

Distribution EOLE - Tâche #36128

Scénario # 35901 (Terminé (Sprint)): Blocage de la transmission de messages utilisant certains mots-clés et/ou ayant certains types de contenu

Etude du blocage avec spamassassin

09/08/2024 17:28 - Emmanuel GARETTE

Statut:	Fermé	Début:	09/08/2024
Priorité:	Normal	Echéance:	
Assigné à:	Emmanuel GARETTE	% réalisé:	100%
Version cible:	Livraison Cadoles - MEN 31/08/2024 (20)	Temps estimé:	0.00 heure
		Temps passé:	0.00 heure
Description Spamassassin n'est pas utilisé pour les comptes authentifiés. Il faut commencer par supprimer les lignes : "!authenticated = *" dans le fichier /etc/exim4/eole.d/acl/spamassassin.conf et redémarrer exim. Dans le répertoire /etc/spamassassin j'ai ajouté un fichier 70_eole.cf Dedans j'ai mis le contenu suivant : <pre>header EOLE_HEADER Subject =~ /\btest\b/i /\bviagra\b/i body EOLE_BODY /\btest\b/i /\bviagra\b/i score EOLE_HEADER 6.00 score EOLE_BODY 6.00 describe EOLE_HEADER Bad Word describe EOLE_BODY Bad Word</pre> Si je met "viagra", "v1agra" ou "viaGra" dans le titre ou le body, le mail ne part pas sur roundcube (voir la capture). Par contre si je met "viagras" cela passe (on regarde le mot complète uniquement).			

Historique

#1 - 09/08/2024 17:29 - Emmanuel GARETTE

- Fichier Capture d'écran du 2024-08-09 16-57-44.png ajouté

#2 - 09/08/2024 17:38 - Emmanuel GARETTE

- Statut changé de Nouveau à À valider

#3 - 09/08/2024 17:41 - Emmanuel GARETTE

- Description mis à jour

#4 - 27/08/2024 13:36 - Laurent Gourvenec

- Statut changé de À valider à Résolu

#5 - 09/09/2024 15:24 - Klaas TJEBBES

- Fichier Capture d'écran_2024-09-09_15-21-35.png ajouté

- Statut changé de Résolu à En cours

Je ne reproduis pas le blocage d'email contenant le mot "viagra". Voir capture ci-jointe.

25 [09/09/2024 15:18:55] vi /etc/exim4/eole.d/acl/spamassassin.conf

```
26 [ 09/09/2024 15:19:34 ] vi 70_eole.cf
27 [ 09/09/2024 15:19:57 ] service spamassassin restart
28 [ 09/09/2024 15:23:08 ] service exim4 restart
29 [ 09/09/2024 15:23:15 ] service exim4-base restart
root@scribe:/etc/spamassassin#
```

```
root@scribe:/etc/spamassassin# cat 70_eole.cf
header EOLE_HEADER Subject =~ /\btest\b/i /\bviagra\b/i
body EOLE_BODY /\btest\b/i /\bviagra\b/i
score EOLE_HEADER 6.00
score EOLE_BODY 6.00
describe EOLE_HEADER Bad Word
describe EOLE_BODY Bad Word
root@scribe:/etc/spamassassin#
```

```
root@scribe:/etc/spamassassin# cat /etc/exim4/eole.d/acl/spamassassin.conf
# Invoke SpamAssassin to obtain $spam_score and $spam_report.
# Depending on the classification, $acl_m9 is set to "ham" or "spam".
#
# If the message is classified as spam, pretend to reject it unless
# user is authenticated.
#
warn
    set acl_m9 = ham
    spam      = nobody:true
    condition = ${if >= {$spam_score_int}{SPAM_SCORE}{1}{0}}
    set acl_m9 = spam
    control   = fakereject
    logwrite  = :reject: Rejected spam (score $spam_score)

# Add an appropriate X-Spam-Status: header to the message.
#
warn
    add_header = X-Spam-Status: ${if eq {$acl_m9}{spam}{Yes}{No}}
    add_header = X-Spam-Score: $spam_score
    logwrite   = :main: Classified as $acl_m9 (score $spam_score)
```

#6 - 10/09/2024 09:12 - Emmanuel GARETTE

- Statut changé de *En cours* à *Résolu*

Effectivement il y a un soucis avec la regexp (visible via la commande spamassassin --lint).

Malheureusement je n'ai pas conservé la machine où j'avais fait les tests.

