



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?

2/23/20
2:30:00.000 PM - 6:30:00.000 PM

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

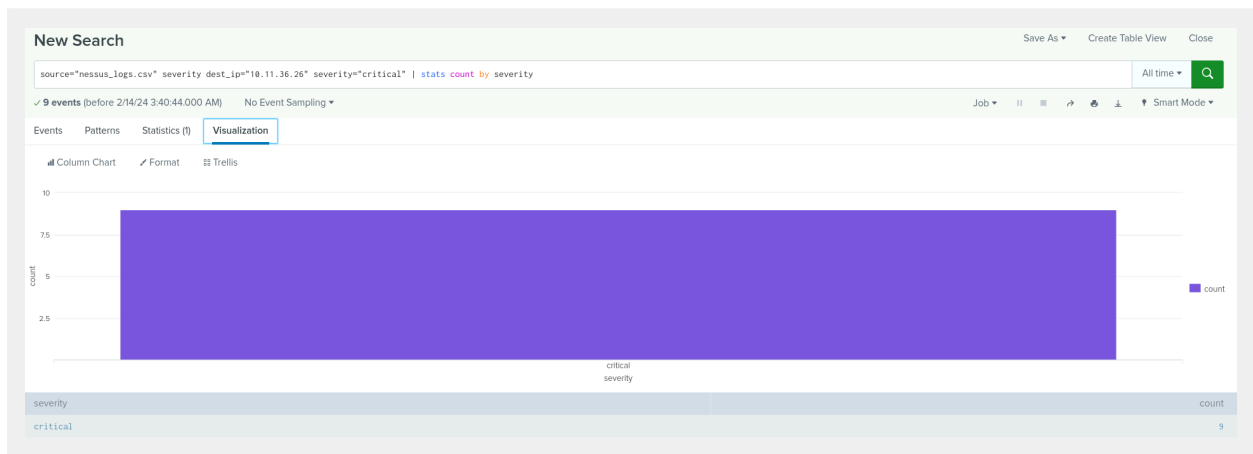
The systems did not fully recover until ~8:30pm on 2/23/20

Provide a screenshot of your report:

_time ▾	IP_ADDRESS ▾	DOWNLOAD_MEGABITS ▾	UPLOAD_MEGABITS ▾	ratio ▾
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 23:30:00	198.153.194.2	123.91	8.51	0.0687
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	0.0611
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	0.0831
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	0.0647
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	0.195
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	0.233
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	0.172
2020-02-22 23:30:00	198.153.194.2	109.16	9.51	0.0871

Step 2: Are We Vulnerable?

Provide a screenshot of your report:



Provide a screenshot showing that the alert has been created:

Alert has been saved

This scheduled search will not run after the Splunk Enterprise Trial License expires.

You can view your alert, change additional settings, or continue editing it.

Additional Settings:

- [Permissions](#)

[Continue Editing](#) [View Alert](#)

Critical Vulnerability

Enabled: Yes. [Disable](#)

App: search

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

Modified: Feb 14, 2024 4:00:43 AM

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

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

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

[Send email](#)

Step 3: Drawing the (Base)line

1. When did the brute force attack occur?


2/21/20
~8:00AM - 2:00PM

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

50+ “An account failed to log on” events in an hour

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

Alert has been saved

 This scheduled search will not run after the Splunk Enterprise Trial License expires.

You can view your alert, change additional settings, or continue editing it.

Additional Settings:

- [Permissions](#)

Continue Editing

View Alert

Admin Brute Force Attack

Enabled: Yes. [Disable](#)

App: search

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

Modified: Feb 14, 2024 3:59:32 AM

Alert Type: Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)

Trigger Condition: .. Number of Results is > 49. [Edit](#)

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

[✉ Send email](#)