THREATQUOTIENT

ThreatQuotient For NVD

(National Vulnerability Database)

January 22, 2019

Version 1.1.0

11400 Commerce Park Dr
Suite 200,
Reston, VA
20191, USA
https://www.threatq.com/
Support: support@threatq.com
Sales: sales@threatq.com

Contents

List of Figures and Tables

1 Introduction

1.1 Application Function

The ThreatQuotient for NVD (National Vulnerability Database) application utilizes the National Vulnerability Database by pulling the entries in the database into the ThreatQ instance. The NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

The NVD is the U.S. government repository of standards-based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance.

1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient for NVD integration. Although it may be used as such, this document is not specifically intended as a site reference guide. It is assumed that the implementation engineer has experience installing and commissioning ThreatQuotient Apps and integrations covered within the document, as well as experience necessary to troubleshoot at a basic level.

1.3 Audience

This document is intended for use by the following parties:

1. ThreatQ System Administrators & Engineers
2. Security Engineers

1.4 Scope

This document only covers the implementation of the ThreatQuotient for NVD connector.

1.5 Assumptions

The following criteria is assumed to be in place and functional to allow the implementation of the ThreatQuotient into the managed estate:

- All ThreatQuotient equipment is online and in service.
- All required firewall ports have been opened.
- A clock source of sufficient accuracy is connected to the network and the network is using it as the primary clock source.

This integration requires:

- ThreatQ version of 4.5 or greater,

2 Implementation Overview

2.1 Prerequisites

Throughout this implementation document, we will refer to several files and directories, some of which will be symbolic, and others may change depending on specifics of the environmental setup.

Ensure all ThreatQ devices are set to the correct time (UTC is recommended), time zone and date, and using a clock source available to all.

To identify which time zone is closest to your present location, use the `timedatectl` command with the `list-timezones` command line option. For example, to list all available time zones in Europe, type:

Figure 1: Time Zone List Example

```
timedatectl list-timezones | grep Europe
Europe/Amsterdam
Europe/Athens
Europe/Belgrade
Europe/Berlin
```

To change the time zone to UTC, type as root:

Figure 2: Time Zone Change Example

```
timedatectl set-timezone UTC
```

2.2 Security and Privacy

Passwords have not been provided in this document. Please contact your project team for this information, if required.

2.3 Setting up the Integration

2.3.1 From The ThreatQuotient Repository

To install this ThreatQuotient for NVD from the ThreatQuotient repository with YUM credentials.

1. Install the ThreatQuotient for NVD application by using the following commands.

Figure 3: Installing From The ThreatQuotient Repository (Example Output)

```
sudo pip install -i
https://<USERNAME>:<PASSWORD>@extensions.threatq.com/threatq/integrations NVD
Collecting NVD
  Downloading https://extensions.threatq.com/threatq/integrations-
dev/+f/2c0/af5861a478c62/NVD-1.1.0-py2-none-any.whl
Requirement already satisfied (use --upgrade to upgrade): requests in
/usr/lib/python2.7/site-packages (from NVD)
Requirement already satisfied (use --upgrade to upgrade): threatqsdk in
/usr/lib/python2.7/site-packages (from NVD)
Requirement already satisfied (use --upgrade to upgrade): threatqcc>=1.1.1 in
/usr/lib/python2.7/site-packages (from NVD)
Requirement already satisfied (use --upgrade to upgrade): python-dateutil in
/usr/lib/python2.7/site-packages (from NVD)
Requirement already satisfied (use --upgrade to upgrade): jinja2==2.8 in
/usr/lib64/python2.7/site-packages (from threatqcc>=1.1.1->NVD)
Requirement already satisfied (use --upgrade to upgrade): six>=1.5 in
/usr/lib/python2.7/site-packages (from python-dateutil->NVD)
Requirement already satisfied (use --upgrade to upgrade): MarkupSafe in
/usr/lib64/python2.7/site-packages (from jinja2==2.8->threatqcc>=1.1.1->NVD)
Installing collected packages: NVD
Successfully installed NVD-1.1.0
```

2. Once the application has been installed, you must create a directory structure for all configuration, logs and files, using the `mkdir -p` command. See example below:
3. A driver which will be called `tq-nvd` is installed.

