dmarc_report

Release 7.0.1

Gene C

Jan 06, 2026

CONTENTS

CHAPTER

ONE

DMARC_REPORT

1.1 Overview

Generate a human readable report from 1 or more standard DMARC and TLS-RPT xml email reports . DMARC reports are made using *dmarc-rpt* while TLS-RPTs use *tls-rpt*

Note:

> All git tags are signed by <arch@sapience.com>. Public key is available via WKD or download from website: https://www.sapience.com/tech After key is on keyring use the PKGBUILD source line ending with *?signed* or manually verify using *git tag -v <tag-name>*

1.2 New / Interesting

7.0.0

- Switch packaging from hatch to uv
- License GPL-2.0-or-later
- Reorg source code

6.x

- Tidy ups: PEP-8, PEP-257, PEP-484 PEP-561
- And Reorganize code especially for PEP-561 (type hints)
- Has passed all tests here, so hopefully no problems. But, always some risk cleaning up code - please let me know if something is not right.

Interesting

- New config file format using single config file. Older 2 fille configs will be automatically converted to the new version 2 format. See *config_files_section* section and *configs* directory for sample config.
- Switch to *py-cidr* package for handling IPs instead of own versions.
- Available - github <https://github.com/gene-git/py-cidr> - AUR <https://aur.archlinux.org/packages/py-cidr>
- Now use python 3's ipaddress module instead of netaddr. Its faster and we no longer require 3rd party library
- Require python version 3.11 or later
- Switch to lxml for better handling of xml namespaces found in some reports
- Add support for handling mbox file with multiple emails containing reports. While some clients save multiple emails in separate *.eml* files, others, like evolution, save them all in a single *.mbox* file. Add support for this.

- tls-rpt

  New tool to generate report for TLS reports for MTA-STS or DANE. See README-tls.md This report has been updated - see Changelog for details.

CHAPTER

TWO

GETTING STARTED

2.1 Applications

Save all DMARC or TLS-RPT reports into a directory. These are typically compressed xml/json files sent as email attachments. The saved reports can be :

- individual email files each with a compressed xml/json attachment. Thunderbird saves them this way. These are saved with a *.eml* extension.
- one single file with several emails, each with the attachment. Evolution saves this way. These are saved with *.mbox* extension.
- Individual compressed, or uncmompressed, xml reports created by saving the attachments from each email.

dmarc-rpt and *tls-rpt* will extract the actual **xml** (*dmarc*) or **json** (tls-rpt) data from all of the above.

2.1.1 Quick start

Save all emails with DMARC or TLS-RPT attachments to a directory, change into that directory and run either dmarc-rpt or tls-rpt as appropriate.

It is generally more convenient to use a config file explained below.

2.1.2 Config Files

Config files are read, in order, from directories :

```
/etc/dmarc_report/
~/.config/dmarc_report/
```

with the settings in latter *~/.config/...* overriding any found in */etc/...*.

There are 2 config file formats supported. The older version 1 format uses 2 separate files:

- *config* - for dmarc-rpt
- *tls-config* - for tls-rpt

New version 2 format uses a single file, *config.v2*. Version 2 config will be used if its found. If only version 1 configs are found they will be automatically converted to version 2, which will then be used going forward.

All config files use standard TOML format. Config files use 3 sections. A global section and one each for dmarc and tls-rpt.

Available config values are set using:

```
command_line_long_opt_name = xxx
```

e.g. to set data report dir use:

```
dir = "/foo/goo/dmarc_reports"
```

A sample config is available in the *conf.d* directory. A typical config might be of the form:

```
# comment
[global]
    theme = 'dark'
    inp_files_disp = "save"
    inp_files_save_dir = "../saved"

[dmarc]
    dom_ips = ['1.1.1.1', '1.2.2.0/24']
    dir = "~/mail-reports/dmarc/xml"

[tls]
    dir = "~/mail-reports/tls/xml"
```

Variables set in *[dmarc]* or *[tls]* sections override any correspodning global ones.

