



# 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?

Command: `source="server_speedtest.csv" host="server-speed-test" | eval ratio = 'UPLOAD_MEGABITS' / 'DOWNLOAD_MEGABITS' | table _time IP_ADDRESS DOWNLOAD_MEGABITS UPLOAD_MEGABITS ratio`

Based on the report the time of the attack was after 2020-02-22 at approximately 23:30:00

2020-02-22 20:30:00	198.153.194.2	188.91	7.51	0.0000
2020-02-22 21:30:00	198.153.194.2	188.91	8.51	0.0716
2020-02-22 21:30:00	198.153.194.2	188.16	9.51	0.0871
2020-02-22 23:30:00.000 to 2020-02-22 23:30:00.001	198.153.194.1	7.87	1.83	0.233
View events	198.153.194.2	12.76	2.19	0.172
Narrow to this time range	198.153.194.2	17.56	3.43	0.195
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	0.0647

Fig 1. The Download megabits value dips

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

About 15 hrs for the system to recover.

2020-02-22 21:30:00	198.153.194.2	188.91	8.51	0.0716
2020-02-22 21:30:00	198.153.194.2	188.16	9.51	0.0871
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
2020-02-23 16:30:00	198.153.194.2	17.56	3.43	0.195

Fig 2. From 23:30:00 to 14:30:00

Provide a screenshot of your report:

New Search

source="server\_speedtest.csv" host="server-speed-test" | eval ratio = "UPLOAD\_MEGABITS" / "DOWNLOAD\_MEGABITS" | table \_time IP\_ADDRESS DOWNLOAD\_MEGABITS UPLOAD\_MEGABITS ratio

23 events (before 2/23 7:56:21.000 PM) No Event Sampling

Events Patterns Statistics (23) Visualization

50 Per Page Format Preview

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-20 14:21:00	198.153.194.1	189.16	5.43	0.0497
2020-02-21 14:38:00	198.153.194.1	185.91	5.51	0.0528
2020-02-21 16:38:00	198.153.194.2	186.91	6.51	0.0669
2020-02-21 18:38:00	198.153.194.2	187.91	7.51	0.0696
2020-02-21 20:38:00	198.153.194.1	188.91	8.51	0.0781
2020-02-21 22:38:00	198.153.194.1	189.91	9.51	0.0885
2020-02-21 23:38:00	198.153.194.1	189.16	18.51	0.09628
2020-02-22 14:38:00	198.153.194.1	185.91	11.51	0.1887
2020-02-22 16:38:00	198.153.194.2	186.91	12.51	0.1178
2020-02-22 18:38:00	198.153.194.2	187.91	13.51	0.1252
2020-02-22 20:38:00	198.153.194.2	188.91	7.51	0.0696
2020-02-22 22:38:00	198.153.194.2	189.91	8.51	0.0774
2020-02-23 00:38:00	198.153.194.2	189.16	9.51	0.0871
2020-02-23 14:38:00	198.153.194.1	7.87	1.83	0.233
2020-02-23 14:38:00	198.153.194.2	12.76	2.19	0.172
2020-02-23 18:38:00	198.153.194.2	17.56	3.43	0.195
2020-02-23 20:38:00	198.153.194.2	65.34	4.23	0.0647
2020-02-23 22:38:00	198.153.194.1	78.34	6.51	0.0831
2020-02-23 23:38:00	198.153.194.2	123.91	8.51	0.0687
2020-02-23 23:38:00	198.153.194.1	122.91	7.51	0.0611
2020-02-24 16:38:00	198.153.194.1	124.91	24.51	0.1962
2020-02-24 18:38:00	198.153.194.2	125.91	25.51	0.2026
2020-02-24 20:38:00	198.153.194.2	126.91	26.51	0.2089

Fig 3.

