NAME

posttls-finger - Probe the TLS properties of an ESMTP or LMTP server.

SYNOPSIS

posttls-finger [*options*] [**inet:**]*domain*[:*port*] [*match* ...]
posttls-finger -S [*options*] **unix:***pathname* [*match* ...]

DESCRIPTION

posttls-finger(1) connects to the specified destination and reports TLS-related information about the server. With SMTP, the destination is a domainname; with LMTP it is either a domainname prefixed with **inet:** or a pathname prefixed with **unix:**. If Postfix is built without TLS support, the resulting posttls-finger program has very limited functionality, and only the **-a**, **-c**, **-h**, **-o**, **-S**, **-t**, **-T** and **-v** options are available.

Note: this is an unsupported test program. No attempt is made to maintain compatibility between successive versions.

For SMTP servers that don't support ESMTP, only the greeting banner and the negative EHLO response are reported. Otherwise, the reported EHLO response details further server capabilities.

If TLS support is enabled when **posttls-finger(1)** is compiled, and the server supports **STARTTLS**, a TLS handshake is attempted.

If DNSSEC support is available, the connection TLS security level (**-l** option) defaults to **dane**; see TLS_README for details. Otherwise, it defaults to **secure**. This setting determines the certificate matching policy.

If TLS negotiation succeeds, the TLS protocol and cipher details are reported. The server certificate is then verified in accordance with the policy at the chosen (or default) security level. With public CA-based trust, when the **-L** option includes **certmatch**, (true by default) name matching is performed even if the certificate chain is not trusted. This logs the names found in the remote SMTP server certificate and which if any would match, were the certificate chain trusted.

Note: **posttls-finger(1)** does not perform any table lookups, so the TLS policy table and obsolete per-site tables are not consulted. It does not communicate with the **tlsmgr(8)** daemon (or any other Postfix daemons); its TLS session cache is held in private memory, and disappears when the process exits.

With the **-r** *delay* option, if the server assigns a TLS session id, the TLS session is cached. The connection is then closed and re-opened after the specified delay, and **posttls-finger(1)** then reports whether the cached TLS session was re-used.

When the destination is a load balancer, it may be distributing load between multiple server caches. Typically, each server returns its unique name in its EHLO response. If, upon reconnecting with **-r**, a new server name is detected, another session is cached for the new server, and the reconnect is repeated up to a maximum number of times (default 5) that can be specified via the **-m** option.

The choice of SMTP or LMTP (**-S** option) determines the syntax of the destination argument. With SMTP, one can specify a service on a non-default port as *host*:*service*, and disable MX (mail exchanger) DNS lookups with [*host*] or [*host*]:*port*. The [] form is required when you specify an IP address instead of a hostname. An IPv6 address takes the form [**ipv6:***address*]. The default port for SMTP is taken from the **smtp/tcp** entry in /etc/services, defaulting to 25 if the entry is not found.

With LMTP, specify **unix:***pathname* to connect to a local server listening on a unix-domain socket bound to the specified pathname; otherwise, specify an optional **inet:** prefix followed by a *domain* and an optional port, with the same syntax as for SMTP. The default TCP port for LMTP is 24.

Arguments:

-a *family* (default: **any**)
Address family preference: **ipv4**, **ipv6** or **any**. When using **any**, posttls-finger will randomly select one of the two as the more preferred, and exhaust all MX preferences for the first address family before trying any addresses for the other.

-A *trust-anchor.pem* (default: none)
A list of PEM trust-anchor files that overrides CAfile and CApath trust chain verification. Specify the option multiple times to specify multiple files. See the main.cf documentation for smtp_tls_trust_anchor_file for details.

-c Disable SMTP chat logging; only TLS-related information is logged.

-C Print the remote SMTP server certificate trust chain in PEM format. The issuer DN, subject DN, certificate and public key fingerprints (see **-d** *mdalg* option below) are printed above each PEM certificate block. If you specify **-F** *CAfile* or **-P** *CApath*, the OpenSSL library may augment the chain with missing issuer certificates. To see the actual chain sent by the remote SMTP server leave *CAfile* and *CApath* unset.

