```
=====MAIL FILTER – Part 3======
==========================
```

1. Setup MailScanner
==================

Copy preconfigured files for Mailwatch from the instructor's server.
The only changes made to these files was to add the MySQL username
and password to allow MailWatch to connect to the database.

```
        $sudo scp afnog@pc37.sse.ws.afnog.org:/home/afnog/*.pm /usr/
share/MailScanner/perl/custom/
        $sudo chmod ugo+x /usr/share/MailScanner/perl/custom/
```

2. Continue MailScanner setup
============================

You will need the following CPAN module

```
        $sudo cpan install Encoding::FixLatin
```

Enable MailScanner

```
        $sudo nano /etc/MailScanner/defaults
```

```
        ##Uncomment the following line:
        run_mailscanner=1
```

Save and Exit the file

Copy preconfigured MailScanner.conf file. A number of changes made,
please go through it.

```
        $sudo mv /etc/MailScanner/MailScanner.conf /etc/MailScanner/
MailScanner.conf.backup
        $sudo scp afnog@pc37.sse.ws.afnog.org:/home/afnog/
MailScanner.conf /etc/MailScanner/
```

Prepare MailScanner directories (they may already exist)

```
        $sudo mkdir /var/spool/MailScanner/spamassassin && sudo
chown postfix:postfix /var/spool/MailScanner/spamassassin
        $sudo chown postfix:clamav /var/spool/MailScanner/incoming
        $sudo chown postfix:www-data /var/spool/MailScanner/
```

quarantine

3. Get clamav updates
==
====

Clamav will automatically attempt to obtain fresh antivirus
signatures from the Internet via
freshclam after installation. Type "freshclam" to see how updates
are fetched. If it fails with a lock issue, it means freshclam is
running in the background and you can move to the next step

        $sudo freshclam

4. Setup Postfix and SpamAssassin
==============================

Fetch an update to the rules (if any). It will return quietly to the
shell if there are no updates:

        $sudo sa-update

Enable SpamAssassin

        $sudo nano /etc/default/spamassassin

        ##Uncomment the following line:
        ENABLED=1

Save and Exit.

Configure Postfix to hold mail first. Effectively a mail arrives and
is put into a hold queue then mailscanner scans the mail for spam or
virus content then it is released. Create the below empty file:

        $sudo nano /etc/postfix/header_checks

        ###Add the following
        /^Received:/ HOLD

Save and Exit

Configure the main.cf file to read the file created above. Add the
following line at the end:

        $sudo nano /etc/postfix/main.cf

```
        ###Add the following
        header_checks = regexp:/etc/postfix/header_checks

=============

ALSO CHECK THAT YOUR XXXX.AFNOG.GURU domain will be accepted. Look
for the line starting with "mydestination" and add your domain name
followed by a comma. It should looks as follows:


mydestination = pc37.sse.ws.afnog.org, XXXXX.afnog.guru,
localhost.sse.ws.afnog.org, , localhost

===============


Save and Exit


Check what the postfix config looks like. Postconf will reveal the
running config on your system:

        $sudo postconf -n


        alias_database = hash:/etc/aliases
        alias_maps = hash:/etc/aliases
        append_dot_mydomain = no
        biff = no
        config_directory = /etc/postfix
        header_checks = regexp:/etc/postfix/header_checks
        inet_interfaces = all
        mailbox_size_limit = 0
        mydestination = pc37.sse.ws.afnog.org, kgc.afnog.guru,
localhost.sse.ws.afnog.org, , localhost
        myhostname = pc37.sse.ws.afnog.org
        mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
        myorigin = /etc/mailname
        readme_directory = no
        recipient_delimiter = +
        relayhost =
        smtp_tls_session_cache_database = btree:${data_directory}/
smtp_scache
        smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
        smtpd_relay_restrictions = permit_mynetworks
permit_sasl_authenticated defer_unauth_destination
        smtpd_tls_cert_file = /etc/ssl/certs/ssl-cert-snakeoil.pem
        smtpd_tls_key_file = /etc/ssl/private/ssl-cert-snakeoil.key
        smtpd_tls_session_cache_database = btree:${data_directory}/
smtpd_scache
        smtpd_use_tls = yes
```

```
5. Setup Mailwatch
==================

Download MailWatch – MailScanner Frontend

        $cd /home/afnog/
        $wget https://github.com/mailwatch/1.2.0/archive/master.zip
        $unzip master.zip
        $cd 1.2.0–master
        $sudo mv mailscanner /var/www/


Set up MailWatch:

        $cd /home/afnog/1.2.0–master


Setup MailWatch conf.php (copy preconfigured). The changes here were
to include the MySQL credentials for MailWatch and also to set the
home directory: [[define('MAILWATCH_HOME', '/var/www/
mailscanner');]]



        $sudo scp afnog@pc37.sse.ws.afnog.org:/home/afnog/conf.php /
var/www/mailscanner/



Setup MailWatch web page for Apache:


        $sudo sh –c 'echo "Alias /mailwatch /var/www/mailscanner"
> /etc/apache2/conf–enabled/mailwatch.conf'



Setup the database. The password is afnog
        $cd /home/afnog/1.2.0–master
        $mysql –u root –p < create.sql


THEN


Setup the mailscanner database, where it will store details on
incoming emails

        $mysql –u root –p


You should get the MySQL shell.
```

```
        mysql>
```

Add the following exactly as it is IN ONE LINE:

```
        GRANT ALL ON mailscanner.* TO mailwatch@localhost IDENTIFIED
BY 'afnog';
        GRANT FILE ON *.* TO mailwatch@localhost IDENTIFIED BY
'afnog';
        FLUSH PRIVILEGES;
        exit
```

