How to setup a linux box with mail filtering.

Grab the latest version of Slackware from www.linuxiso.org and install it on a machine with two network cards. Make sure to do a FULL install so that you are not missing any software. Its not terribly large and it's a real pain when you have to stop and install software that you need in order to complete this process. So for sanities sake, just do a full install. Also with the full installation you don't have to worry about attending the installation!

During the installation it will have you configure your network, make sure that you do this, because you will be downloading software directly from the net and installing it. I would also make sure you have an ftp available on another box that you can pull down software from. This is the way I do things, if you have a better way, good for you. Make sure that you have a DNS server setup and that you CAN ping to the Internet via hostname(Ctrl+X kills a ping command). If you are good here, just head back to your comfortable office computer and use putty to secure shell into the newly working linux server.

Email Setup with SpamAssassin

-Download postfix from www.postfix.org (you can use wget from the machine if you know the exact URL to the file instead of FTPing from another computer).

I usually rename the gz file to postfix.tar.gz for easy ftping. Once on my system to a scrap folder I setup in the root directory, I just run:

```
# gunzip * (this will unzip any file in the directory)
# tar –xvf  postfix.tar
```

It will extract to a directory that you will now see when you run the "#dir" command. Just do a "#cd post*" to get into the directory and then a "#more INSTALL" to see how to install it.
-Here is the gist of the installation:

1. Make a user called postfix and a group called postdrop
2. Make sure postfix is not in the postdrop group.
3. Run "#make"
4. Run "#make install" (I would at this point accept all the defaults accept the samples folder and the readme folders. I just make them subfolders under postfix or you can leave it and move the files later. It should compile and distribute the files for you and you should be set to go).

Notes: To add the postfix user, type "#adduser postfix" and answer the relevant information. Change directory to the /etc/ and then pico the "passwd" file and make sure that you set the home directory as /no/where and the shell to /no/shell "/no/where:/no/shell". To add the group, type "#addgroup".

-Configure it the way you want to, this is somewhat cumbersome if you don't know anything about postfix so I suggest READing the documentation on it. It's a very stable, secure, and tight MTA (mail transfer agent). Remember that since you are going to be using spamassassin, there is no need to block people using any UCE controls. So don't setup RBL's, headchecks or bodychecks. You just need to get the mail from point A to point B.

Basic Setup information
-Add your domain in the relay_domains.map file like so: "domain.com RELAY" and set the server you are forwarding all the mail to, once its processed, in the transport.map file like so: "domain.com smtp:[192.168.1.3]". You can also use a hostname instead of the IP.
-Once you think its configured correctly, don't forget to do a "postmap" on any of the regexp or map files in the directory. I usually do it this way to save myself typing:

```
# postmap *.map
# postmap *.regexp
```

Now start postfix:

```
# postfix start
```

-Make sure to take a look at the maillog to see if any errors are reported, in that case you didn't configure postfix correctly and need to resolve the errors. To watch the error log, just do the following command: "# tail –f /var/log/maillog" This command is VERY useful in finding problems with your configuration or just looking at the flow of mail thru your server. To open and search or view the whole maillog file, just do a "#more /var/log/maillog" and hit the space bar to go down 10 lines at a time or do "/thensomesearchtext" to search the document.

Change directory to /etc/rc.d/ again and pico the rc.local file. Add "postfix start" at the bottom and save it.

"#postfix stop" stops postfix and "#postfix reload" updates the configuration. Remember these commands as they will be needed after any configuration changes or emergencies.

Spamassassin

Ok, this is the FUN part! Actually it's more of a pain, but well worth it in the end.

Go to www.spamassassin.org, then to the documentation page. Click on the top-level installation file and read thru it. Do NOT do anything until you have read the whole thing. Here is an abstract of what you have to do and I recommend this order.

