



# 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?

DDOS attack occurred approx 830pm on 23.02.2020. This is where the download and upload speeds significantly drop compared to the average speeds.

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

The speeds get back to normal indicating that the attack ends approx 730am 24.02.2020, making the attack last for about 11 hours.

Provide a screenshot of your report:

source="server\_speedtest.csv" | eval ratio=(DOWNLOAD\_MEGABITS/'UPLOAD\_MEGABITS') | table \_time, IP\_ADDRESS, DOWNLOAD\_MEGABITS, UPLOAD\_MEGABITS, ratio

23 events (before 7/7/24 5:08:38.000 PM) No Event Sampling

Events (23) Patterns Statistics (23) Visualization

20 Per Page Format Preview

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-25 04:30:00	198.153.194.2	126.91	26.51	4.787
2020-02-25 02:30:00	198.153.194.2	125.91	25.51	4.936
2020-02-25 00:30:00	198.153.194.1	124.91	24.51	5.096
2020-02-24 07:30:00	198.153.194.2	123.91	8.51	14.6
2020-02-24 07:30:00	198.153.194.1	122.91	7.51	16.4
2020-02-24 04:30:00	198.153.194.1	78.34	6.51	12.0
2020-02-24 04:30:00	198.153.194.2	65.34	4.23	15.4
2020-02-24 02:30:00	198.153.194.2	17.55	3.43	5.12
2020-02-23 22:30:00	198.153.194.1	7.87	1.83	4.30
2020-02-23 22:30:00	198.153.194.2	12.76	2.19	5.83
2020-02-23 07:30:00	198.153.194.2	109.16	9.51	11.5
2020-02-23 06:30:00	198.153.194.2	109.91	8.51	12.9
2020-02-23 04:30:00	198.153.194.2	108.91	7.51	14.5
2020-02-23 02:30:00	198.153.194.2	107.91	13.51	7.987
2020-02-23 00:30:00	198.153.194.2	106.91	12.51	8.546
2020-02-22 22:30:00	198.153.194.1	105.91	11.51	9.202
2020-02-22 07:30:00	198.153.194.1	109.16	10.51	10.35
2020-02-22 06:30:00	198.153.194.1	109.91	9.51	11.6
2020-02-22 04:30:00	198.153.194.1	108.91	8.51	12.8
2020-02-22 02:30:00	198.153.194.2	107.91	7.51	14.4

## Step 2: Are We Vulnerable?

Provide a screenshot of your report:

Using the below command, we can see that there are 49 counts of critical vulnerabilities for the provided IP address.

```
source="nessus_logs.csv" dest_ip="10.11.36.23" severity="critical" | stats count
```

New Search

source="nessus\_logs.csv" dest\_ip="10.11.36.23" severity="critical" | stats count

✓ 49 events (before 7/17/24 5:42:00.000 PM) No Event Sampling

Events (49) Patterns Statistics (1) Visualization

50 Per Page Format Preview

count
49

Provide a screenshot showing that the alert has been created:

Create the alert by clicking 'save as' and then 'alert' after we've generated our results from the query above:

The screenshot displays a configuration window for an alert, organized into three main sections: Settings, Trigger Conditions, and Trigger Actions.

**Settings**

- Title:** Critical Vulnerabilities Alert for DB Server
- Description:** Generate report to be emailed to soc@vandalay.com when critical vulnerabilities are detected by Nessus scan on DB server IP 10.11.36.23
- Permissions:** Private (selected) and Shared in App
- Alert type:** Scheduled (selected) and Real-time
- Frequency:** Run every day ▼
- At:** 0:00 ▼
- Expires:** 24 (selected) and hour(s) ▼

**Trigger Conditions**

- Trigger alert when:** Number of Results ▼
- Comparison:** is greater than ▼
- Value:** 0
- Trigger:** Once (selected) and For each result
- Throttle ?** ☐

**Trigger Actions**

The Trigger Actions section is currently empty.

When triggered

Send email

To

soc@vandalay.com

Comma separated list of email addresses.  
Email addresses represented by tokens are  
validated only at the time of the search.  
[Show CC and BCC](#)

Priority

Highest

Subject

Splunk Alert: Critical Vulnerabilities

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 Critical  
Vulnerabilities was triggered.

Include

☒ Link to Alert

☒ Link to Results

☐ Search String

☐ Inline [Table](#)

☐ Trigger Condition

☐ Attach CSV

☐ Trigger Time

☐ Attach PDF

☒ Allow Empty Attachment

Then once saved, we can see the alert.

Critical Vulnerabilities Alert for DB Server

Generate report to be emailed to soc@vandalay.com when critical vulnerabilities are detected by Nessus scan on DB server IP 10.11.36.23

Enabled: ..... Yes. [Disable](#)

App: ..... search

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

Modified: ..... Jul 17, 2024 5:59:22 PM

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

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

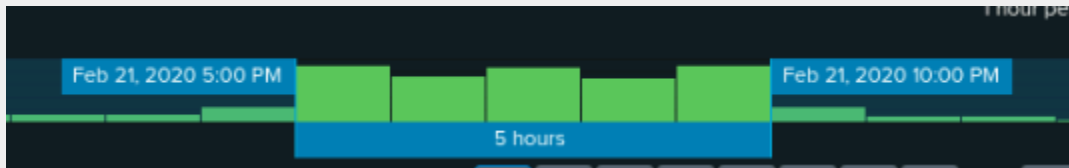
Actions: ..... 1 Action [Edit](#)

[Send email](#)

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

#### 1. When did the brute force attack occur?

The brute force attack occurred at approx 5pm on 21.02.2020 and lasted for approx 5 hours, finishing around 10pm.

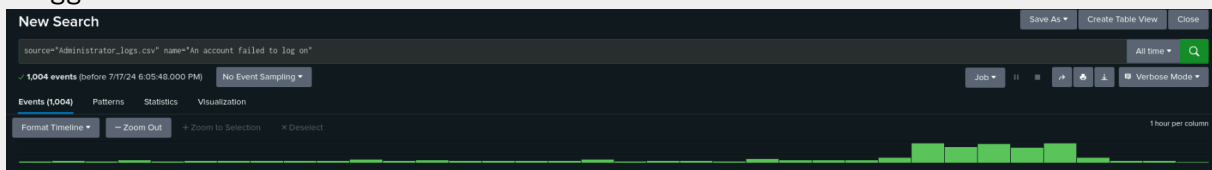


#### 2. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring:

Considering that the range of events is 6 to 34 pre and post attack, we can assume a normal baseline of 30 events. I would set a scale for alert as

0 - 25 = green alert  
25 - 50 = amber alert  
50+ = red alert

The threshold I will be setting in the alert will be 30 events, which will trigger an email to be sent to the soc team.



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

Same as above, used the Save As > Alert tabs to create the alert. Set to run every hour triggered when 30 events occur, sending a highest priority email to the soc team for further investigation.

Title	Brute Force Alert	
Description	Generate an alert for a potential brute force attack once threshold of 30 events has occurred.	
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 ▾	30
Trigger	Once	For each result
Throttle ?	<input type="checkbox"/>	
Trigger Actions		
	+ Add Actions ▾	

## Brute Force Alert

Generate an alert for a potential brute force attack once threshold of 30 events has occurred.

Enabled: ..... Yes. [Disable](#)

App: ..... search

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

Modified: ..... Jul 17, 2024 6:30:51 PM

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

Trigger Condition: .. Number of Results is > 30. [Edit](#)

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

[✉ Send email](#)