THEN

Login as the Mailwatch user using the credentials used in the Mysql
entry above. We will set the username and password to be used to
login to the MailWatch web interface. Typically this should be a
strong alphanumeric password or passphrase. We will use afnog for
this class however:

```
        $mysql mailscanner –u mailwatch –p

        INSERT INTO users SET username = 'mailwatch', password =
MD5('afnog'), fullname = 'mailadmin', type = 'A';
        exit
```

Finally, set the rights to the images directory

```
        $sudo chown –R root:www–data /var/www/mailscanner/images/
        $sudo chmod –R 775 /var/www/mailscanner/images/
```

6. ALWAYS CHECK LOGS
========================

You should also run the SpamAssassin check. Look for errors and fix
(if any). It may require you to run sa–update in order to fix the
errors.

```
        $sudo spamassassin –D ––lint
```

You should get similar output at the very end.

```
        dbg: check:
subtests=__BODY_TEXT_LINE,__EMPTY_BODY,__GATED_THROUGH_RCVD_REMOVER,
__HAS_FROM,__HAS_MESSAGE_ID,__HAS_MSGID,__HAS_SUBJECT,__KHOP_NO_FULL
```

_NAME,__MISSING_REF,__MISSING_REPLY,__MSGID_OK_DIGITS,__MSGID_OK_HOS
T,__MSOE_MID_WRONG_CASE,__NONEMPTY_BODY,__NOT_SPOOFED,__SANE_MSGID,_
_TO_NO_ARROWS_R,__UNUSABLE_MSGID
May 29 12:14:46.384 [12173] dbg: timing: total 1061 ms – init: 798
(75.2%), parse: 0.55 (0.1%), extract_message_metadata: 1.14 (0.1%),
get_uri_detail_list: 0.58 (0.1%), tests_pri_-1000: 5 (0.5%),
compile_gen: 117 (11.0%), compile_eval: 16 (1.5%), tests_pri_-950:
3.7 (0.4%), tests_pri_-900: 4.0 (0.4%), tests_pri_-400: 3.5 (0.3%),
tests_pri_0: 197 (18.5%), tests_pri_500: 45 (4.3%)

You should make sure that MailScanner is working properly and can
communicate with ClamAV and SpamAssassin.
Do not run the following command from the root director (/root) as
it will produce errors

        $sudo MailScanner --lint --debug

You should see something like this:

        Checking for SpamAssassin errors (if you use it)...
        Using SpamAssassin results cache
        Connected to SpamAssassin cache database

        AND

        Filename Checks: Windows/DOS Executable (1 eicar.com)
        Other Checks: Found 1 problems
        Virus and Content Scanning: Starting
        ./1/eicar.com: Eicar-Test-Signature FOUND

        Virus Scanning: ClamAV found 2 infections
        Infected message 1 came from 10.1.1.1
        Virus Scanning: Found 2 viruses

==
=======
        Virus Scanner test reports:
        ClamAV said "eicar.com contains Eicar-Test-Signature"

6. START everything
====================

If all is well then restart everything:

        $sudo service postfix restart && sudo service apache2
restart && sudo service mailscanner restart

And check the log:

        $sudo tail -f /var/log/mail.log

You should get similar output:

        May 29 12:19:15 pc39 MailScanner[12825]: MailScanner E-Mail
Virus Scanner version 4.85.2 starting...
        May 29 12:19:15 pc39 MailScanner[12825]: Reading
configuration file /etc/MailScanner/MailScanner.conf
        May 29 12:19:15 pc39 MailScanner[12825]: Reading
configuration file /etc/MailScanner/conf.d/README
        May 29 12:19:15 pc39 MailScanner[12825]: Read 868 hostnames
from the phishing whitelist
        May 29 12:19:15 pc39 MailScanner[12825]: Read 5807 hostnames
from the phishing blacklists
        May 29 12:19:15 pc39 MailScanner[12825]: Config: calling
custom init function SQLBlacklist
        May 29 12:19:15 pc39 MailScanner[12825]: Starting up SQL
Blacklist
        May 29 12:19:15 pc39 MailScanner[12825]: Read 0 blacklist
entries
        May 29 12:19:15 pc39 MailScanner[12825]: Config: calling
custom init function SQLWhitelist
        May 29 12:19:15 pc39 MailScanner[12825]: Starting up SQL
Whitelist

Test that port 25 is open and that Postfix is listening
        $sudo telnet localhost 25

        afnog@pc39:/etc/spamassassin$ sudo telnet localhost 25
        Trying ::1...
        Connected to localhost.
        Escape character is '^]'.
        220 pc39.sse.ws.afnog.org ESMTP Postfix (Debian/GNU)

Type quit to exit

8. TEST THE EMAIL SERVER, SEND OUT AN EMAIL
====================

```
$sudo apt-get remove mailutils
$sudo apt-get install mailutils
```

Then test your email server to see if it will send an email out.

```
$echo "This is my email, hello" | mail -s "This is a test
message" youremailaddress@gmail.com
```

9. LOGIN TO MAILWATCH
====================

Username is "mailwatch" password is "afnog"

Please note that Chrome may not be able to login so try another browser if that is the case.

    https://pcX.sse.ws.afnog.org/mailwatch

    OR

    https://XXXX.afnog.guru/mailwatch

PLEASE NOTE: In the real world this page _MUST_ be accessed over HTTPS and as was mentioned earlier, the username should be changed and the password made more difficult to guess.