First use CPAN to install all of the required perl modules. CPAN is easy to use; just do this to get started:

```
# perl –MCPAN –e shell
```

-This will get you into CPAN, if it asks you for manual configuration, just say NO unless you know what you are doing.
-To install a module just do it like this: "install Module::Name" Obviously Module::Name is not the name of a module but here is a live example: "install Net::DNS"

-Do this for ALL of the required modules and all of the optional modules except for SSL and Net::Ident

-Once you are done with CPAN stuff move on to DCC, Pyzor, and Razor. The instructions for installation on the spamassassin site are correct. Razor and Pyzor require two other things to be done:
***Note on Razor, if you are following the instructions for the installation and get an error on the SHA1 module not being present even though you installed it via CPAN, go to www.cpan.org and download the Digest::SHA1 module and manually install it like so: Uncompress it and cd into the directory you uncompressed, use the following commands to set it up on the server:

```
#perl Makefile.PL
#make
#make install
```

-Ok, now you can do this stuff below to setup razor.
-Oh if you get errors during the razor registration process add more DNS servers to your /etc/resolv.conf file and try again. Razor will not work until you complete this successfully.

Razor: mv the patch from a folder in the razor install folders to the Razor2 directory, which is here: /usr/lib/perl5/site_perl/5.8.0/i486-linux/Razor2/ and patch razor.

```
# cp Razor2.patch /usr/lib/perl5/site_perl/5.8.0/i486-linux/Razor2/
# cd /usr/lib/perl5/site_perl/5.8.0/i486-linux/Razor2/
# patch -p0 < Razor2.patch
```

-If you download the new version of perl then it will be 5.8.1 instead of 5.8.0
-You are now done with razor.
-Pyzor is easy because all you have to do is run "# pyzor discover" and you are done.

Now assuming that all is well you can move on to the core Spamassassin installation.

Go back into CPAN

```
# perl –MCPAN –e shell
```

then do "install "Mail::SpamAssassin"

It will ask you to put in your postmaster email address then it will ask to run tests, run the tests. If they fail, Spamassassin will NOT install. So if they do fail, just do the install mail::spamassassin again and keep trying until Razor works and the tests don't fail. If the tests don't fail, then it will finish out the installation and your good to go! If it doesn't ask to test Razor then you might have something wrong with your razor installation.

You can test Spamassassin by running this command and looking at the stats:
"#Spamassassin –D --lint"

We are now going to setup a few scripts to filter mail, learn spam and ham, and then start Spamassassin.

-Need to add users and a group before you test the filter.sh script.

Users:
filter
spam
ntspam (or notspam if you wish, just make sure to modify the learn.sh script)

Group:
filter (but this time it's a group)

Easy addition of users can be done using the command "useradd username" (groups is "groupadd groupname")

Descriptions:
-filter is gonna be the user who the spamassassin deamon runs under.
-spam is going to be the email address you are going to send to email to the server so that it learns it as spam.
-ntspam is going to be the email address you are going to send email to the server so that it learns it as ham (not spam).
-filter is the group, filter doesn't have to be in it, but you will need this group.

Moving on
-Change directory to /var/spool/ and create a directory called "filter" then do a "#chown filter:filter filter", that will give the user filter which you create below the ability to do what it needs to do in this directory.
-Change directory to /usr/local/sbin/ create a new file called filter.sh and paste the following into it:

```
SM="/usr/sbin/sendmail -i"

cd /var/spool/filter
trap "rm -f out.$$" 0 1 2 3 15
cat | /usr/bin/spamc > out.$$
if egrep -q "X-Spam-Flag: YES" < out.$$
```

```
then
        $SM quarantine@yourdomain.com < out.$$
else
        $SM "$@" < out.$$
fi
exit $?
```

-Save the file and then run “chmod 755 filter.sh” to make it executable. Do a ./filter.sh to run it and make sure you don’t get any path errors. Make sure that spamc is in /usr/bin/ and Sendmail is in /usr/sbin otherwise you will get an error. DON’T move them if they are not, just redirect the path in the file to match the location. Do a find if you don’t know where they are and cant find them manually.

```
# find / -name ‘sendmail’
```

That should print out the locations of the executable Sendmail script.