-d *mdalg* (default: **sha1**)
The message digest algorithm to use for reporting remote SMTP server fingerprints and matching against user provided certificate fingerprints (with DANE TLSA records the algorithm is specified in the DNS).

-f Lookup the associated DANE TLSA RRset even when a hostname is not an alias and its address records lie in an unsigned zone. See smtp_tls_force_insecure_host_tlsa_lookup for details.

-F *CAfile.pem* (default: none)
The PEM formatted CAfile for remote SMTP server certificate verification. By default no CAfile is used and no public CAs are trusted.

-g *grade* (default: medium)
The minimum TLS cipher grade used by posttls-finger. See smtp_tls_mandatory_ciphers for details.

-h *host_lookup* (default: **dns**)
The hostname lookup methods used for the connection. See the documentation of smtp_host_lookup for syntax and semantics.

-k *certfile* (default: *keyfile*)
File with PEM-encoded TLS client certificate chain. This defaults to *keyfile* if one is specified.

-K *keyfile* (default: *certfile*)
File with PEM-encoded TLS client private key. This defaults to *certfile* if one is specified.

-l *level* (default: **dane** or **secure**)
The security level for the connection, default **dane** or **secure** depending on whether DNSSEC is available. For syntax and semantics, see the documentation of smtp_tls_security_level. When **dane** or **dane-only** is supported and selected, if no TLSA records are found, or all the records found are unusable, the *secure* level will be used instead. The **fingerprint** security level allows you to test certificate or public-key fingerprint matches before you deploy them in the policy table.

Note, since **posttls-finger** does not actually deliver any email, the **none**, **may** and **encrypt** security levels are not very useful. Since **may** and **encrypt** don't require peer certificates, they will often negotiate anonymous TLS ciphersuites, so you won't learn much about the remote SMTP server's certificates at these levels if it also supports anonymous TLS (though you may learn that the server supports anonymous TLS).

-L *logopts* (default: **routine,certmatch**)
Fine-grained TLS logging options. To tune the TLS features logged during the TLS handshake, specify one or more of:

0, none These yield no TLS logging; you'll generally want more, but this is handy if you just want the trust chain:
$ posttls-finger -cC -L none destination

1, routine, summary
These synonymous values yield a normal one-line summary of the TLS connection.

2, debug
These synonymous values combine routine, ssl-debug, cache and verbose.

3, ssl-expert
These synonymous values combine debug with ssl-handshake-packet-dump. For experts only.

4, ssl-developer
These synonymous values combine ssl-expert with ssl-session-packet-dump. For experts only, and in most cases, use wireshark instead.

ssl-debug
Turn on OpenSSL logging of the progress of the SSL handshake.

ssl-handshake-packet-dump
Log hexadecimal packet dumps of the SSL handshake; for experts only.

ssl-session-packet-dump
Log hexadecimal packet dumps of the entire SSL session; only useful to those who can debug SSL protocol problems from hex dumps.

untrusted
Logs trust chain verification problems. This is turned on automatically at security levels that use peer names signed by Certification Authorities to validate certificates. So while this setting is recognized, you should never need to set it explicitly.

peercert
This logs a one line summary of the remote SMTP server certificate subject, issuer, and fingerprints.

certmatch
This logs remote SMTP server certificate matching, showing the CN and each subjectAltName and which name matched. With DANE, logs matching of TLSA record trust-anchor and end-entity certificates.

cache This logs session cache operations, showing whether session caching is effective with the remote SMTP server. Automatically used when reconnecting with the **-r** option; rarely needs to be set explicitly.

verbose
Enables verbose logging in the Postfix TLS driver; includes all of peercert..cache and more.

The default is **routine,certmatch**. After a reconnect, **peercert**, **certmatch** and **verbose** are automatically disabled while **cache** and **summary** are enabled.

