CHAPITRE 8

Dspam

Maintenant que nous possédons un très bel outil qui nous permet d'envoyer et de recevoir des e-mails, il ne saurait tarder à ce que vous receviez quelques spams.

Nous allons donc installer un antispam.

Pour commencer installons déjà un antispam. Etant un habitué de Spamassassin et en cherchant sur la toile de quoi aller plus loin avec SA j'ai découvert Dspam. Alors j'ai choisi d'utiliser du coup ce dernier pour mon tutorial. Je préfère la démarche de mise en place autour de Dspam, malgré que je le connaisse peu, je me sens plus à l'aise qu'avec SA.

Dspam offre aussi un atout performance par rapport à SA ce qui n'est pas négligeable surtout si vous hébergez beaucoup de boites plus ou moins spammées.

Puisque nous hébergeons des utilisateurs virtuels sur notre Postfix et Dspam offre la possibilité d'être couplé à Mysql et d'être configurable utilisateur par utilisateur, nous allons par conséquent exploiter cette possibilité.

Dspam à la particularité de devoir tout apprendre, c'est à dire qu'au début aucun spam ne sera recensés. Nous allons configurer deux boites e-mails « spam@bebenet.local » et « ham@bebenet.local » auxquelles nous transférerons respectivement les faux négatifs et les faux positifs afin que Dspam apprenne à reconnaître les bons des mauvais e-mails.

Maintenant que le décor est planté, cette configuration aura le démérite que chaque utilisateur devra commencer de zéro avec Dspam mais Dspam aura la finesse de filtrer la boite e-mail de l'utilisateur tout comme ce dernier lui aura appris. Un véritable filtre personnalisé.

Néanmoins il existe des méthodes pour que Dspam apprenne plus vite à partir d'une base de spam préétablie. Je n'utiliserai pas cette fonctionnalité pour deux raisons.

La première est du fait que les bases de spams vieillissent très vite et les spams appris ne seront plus d'actualité ce qui ne servira en rien à Dspam.

La deuxième provient de mon expérience personnelle avec Dspam. Recevant une centaine de spam par jour Dspam n'a pas mis plus de deux heures pour commencer à attraper les premiers spams en trois jours il filtrait tout. Après les quelques semaines qui se sont passées entre la rédaction de se tuto et sa publication. Voici les statistique de mon Dspam.

2 883 spam détecté dont 7 faux positifs et sur les 758 e-mail détecté comme valide seulement 53 faux négatif. Bien entendu ces résultats peuvent fortement varier en fonction de la typologie et de la variabilité des e-mails reçus.

Dspam à son installation cherchera à se connecter en « root » sur notre base de données. Etant donné que nous avions renommer l'utilisateur « root » en « bebeserv », nous ferons machine arrière le temps de l'installation.

Il est temps d'installer Dspam maintenant – place à l'action :

```
ALBAN@bebeserv:~$ sudo -i
Password:
bebeserv:/etc/mysql# mysql -u bebeserv -p
Enter password:
[...]

mysql> rename user bebeserv@localhost to root@localhost;
Query OK, 0 rows affected (0.00 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye
bebeserv:~# apt-get update
[...]
bebeserv:~# apt-get install dspam dspam-drv-mysql dspam-doc
[...]
```

Lors de l'installation, répondez oui à « dbconfig-common », entrez le mot de passe « root » (enfin « bebeserv ») de Mysql puis le mot de passe de l'utilisateur Dspam qui sera créé et confirmer ce mot de passe.

```
bebeserv:/etc/mysql# mysql -u root -p
Enter password:
[...]

mysql> rename user root@localhost to bebeserv@localhost;
Query OK, 0 rows affected (0.00 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye
```

Je vous passe ici l'exploration de la base de données créée qui doit normalement se prénomée par un nom un peu barbare dixit : « libdspam7drvmysql » et l'utilisateur attribué sera nommé « libdspam7-drv-my ».

