Suricata Update Documentation

Release 1.0.0a1

OISF

Dec 05, 2017

Contents

CHAPTER 1

Quick Start

1.1 Install Suricata Update

Suricata-Update is a tool written in Python and best installed with the `pip` tool for installing Python packages.

Pip can install `suricata-update` globally making it available to all users or it can install `suricata-update` into your home directory for use by your user.

Note: At some point `suricata-update` should be bundled with Suricata avoid the need for a separate installation.

To install `suricata-update` globally:

```
pip install --pre --upgrade suricata-update
```

or to install it to your own directory:

```
pip install --user --pre --upgrade suricata-update
```

Note: When installing to your home directory the `suricata-update` program will be installed to $HOME/.local/bin, so make sure this directory is in your path:

```
export PATH=$HOME/.local/bin:$PATH
```

1.2 Directories and Permissions

In order for `suricata-update` to function, the following permissions are required:

- Directory /etc/suricata: read access

- Directory /var/lib/suricata/rules: read/write access
- Directory /var/lib/suricata/update: read/write access

One option is to simply run `suricata-update` as root or with `sudo`.

Note: It is recommended to create a `suricata` group and setup the above directories with the correction permissions for the `suricata` group then add users to the `suricata` group.

More documentation will be provided about this, including a tool to verify and maybe setup the permissions.

1.3 Update Your Rules

Without doing any configuration the default operation of `suricata-update` is use the Emerging Threats Open ruleset.

Example:

```
suricata-update
```

This command will:

- Look for the `suricata` program on your path to determine its version.
- Look for /etc/suricata/enable.conf, /etc/suricata/disable.conf, /etc/suricata/drop.conf, and /etc/suricata/modify.conf to look for filters to apply to the downloaded rules. These files are optional and do not need to exist.
- Download the Emerging Threats Open ruleset for your version of Suricata, defaulting to 4.0.0 if not found.
- Apply enable, disable, drop and modify filters as loaded above.
- Write out the rules to `/var/lib/suricata/rules/suricata.rules`.
- Run Suricata in test mode on `/var/lib/suricata/rules/suricata.rules`.

Note: Suricata-Update is also capable of triggering a rule reload, but doing so requires some extra configuration that will be covered later.

1.4 Configure Suricata to Load Suricata-Update Managed Rules

Suricata-Update takes a different convention to rule files than Suricata traditionally has. The most noticeable difference is that the rules are stored by default in `/var/lib/suricata/rules/suricata.rules`.

One way to load the rules is to the the `-S` Suricata command line option. The other is to update your `suricata.yaml` to look something like:

```
default-rule-path: /var/lib/suricata/rules
rule-files:
  - suricata.rules
```

Note: In the future we expect Suricata to use this new convention by default.

1.5 Discover Other Available Rule Sources

First update the rule source index with the `update-sources` command, for example:

```
suricata-update update-sources
```

Then list the sources from the index. Example:

```
suricata-update list-sources
```

Now enable the **ptresearch/attackdetection** ruleset:

```
suricata-update enable-source ptresearch/attackdetection
```

And update your rules again:

```
suricata-update
```

1.6 List Enabled Sources

```
suricata-update list-enabled-sources
```

1.7 Disable a Source

```
suricata-update disable-source et/pro
```

Disabling a source keeps the source configuration but disables. This is useful when a source requires parameters such as a code that you don't want to lose, which would happen if you removed a source.

Enabling a disabled source re-enables without prompting for user inputs.

1.8 Remove a Source

```
suricata-update remove-source et/pro
```

This removes the local configuration for this source. Re-enabling **et/pro** will requiring re-entering your access code.

CHAPTER 2

suricata-update - Update

2.1 Synopsis

`suricata-update` [OPTIONS]

2.2 Description

`suricata-update` aims to be a simple to use rule download and management tool for Suricata.

2.3 Options

-h, --help
Show help.

-c `<filename>`**, --config** `<filename>`
Path to the suricata-update config file.

Default: */etc/suricata/update.yaml*

-o, --output
The directory to output the rules to.

Default: */var/lib/suricata/rules*

--suricata=`<path>`
The path to the Suricata program used to determine which version of the ET pro rules to download if not explicitly set in a `--url` argument.

--suricata-version `<version>`
Set the Suricata version to a specific version instead of checking the version of Suricata on the path.

--force
Force remote rule files to be downloaded if they otherwise wouldn't be due to just recently downloaded, or the remote checksum matching the cached copy.

--merged=<filename>
Write a single file containing all rules. This can be used in addition to `--output` or instead of `--output`.

--no-merge
Do not merge the rules into a single rule file.

Warning: No attempt is made to resolve conflicts if 2 input rule files have the same name.

--yaml-fragment=<filename.yaml>
Output a fragment of YAML containing the *rule-files* section will all downloaded rule files listed for inclusion in your *suricata.yaml*.

--url=<url>
A URL to download rules from. This option can be used multiple times.

--local=<filename or directory>
A path to a filename or directory of local rule files to include.

If the path is a directory all files ending in *.rules* will be loaded.

