POSTFIX - MORE ANTISPAM

Spam really is the bane of the internet and email, and anything that can be down to help cut it down is always welcome. Previously we have looked at greylisting and using spamassassin with add-ons. Now lets look at how we can use the normal postfix configurations to also play a part in stopping spam. I am assuming that everyone will be using some *2.x* version of postfix, and that any other configuration lines for greylisting or sender checking or anything else will be added separately.

Starting
Two main things to remember are..

- the order of the configuration file is important, especially the the different sections
- this configuration relates the the *main.cf* file

The Configuration

```
mynetworks_style = subnet
strict_rfc821_envelopes = yes
disable_vrfy_command = yes
smtpd_delay_reject = yes
smtpd_helo_required = yes
```

Here we do some important things, we disable the *VRFY* command, setup our internal networks, tell the server we expect our clients to follow the RFC and lastly say that we require clients to use the *HELO* command. These settings stop some spam because they enforce proper standards and allow us to do other checks further on.

```
smtpd_helo_restrictions =
     permit_mynetworks,
     reject_invalid_hostname,
     regexp:/etc/postfix/helo.chk
     permit
```

This is just a simple and quick check we perform during the *HELO* phase of the email transaction, we allow our networks and do a quick check for the other clients. Do not forget to create the */etc/postfix/helo.chk* file as below (you can set it up to do a lot more, these are just some basics)..

```
/^[0-9.]+$/                     550 Your software is not RFC 2821 compliant
/^[0-9]+(\.[0-9]+){3}$/         550 Your software is not RFC 2821 compliant
```

Now we move onto the main checks.

```
smtpd_recipient_restrictions =
  reject_unknown_sender_domain,
  reject_unknown_recipient_domain,
  reject_unauth_pipelining,
  reject_non_fqdn_sender,
  reject_non_fqdn_recipient,
  permit_mynetworks,
  reject_unauth_destination,
  reject_rbl_client relays.ordb.org,
  reject_rbl_client sbl-xbl.spamhaus.org,
  reject_rbl_client list.dsbl.org,
  reject_rbl_client blackhole.securitysage.com,
  reject_rbl_client cbl.abuseat.org,
  reject_rbl_client dnsbl.njabl.org,
  reject_rbl_client blackholes.wirehub.net,
  reject_rbl_client bl.spamcop.net,
  reject_rbl_client dsn.rfc-ignorant.org,
  reject_rbl_client bl.csma.biz,
  reject_rbl_client block.rhs.mailpolice.com,
  reject_rbl_client relays.bl.kundenserver.de,
  reject_rbl_client dnsbl.rangers.eu.org,
  permit
```

The *smtpd_recipient_restrictions* section is where most of our checks happen. The first couple of lines (the

reject lines) are there to stop noticeably bad email senders, spammers who are not even trying hard. The next section is just the two lines where you permit your own networks and then reject any email not destined for your own domain, these are very important as it stops your box from being an open relay, and the order is very important. The last grouping of lines are *DNS blacklists*. The concept of DNS blacklists can be very controversial, but in my experience using the right ones can be very effective. The ones listed here are the ones I personally use and are very happy with.

```
smtpd_data_restrictions =
  reject_unauth_pipelining,
  permit
```

One last check just to make sure a email client sticks to a proper email transaction format by stopping them from pushing through a chunk of commands.

Blacklists?

Blacklists are split into *DNSbl* (DNS Blacklist) and *RHDNSbl* (Right Hand DNS Blacklist). When you use them you submit information regarding the email sender to the stated server and it responds in a certain way telling your email server whether it thinks the sender is a spammer or not. The difference between the two is in the information submitted. A *DNSbl* has the IP address of the sender submitted and it checks that, this means that anyone from a certain IP address could be flagged. With a *RHDNSbl*, the "*right hand*" side of the senders address (after the @) is checked, no the IP address. Yes I know there are arguments for and against each and for and against the entire practice of using them at all, but till they stop helping with spam I will carry on using them.

Final Words

There you go, not difficult and very easy to implement on any postfix server as no additional software is needed. Please bear in mind that any site-specific settings you have will need to be added. These settings basically implement two simple things; the usage of proper email standards and the checking of the sender against known bad guys. But even so, you will be very surprised how much they can help. Use this in conjunction with other antispam measures discussed, and watch the spam decrease (alas, some will still get through). As always, have fun and learn.