Place à la configuration :

```
bebeserv:~# nano /etc/dspam/dspam.conf

StorageDriver /usr/lib/dspam/libmysql_drv.so
```

```
DeliveryHost        127.0.0.1
DeliveryPort        10026
DeliveryIdent       localhost
DeliveryProto       SMTP

Preference "signatureLocation=message"  # 'message' or 'headers'
Preference "showFactors=on"
Preference "spamAction=tag"
Preference "spamSubject=***SPAM***"

#
# Purge configuration: Set dspam_clean purge default options, if not
otherwise
# specified on the commandline
#
#PurgeSignatures 14          # Stale signatures
#PurgeNeutral    90          # Tokens with neutralish probabilities
#PurgeUnused     90          # Unused tokens
#PurgeHapaxes    30          # Tokens with less than 5 hits
(hapaxes)
#PurgeHits1S    15          # Tokens with only 1 spam hit
#PurgeHits1I    15          # Tokens with only 1 innocent hit

#
# Purge configuration for SQL-based installations using purge.sql
#
PurgeSignature  off # Specified in purge.sql
PurgeNeutral   90
PurgeUnused    off # Specified in purge.sql
PurgeHapaxes   off # Specified in purge.sql
PurgeHits1S    off # Specified in purge.sql
PurgeHits1I    off # Specified in purge.sql

Opt out

ServerPort              10027
ServerQueueSize 32
ServerPID              /var/run/dspam/dspam.pid

ServerMode standard

ServerParameters        "--deliver=innocent -d %u"
ServerIdent             "localhost.localdomain"

DeliveryHost 127.0.0.1
DeliveryPort 10026
DeliveryIdent localhost
DeliveryProto SMTP
```

Enregistrer et quitter.

Maintenant enregistrons les préférences des utilisateurs par défaut :

```
bebeserv:~# nano /etc/dspam/default.prefs

trainingMode=TEFT
spamAction=tag
```

```
spamSubject=***SPAM***
signatureLocation=message
showFactors=on
optIn=off
optOut=on
```

Enregistrez et quittez.

Activons Dspam :

```
bebeserv:~# nano /etc/default/dspam

START=yes
```

Enregistrez et quittez.

Maintenant faisons les même réglages dans la base de données de Dspam :

```
bebeserv:~# dspam_admin ch pref default trainingMode TEFT
[...]
bebeserv:~# dspam_admin ch pref default spamAction tag
[...]
bebeserv:~# dspam_admin ch pref default spamSubject "***SPAM***"
[...]
bebeserv:~# dspam_admin ch pref default enableBNR on
[...]
bebeserv:~# dspam_admin ch pref default enableWhitelist on
[...]
bebeserv:~# dspam_admin ch pref default statisticalSedation 5
[...]
bebeserv:~# dspam_admin ch pref default  signatureLocation headers
[...]
bebeserv:~# dspam_admin ch pref default whitelistThreshold 10
[...]
bebeserv:~# dspam_admin ch pref default showFactors on
[...]
```

C'est terminer pour Dspam nous pouvons démarrer le démon :

```
bebeserv:~# /etc/init.d/dspam start
[...]
```

Il nous reste à coupler Dspam à Postfix.

Commencez par préparer nos deux boites e-mail « spam@bebenet.local » et « ham@bebenet.local » :

```
bebeserv:~# cd /etc/postfix/conf.d/
bebeserv:/etc/postfix/conf.d# nano virtual_mailbox

spam@bebenet.local      bebenet.local/spam/
ham@bebenet.local       bebenet.local/ham/

Enregistrez et quittez.
Rechargeons la base :

bebeserv:/etc/postfix/conf.d# postmap virtual_mailbox
```

C'est deux boîtes e-mail sont fictive en fait et ne recevront jamais de messages. Elles seront couplé à Dspam et nous allons préparer ce couplage grâce à ce fichier :

```
bebeserv:/etc/postfix/conf.d# nano transport

spam@paradoxal.org      dspam-spam:
ham@paradoxal.org       dspam-ham:
```

Enregistrez et quittez.

Ce fichier va rediriger nos deux boites e-mail non pas vers le transport classique « virtual » mais vers deux nouveaux transports que nous allons définir un peu plus loin.

Ces deux boites e-mail ne devrons pas être scannées par Dspam (logique) et nous allons aussi préparer un fichier qui va nous permettre de définir les boites à scanner et celle à ne pas scanner.

```
bebeserv:/etc/postfix/conf.d# nano dspam_filter_access

#les 2 boites à ne pas filtrer (celles où sont envoyé les emails
pour l'apprentissage de Dspam)
/^(spam|ham)@.*$/ OK
#puis domaines qui n'ont que la vérification antivirus, dans notre
cas, tous les autres domaines :
/^.*$/ FILTER dspam-filter:127.0.0.1:10027
```

Enregistrez et quittez.

