POSTFIX - GREYLISTING

Spam, junk email, the bane of any network administrator's life. Well, if you use linux and the postfix email server try this trick. Implement greylisting. Greylisting is basically denying all emails from anyone for a short period of time. The idea behind it is that all normal email servers try to resend failed emails, whereas spammers cannot afford to spend time retrying all failed addresses. So if all emails are rejected for a short time, most of the emails that get resent should be from proper email servers. It is actually fairly easy, take a look..

What do you need?
This is fairly simple. You need

- Linux (My test box is Redhat 9)
- Postfix (box has version 2.3. You can use *postconf mail_version* to get the version)
- PostGrey (try get it from here)
- Perl (version 5.6 or up)
- Net::Server Perl module (use *perl -e shell -MCPAN* or checkout Dag's site)
- IO::Multiplex Perl module (use *perl -e shell -MCPAN* or checkout Dag's site)
- BerkeleyDB Perl module (use *perl -e shell -MCPAN* or checkout Dag's site)
- Berkeley DB library greater than 4.1 (get it here)

Set it all up
Firstly install all the perl modules mentioned above (use either the perl sheel or use rpms) then install the postgrey package (I used the source, but you can use the rpm). I extracted the source into */admin/postgrey*. In that folder you will see two *postgrey_whitelist* files, copy these to */etc/postfix* and edit as needed. Generally you only want to edit the clients file with the IP addresses of your local lan, the syntax is _/^192\.168\.14\..*/_ . The following thing to do is test it, try running *postgrey --inet=10023*, this will start the process attached to the console (meaning you have to use *ctrl-c* to kill it), if you get any errors you will know what to fix. Next you want to create the user that the process will run as, use something like..

```
useradd -d /var/spool/postfix/postgrey -m postgrey
```

Now you want to get postgrey to run as the system starts up. You can put it into your */etc/rc.d/rc.local*, add it to the postfix init script, or create a separate init script for it. Whichever way you do it, you will want to start it with a command looking like (there are other switches, so take a look)..

```
postgrey --inet=10023 -d --auto-whitelist-clients --use-group=postgrey
```

Now we head again to the */etc/postfix* folder to edit the *main.cf* file. Look for the *smtpd_recipient_restrictions* section, and after the *reject_unauth_destination* line add the following line (do not forget the commas at the end of the lines), and restart postfix..

```
check_policy_service inet:127.0.0.1:10023
```

Now if you check your */var/log/maillog*, you should start seeing messages like this..

```
Recipient address rejected: Greylisted for 300 seconds
```

Running it
Well thats it, you have now added greylisting to your postfix server, not difficult. You can whitelist other senders or recipients in the two files which you moved into */etc/postfix*. Also, as I mentioned, the postgrey script itself has a couple more options which can be set via the startup command that you can look at. Otherwise, just sit back and see what happens to the spam.

Final Words
Greylisting is a very useful step in combating spam, but it is still just a step, it will not solve the problem. So implement it, but know that you will have to do more in order to more fully stop the spam and virus problem. As always have fun and learn.