Wildcards are accepted but to avoid shell expansion the argument must be quoted, for example:

```
--local '/etc/suricata/custom-*.rules'
```

This option can be specified multiple times.

--sid-msg-map=<filename>
Output a v1 style sid-msg.map file.

--sid-msg-map-2=<filename>
Output a v2 style sid-msg.map file.

--disable-conf=<disable.conf>
Specify the configuration file for disable filters.

See *Example Configuration to Enable Disable (–disable-conf)*

--enable-conf=<enable.conf>
Specify the configuration file for enable rules.

See *Example Configuration to Enable Rules (–enable-conf)*

--modify-conf=<modify.conf>
Specify the configuration file for rule modification filters.

See *Example Configuration to modify Rules (–modify-conf)*

--drop-conf=<drop.conf>
Specify the configuration file for drop filters.

See *Example Configuration to convert Rules to Drop (–drop-conf)*

--ignore=<pattern>
Filenames to ignore. This is a pattern that will be matched against the basename of a rule files.

This argument may be specified multiple times.

Default: **deleted.rules*

Example:

```
--ignore dnp3-events.rules --ignore deleted.rules --ignore "modbus*"
```

Note: If specified the default value of **deleted.rules* will no longer be used, so add it as an extra ignore if needed.

--no-ignore
Disable the –ignore option. Most useful to disable the default ignore pattern without adding others.

--etopen
Download the ET/Open ruleset.

This is the default action of no `--url` options are provided or no sources are configured.

Use this option to enable the ET/Open ruleset in addition to any URLs provided on the command line or sources provided in the configuration.

--dump-sample-configs
Output sample configuration files for the `--disable`, `--enable`, `--modify` and `--threshold-in` commands.

--threshold-in=`<threshold.conf.in>`
Specify the threshold.conf input template.

--threshold-out=`<threshold.conf>`
Specify the name of the processed threshold.conf to output.

-T `<command>`, **--test-command** `<command>`
Specifies a custom test command to test the rules before reloading Suricata. This overrides the default command and can also be specified in the configuration file under `test-command`.

--no-test
Disables the test command and proceed as if it had passed.

--reload-command=`<command>`
A command to run after the rules have been updated; will not run if no change to the output files was made. For example:

```
--reload-command=sudo kill -USR2 $(cat /var/run/suricata.pid)
```

will tell Suricata to reload its rules.

--no-reload
Disable Suricata rule reload.

-V, --version
Display the version of **suricata-update**.

-q, --quiet
Run quietly. Only warning and error messages will be displayed.

-v, --verbose
Provide more verbose output.

2.4 Rule Matching

Matching rules for disabling, enabling, converting to drop or modification can be done with the following:

- signature ID

- regular expression
- rule group
- filename

2.4.1 Signature ID Matching

A signature ID can be matched by just its signature ID, for example:

```
1034
```

The generator ID can also be used for compatibility with other tools:

```
1:1034
```

2.4.2 Regular Expression Matching

Regular expression matching will match a regular expression over the complete rule. Example:

```
re:heartbleed
re:MS(0[7-9]|10)-\d+
```

2.4.3 Group Matching

The group matcher matches against the group the rule was loaded from. Basically this is the filename without the leading path or file extension. Example:

```
group:emerging-icmp.rules
group:emerging-dos
```

Wild card matching similar to wildcards used in a Unix shell can also be used:

```
group:*deleted*
```

2.4.4 Filename Matching

The filename matcher matches against the filename the rule was loaded from taking into consideration the full path. Shell wildcard patterns are allowed:

```
filename:rules/*deleted*
filename:*/emerging-dos.rules
```

2.4.5 Modifying Rules

Rule modification can be done with regular expression search and replace. The basic format for a rule modification specifier is:

```
<match> <from> <to>
```

where <match> is one of the rule matchers from above, <from> is the text to be replaced and <to> is the replacement text.

Example converting all alert rules to drop:

```
re:. ^alert drop
```

Example converting all drop rules with noalert back to alert:

```
re:. "^drop(.*)noalert(.*)" "alert\\1noalert\\2"
```

