



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 attack time was approximately 2/23/2020 2:30 PM,GMT

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

It took approximately 9hrs for our systems to recover.

Provide a screenshot of your report:

New Search

source="server_speedtest.csv" host="Module_19_Challenge" index="module_19_challenge" sourcetype="Module_19_Challenge"

| where _time >= strftime("2020-02-23", "%Y-%m-%d") AND _time < strftime("2020-02-24", "%Y-%m-%d")

| eval ratio = UPLOAD_MEGABITS / DOWNLOAD_MEGABITS

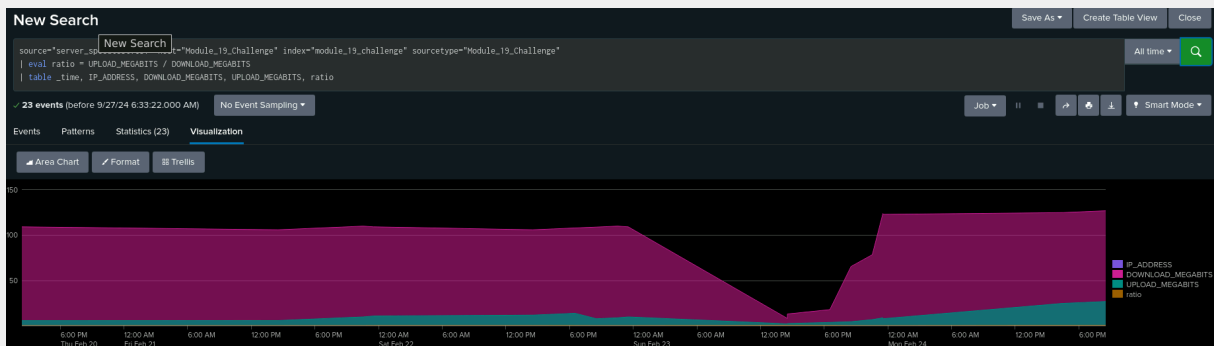
| table _time, IP_ADDRESS, DOWNLOAD_MEGABITS, UPLOAD_MEGABITS, ratio

7 events (before 9/27/24 5:25:00:000 AM) No Event Sampling

Events Patterns Statistics (7) Visualization

20 Per Page Format Preview

_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
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 18:30:00	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
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	0.0831
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	0.0611
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	0.0687



Step 2: Are We Vulnerable?

Provide a screenshot of your report:

New Search

```
index="module_19_challenge" sourcetype="nessus_logs" source="nessus_logs.csv" host="7192b893130d" dest_ip="10.11.36.23" severity="critical"
| stats count as Critical_Vulnerabilities
| table Critical_Vulnerabilities
```

49 events (before 9/27/24 5:34:51.000 AM) No Event Sampling

Events Patterns Statistics (1) Visualization

20 Per Page Format Preview

Critical_Vulnerabilities

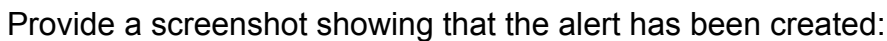
49

Mod_19 - Are We Vulnerable? Edit More Info Add to Dashboard

All time 49 events (before 9/27/24 5:36:53.000 AM)

20 per page

Time	Event
2/20/20 5:33:01.000 PM	<pre>,"start_time":"Thu Feb 20 17:33:01 2020" end_time="Thu Feb 20 17:33:01 2020" dest_dns="HOST-003" dest_nt_host="ops-sys-006" dest_mac="ad:7b:3d:db:49:8b" dest_ip="10.11.36.13" os="Cisco Router" dest_port_proto="el-random(827/tcp)" severity_id="41" signature_id="12258" signature="Additional DNS Hostnames" ---splunk-ta-nessus-end-of-event--- "2020-02-20T17:33:19:000-0800,,,,,,,,,HOST-003,,,,,,,,,HOST-003,10.11.36.23,false,,ad:7b:3d:db:49:8b,ops-sys-006,,untrust,827,el-random(827/tcp),false,false,false,,Thu Feb 20 17:33:01 2020,nessus_misconfigured_wireless_device,nessus_plugin_avail,nessus_system_version,127.0.0.1,,main,,,4,,,Cisco Router,12258,,,Cisco Router,,,,,Nessus,,,Err:509,,,,critical,4,,,Additional DNS Hostnames,,12258,eventgen,nessus,prd-p-vj7zgfpcb88,,,,,,,,,,,,,Thu Feb 20 17:33:01 2020,,,,,Inventory os report Show all 13 lines host = 7192b893130d source = nessus_logs.csv sourcetype = nessus_logs</pre>
2/20/20 5:27:48.000 PM	<pre>,"start_time":"Thu Feb 20 17:27:48 2020" end_time="Thu Feb 20 17:27:48 2020" dest_dns="HOST-003" dest_mac="0b:4a:fe:06:36:92" dest_ip="10.11.36.29" os="Microsoft Windows XP Service Pack 2" os="Microsoft Windows XP Service Pack 3" dest_port_proto="general" severity_id="14" signature_family="Service detection" signature_id="12122" signature="Terminal Services Encryption Level is not FIPS-140 Compliant" ---splunk-ta-nessus-end-of-event--- "2020-02-20T17:33:19:000-0800,,,,,,,,,HOST-003,,,,,,,,,HOST-003,10.11.36.23,false,,0b:4a:fe:06:36:92,,untrust,,general,,false,,false,false,,Thu Feb 20 17:27:48 2020,nessus_misconfigured_device,nessus_plugin_avail,nessus_system_version,127.0.0.1,,main,,,4,,,Microsoft Windows XP Service Pack 2,Microsoft Windows XP Service Pack 3,,12122,,,Microsoft Windows XP Service Pack 2,Microsoft Windows XP Service Pack 3,,,,,Nessus,,,Err:509,,,,critical,4,,,Terminal Services Encryption Level is not FIPS-140 Compliant,Service detection,12122,eventgen,nessus,prd-p-vj7zgfpcb88,,,,,,,,,,,,,Thu Feb 20 17:27:48 2020,,,,,Inventory Show all 15 lines host = 7192b893130d source = nessus_logs.csv sourcetype = nessus_logs</pre>