In the case that a proxy is setup within the ThreatQ instance the following switch will need to be used `--external-proxy or -ep`. This enables a proxy to be used to contact the internet for the data required by this connector. This specifies an internet facing proxy, NOT a proxy to the ThreatQ instance.

Figure 4: Creating Integration Directories (Example)

```
mkdir -p /etc/tq_labs/
mkdir -p /var/log/tq_labs/
```

4. Issue the following commands to initialize the integration.

   You will be asked the following questions:
   During this initial execution, several prompts will be displayed for the following information:

   - **ThreatQ Host:** Hostname or IP Address of the ThreatQ server.
     - If this is a hostname, it must be resolvable on the Installation Point.
   - **Client ID:** This is the OAuth Management value found in **Settings icon > OAuth Management**.
   - **E-Mail Address:** This is the e-mail address of the ***ThreatQ*** user for this integration.
     - This should be a dedicated user (e.g. nvd@threatq.com).
   - **Password:** This is the password for the above ***ThreatQ*** user.

- **Status:** This is the default status of newly created IoCs.

Figure 5: Running the Integration

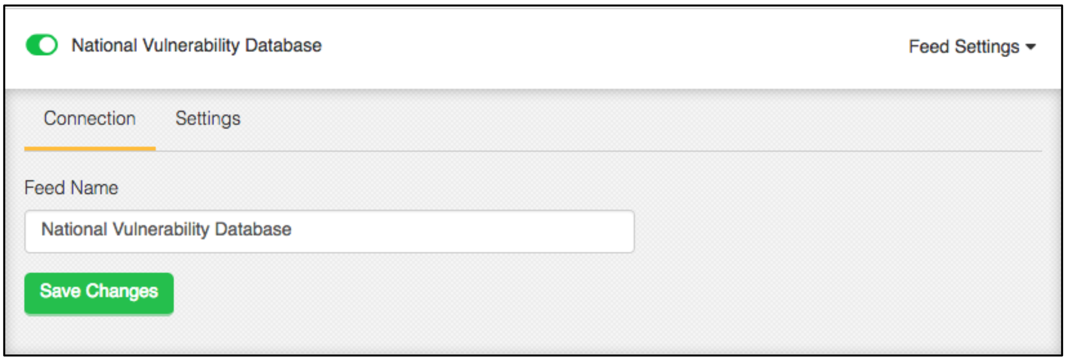
```
$> tq-nvd -c /file/path/to/config/ -ll /file/path/to/logs/ -v3
ThreatQ Host: <ThreatQ Host IP or Hostnme >
Connector Name: National Vulnerability Database
Client ID: <ClientID>
E-Mail Address: <EMAIL ADDRESS>
Password: <PASSWORD>
Status: Active
Connector configured.  Set information in UI.
0000-00-00 00:00:00 - tqNvd.tq_driver CRITICAL: Connector has been created, please
use UI for final configuration
```

The driver will run once, where it will connect to the ThreatQ instance and install the UI component of the connector.

2.4 Configuring the connector

Once completed, navigate in the ThreatQ user interface to **Gear > Incoming Feeds > Labs** (In versions earlier to version 4.5 this will be "**ThreatQ Labs**") and locate the National Vulnerability Database entry.

Figure 6: ThreatQ UI Configuration



Feed Name: National Vulnerability Database

1. Under **Settings**, change **How frequent should we pull information from this feed?** to **Every Day**.

   Once complete, click **Save Changes** and ensure that the toggle next to the name is enabled.

2.5 Executing the Driver

Several configuration options are available for the import of CVEs.

2.5.1 Historical Import

During the initial run of the connector, you can run a historical import.

