MyWebUniversity
python
Rocky Linux
Manual Pages
FPDF Library
PDF generator
FPDF
Full credit is given to the above companies including the OS that this PDF file was generated!

Rocky Enterprise Linux 9.2 Manual Pages on command 'danetool.1'

$ man danetool.1

```
danetool(1)                User Commands                danetool(1)

NAME

    danetool - GnuTLS DANE tool

SYNOPSIS

    danetool [-flags] [-flag [value]] [--option-name[[=| ]value]]

    All arguments must be options.

DESCRIPTION

    Tool to generate and check DNS resource records for the DANE protocol.

OPTIONS

    -d num, --debug=num

        Enable  debugging.   This  option takes an integer number as its

        argument.  The value of num is constrained to being:

            in the range 0 through 9999

        Specifies the debug level.

    -V, --verbose

        More verbose output.

    --outfile=str

        Output file.
```

--load-pubkey=str

Loads a public key file.

This can be either a file or a PKCS #11 URL

--load-certificate=str

Loads a certificate file.

This can be either a file or a PKCS #11 URL

--dlv=str

Sets a DLV file.

This sets a DLV file to be used for DNSSEC verification.

--hash=str

Hash algorithm to use for signing.

Available hash functions are SHA1, RMD160, SHA256, SHA384,
SHA512.

--check=str

Check a host's DANE TLSA entry.

Obtains the DANE TLSA entry from the given hostname and prints
information. Note that the actual certificate of the host can be
provided using --load-certificate, otherwise danetool will con?
nect to the server to obtain it. The exit code on verification
success will be zero.

--check-ee

Check only the end-entity's certificate.

Checks the end-entity's certificate only. Trust anchors or CAs
are not considered.

--check-ca

Check only the CA's certificate.

Checks the trust anchor's and CA's certificate only. End-enti?
ties are not considered.

--tlsa-rr

Print the DANE RR data on a certificate or public key. This op?
tion must appear in combination with the following options:
host.

This command prints the DANE RR data needed to enable DANE on a

DNS server.

--host=hostname

Specify the hostname to be used in the DANE RR.

This command sets the hostname for the DANE RR.

--proto=protocol

The protocol set for DANE data (tcp, udp etc.).

This command specifies the protocol for the service set in the DANE data.

--port=str

The port or service to connect to, for DANE data.

--app-proto

This is an alias for the --starttls-proto option.

--starttls-proto=str

The application protocol to be used to obtain the server's certificate (https, ftp, smtp, imap, ldap, xmpp, lmtp, pop3, nntp, sieve, postgres).

When the server's certificate isn't provided danetool will connect to the server to obtain the certificate. In that case it is required to know the protocol to talk with the server prior to initiating the TLS handshake.

--ca Whether the provided certificate or public key is a Certificate Authority.

Marks the DANE RR as a CA certificate if specified.

--x509 Use the hash of the X.509 certificate, rather than the public key.

This option forces the generated record to contain the hash of the full X.509 certificate. By default only the hash of the public key is used.

--local

This is an alias for the --domain option.

--domain, --no-domain

The provided certificate or public key is issued by the local domain. The no-domain form will disable the option. This op?

tion is enabled by default.

DANE distinguishes certificates and public keys offered via the DNSSEC to trusted and local entities. This flag indicates that this is a domain-issued certificate, meaning that there could be no CA involved.

--local-dns, --no-local-dns

Use the local DNS server for DNSSEC resolving. The no-local-dns form will disable the option.

This option will use the local DNS server for DNSSEC. This is disabled by default due to many servers not allowing DNSSEC.

--insecure

Do not verify any DNSSEC signature.

Ignores any DNSSEC signature verification results.

--inder, --no-inder

Use DER format for input certificates and private keys. The no-inder form will disable the option.

The input files will be assumed to be in DER or RAW format. Un?like options that in PEM input would allow multiple input data (e.g. multiple certificates), when reading in DER format a sin?gle data structure is read.

--inraw

This is an alias for the --inder option.

--print-raw, --no-print-raw

Print the received DANE data in raw format. The no-print-raw form will disable the option.

This option will print the received DANE data.

--quiet

Suppress several informational messages.

In that case on the exit code can be used as an indication of verification success

-v arg, --version=arg

Output version of program and exit. The default mode is `v', a simple version.  The `c' mode will print copyright information and `n' will print the full copyright notice.

-h, --help

Display usage information and exit.

-!, --more-help

Pass the extended usage information through a pager.

EXAMPLES

DANE TLSA RR generation

To create a DANE TLSA resource record for a certificate (or public key) that was issued localy and may or may not be signed by a CA use the following command.

```
$ danetool --tlsa-rr --host www.example.com --load-certificate cert.pem
```

To create a DANE TLSA resource record for a CA signed certificate, which will be marked as such use the following command.

```
$ danetool --tlsa-rr --host www.example.com --load-certificate cert.pem   --no-domain
```

The former is useful to add in your DNS entry even if your certificate is signed by a CA. That way even users who do not trust your CA will be able to verify your certificate using DANE.

In order to create a record for the CA signer of your certificate use the following.

```
$ danetool --tlsa-rr --host www.example.com --load-certificate cert.pem   --ca --no-domain
```

To read a server's DANE TLSA entry, use:

```
$ danetool --check www.example.com --proto tcp --port 443
```

To verify an HTTPS server's DANE TLSA entry, use:

```
$ danetool --check www.example.com --proto tcp --port 443 --load-certificate chain.pem
```

To verify an SMTP server's DANE TLSA entry, use:

```
$ danetool --check www.example.com --proto tcp --starttls-proto=smtp --load-certificate chain.pem
```

EXIT STATUS

One of the following exit values will be returned:

0 (EXIT_SUCCESS)

Successful program execution.

1 (EXIT_FAILURE)

The operation failed or the command syntax was not valid.

SEE ALSO

certtool (1)

AUTHORS

COPYRIGHT

BUGS

Please send bug reports to: bugs@gnutls.org