Published on *Jisc community* (https://community-stg.jisc.ac.uk)

Home > Network and technology service docs > Janet Mail Services > Spam-relay Tester And Notification system

Spam-relay Tester And Notification system

Spam-relay Tester And Notification system

This note describes the facilities available to managers of e-mail services for checking that e-mail systems at Janet connected organisations are secure against unauthorised relaying.

Contents [2] | Top [3]

The Janet tester

The Janet mail relay team operate the **S**pam-relay **T**ester **A**nd **N**otification system, which will attempt to connect to your mailer and relay a series of individual messages through it just as the bulk mailers do in preparation for a spam run. It then mails you a report on any vulnerabilities it found.

The tests involve SMTP sessions in which certain sequences of commands are sent to your system and various forms of address are used in attempted message transfers. They include some sequences and addresses which do not conform to the relevant standards (principally RFC 2821 [4] and RFC 2822 [5]). It is possible in principle that the tests might cause your mail system to malfunction, although the danger is no greater than that to which you are exposed merely by connection to JANET or the Internet.

Request a test

To request a series of tests, send a message to relaytest@ja.net [1] with
Subject: relay test
and with a single line in the message body
test <mailer-address>
in which <mailer-address> is the IP address of the Janet mailer you want tested without the enclosing <>.
The IP address should be in the usual "dotted-quad" form - something like:-
test 10.1.1.2

You can request tests on several systems in a single message either by writing more than one address on the line:

test <mailer1-address> <mailer2-address> . . .

or by writing separate lines:

test <mailer1-address>

test <mailer2-address>

. . .

The 'series of tests' refers to the fact the a single test request will generate a series of emails, which comprises just a single test. Each request of this type is a 'one-off' request.

Once it is completed, the request is deleted, although if relaying is found, it will automatically be retested every couple of months until fixed just to make sure the administrator does not forget about it, but the administrator can also request further (one-off) tests any time just by submitting another test request.

If you wish to make regular tests of your mail systems accessible from Janet, please book them by arrangement with the mail relay team at relaytest-admin@ja.net [6]. The test request mechanism is just the same, and you will need to set up some manual or automatic process to send the usual mail messages at the intervals agreed; but the advance scheduling enables operational staff to manage the limited machine resources available. The expected form of scheduling is on an annual cycle with requirements such as
"the third Thursday of each February, May, August and November".

Up | Previous | Contents

When to run tests

You are most likely to use the tester:

- After installing or enhancing the anti-relaying configuration of your mailer.
- After any system or network upgrade, to check that your anti-relaying arrangements are still in place.
- Periodically, to confirm the relaying integrity of your mailers and possibly of other systems and to take advantage of any updates to the tester itself.

Up | Previous | Contents

Conditions of use

- You may only request testing for systems in Janet for which you are an administrator or manager.
- You must inform network security staff and any others you have reason to think may notice testing in progress. Connection attempts come from either of the address blocks 128.86.16/24 or 128.86.8/24 and may have any source port number.
- You agree to the use of your machine's resources which will result from the tests.
- Although these tests are carried out in good faith after extensive development and piloting and are believed harmless to target systems, you accept responsibility for any disruption to your services and for any inconvenience or effort resulting from the tests.
- The results of tests will be mailed back to you, and a copy sent to the Janet mail relay team who may in turn pass them to Janet(UK). Any of these people may use the results to offer you advice, and may discuss with your organization any deficiencies found. Janet(UK) may use for any purpose statistical summaries of results from which no individual organization can be identified. Apart from that, information about tests and results will not be revealed to anyone else.

Up | Previous | Contents

Responses

The address relaytest@ja.net [1] delivers your message to an automatic testing and reporting process. The tester will immediately return a message saying whether or not the test request is authorised.

Test results and reports are sent to the address from which the request came, to *postmaster* at the host address being tested and to *postmaster* at the Janet organization concerned. The result messages will indicate the address from which the test request was received.
If the tests are not complete in a few hours you will also get a progress report.

The elapsed time varies between 20 minutes and two days (or three days over a weekend), depending on the way your mailer reacts. Timing out after a long delay is one way in which it can **pass** some of the tests!

Up | Previous | Contents

Tests which time out

There are a few common circumstances in which testing may take a long time:

- A lot of tests are currently queued.
- The host being tested is down:
  (crashed, powered off, being stolen, *etc*).
- The host being tested is rejecting connections from the test source:
  (SMTP listener has died, unreachable through firewall or similar provisions, refused due to high load, *etc*).

Once a test is queued it attempts to make a connection to the relay being tested. If this fails it will try again later. The test will run for up to two days before timing out.

If a host under test returns a *4XX* SMTP error code (temporary retryable failures) the test message is requeued. The relay team may have to abort any outstanding tests without notice if the relay tester is busy and particular tests stay in this state for more than 12 hours. *4XX* codes are not normally appropriate for relaying refusals except during testing, as they cause the remote machine to hold on to the mail and try again later.

The test sequence will end when one of the following criteria is met:

- A relayed message is detected.
  All outstanding tests to the host will be aborted and an automatic notification sent.
- 60 minutes have passed since the final test message was sent, and no messages have been relayed back.
- 2 days have passed (not including Sundays) since the test started, and no messages have been relayed back.

Up | Previous | Contents

Tests you didn't request

The Janet mail relay team will start tests at once on any Janet system which is reported to them (usually from outside Janet) as having relayed spam.

If the tests discover no vulnerability to relaying, the relay team will respond to the report by asking for further information. If the tests do indicate some vulnerability then the relay team will contact the administrator of the system concerned and will advise on correcting and re-testing it.

It is possible for anyone to ask for a test on any Janet system, and in general such requests will be honoured. However, you must not abuse this service by testing other people's mailers. If you suspect a relaying problem at another site, contact the postmaster or mail administrator concerned and invite them to send their own request.

If it is hard to reach such a person, contact Janet Service Desk [7]instead. If the relaying or other behaviour of another site's mailer seems to you to be an immediate threat to the use of mail in all or part of Janet, the proper contact is Janet-CSIRT [8]

Up | Previous | Contents

Active testing by Janet

From time to time Janet(UK) may consider it necessary to test some large collection of Janet mail systems, in which case a general warning will be given in advance.

Up | Previous | Contents

References

The separate page Janet site e-mail requirements [9] includes some background on e-mail, and explains terms used here.

- RFC is *Request For Comments*
- RFC 2821 [4] *Simple Mail Transfer Protocol* (SMTP)
- RFC 2822 [5] *Internet message format*
- RFC 1123 [10] *Requirements for Internet hosts*
  (updates and clarifications to various earlier RFCs, some of which are included in the more recent mail RFCs above)

Up | Previous | Contents

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/spam-relay-tester-and-notification-system-0

Links
[1] mailto:relaytest@ja.net
[2] https://community.ja.net/library/janet-services-documentation/spam-relay-tester-and-notification-system#content
[3] https://community.ja.net/library/janet-services-documentation/spam-relay-tester-and-notification-system-0#top
[4] http://www.ietf.org/rfc/rfc2821.txt
[5] http://www.ietf.org/rfc/rfc2822.txt
[6] mailto:relaytest-admin@ja.net
[7] mailto:service@ja.net
[8] https://community.ja.net/library/janet-services-documentation/contact-csirt
[9] https://community.ja.net/library/janet-services-documentation/janet-site-e-mail-requirements
[10] http://www.ietf.org/rfc/rfc1123.txt