⚠ Running the ThreatQuotient for NVD connector for **ALL** CVE’s will look for all entries, if no time frame is given, it will pull every entry. This can take in excess of **18 Hours. Each year averages 10K CVE’s**.

```
tq-nvd -c /path/to/config/directory/ -ll /path/to/log/directory/ -v
VERBOSITY_LEVEL -i -s START_YEAR -e END_YEAR
```

2.5.2 Import *ALL* History (2002 - Present)

During the initial run of the connector, you can run a historical import.

```
tq-nvd -c /path/to/config/directory/ -ll /path/to/log/directory/ -v
VERBOSITY_LEVEL -i
```

2.5.3 Import *SPECIFIC* History (2010 - 2016)

During the initial run of the connector, you can run a historical import.

```
tq-nvd -c /path/to/config/directory/ -ll /path/to/log/directory/ -v
VERBOSITY_LEVEL -i -s 2010 -e 2016
```

3 CRON

To run this script on a reoccurring basis use CRON or some other system schedule. The argument in the cron script ***must*** specify the config and log locations.

Each of these should be added to {{cron}} or another task scheduler to refresh the data in the individual components. This can be run multiple times a day and should not be run more often than once per hour.

3.1.1 Setting Up the CRONJOB

1. Login via a CLI terminal session to you ThreatQ host.
2. Input the commands below.

   Figure 7: Command Line Crontab Command

   ```
   $> crontab -e
   ```

   This will enable the editing of the crontab, using vi.

   Depending on how often you wish the cronjob to run, you will need to adjust the time to suit the environment.

3. Input the commands below – this example shows every **2nd day of the month.**

   Figure 8: Command Line Crontab tq-nvd Command

   ```
   0 23 */2 * * tq-nvd -c /file/path/to/config/ -ll /file/path/to/logs/ -v3
   ```

   To run this script on a reoccurring basis use CRON or some other on system schedule. CRON is shown below.

   The argument in the cron script ***must*** specify the config and log locations.

   In the case that a proxy is setup within the ThreatQ instance the following switch will need to be used `--external-proxy or -ep`

   This enables a proxy to be used to contact the internet for the data required by this connector. This specifies an internet facing proxy, NOT a proxy to the ThreatQ instance.

Appendix A: Supplementary Information

Uninstalling the Connector

```
sudo pip uninstall tq-nvd
```

tq-nvd command line options

The tq-nvd driver has several command line arguments that will help you and your customers execute this. They are listed below. You can see these by executing `/usr/bin/tq-nvd --help.`

```
usage: tq-nvd Connector [-h] [-ll LOGLOCATION][-c CONFIG] [-v VERBOSITY]
```

```
tq-nvd
```

optional arguments:

```
  -h, --help
```

Shows the help message and exit

```
  -ll LOGLOCATION, --loglocation LOGLOCATION
```

This sets the logging location for this connector. The location should exist and be writable by the current user. A special value of 'stdout' means to log to the console (this happens by default).

```
  -c CONFIG, --config CONFIG
```

This is the location of the configuration file for the connector. This location must have read and write permissions for the current user. If no config file is given, the current directory will be used. This file is also where some information from each run of the connector may be put (e.g. last run time, private OAuth, etc).

```
  -v {1,2,3}, --verbosity {1,2,3}
```

This is the logging verbosity level. The Default is 1 (Warning).

```
  -external-proxy, -ep
```

This enables a proxy to be used to contact the internet for the data required by this connector. This specifies an internet facing proxy, NOT a proxy to the ThreatQ instance.

Trademarks and Disclaimers

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR THREATQUOTIENT REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THIRD PARTY SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. THREATQUOTIENT AND THIRD-PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL THREATQUOTIENT OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF THREATQUOTIENT OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

ThreatQuotient and the ThreatQuotient Logo are trademarks of ThreatQuotient, Inc. and/or its affiliates in the U.S. and other countries.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.