Voici un fichier 70_eole.cf fonctionnel :

```
header EOLE_HEADER_1 Subject =~ /\bviagra\b/i
header EOLE_HEADER_2 Subject =~ /\bttest\b/i
meta EOLE_HEADER ( (EOLE_HEADER_1 + EOLE_HEADER_2) > 1)
body EOLE_BODY_1 /\bviagra\b/i
body EOLE_BODY_2 /\bttest\b/i
meta EOLE_BODY ( (EOLE_BODY_1 + EOLE_BODY_2) > 1)
score EOLE_HEADER 6.00
score EOLE_BODY 6.00
describe EOLE_HEADER Bad Word
describe EOLE_BODY Bad Word
```

#7 - 12/09/2024 15:23 - Klaas TJEBBES

- Statut changé de *Résolu* à *En cours*

Pas mieux :

```
root@scribe:/etc/spamassassin# cat 70_eole.cf
header EOLE_HEADER_1 Subject =~ /\bviagra\b/i
header EOLE_HEADER_2 Subject =~ /\bttest\b/i
meta EOLE_HEADER ( (EOLE_HEADER_1 + EOLE_HEADER_2) > 1)
body EOLE_BODY_1 /\bviagra\b/i
body EOLE_BODY_2 /\bttest\b/i
meta EOLE_BODY ( (EOLE_BODY_1 + EOLE_BODY_2) > 1)
score EOLE_HEADER 6.00
score EOLE_BODY 6.00
describe EOLE_HEADER Bad Word
describe EOLE_BODY Bad Word
```

Et un email contenant :

"qui veut mon viagra ?"

passé toujours entre 6a.01 et 6a.02.

Dans le doute, j'ai revérifié "/etc/exim4/eole.d/acl/spamassassin.conf" et fait un `StartAll`.

#8 - 13/09/2024 08:18 - Emmanuel GARETTE

- Statut changé de En cours à Résolu

Spamassassin n'a pas de mécanisme de liste noire a proprement parlait. Il rajoute juste quelque chose au score global du mail.

Sur mes tests on voit que dans le header spam assassin met bien tout le temps un score supérieur à 1, dans le corps du texte cela dépend de la phrase qu'on met.

Par défaut, s'il y a un body on part de -1. S'il trouve le mot, il fait +1 donc (EOLE_BODY_1 + EOLE_BODY_2) == 0 et n'est pas > 1.

Une solution est d'augmenter le score lorsqu'on détecte un mot. Mais rien ne dit que cela fonctionnera 100% des cas. S'il récupère un score de -10 par ailleurs, cela passera.

Je propose donc ces modifications suivantes :

```
header EOLE_HEADER_1 Subject =~ /\bviagra\b/i
header EOLE_HEADER_2 Subject =~ /\btest\b/i
body EOLE_BODY_1 /\bviagra\b/i
body EOLE_BODY_2 /\btest\b/i
score EOLE_BODY_1 6.00
score EOLE_BODY_2 6.00
meta EOLE_BAD_WORD ( (EOLE_HEADER_1 + EOLE_HEADER_2 + EOLE_BODY_1 + EOLE_BODY_2) > 1)
score EOLE_BAD_WORD 6.00
describe EOLE_BAD_WORD Bad Word
```

#9 - 19/09/2024 18:06 - Klaas TJEBBES

- Fichier test1.png ajouté

Avec un message contenant plusieurs fois le mot "viagra" (voir capture ci-jointe), mon message est bloqué. Par contre le log montre un score inférieur à 6 (5.2)

```
2024-09-19T17:57:46.487849+02:00 scribe.domscribe.ac-test.fr spamd[109010]: spamd: connection from 127.0.0.1 [
127.0.0.1]:57060 to port 783, fd 5
2024-09-19T17:57:46.493666+02:00 scribe.domscribe.ac-test.fr spamd[109010]: spamd: checking message <b1fb3d756
41931c8a3497d380a97af5b@i-ac-test.fr> for nobody:8
2024-09-19T17:57:46.534546+02:00 scribe.domscribe.ac-test.fr spamd[109010]: spamd: clean message (5.2/6.0) for
nobody:8 in 0.0 seconds, 823 bytes.
2024-09-19T17:57:46.534661+02:00 scribe.domscribe.ac-test.fr spamd[109010]: spamd: result: . 5 - ALL_TRUSTED,A
WL,DRUGS_ERECTILE,EOLE_BODY_1 scantime=0.0,size=823,user=nobody,uid=8,required_score=6.0,rhost=127.0.0.1,raddr
=127.0.0.1,rport=57060,mid=<b1fb3d75641931c8a3497d380a97af5b@i-ac-test.fr>,autolearn=no autolearn_force=no
2024-09-19T17:57:46.557060+02:00 scribe.domscribe.ac-test.fr spamd[109009]: prefork: child states: II
```

#10 - 18/10/2024 10:14 - Joël Cuissinat

- Statut changé de Résolu à Fermé
- Restant à faire (heures) mis à 0.0

Pour mémoire, le seuil peut être modifié avec la variable experte **exim_spam_score** "Seuil de détection d'un spam (multiplié par 10)" : https://eole.ac-dijon.fr/documentations/2.8/completes/HTML/ModuleScribe/co/02b_messagerie_2.html

Fichiers

Capture d'écran du 2024-08-09 16-57-44.png	46,6 ko	09/08/2024	Emmanuel GARETTE
Capture d'écran_2024-09-09_15-21-35.png	60,3 ko	09/09/2024	Klaas TJEBBES
test1.png	110 ko	19/09/2024	Klaas TJEBBES