This sample config says to read all the saved dmarc email reports from *~/mail-reports/dmarc/xml* and the tls reports from *~/mail-reports/tls/xml*.

And to save the raw files after processing report by moving them to *~/mail-reports/dmarc/saved* or *~/mail-reports/tls/saved*.

For dmarc it says that ips listed in *dom_ips* are for your own domains.

Command line options override the corresponding config setting. See *Options* section for more detail.

2.1.3 dmarc-rpt Usage

Change to the directory containing the one or more dmarc report files and simply run

```
dmarc-rpt
```

When using the *–dir* option (or config setting *dir*) it is not necessary to change directories before running the report.

Any email files, those ending with *.eml* will be processed first. These are assumed to contain the report as a mime attachment. The attachment is extracted from any such email files. Some mail clients save multiple emails as a single mbox file. Each email in the mbox file will be similarly processed and have the attached report extracted.

Then all remaining files are read and processed. The tool processes all xml and gzip/zip compressed xml dmarc report files and generates a human readable report.

We follow Postel's law and try to be liberal in what we accept as input. To that end we accept the dmarc XML report file, a gzip/zip compressed version of same or a saved email file text file with the report itself being a mime attachment.

Any file with extension *.eml* is treated as an email file.

To avoid line wrapping, the report should be viewed on wide enough terminal; roughly 112 or chars or more.

For convenience after report is generated, the input files can be automatically moved to a save direcory, left where they are or removed. A typical sequents of events is to save the email reports, run dmarc-rpt. By auto moving (or removing) the input files, makes it simpler when doing the next batch of dmarc reports.

Then save all the raw .eml files into ~/dmarc/reports and run before running the report

```
dmarc-rpt
```

All attachments from dmarc email reports would be saved into "~/dmarc/saved/2023-01" in this example.

2.1.4 tls-rpt Usage

tls-rpt works in a similar way to dmarc-rpt, except it operates on TLS-RPT (compressed) xml inputs.

Command line options are shown first in parens below, followed by the corresponding config version in square brackets, if available.

2.1.5 Common Options

These apply to both dmarc-rpt and tls-rpt

- (*-h, –help*) Help for command line options.
- (*-d, –dir*) [*dir = /path/xxx/*]

  Allows specifying the directory with the dmarc report files to be processed. The directory holding the report files (.eml, .xml, .gz or .zip) By default, dir is the current directory.

- (*-k, –keep*)

  Prevent the *.eml* being removed after the attached xml reports are extracted.

- (*-thm, –theme*)

  Report is now in color. Default theme is 'dark'. Theme can be 'light' 'dark' or 'none', which turns off color report.

- (*-v, –verb*)

  More verbose output

- (*-ifd, –inp_file_disp*)

  Input file disposition options one of : none,save,delete If set to save then all input files (xml, compressed xml and any kept eml files) are moved to directory specified by *inp_files_save_dir*.

- (*-ifsd, –inp_files_save_dir*)

  When *inp_file_disp* is set, then input files are moved to this directory after report is generated. Files are saved by year-month under the save directory

2.1.6 dmarc-rpt Specific Options

These are only applicable for dmarc-rpt.

- (*-ips, –dom_ips*) [*dom_ips = [ip, cidr, . . .]*]

  Set the ips for your own domain(s), which will then be colored to make them easy to spot. Command line option is a comma separated list of IPs. e.g.:

```
    --dom_ips "1.1.1.0/24,2.2.2.16/29"

When used in config file format as array of IP stringsC.
e.g.::

     dom_ips = ['1.1.1.0/24', '2.2.2.16/29']
```

- (*fdm, –dmarc_fails*)

  Only include dmarc failures in report

- (*fdk, –dkim_fails*)

  Only include dkim failures in report

- (*fsp, –spf_fails*)

  Only include spf failures in report

2.2 Saving Email Reports From Email Client

In most mail clients, such as thunderbird, one can select multiple email reports and then use *File -> Save As* to save the email files into a directory of your choosing. Each email gets saved with a *.eml* extension.