Options with this script: Use this script if you **don’t** want to redirect the spam to another email box, it will just pass it thru to the user. I suggest turning on the change subject line function and setting up a mailbox rule to redirect subjects with the SPAM subject to a folder:

```
SM="/usr/sbin/sendmail -i"
cd /var/spool/filter
trap "rm -f out.$$" 0 1 2 3 15
cat | /usr/bin/spamc > out.$$
$SM "$@" < out.$$
exit $?
```

Next we are going to create the learning script. Just create a new file called learn.sh and paste this into it:

```
#!/bin/sh

if [ -e /var/mail/spam ]; then
/usr/local/bin/sa-learn --spam \
--mbox /var/mail/spam
rm /var/mail/spam > /dev/null
fi

if [ -e /var/mail/ntspam ]; then
/usr/local/bin/sa-learn --ham \
--mbox /var/mail/ntspam
rm /var/mail/ntspam > /dev/null
fi

/usr/local/bin/sa-learn –rebuild
```

-Save the file and then run “chmod 755 learn.sh” to make it executable. No need to test this script.

Just need to create an automatic startup script for spamd. Just change directory to /etc/rc.d/ and copy/paste this into a file called “spamd.sh”, its one line:

```
/usr/bin/spamd -a -d -u filter -m 20 &
```

-Save the file and then run “chmod 755 spamd.sh” to make it executable.

-Make sure to start the spamd by running ./spamd.sh in the /etc/rc.d/ directory. If you get directory errors, just modify the directories in the script to show the correct location of the spamd.

-Modify the /etc/rc.d/rc.local file and put “/etc/rc.d/spamd.sh” at the bottom of the file and save it. This will make sure that if you reboot your server the spamd will start again.

-Time to add a nifty cronjob to process all the email that people send to the server so that it learns it as spam!!! Just do this(note this will run the learn.sh script every 5 minutes between 7am and 10pm):

```
# contab –e
```

arrow down to the last line and then over to the end of the line. Hit “i” on your keyboard and then arrow over to the right end of the line. Hit return and then type this is:

```
# Process Spam and Ham every 5 minutes
0,5,10,15,20,25,30,35,40,45,50,55 7-21 * * * /usr/loca/sbin/learn.sh >> /learned.log
```

Hit esc twice then type “:x” then hit enter. If you screw up royally during this, just hit esc twice and type “:q!” then enter. That will get you out without saving. It is very important that you don’t screw this file up! This editor is VI and I suggest you learn how to use it, UNIX people don’t like people who don’t know VI. No, they are not bad people, they just have a thing about VI.

Ok, last part! Change directory to /etc/postfix/ and “pico master.cf“ . Scroll down a little bit until you get to a line that looks like this:

```
smtp      inet  n      -      n      -      -      smtpd
```

Change that line to look like this:

```
smtp      inet  n      -      n      -      -      smtpd -o content_filter=spamfilter:
```

Now under that line add this:

```
spamfilter unix -      n      n      -      -      pipe
  flags=Rq user=filter argv=/usr/local/sbin/filter2.sh -f ${sender} -- ${recipient}
```

-Ok, just save the file. Now run “postfix reload”

-I suggest at this point looking at the mail coming thru using the tail command:

```
# tail –f /var/log/maillog
```

-If no mail is going thru, well let just create some!

Open your telnet in windows and do a:

```
C:\telnet ip.addresss.of.spamserver 25
```

Type:

```
“helo”
“mail from: <user@whatever.com>”
“rcpt to: <user@yourdomain.com>”
“data”
```

Type whatever you want to here then return and type “.” And then return again.
It should say mail queued!

While you are doing a generic email make sure to take a look at the putty window to see what the log shows.

If all is well then you have a working anti-spam server!!

Useful programs:
Webmin – Used as web admin console for your linux server, not hard to setup and easy to run!
Putty – Very useful ssh/telnet tool for windows.

Websites:
www.spamassassin.org
www.postfix.org
www.webmin.com
www.apache.org