tetaneutral.net - Evolution #99

spam sur le serveur smtp

12/10/2011 09:13 - Laurent GUERBY

Statut:	Fermé	**Début:**	12/10/2011
Priorité:	Normal	**Echéance:**	
Assigné à:	Mehdi Abaakouk	**% réalisé:**	70%
Catégorie:		**Temps estimé:**	1.00 heure
Version cible:			

Description

Une machine sur le reseau ouvert de Myrys a envoyé des milliers de spam via le serveur SMTP de l'association.

Il faut que spamd filtre les emissions lors d'un relay

Historique

#1 - 12/10/2011 09:14 - Laurent GUERBY

Solution temporaire : exclusion de l'IP NAT du CISCO Myrys :

/etc/postfix/main.cf
mynetworks = 127.0.0.0/8, !91.224.148.5, 91.224.148.0/23

#2 - 12/10/2011 09:14 - Laurent GUERBY

<guerby> sileht, ya plein de Oct 9 06:25:12 lists spamd[22646]: config: cannot create user preferences file /nonexistent/.spamassassin/user_prefs: No such file or directory
<guerby> Oct 9 06:25:12 lists spamd[22646]: spamd: failed to create readable default_prefs: /nonexistent/.spamassassin/user_prefs
<guerby> sileht, dans /var/log/mail.info-20111012
<guerby> sileht, c'est normal ou il manque un bout de config ?
<sileht> guerby, dans spamassasin y'a 2 mode:
<sileht> en root, puis il se fork en l'utilisateur final pour lire ses preferences
<sileht> en utilisateur non priviligié, et seul les regles system marche
<sileht> comme tu fait open relay , la 2 solutions me parait plus approprié

#3 - 12/10/2011 13:07 - Mehdi Abaakouk

Voici les modifications que j'ai effectué pour spamassassin:

groupadd -g 501 spamd
useradd -u 501 -g 501 -s /sbin/nologin -d /var/lib/spamd spamd
mkdir /var/lib/spamd
chown spamd:spamd /var/lib/spamd

dans /etc/default/spamassassin:
OPTIONS="--create-prefs --max-children 5 --username spamd --helper-home-dir /var/lib/spamd"

dans /etc/spamassassin/local.cf ajouter:
bayes_path /var/lib/spamd/bayes
bayes_file_mode 0666

changer le user dans /etc/postfix/master.cf:
spamassassin unix - n n - - pipe
user=spamd argv=/usr/bin/spamc -f -e
/usr/sbin/sendmail -oi -f ${sender} ${recipient}

#4 - 12/10/2011 13:27 - Mehdi Abaakouk

Ajout des blacklist sbl-xbl dans /etc/postfix/main.cf:

smtpd_recipient_restrictions = permit_mynetworks,
reject_rbl_client sbl-xbl.spamhaus.org,
reject_unauth_destination

#5 - 27/10/2011 14:05 - Laurent GUERBY

Reflexions sur SMTP :

http://ask.slashdot.org/comments.pl?cid=37014576&sid=2368584&tid=14

#6 - 28/10/2011 11:51 - Thomas Barandon

Pour l'avoir utilisé dans mon ancienne boite, gmail for domains est juste excellent, mais on est loin du DIY ou encore de la net neutrality...
La MES et l'administration d'une infra mail est toujours très lourde et à risque mais aussi très intéressant à maintenir et faire évoluer.

D'ailleurs, je m'étonne de pas avoir vu de roundcube ou autre poper sur l'infra ttn ! :) (ou alors j'ai mal regardé)

Laurent GUERBY wrote:

> Reflexions sur SMTP :
>
> http://ask.slashdot.org/comments.pl?cid=37014576&sid=2368584&tid=14

#7 - 08/12/2011 00:05 - Laurent GUERBY

91.224.149.207 blacklisted at b.barracudacentral.org (in reply to RCPT TO
command)

root@h3:~# host 207.149.224.91.b.barracudacentral.org
207.149.224.91.b.barracudacentral.org has address 127.0.0.2
root@h3:~# host 208.149.224.91.b.barracudacentral.org
Host 208.149.224.91.b.barracudacentral.org not found: 3(NXDOMAIN)
root@h3:~# host 206.149.224.91.b.barracudacentral.org
Host 206.149.224.91.b.barracudacentral.org not found: 3(NXDOMAIN

Request sent.

#8 - 08/12/2011 00:09 - Laurent GUERBY

Your confirmation number is BBR21323299285-69007-2730.

http://barracudacentral.org/rbl/how-to-use

#9 - 08/01/2012 21:55 - Laurent GUERBY

fab- : 504 5.5.2 <chiliproject>: Helo command rejected: need fully-qualified hostname
guerby myhostname = chiliproject
guerby myhostname = chiliproject.tetaneutral.net
/etc/init.d/postfix restart

#10 - 10/08/2018 08:54 - Matthieu Herrb

- Statut changé de Nouveau à Fermé

fermeture de tous les vieux tickets non suivis depuis plusieurs années