2.5 Example Configuration Files

2.5.1 Example Configuration File (/etc/suricata/update.yaml)

```
# Configuration with disable filters.
# - Overrided by --disable-conf
# - Default: /etc/suricata/disable.conf
disable-conf: /etc/suricata/disable.conf

# Configuration with enable filters.
# - Overrided by --enable-conf
# - Default: /etc/suricata/enable.conf
enable-conf: /etc/suricata/enable.conf

# Configuration with drop filters.
# - Overrided by --drop-conf
# - Default: /etc/suricata/drop.conf
drop-conf: /etc/suricata/drop.conf

# Configuration with modify filters.
# - Overrided by --modify-conf
# - Default: /etc/suricata/modify.conf
modify-conf: /etc/suricata/modify.conf

# List of files to ignore. Overrided by the --ignore command line option.
ignore:
  - "*deleted.rules"

# Provide an alternate command to the default test command.
#
# The following environment variables can be used.
# SURICATA_PATH - The path to the discovered suricata program.
# OUTPUT_DIR - The directory the rules are written to.
# OUTPUT_FILENAME - The name of the rule file. Will be empty if the rules
#                   were not merged.
#test-command: ${SURICATA_PATH} -T -S ${OUTPUT_FILENAME} -l /tmp

# Provide a command to reload the Suricata rules.
# May be overrided by the --reload-command command line option.
#reload-command: sudo systemctl reload suricata

# Remote rule sources. Simply a list of URLs.
sources:
  # Emerging Threats Open with the Suricata version dynamically replaced.
```

```
  - https://rules.emergingthreats.net/open/suricata-%(__version__)s/emerging.rules.
↪tar.gz
  # The SSL blacklist, which is just a standalone rule file.
  - https://sslbl.abuse.ch/blacklist/sslblacklist.rules

# A list of local rule sources. Each entry can be a rule file, a
# directory or a wild card specification.
local:
  # A directory of rules.
  - /etc/suricata/rules
  # A single rule file.
  - /etc/suricata/rules/app-layer-events.rules
  # A wildcard.
  - /etc/suricata/rules/*.rules
```

2.5.2 Example Configuration to Enable Rules (–enable-conf)

```
# suricata-update - enable.conf

# Example of enabling a rule by signature ID (gid is optional).
# 1:2019401
# 2019401

# Example of enabling a rule by regular expression.
# - All regular expression matches are case insensitive.
# re:heartbleed
# re:MS(0[7-9]|10)-\d+

# Examples of enabling a group of rules.
# group:emerging-icmp.rules
# group:emerging-dos
# group:emerging*
```

2.5.3 Example Configuration to Enable Disable (–disable-conf)

```
# suricata-update - disable.conf

# Example of disabling a rule by signature ID (gid is optional).
# 1:2019401
# 2019401

# Example of disabling a rule by regular expression.
# - All regular expression matches are case insensitive.
# re:heartbleed
# re:MS(0[7-9]|10)-\d+

# Examples of disabling a group of rules.
# group:emerging-icmp.rules
# group:emerging-dos
# group:emerging*
```

2.5.4 Example Configuration to convert Rules to Drop (–drop-conf)

```
# suricata-update - drop.conf
#
# Rules matching specifiers in this file will be converted to drop rules.
#
# Examples:
#
# 1:2019401
# 2019401
#
# re:heartbleed
# re:MS(0[7-9]|10)-\d+
```

2.5.5 Example Configuration to modify Rules (–modify-conf)

```
# suricata-update - modify.conf

# Format: <sid> "<from>" "<to>"

# Example changing the seconds for rule 2019401 to 3600.
#2019401 "seconds \d+" "seconds 3600"

# Change all trojan-activity rules to drop. Its better to setup a
# drop.conf for this, but this does show the use of back references.
#re:classtype:trojan-activity "(alert)(.*)" "drop\\2"

# For compatibility, most Oinkmaster modifysid lines should work as
# well.
#modifysid * "^drop(.*)noalert(.*)" | "alert${1}noalert${2}"
```

CHAPTER 3

update-sources - Update the source index

3.1 Synopsis

```
suricata-update update-sources
```

3.2 Description

The `update-sources` command downloads the latest index of available sources.

3.3 Options

`-q, --quiet`
Run quietly. Only warning and error messages will be displayed.

`-v, --verbose`
Provide more verbose output.

3.4 Files and Directories

`/var/lib/suricata/rules/.cache/index.yaml` Where the downloaded source index is cached.

3.5 Environment Variables

SOURCE_INDEX_URL This environment variable allows the specification of an alternate URL to download the index from.

3.6 URLs

https://raw.githubusercontent.com/jasonish/suricata-intel-index/master/index.yaml
The default URL used to download the index from.

CHAPTER 4

enable-source - Enable a source

4.1 Synopsis

```
suricata-update enable-source <source-name> [param=val ...]
```

4.2 Description

Enable a source that is listed in the index.

If the index requires user provided parameters the user will be prompted for them. Alternatively they can be provided on command line to avoid the prompt.

For example:

```
suricata-update enable-source et/pro secret-code=xxxxxxxxxxxxxxxx
```

This will prevent the prompt for the et/pro secret code using the value provided on the command line instead.

CHAPTER 5

add-source - Add a source by URL

5.1 Synopsis

```
suricata-update add-source <name> <url>
```

5.2 Description

The `add-source` adds a source to the set of enabled sources by URL. It is useful to add a source that is not provided in the index.

5.3 Options

-q, --quiet
Run quietly. Only warning and error messages will be displayed.

-v, --verbose
Provide more verbose output.

CHAPTER 6

disable-source - Disable an enabled source

6.1 Synopsis

```
suricata-update disable-source <name>
```

6.2 Description

The `disable-source` command disables a currently enabled source. The configuration for the source is not removed, allowing it to be re-enabled without having to re-enter any required parameters.

CHAPTER 7

remove-source - Remove a configured source

7.1 Synopsis

```
suricata-update remove-source <name>
```

7.2 Description

Remove a source configuration. This removes the source file from `/var/lib/suricata/update/sources`, even if its disabled.

Index

Symbols

C