



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?

2/23/2020 between 14:30 to 23:30

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

Nine hours

Provide a screenshot of your report:

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS
2020-02-21 18:30:00	198.153.194.2	107.31	7.51
2020-02-21 16:30:00	198.153.194.2	106.91	6.51
2020-02-21 14:30:00	198.153.194.1	105.91	5.51
2020-02-20 14:21:00	198.153.194.1	109.16	5.43
2020-02-23 23:30:00	198.153.194.2	123.91	8.51
2020-02-23 23:30:00	198.153.194.1	122.91	7.51
2020-02-23 22:30:00	198.153.194.1	78.34	6.51
2020-02-23 20:30:00	198.153.194.2	65.34	4.23
2020-02-23 18:30:00	198.153.194.2	17.56	3.43
2020-02-23 14:30:00	198.153.194.1	7.87	1.83
2020-02-23 14:30:00	198.153.194.2	12.76	2.19
2020-02-22 23:30:00	198.153.194.2	109.16	9.51
2020-02-22 22:30:00	198.153.194.2	109.91	8.51
2020-02-22 20:30:00	198.153.194.2	108.91	7.51

Step 2: Are We Vulnerable?

Provide a screenshot of your report:

severity	count
critical	736
high	716
informational	698
low	760
medium	788

Provide a screenshot showing that the alert has been created:

Save As Alert



Settings

Title Critical Vulnerabilities from IP 10.11.36.23

Description Optional

Permissions

Private

Shared in App

Alert type

Scheduled

Real-time

Run every day ▼

Cancel

Save

At 0:00 ▼

Expires

24

hour(s) ▼

Trigger Conditions

Trigger alert when

Number of Results ▼

is greater than ▼

0

Trigger

Once

For each result

Throttle ?

☐

Cancel

Save

When triggered

✉ Send email

Remove

To

soc@vandalay.com

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

Priority

Normal ▼

Subject

Splunk Alert: Critical Vulnerabilities

The email subject, recipients and message can include tokens that insert

Cancel

Save

Message

The alert condition for 'Critical Vulnerabilities from IP 10.11.36.23' was triggered.

Include

☒ Link to Alert

☒ Link to Results

☐ Search String

☐ Inline [Table ▼](#)

☐ Trigger Condition

☐ Attach CSV

☐ Trigger Time

☐ Attach PDF

☒ Allow Empty

Cancel

Save

Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

2/21/2020 from 9:00 to 14:00

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

My baseline is roughly 20 logins per hour and my threshold would be greater than or equal to 30 attempts.

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

Save As Alert

Settings

Title

Exceeded failed login attempts

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 ▾

30

Trigger

Once

For each result

Throttle ?

☐

When triggered

Send email

Remove

To

soc@vandalaycom

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

Priority

Normal ▾

Subject

Splunk Alert: Exceeded failed login

The email subject, recipients and message can include tokens that insert

	<p>Message</p> <div>The alert condition for 'Exceeded failed login attempts' was triggered.</div> <p>Include</p> <table><tr><td><input checked="" type="checkbox"/> Link to Alert</td><td><input checked="" type="checkbox"/> Link to Results</td></tr><tr><td><input type="checkbox"/> Search String</td><td><input type="checkbox"/> Inline Table ▼</td></tr><tr><td><input type="checkbox"/> Trigger Condition</td><td><input type="checkbox"/> Attach CSV</td></tr><tr><td><input type="checkbox"/> Trigger Time</td><td><input type="checkbox"/> Attach PDF</td></tr><tr><td><input checked="" type="checkbox"/> Allow Empty</td><td></td></tr></table>	<input checked="" type="checkbox"/> Link to Alert	<input checked="" type="checkbox"/> Link to Results	<input type="checkbox"/> Search String	<input type="checkbox"/> Inline Table ▼	<input type="checkbox"/> Trigger Condition	<input type="checkbox"/> Attach CSV	<input type="checkbox"/> Trigger Time	<input type="checkbox"/> Attach PDF	<input checked="" type="checkbox"/> Allow Empty		
<input checked="" type="checkbox"/> Link to Alert	<input checked="" type="checkbox"/> Link to Results											
<input type="checkbox"/> Search String	<input type="checkbox"/> Inline Table ▼											
<input type="checkbox"/> Trigger Condition	<input type="checkbox"/> Attach CSV											
<input type="checkbox"/> Trigger Time	<input type="checkbox"/> Attach PDF											
<input checked="" type="checkbox"/> Allow Empty												
<div><div>Cancel</div><div>Save</div></div>												