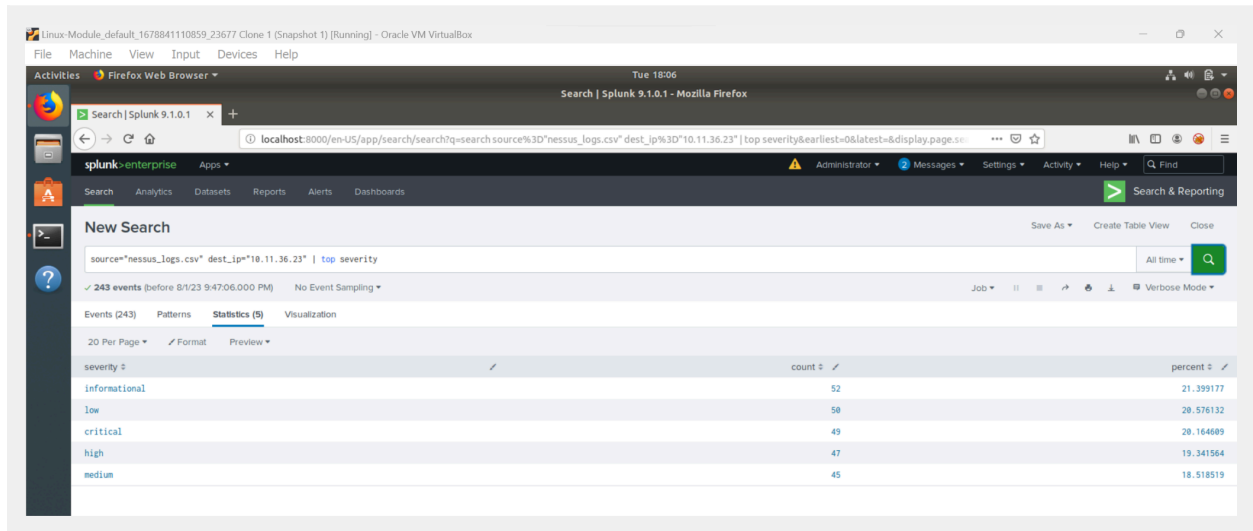
☐ all fields
☒ _time
☒ _raw
☒ CONNECTION_MODE
data_hour
data_mday
data_minute
data_month
data_wday
data_year
data_zone
DISTANCE_MILES
☒ DOWNLOAD_MEGABITS
host
index
☒ IP_ADDRESS
LATENCY_MS
linecount
punct
☒ ratio
SERVER_NAME
☒ _source

Done

#	_time	DOWNLOAD_MEGA...	IP	IP_ADDRESS	# ratio	# source	UPLOAD_MEGABITS	> _raw
6	2020-02-23T22:30:00.000Z	78.34		198.153.194.1	0.0831	server_speedtest.csv	6.51	198.153.19
7	2020-02-23T20:30:00.000Z	65.34		198.153.194.2	0.0647	server_speedtest.csv	4.23	198.153.19
8	2020-02-23T18:30:00.000Z	17.56		198.153.194.2	0.195	server_speedtest.csv	3.43	198.153.19
9	2020-02-23T14:30:00.000Z	7.87		198.153.194.1	0.233	server_speedtest.csv	1.83	198.153.19
10	2020-02-23T14:30:00.000Z	12.76		198.153.194.2	0.172	server_speedtest.csv	2.19	198.153.19
11	2020-02-23T23:30:00.000Z	189.16		198.153.194.2	0.0871	server_speedtest.csv	9.51	198.153.19
12	2020-02-23T22:30:00.000Z	189.91		198.153.194.2	0.0774	server_speedtest.csv	8.51	198.153.19
13	2020-02-22T20:30:00.000Z	188.91		198.153.194.2	0.0698	server_speedtest.csv	7.51	198.153.19
14	2020-02-22T18:30:00.000Z	187.91		198.153.194.2	0.1252	server_speedtest.csv	13.51	198.153.19
15	2020-02-22T16:30:00.000Z	186.91		198.153.194.2	0.1178	server_speedtest.csv	12.51	198.153.19
16	2020-02-22T14:30:00.000Z	185.91		198.153.194.1	0.1087	server_speedtest.csv	11.51	198.153.19
17	2020-02-21T23:30:00.000Z	189.16		198.153.194.1	0.09628	server_speedtest.csv	10.51	198.153.19
18	2020-02-21T22:30:00.000Z	189.91		198.153.194.1	0.0885	server_speedtest.csv	9.51	198.153.19
19	2020-02-21T20:30:00.000Z	188.91		198.153.194.1	0.0781	server_speedtest.csv	8.51	198.153.19
20	2020-02-21T18:30:00.000Z	187.91		198.153.194.2	0.0698	server_speedtest.csv	7.51	198.153.19
21	2020-02-21T16:30:00.000Z	186.91		198.153.194.1	0.0609	server_speedtest.csv	6.51	198.153.19
22	2020-02-21T14:30:00.000Z	185.91		198.153.194.1	0.0528	server_speedtest.csv	5.51	198.153.19
23	2020-02-20T14:21:00.000Z	189.16		198.153.194.1	0.0497	server_speedtest.csv	5.43	198.153.19

Step 2: Are We Vulnerable?

Provide a screenshot of your report:



The screenshot shows the Splunk Enterprise web interface. The search bar contains the query: `source="nessus_logs.csv" dest_ip="10.11.36.23" | top severity`. The results show 243 events. The 'Statistics' tab is selected, displaying a table with the following data:

severity	count	percent
informational	52	21.399177
low	50	20.576132
critical	49	20.164089
high	47	19.341564
medium	45	18.518519

Provide a screenshot showing that the alert has been created:

Save As Alert



Settings

Title

Description

Permissions ☒ Private ☐ Shared in App

Alert type ☒ Scheduled ☐ Real-time

Run every hour ▼

At minutes past the hour

Expires hour(s) ▼

Trigger Conditions

Trigger alert when

Trigger ☒ Once ☐ For each result

Throttle ? ☐

Trigger Actions

When triggered

[Remove](#)

Save As Alert

Trigger Actions

+ Add Actions ▾

When triggered ▾

✉ Send email

Remove

To

soc@vandalay.com

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

Priority

Normal ▾

Subject

Splunk Alert: Nessus Vulnerability

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

Message

The alert condition for 'Nessus Vulnerability' was triggered.

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?

The brute force attack occurred on Feb 20, 2020 at 5 pm

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

A baseline for normal activity would be 15 and 18 would be the threshold for an alert.

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
- Description:** Optional
- Permissions:** Private
- Alert type:** Scheduled
- Run every day** (dropdown)
- At:** 12:00 (dropdown)
- Expires:** 24 hour(s) (dropdown)
- Trigger Conditions:**
 - Trigger alert when:** Number of Results (dropdown)
 - is greater than** (dropdown) 18
 - Trigger:** Once
- Throttle ?** ☐
- Trigger Actions:**
 - + Add Actions** (dropdown)
 - When triggered** (dropdown) Send email [Remove](#)

Buttons: [Cancel](#) [Save](#)

Save As Alert

Throttle ?☐

Trigger Actions

+ Add Actions ▾

When triggered

✉ Send email

Remove

To

SOC@vandalay.com

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

Priority

Normal ▾

Subject

Splunk Alert: \$name\$

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

Message

The alert condition for Brute force attacks was triggered after 18 events occurred

Include

☒ Link to Alert

☒ Link to Results

☐ Search String

☐ Inline

Table ▾

☐ Trigger

☐ Attach CSV

Cancel

Save

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.