

Re: Spam filter

Source: <http://unix.derkeiler.com/Newsgroups/comp.unix.bsd.freebsd.misc/2007-11/msg00055.html>

- *From:* Bolwerk <bolwerk@xxxxxxxx>
 - *Date:* Sun, 11 Nov 2007 12:46:19 -0500
-

Speechless wrote:

On Sat, 10 Nov 2007 14:14:18 -0500, Bolwerk <bolwerk@xxxxxxxx> wrote:

Hi, I'm using FreeBSD 6.2 with postfix/postfix admin/courier imap+pop3.

But, but...above it says you are using gmail.com :)

Accounts are stored in a MySQL database, and I use maildirs stored in /var/vmail/

We're in the process of migrating our mail accounts over from Windows Server 2003 running IMail. As of now, we have a few hundred accounts, but expect significantly more in the future.

What I'd like to do is set up a decent anti-spam solution now, while we're small --- we already get a lot of it.

I'm open to other ideas,

I'm just curious...why not monkey see, monkey do...since you are using Gmail, why not Gmail for everyone else in your organization? Did you know that Gmail also offers a corporate version of their service that allows you to use your own domain name and manage your user accounts?

I suggested outsourcing the mail, actually. But they have okay reasons for wanting it inhouse (I don't agree per se, but they have a case). Either way, we have a dedicated FreeBSD mail server, and it's in to stay. I got somebody off Windows. :)

Gmail is my personal account. I don't want my personal mail hosted at a place where I work, and I may move onto a different organization someday.

Besides, they're a for-profit organization serving a specific religious community, with a domain name that has a religious connotation. While I have no problem with their beliefs, they do not represent my feelings

Re: Spam filter

concerning religion ——— which I don't like to publicly put on display anyway. I am personally friendly with the managers, and am in their employ, but my job is simply to handle their network infrastructure. Most of the organization has no idea that I even exist.

but what I have in mind right now is to set up something along the line of a spam filter that dumps junk mail in a folder called "spam" or "junk" for the users to check

a) You might be underestimating the size of the problem.

See: http://www.acme.com/mail_filtering/

He is talking about receiving 1 million plus spams PER DAY at just one e-mail address that saturates his T1 line and...you have how many e-mail addresses?

Somewhere in the low hundreds now, scattered across a few domains. I've implemented some anti-spam measures already, including at the firewall level, that have helped a lot. I've also encouraged a general policy towards spam reduction that includes keeping e-mail addresses off web sites, using web forms instead, and creating event-specific addresses for when ending up on the web is unavoidable. For instance, if they advertise an event, the e-mail address would be something like [event_name][YYYYMMDD]@[domain], which can then be deleted after the event is past.

I explained that although you may not receive spam, it's still a good idea to prevent it from happening in the first place with web forms, strong password policies (to prevent hijackings), and to use usernames that aren't simple common names (bob: bad, bob_williams: better). We pay for bandwidth by the gigabyte, so each rejected message adds up and costs money in the end. So I strongly discourage any public posting of addresses.

Nonetheless, past mistakes and unwillingness on some people's parts to change their e-mail address means some still gets through. The firewall helps a lot, but it's not anywhere close to 100%.

I'm not entirely comfortable with all out blacklisting, so I haven't enabled that firewall feature.

b) You might want to consider farming the problem out to an e-mail filtering service like: <http://www.postini.com/>

In addition to them being very good at what they do (personal experience as a satisfied customer), when you crunch all the numbers, you might also find them to be very cost effective when compared to the costs involved in supporting an in-house anti-spam infrastructure as an alternative.

I'll look into that.

if they want to. I would prefer this to outright deleting spam, just in case something legit comes through. I presume that it wouldn't be heard to clean out such a folder; if the software doesn't already do it, I imagine a single

Re: Spam filter

crond script could be written to traverse the directories and delete messages older than 15 days during off-peak hours.

Given my configuration, what might be the easiest way to do this? I've actually been a little overwhelmed by my options, and am admittedly a little new to administering mail with postfix.

Thank you!

Some tools you might want to look at:

<http://postgrey.schweikert.ch/>

– greylisting

<http://crm114.sourceforge.net/>

– filtering

<http://www.openspf.org/>

– Sender Policy Framework (to deal with botnets)

Thank you for your thoughts. You gave me a lot to think about. :)

.