## Step 2: Are We Vulnerable?

Provide a screenshot of your report:

Command: **source="nessus\_logs.csv" dest\_ip="10.11.36.23" | stats count by severity**

New Search

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

243 events (before 2/23 8:35:41.000 PM) No Event Sampling

Events Patterns Statistics (5) Visualization

50 Per Page Format Preview

severity	count
critical	49
high	47
informational	52
low	58
medium	45

Fig 4. General Severity Sort

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

New Search

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

49 events (before 2/23 8:49:53.000 PM) No Event Sampling

Events Patterns Statistics (9) Visualization

50 Per Page Format Preview

severity	count
critical	49

Fig 6. Filter Severity by Critical

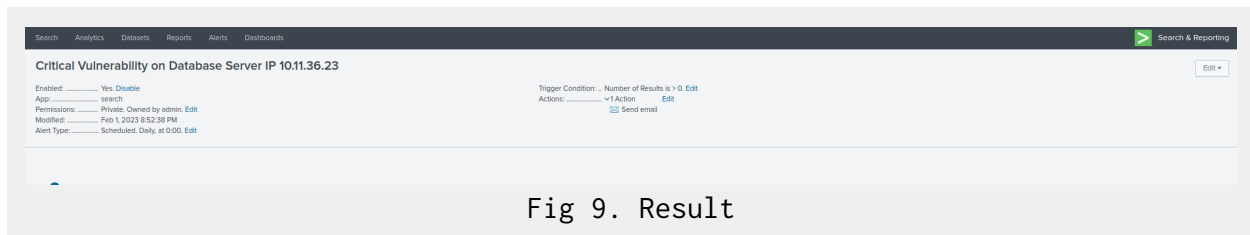
Provide a screenshot showing that the alert has been created:

The screenshot shows the 'Save As Alert' dialog box in Splunk. The dialog is titled 'Save As Alert' and has a close button (X) in the top right corner. It contains several sections: 'Settings' with fields for 'Title' (Critical Vulnerability on Database Server IP 10.1.36.23) and 'Description' (Optional); 'Permissions' with 'Private' and 'Shared In App' options; 'Alert type' with 'Scheduled' and 'Real-time' options; 'Trigger Conditions' with 'Trigger alert when' set to 'Number of Results' greater than 0; 'Trigger' set to 'Once'; 'Throttle' set to 'Off'; and 'Trigger Actions' with a '+ Add Actions' button. The 'Save' button is highlighted in green.

Fig 7. Naming alert and set Alert type

The screenshot shows the 'Save As Alert' dialog box in Splunk, specifically the 'When triggered' section. The section is expanded, showing a list of actions. The first action is 'Send email', which is selected. The email settings include 'To' (soc@vandalay.com), 'Priority' (Normal), 'Subject' (Splunk Alert: \$name\$), and 'Message' (The alert condition for '\$name\$' was triggered). The 'Include' section has checkboxes for 'Link to Alert', 'Link to Results', 'Search String', 'Trigger Condition', 'Trigger Time', 'Allow Empty Attachment', 'Attach CSV', and 'Attach PDF'. The 'Type' is set to 'HTML & Plain Text'. The 'Save' button is highlighted in green.

