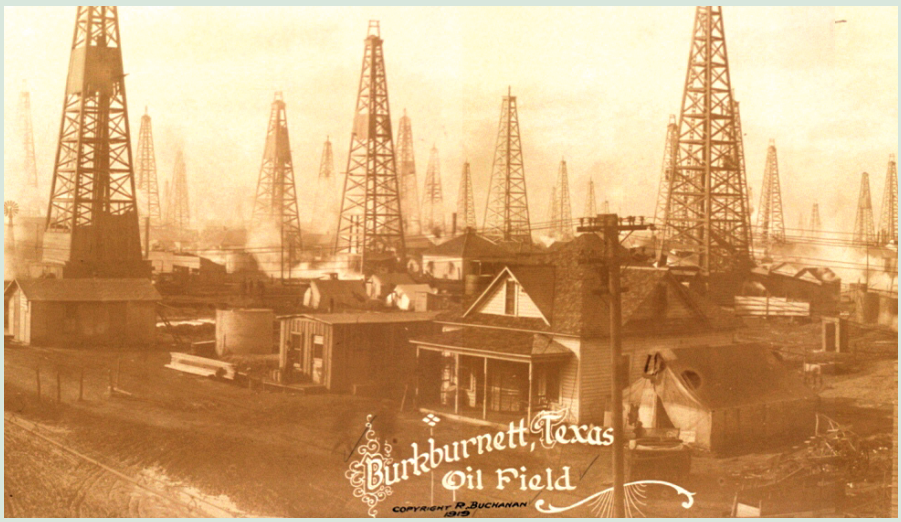
The Sysadmin's Daily Grind: SMTP Relay Check

Muck Spreaders

Only a few, cognitively challenged individuals really believe in the information value of unsolicited mass advertising mail. This makes it all the more important to keep your own network clear of spam spreaders. Enter Smtprc.

BY CHARLY KÜHNAST



Everyone gets mad about spam – and I am no exception. My spam filter statistics tell me that approximately half the mail that reaches me is unsolicited. And the fact that most of these messages are written in languages I don't even understand doesn't improve things.

When I configure a mail server, of course, I make sure that it is relay proof, that is, that it will only accept outgoing mail from registered users and check incoming mail to ensure that it is intended for a user in my network. My server will not accept mail from unknown users and forwards it to users in completely different networks.

Charly, the Spammer

What should I do with customers who had their own subnets and are allowed to install their own servers in these networks? The worst thing that can happen is that one of the customers mail servers might be used as an open relay for spam, and the admin responsible for the server will respond to words of advice from irritated peers.

Of course, the abuse handling buck stops at my desk! Needless to say, I prefer to take care of scenarios like this proactively. To do so, I assume the role of a spammer and try to forward a few test messages using my customer's server. These messages should never reach their destination. Before my test messages get through, there must be something wrong with the server's configuration, and this prompts me to instruct my customer in polite, but clear-cut terms on hardening his system. The tool that does this job is called Smtprc (SMTP Relay Check) [1].

After unpacking the 33 Kbyte tarball you simply type "make" to produce a fully functional executable called "smtprc". The central configuration file for Smtprc is called "auto.conf". The first thing to do is to specify the network address range to check:

```
IPRANGE:10.50.5.20-140
```

Smtprc stores its findings in a HTML file; the path to the file is defined as follows

```
WEBPAGE:/www/pages/relaycheck/result.html
```

The e-mail address that Smtprc attempts to send dummy spam to the defined as follows:

```
RELAYEMAIL:admin@my-domain.com
```

If a message arrives at this address, then there is obviously something wrong with the customer's server configuration. The other options in "auto.conf" are used to fine tune time-outs, the number of threads, and similar things. If the network ranges that you need to check are not too large, the default settings should be just fine.

The "rcheck.conf" file contains a list of the tricks that Smtprc will try when attempting to forward mail; the file can be extended, if required.

This may not reduce the amount of incoming spam, but thanks to Smtprc at least my servers are not to blame. ■

SYSADMIN

INFO

[1] Smtprc: *http://sourceforge.net/projects/smtprc*

THE AUTHOR

Charly Kühnast is a Unix System Manager at the data- center in Moers, near Germany's famous River Rhine. His tasks include ensuring fire-wall security and availability and taking care of the DMZ (demilitarized zone). Although Charly started out on IBM mainframes, he has been working almost exclusively with Linux since 1995.