

Содержание

17 Detecting SSH bruteforce attacks using triggers in QoE 3
 System trigger to detect SSH bruteforce attacks 3

17 Detecting SSH bruteforce attacks using triggers in QoE

[Triggers](#) are used to search for data in the QoE Stor by specified parameters. After the trigger action one of the following steps is possible:

- notification in GUI
- HTTP action
- sending an email

The required options of the Stingray Service Gateway:

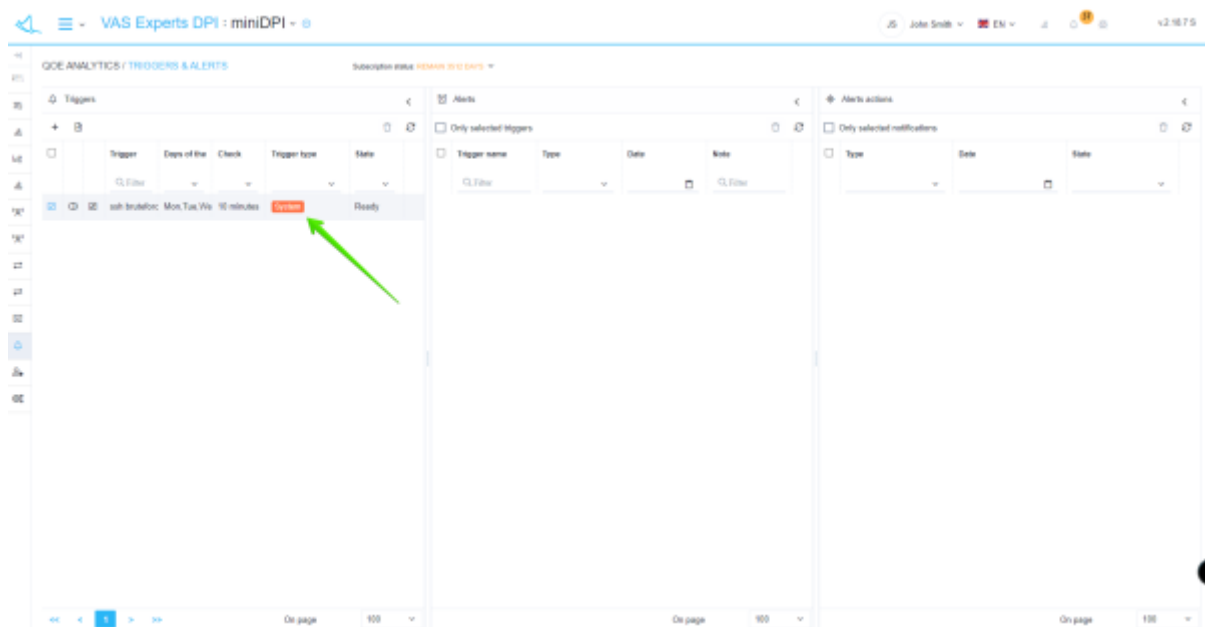
- [Statistics gathering and analysis on protocols and directions](#)
- [Subscriber notifications](#)

Required additional modules:

- [DPIUI2 \(GUI - Graphical User Interface\)](#)
- [QoE Stor \(Statistics collection module\)](#)

System trigger to detect SSH bruteforce attacks

Trigger to detect SSH bruteforce attacks (Name - "ssh bruteforce") is a system trigger and is available in the subsection "QoE Analytics" - "Triggers and Notifications" (disabled by default).



General trigger information

Common

Trigger name * ssh bruteforce Severity Hight Trigger Disabled

Days of the week * Mon, Tue, Wed, Thu, Fri, Sat, Sun Check frequency * 10 minutes Number of positives 0

Start date 10/01/2019 End date 12/31/2099 Start time 00:00 End time 23:55

- The name of the trigger "ssh bruteforce";
- Days of the week - all;
- Checking frequency - every 10 minutes;
- Trigger frequency - 0;
- Start/end dates and times are customizable if needed.



Every day at intervals of 10 minutes the data will be checked under the conditions described below.

Queries

| Queries | | | | | | |
|----------------------------------------|------------|----------------|--|------------------|------------------|--|
| + | | | | | | |
| | Query name | Report | | Period from | Period to | |
| <input checked="" type="checkbox"/> On | A | Ssh bruteforce | | now - 30 minutes | now - 20 minutes | |

For this trigger, an uneditable query with the following parameters is set:

- Table to scan: Raw full netflow → Tables → Attacks detection → SSH bruteforce;
- Period from: now - 30 minutes
- Period from: now - 20 minutes

Conditions

| Conditions | | | | | | | |
|----------------------------------------|------|------------|----------|------------|------------------|----------|-------|
| + | | | | | | | |
| | Bind | Query name | Function | Combinator | Series | Operator | Value |
| <input checked="" type="checkbox"/> On | AND | A | avg | | Session lifetime | <= | 20 |
| <input checked="" type="checkbox"/> On | AND | A | max | | Sessions per su | >= | 1500 |

- Add "+" 2 fields

- Bind - AND
- Function - avg
- Series in field 1 - session lifetime to subscriber $\leq 20(\text{ms})$
- Series in field 2 - number of sessions per subscriber ≥ 1500



We set the conditions for the trigger action: The average duration of an SSH-session to a subscriber is less than 20ms and the number of SSH-sessions for the subscriber is more than 1500 in the processed time period.

Errors processing

| No data & error handling | |
|--------------------------|---------------------------------|
| If no data * | If execution error or timeout * |
| No data | Keep last state |

- In the "If no error" field - no data
- In the "If execution error or timeout" field - save the last state



In this configuration, if there are no errors, the data will not be saved, if there are errors - the information about the suspicious activity will be saved.