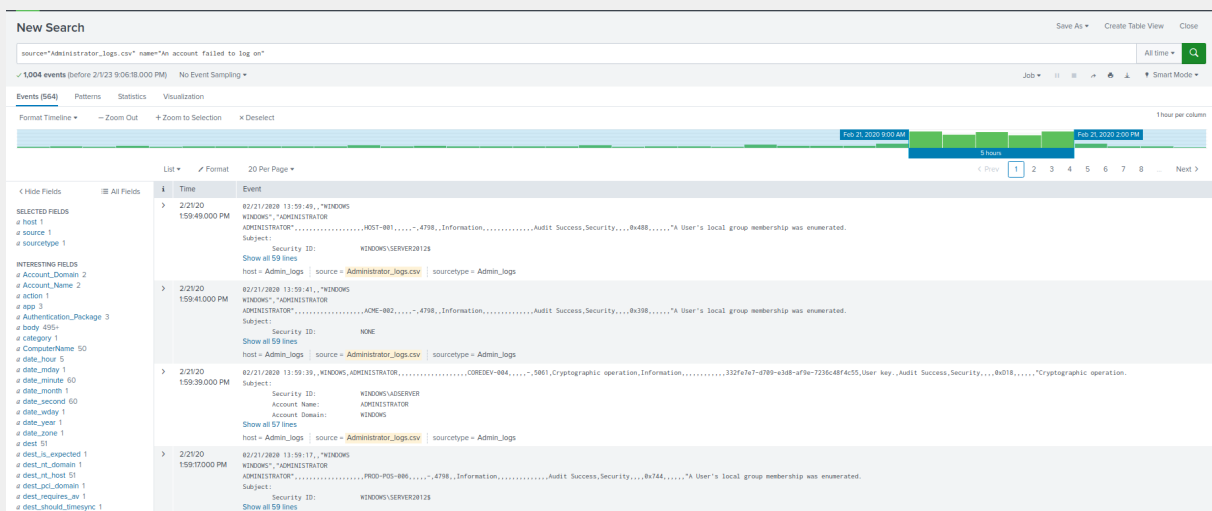
Fig 8. Setting email alert type



## Step 3: Drawing the (Base)line

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

Command: **source="Administrator\_logs.csv" name="An account failed to log on"**



The brute force attack occurred between Feb 21, 2020 9:00 am to Feb 21, 2020 2:00 pm for a time of 5 hrs

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

Normal activity: 20 logins  
Brute Force attack: 25 logins

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

Search Analytics Dashboards Reports Alerts Databases

### New Search

source="Administrator\_logs.csv" name="an account failed to log on"

1,004 events (before 2/1/23 9:06:10:000 PM) No Event Sampling +

Events (1,004) Patterns Statistics Visualization

Format Timeline + Zoom Out + Download Selections + Download

Hide Fields	All Fields	Time	Event
SELECTED FIELDS		2/21/20	62/21/2020 17:12:47, "WINDOWS
host 1		5:12:47:000 PM	ADMINISTRATOR" ... NTLM ... Rm7, ...
source 1			Subject: Security ID: ...
source_type 1			Show all 25 lines
INTERESTING FIELDS			
Account_Domain 2		2/21/20	62/21/2020 17:16:52, "WINDOWS
Account_Name 2		5:10:52:000 PM	ADMINISTRATOR" ... NTLM ... Rm7, ...
action 1			Subject: Security ID: ...
app 3			Show all 25 lines
Authentication_Package 3			host = Admin_Logs   source = Administrator_Log
body 100			
Caller_Process_Name 16		2/21/20	62/21/2020 17:16:48, "WINDOWS
Caller_Process_Name 1		5:10:48:000 PM	ADMINISTRATOR" ... NTLM ... Rm7, ...
Category 1			Subject: Security ID: ...
ComputerName 50			Show all 25 lines
date_hour 24			host = Admin_Logs   source = Administrator_Log
date_inday 2			
date_minute 60			
date_month 1			
date_second 60			
date_week 2			
date_year 1			
dest_ip 1			
dest_ip_expected 1			
dest_ip_category 1			
dest_ip_host 50			

#### Save As Alert

**Settings**

Title: Brute Force Attack

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 25

Trigger: Once For each result

Throttle: ☐

**Trigger Actions**

+ Add Actions

When triggered: Send email Remove

To:

Comma separated list of email addresses. Show CC and BCC

Cancel Save

Fig 11. Setting alert every hour

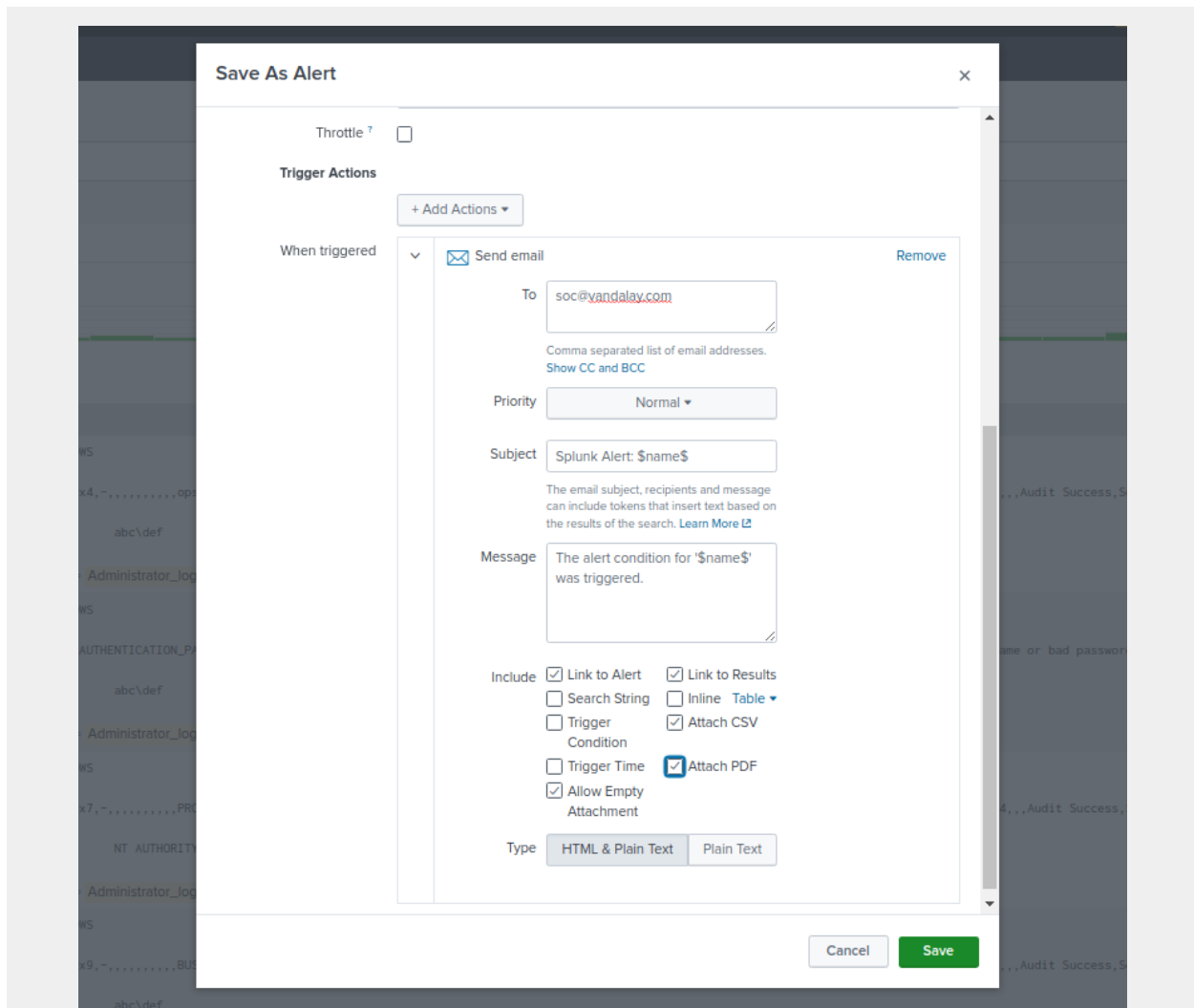


Fig 12.

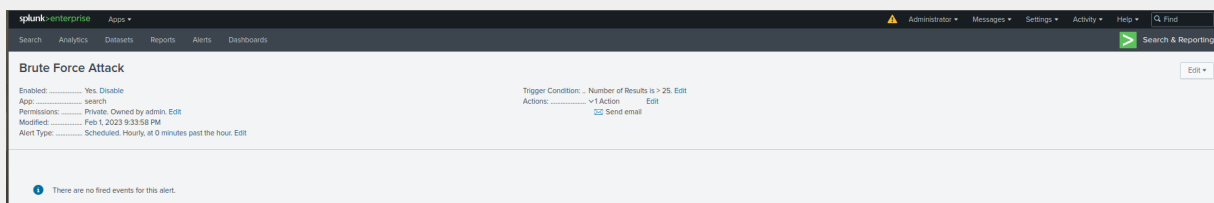


Fig 13. Result of creating alert