Provide a screenshot showing that the alert has been created:

Save As Alert



Settings

Title Mod_19 - We Vulnerable

Description Optional

Permissions Private

Shared in App

Alert type Scheduled

Real-time

Run every day ▼

At 20:00 ▼

Expires 24

hour(s) ▼

Trigger Conditions

Trigger alert when Number of Results ▼

is greater than ▼

0

Trigger

Once

For each result

Throttle ? ☐

Trigger Actions

+ Add Actions ▾

When triggered

✉ Send email

Remove

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

Normal ▾

Subject

critical - customer data server

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

Save As Alert

Subject

critical - customer data server

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

Message

This is an alert for a report for a
report determining how many
critical vulnerabilities exist on the
customer data server.

Include

☒ Link to Alert

☒ Link to Results

☐ Search String

☐ Inline [Table ▾](#)

☐ Trigger Condition

☐ Attach CSV

☐ Trigger Time

☐ Attach PDF

☒ Allow Empty Attachment

Type

HTML & Plain Text

Plain Text

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

Mod_19 - We Vulnerable

Enabled: Yes. [Disable](#)

App: search

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

Modified: Sep 27, 2024 5:44:52 AM

Alert Type: Scheduled, Daily, at 20:00. [Edit](#)

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

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

[Send email](#)

There are no fired events for this alert.

Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

Between
9am Friday 21/02/2020 (124 events) - 1pm Friday 21/02/2020 (123 events)

124 events at 9 AM on Friday, February 21, 2020

123 events at 1 PM on Friday, February 21, 2020

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

The normal baseline would be around 15 failed logins per hour. So I would set the alert at 18 per hour to avoid too many false positives.

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

Save As Alert



Settings

Title Brute Force Attack Detection

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 ▾

0

Cancel

Save

Save As Alert



Trigger

Once

For each result

Throttle ?

☐

Trigger Actions

+ Add Actions ▾

When triggered



Send email

[Remove](#)

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

Normal ▾

Subject

Brute Force Attack Detected!

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

Save As Alert



Message

Alert! Brute Force Attack Detected on Admin Account!

It looks like someone's trying to get into our admin account more often than George claims to be an importer-exporter at Vandalay Industries! If this attack continues, we'll be importing trouble and exporting excuses. Don't let them steal our latex!

What happened:

Multiple failed login attempts detected, suggesting a brute force attack. Whoever it is, they're trying harder than George trying to convince everyone he's an architect.

What to do next:

Call Mr. Vandelay! (Or better yet, notify your SOC team). Verify the source and take action before we end up in a Festivus grievance situation. Remember, if you see George, he's not really working here—he's just pretending. But this brute force attack is no joke!

Email sent from the latex export division of Vandalay

- Include
- ☒ Link to Alert
 - ☒ Link to Results
 - ☐ Search String
 - ☐ Inline [Table](#) ▼
 - ☐ Trigger Condition
 - ☐ Attach CSV
 - ☐ Trigger Time
 - ☐ Attach PDF
 - ☒ Allow Empty Attachment

Type

HTML & Plain Text

Plain Text

Brute Force Attack Detection

Enabled: Yes. [Disable](#)
App: search
Permissions: Private, Owned by admin. [Edit](#)
Modified: Sep 27, 2024 6:29:57 AM
Alert Type: Scheduled. Hourly, at 0 minutes past the hour. [Edit](#)

Trigger Condition: .. Number of Results is > 0. [Edit](#)
Actions: 1 Action [Edit](#)
[✉ Send email](#)