CHAPTER

THREE

APPENDIX

3.1 Dependencies

- Run Time : * python (3.13 or later) * python-dateutil * python-lxml * py-cidr (2.7.0 or later) * tomli-w (for writing version 2 configs converted from version 1)
- Building Package: * git * wheel (aka python-wheel) * build (aka python-build) * installer (aka python-installer) * poetry (aka python-poetry) - rsync
- Optional for building docs:
  - sphinx
  - texlive-latexextra (archlinux packaguing of texlive tools)

3.2 Installation

Available on

- Github
- Archlinux AUR

On Arch you can build using the PKGBUILD provided in packaging directory or from the AUR package. To build manually, clone the repo and

```
rm -f dist/*
python -m build --wheel --no-isolation
root_dest="/"
./scripts/do-install $root_dest
```

When running as non-root then set root_dest a user writable directory

3.3 Philosophy

We follow the *live at head commit* philosophy as recommended by Google's Abseil team[1]. This means we recommend using the latest commit on git master branch.

[1] https://abseil.io/about/philosophy#upgrade-support

3.4 License

Created by Gene C. and licensed under the terms of the GPL-2.0-or-later license.

- SPDX-License-Identifier: GPL-2.0-or-later
- Copyright (c) 2023, Gene C

CHAPTER

FOUR

SMTP TLS-RPT

4.1 Overview

Generate a human readable tls report from one or more standard tls report files. These reports are used for a email domain with support for either DANE or MTA-STS or both.

4.1.1 Usage

Run from command line: .. code-block:: bash

    tls-rpt

Generates reports from one or more emailed tls reports. Similar to dmarc-rpt, the tool can consume email files (.eml) or the json attachments (plain or compressed) delivered as part of the usual mts-sts reports - and in directory specified by *inp_files_save_dir*.

tls-rpt is provided as part of the dmarc_report package

Background

TLS Reports are oprionally generated for a mail domaain when so requested by a TXT record in the domain's DNS. The tool parses and summarizes such email reports for human consumption.

SMTP TLS reporting is described by [RFC 8460][1] where it summarizes:

```
A number of protocols exist for establishing encrypted channels
between SMTP Mail Transfer Agents (MTAs), including STARTTLS, DNS-
Based Authentication of Named Entities (DANE) TLSA, and MTA Strict
Transport Security (MTA-STS).
```

MTA-STS, is explained by [RFC 8641][2] where it is summarized:

```
SMTP MTA Strict Transport Security (MTA-STS) is a mechanism enabling
mail service providers (SPs) to declare their ability to receive
Transport Layer Security (TLS) secure SMTP connections and to specify
whether sending SMTP servers should refuse to deliver to MX hosts
that do not offer TLS with a trusted server certificate.
```

while DANE is documented in [RFC 6698][3], [RFC 7671][4] and [RFC 7672][5]

[1] TLS Report [RFRC 8460] https://www.rfc-editor.org/rfc/rfc8460.txt
[2] MTA-STS [RFC 8461] https://www.rfc-editor.org/rfc/rfc8461.txt
[3] DANE [RFC 6698] https://www.rfc-editor.org/rfc/rfc6698.txt
[4] DANE [RFC 7671] https://www.rfc-editor.org/rfc/rfc7671.txt
[5] DANE SMTP [RFC 7672] https://www.rfc-editor.org/rfc/rfc7672.txt

```
Encrypted communication on the Internet often uses Transport Layer
Security (TLS), which depends on third parties to certify the keys
used.  This document improves on that situation by enabling the
administrators of domain names to specify the keys used in that
domain's TLS servers.  This requires matching improvements in TLS
client software, but no change in TLS server software
```

Discussion

To receive TLS reports requires a DNS record requesting a TLS report along with either a DANE TLSA record or MTA-STS. MTA-STS requires both a policy and and a DNS record.