Actions

E-mail

Actions

Notification x E-mail x

Send to On

Your@email.com

Subject

Trigger fired: {trigger.name}

Message 📎 </>

Ид: {trigger.id}

Триггер: {trigger.name}

Статус: {trigger.state}

Важность: {trigger.severity}

Запросы:

{trigger.queries}

- For automatic filling of the form - click on the "</>" icon
- In the "Send to" field - specify an email address
- With this setting, when triggered, a notification will be sent to the specified email address: ID, trigger name, status, link to the report (saved state).

Notification

Actions

Notification x E-mail x

Notification title On

{trigger.name}

Notification subtitle

{trigger.id}

Notification type

Warning

Message 📎 </>

Ид: {trigger.id}

Триггер: {trigger.name}

Статус: {trigger.state}

Важность: {trigger.severity}

Запросы:

{trigger.queries}

- For automatic filling of the form - click on the "</>" icon
- Select the type of notification - "Warning"
- This setting will create a notification in the Stingray Service Gateway

| Alerts | | | | | Alerts actions | | | | |
|-------------------------------------------------|-------------------------------------|--------------------------------|-------------------------------|-------------------------------------|------------------------------------------------------|--------------------------------|-------------------------------|--------------------------------|--------------------------|
| <input type="checkbox"/> Only selected triggers | | | | | <input type="checkbox"/> Only selected notifications | | | | |
| <input type="checkbox"/> | Trigger name | Type | Date | Note | <input type="checkbox"/> | Type | Date | State | |
| | <input type="text" value="Filter"/> | <input type="text" value="v"/> | <input type="text" value=""/> | <input type="text" value="Filter"/> | | <input type="text" value="v"/> | <input type="text" value=""/> | <input type="text" value="v"/> | |
| <input type="checkbox"/> | ssh bruteforce | Alerting | 20.05.2021 14:45:24 | count(sess_subscrib | <input checked="" type="checkbox"/> | notification | 20.05.2021 14:45:44 | Complete | <input type="checkbox"/> |
| <input type="checkbox"/> | ssh bruteforce | Ok | 20.05.2021 14:31:43 | | | | | | <input type="checkbox"/> |
| <input type="checkbox"/> | ssh bruteforce | Ok | 20.05.2021 14:13:24 | count(sess_subscrib | | | | | <input type="checkbox"/> |
| <input type="checkbox"/> | ssh bruteforce | Ok | 20.05.2021 14:12:03 | count(sess_subscrib | | | | | <input type="checkbox"/> |
| <input type="checkbox"/> | ssh bruteforce | Ok | 20.05.2021 14:10:42 | count(sess_subscrib | | | | | <input type="checkbox"/> |
| <input type="checkbox"/> | ssh bruteforce | Ok | 20.05.2021 14:09:24 | count(sess_subscrib | | | | | <input type="checkbox"/> |
| <input type="checkbox"/> | ssh bruteforce | Ok | 20.05.2021 14:08:03 | count(sess_subscrib | | | | | <input type="checkbox"/> |
| <input type="checkbox"/> | ssh bruteforce | Ok | 20.05.2021 14:06:42 | count(sess_subscrib | | | | | <input type="checkbox"/> |
| <input type="checkbox"/> | ssh bruteforce | Ok | 20.05.2021 14:05:23 | count(sess_subscrib | | | | | <input type="checkbox"/> |
| <input type="checkbox"/> | ssh bruteforce | Ok | 20.05.2021 14:04:04 | count(sess_subscrib | | | | | <input type="checkbox"/> |
| <input type="checkbox"/> | ssh bruteforce | Ok | 20.05.2021 14:02:43 | count(sess_subscrib | | | | | <input type="checkbox"/> |

You can get a link to the report in the notification menu

Notifications

Triggers

ssh bruteforce (1)

Id: 1

20.05.2021 02:45

Details

Mark as read

Delete

Subscribers synchronization

Hardware: miniDPI

Success

Subscribers synchronization

Hardware: centos8

Success

Subscribers synchronization

Hardware: miniDPI

Success

Subscribers synchronization

Hardware: centos8

Success

Subscribers synchronization

Hardware: miniDPI

Success

Subscribers synchronization

Hardware: centos8

Success

<<

<

1

2

3

4

5

>

>>

Choose the notification Click "Details"

← Triggers

Status **New**

Notification date **20.05.2021 02:45**

Notify type **⚠ Warning**

Notification content

ssh bruteforce (1)

Id: 1

Trigger: ssh bruteforce

Status: firing

Severity: hight

Queries:

A: QoETableFullnetflowRawSshBruteForceWidget

Reasons for the occurrence of notification:

count(sess_subscribers) > 0 is true in query A

Links to reports:

A: https://localhost/#QoEAnyReport/report_id=896Fj5ZLpG8WenE

Click on the link to the report - the report will open in a new browser tab.

HTTP action

Actions

Notification × E-mail × Http × +

Method POST Url https://your_redmine_host/issues.xml?key=your_redmine_api_key On

Headers < Body >

+ 📄 </>

| Name | Value | |
|--------------|-----------------|---|
| Content-Type | application/xml | 📄 |

```
<?xml version="1.0"?>
<issue>
  <project_id>1</project_id>
  <subject>Сработал триггер: {trigger.name}</subject>
  <priority_id>1</priority_id>
  <description>Ид: {trigger.id}
  Триггер: {trigger.name}
  Статус: {trigger.state}
  Важность: {trigger.severity}

  Запросы:
  {trigger.queries}
</issue>
```

REDMINE JSON
REDMINE XML

- For automatic filling of the form - click on the "</>" icon
- Choose the most suitable method for your ticket system and enter the URL.