-m *count* (default: **5**)
When the **-r** *delay* option is specified, the **-m** option determines the maximum number of reconnect attempts to use with a server behind a load balancer, to see whether connection caching is likely to be effective for this destination. Some MTAs don't expose the underlying server identity in their EHLO response; with these servers there will never be more than 1 reconnection attempt.

-M *insecure_mx_policy* (default: **dane**)
The TLS policy for MX hosts with "secure" TLSA records when the nexthop destination security level is **dane**, but the MX record was found via an "insecure" MX lookup. See the main.cf documentation for smtp_tls_insecure_mx_policy for details.

-o *name=value*
Specify zero or more times to override the value of the main.cf parameter *name* with *value*. Possible use-cases include overriding the values of TLS library parameters, or "myhostname" to configure the SMTP EHLO name sent to the remote server.

-p *protocols* (default: !SSLv2)
List of TLS protocols that posttls-finger will exclude or include. See smtp_tls_mandatory_protocols for details.

-P *CApath/* (default: none)
The OpenSSL CApath/ directory (indexed via c_rehash(1) for remote SMTP server certificate verification. By default no CApath is used and no public CAs are trusted.

-r *delay*
With a cacheable TLS session, disconnect and reconnect after *delay* seconds. Report whether the session is re-used. Retry if a new server is encountered, up to 5 times or as specified with the **-m** option. By default reconnection is disabled, specify a positive delay to enable this behavior.

-S Disable SMTP; that is, connect to an LMTP server. The default port for LMTP over TCP is 24. Alternative ports can specified by appending "*:servicename*" or "*:portnumber*" to the destination argument.

-t *timeout* (default: **30**)
The TCP connection timeout to use. This is also the timeout for reading the remote server's 220 banner.

-T *timeout* (default: **30**)
The SMTP/LMTP command timeout for EHLO/LHLO, STARTTLS and QUIT.

-v Enable verbose Postfix logging. Specify more than once to increase the level of verbose logging.

-w Enable outgoing TLS wrapper mode, or SMTPS support. This is typically provided on port 465 by servers that are compatible with the ad-hoc SMTP in SSL protocol, rather than the standard STARTTLS protocol. The destination *domain*:*port* should of course provide such a service.

[**inet:**]*domain*[:*port*]
Connect via TCP to domain *domain*, port *port*. The default port is **smtp** (or 24 with LMTP). With SMTP an MX lookup is performed to resolve the domain to a host, unless the domain is enclosed in **[]**. If you want to connect to a specific MX host, for instance *mx1.example.com*, specify [*mx1.example.com*] as the destination and *example.com* as a **match** argument. When using DNS, the destination domain is assumed fully qualified and no default domain or search suffixes are applied; you must use fully-qualified names or also enable **native** host lookups (these don't support **dane** or **dane-only** as no DNSSEC validation information is available via **native** lookups).

unix:*pathname*
Connect to the UNIX-domain socket at *pathname*. LMTP only.

match ...
With no match arguments specified, certificate peername matching uses the compiled-in default strategies for each security level. If you specify one or more arguments, these will be used as the list of certificate or public-key digests to match for the **fingerprint** level, or as the list of DNS names to match in the certificate at the **verify** and **secure** levels. If the security level is **dane**, or **dane-only** the match names are ignored, and **hostname, nexthop** strategies are used.

ENVIRONMENT

MAIL_CONFIG
Read configuration parameters from a non-default location.

MAIL_VERBOSE
Same as **-v** option.

SEE ALSO

smtp-source(1),
SMTP/LMTP message source
smtp-sink(1),
SMTP/LMTP message dump

README FILES

Use "**postconf readme_directory**" or "**postconf html_directory**" to locate this information.
TLS_README, Postfix STARTTLS howto

LICENSE

The Secure Mailer license must be distributed with this software.

AUTHOR(S)

Wietse Venema
IBM T.J. Watson Research
P.O. Box 704
Yorktown Heights, NY 10598, USA

Viktor Dukhovni