4.1.2 TLS Report DNS Record

Example

_smtp._tls.example.org IN TXT "v=TLSRPTv1;rua=mailto:tlsrpt@example.com"

The TLS reports will be sent to the email provided by the string following *rua=*. In this example reports would be sent to *tlsrpt@example.com*.

4.1.3 MTA-STS

Requieres both a DNS record and a policy file available from the email's domain web server.

Policy file example to be provided by web server:

```
https://mta-sts.example.com/.well-known/mta-sts.txt
```

The policy mode can be set to *enforce* or *testing*. Example *mta-sts.txt* file:

```
version: STSv1
mode: enforce
mx: example.com
mx: \*.example.com
max_age: 1296000
```

DNS TXT record example:

```
_mta-sts.example.org.  IN TXT "v=STSv1; id=202301011200;"
```

4.1.4 DANE TLSA

DNS record example:

```
_25._tcp.example.com. TLSA 3 1 1 (xxx)
```

where xxx would be the appropriate public key hash.

Using tls-rpt

Save all tls email reports into a directory. Change to the directory containing one or more dmarc report files and simply run .. code-block:: back

tls-rpt

Using the –dir option (or setging the config option *dir*) makes unnecessary to change directories before running the report.

Any email files, those ending with *.eml* will be processed first. These are assumed to contain the dmarc report as a mime attachment. The attachment is extracted from such email files.

Subsequently, all remaining files are read and processed. The tool processes all json and gzip/zip compressed json tls report files and produces a human readable report.

Any file with extension *.eml* is treated as an email file.

For convenience after report is generated, the input files can be automatically moved to a save direcory, left where they are or removed. A typical sequents of eveents is to save the email reports, run dmarc-rpt. By auto moving (or removing) the input files, makes it simpler when doing the next batch of dmarc reports.

For example, you might save all .eml files in same directory and with config settings:

```
dir = "~/tlsrpt/reports"
inp_files_disp = "save"
inp_files_save_dir = "../saved"
```

Then save all the raw .eml files into ~/tlsrpt/reports and run

```
tls-rpt
```

All attachments from email reports would be saved into "~/tlsrpt/saved/2023-01" in this example.

4.1.5 tls-rpt Options

Options are read first from config files then command line. Config files are read from */etc/dmarc_report/config-tls* then *~/.config/dmarc_report/config-tls*. Config files are in standard TOML format.

Config settings use corresponding command line option:

```
long-option = xxx.
```

e.g. to set data report dir in config use

```
dir = /foo/goo/other
```

The command line options are shown first in parens followed by corresponding config in square brackets if available.

- (*-d, –dir*) [*dir = /some/path*]

  Allows specifying the directory with the dmarc report files to be processed. The directory holding the report files (.eml, .json, .gz or .zip) By default, dir is the current directory.

- (*-k, –keep*) [*keep = true*]

  Prevent the *.eml* being removed after the attached xml reports are extracted.

- (*-thm, –theme*)

  Report is now in color. Default theme is 'dark'. Theme can be 'light' 'dark' or 'none', which turns off color report.

- (*-ifd, –inp_file_disp*)

  Input file disposition options one of : none,save,delete If set to save then all input files (xml, compressed xml and any kept eml files) are moved to directory specified by *inp_files_save_dir*.

- (*-ifsd, –inp_files_save_dir*)

  When *inp_file_disp* is set, then input files are moved to this directory after report is generated. Files are saved by year-month under the save directory

- (*-h, –help*)

  Help for command line options.

4.1.6 Saving Email Reports From Email Client

In most mail clients, such as thunderbird, one can select multiple email reports and then use *File -> Save As* to save the email files into a directory of your choosing. Each email gets saved with a *.eml* extension.

4.1.7 License

CHAPTER

FIVE

LICENSE

mkpkg is a an Archlinux package build tool.