Voilà comme vous pouvez le voir ce dernier fichier utilise les expressions régulières, pour que Postfix puisse les comprendre nous allons devoir lui installer un complément :

```
bebeserv:/etc/postfix/conf.d# apt-get install postfix-pcre
[...]
```

Voilà nos fichiers de configuration sont prêt, il faut maintenant définir les nouveaux transports dans Postfix :

```
bebeserv:/etc/postfix/conf.d# cd ..
bebeserv:/etc/postfix# nano master.cf
```

A la fin du fichier rentrez ceci :

```
dspam-spam   unix    -       n       n       -       10      pipe
     flags=Rhq user=dspam argv=/usr/bin/dspam --user $sender --
class=spam --source=error

dspam-ham   unix    -       n       n       -       10      pipe
     flags=Rhq user=dspam argv=/usr/bin/dspam --user $sender --
class=innocent --source=error

dspam-filter unix - - n - 10 lmtp
     -o smtp_send_xforward_command=yes
     -o disable_mime_output_conversion=yes
     -o smtp_generic_maps=

localhost:10026 inet n - n - - smtpd
     -o content_filter=
     -o
receive_override_options=no_unknown_recipient_checks,no_header_body_
checks
     -o smtpd_helo_restrictions=
     -o smtpd_client_restrictions=
     -o smtpd_sender_restrictions=
     -o smtpd_recipient_restrictions=permit_mynetworks,reject
     -o mynetworks=127.0.0.0/8
     -o smtpd_authorized_xforward_hosts=127.0.0.0/8
```

Enregistrez et quittez.

Il nous reste plus qu'à dire à Postfix d'utiliser tout ceci :

```
bebeserv:/etc/postfix# nano main.cf
```

Rajoutez cette ligne :

```
transport_maps = hash:/etc/postfix/conf.d/transport
```

et modifiez celle-ci :

```
smtpd_recipient_restrictions =
     permit_mynetworks,
     permit_sasl_authenticated,
```

```
     reject_invalid_hostname,
     reject_unauth_destination,
     reject_unknown_sender_domain,
     reject_unknown_recipient_domain,
     reject_unauth_destination,
     check_recipient_access
pcre:/etc/postfix/conf.d/dspam_filter_access
```

Enregistrez et quittez.

Rechargeons la configuration de Postfix pour terminer le travail :

```
bebeserv:/etc/postfix# /etc/init.d/postfix reload
[...]
```

Voilà c'est terminé, vous possédez maintenant un antispam, bien sûr il faudra lui apprendre à reconnaître les spams mais je ne doute pas que vous en serez très vite satisfait.

Votre antispam est paramétrable par utilisateur ne l'oubliez pas ! Si l'un d'entre eux demande un tag différent c'est possible. Vous pouvez aussi voir les statistiques de Dspam par utilisateur pour voir son travail. Pour ceci regarder les commandes « dspam_admin », « dspam_stats ».

Pour voir les préférences par défaut :

```
bebeserv:/etc/postfix# dspam_admin list preference default
[...]
```

Pour voir les statistiques d'un utilisateur :

```
bebeserv:/etc/postfix# dspam_stats -H user@bebenet.local
[...]
```

Bientôt je ferais le tuto pour installer un antivirus email. Si aujourd'hui la majorité des emails reçu sont des virus (donc faire d'abord le tuto d'un antivirus aurais été mieux) et bien je pense que non. Dspam consomme tellement peu et reconnaît (pour l'instant) tellement bien les spams qu'il fait très bien le ménage que le besoin d'un antivirus ne se fait pas vraiment sentir.

Une fois que vous aurez confiance en votre Dspam. Vous pourrez lui demander de ne pas vous transmettre les spams et ainsi à ce moment là branchez un antivirus sur votre Postfix. La consommation de ressources en sera bien moindre.

A très bientôt

```
bebeserv:/etc/postfix# exit
logout
ALBAN@bebeserv:~$
```