Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Greylisting: un sistema molt efectiu per a combatre el spam (7731 lectures)

Per **Kiko Piris**, ***kiko*** ()

Creado el 02/12/2005 14:38 modificado el 02/12/2005 14:38

Si administres el servidor de correu d'un (o més d'un) domini i hi reps spam, aquest article probablement t'interessarà (si vols deixar-lo de rebre a aquest spam, es clar! ;).

El primer que s'ha de dir és que aquest sistema, per a que sigui efectiu, s'ha d'instal.lar a tots i cadascun dels servidors MX del domini que volguem protegir.

Si tenim un MX de backup i no hi podem configurar el *greylisting daemon*, el sistema perd moltíssima efectivitat (perque molts spammers utilitzen els MX de més baixa prioritat a posta).

Si tenim una adreça de correu d'un ISP que recollim via pop o imap, aquest sistema no ens serveix (a no esser que convencem als postmasters del ISP per a que l'instal.lin :P).

Si tenim un domini propi però no administram els servidors MX d'aquest domini (perque hi recollim el correu via pop o imap o bé perque el correu ens ve redirigit a una altra bústia), tampoc podem fer servir *greylisting* al nostre servidor de correu (bé, el podem fer servir, però no ens servirà absolutament per a rès ;).

Això és un sistema **complementari** a els que ja poguem estar utilitzant per a combatre el spam que rebem. Per entendre'ns, la idea no és substituir al SpamAssassin[1]. El que sí fa és *ajudar-lo* i molt!.

Bé, una vegada dit això...

Què putes és això del *greylisting*?

Com diu a la pàgina del projecte[2], el sistema s'aprofita del fet que els spammers no es comporten com s'hauria de comportar qualsevol servidor de correu *normal*.

Com funciona? realment és senzill, tal i com explica aquí[3]:

Quan el servidor de correu rep un missatge, formam una tupla amb aquestes 3 dades:

1. l'adreça **ip del host** que ens vol entregar el correu,
2. l'adreça de correu del **remetent**
3. i l'adreça de correu del **destinatari**

(Alerta que quan parlam d'adreces de correu, ens estem referint sempre a les *envelope address*, que no tenen per què coincidir amb el *From:* i el *To:* que ens mostra el client de correu).

Si és la primera vegada que ens apareix aquesta tupla, refusam el correu amb un codi d'error temporal (450, que indica al servidor remetent que ho reintenti més tard) durant un periode determinat de temps (5 minuts, per exemple).

Quan el servidor remetent ho reintenti, i hagin passat aquests 5 minuts, el nostre servidor acceptarà el correu (la gràcia de tot l'invent està en que els spammers quasi mai ho reintenten).

A partir d'ara, aquesta tupla és recordada pel nostre *greylisting daemon*, i els correus que ens arribin a la mateixa adreça destinataria, provinent del mateix remetent i entregats pel mateix servidor de correu no hauran d'esperar (aquesta tupla

serà recordada durant un temps determinat, 30 dies, per exemple).

I com ho puc fer servir jo això?

Aquí vos contaré com configurar-ho per a un servidor de correu Postfix[4] **versió 2.1 o superior** mitjançant Postgrey[5].

Suposarem que tenim el nostre servidor Postfix correctament configurat i funcionant. Aleshores instal.larem el Postgrey.

Amb Debian[6] unstable[7] o Debian[6] testing[8] tot es redueix a fer el típic aptitude install postgrey[9]

Amb Debian[6] stable[10] també tenim el paquet disponible[11]. Però en aquest darrer cas, lo recomanable és agafar-lo de debian-volatile[12] (aquí trobareu un article d'en Celso[13] explicant més coses sobre *debian-volatile*).

Com configuram Postfix? difícilment podria esser més senzill. Es tracta d'afegir una *smtpd_recipient_restriction*, tal que així:

```
smtpd_recipient_restrictions =
   ...
   permit_mynetworks
   ...
   reject_unauth_destination
   check_policy_service inet:127.0.0.1:60000
```

I ja està!

El postgrey es pot configurar de la següent manera:

A **/etc/postgrey/whitelist_recipients.local** hi posariem les adreces destinataries a qui no volem que s'hi apliqui greylisting (si, per exemple, algun usuari del nostre domini no vol que el seu correu sigui retardat en cap cas).

A **/etc/postgrey/whitelist_clients.local** hi posariem les adreces dels servidors que no ens interessa "fer esperar".

Per exemple, al *whitelist_clients.local* jo hi he posat l'adreça ip del servidor de correu de bulma.net, perque el correu de la meva adreça de bulma.net (redirigit a una adreça del meu domini) ve d'un servidor que se segur que ho reintentarà i és absurd fer-lo esperar.

En el cas del spam que rebo a aquesta adreça de bulma.net, el postgrey del meu servidor no pot fer-hi rès. Si volgués beneficiar-me dels avantatges del greylisting a aquesta adreça, haurien d'esser el(s) postmaster(s) de bulma.net qui l'instal.lassin al MX de bulma.net.

Com a darrer comentari, dir que a Debian[6] hi ha un paquet que es diu greylistd[14] per a utilitzar-lo amb Exim 4[15]. Vist lo fàcil que és configurar-ho amb Postfix, no crec que ho sigui molt més amb Exim. Estaria bé que algú que utilitzi Exim ho provàs i ho contàs als comentaris (o a un altre article!).

Traducció automàtica d'aquest article (gràcies a interNOSTRUM)[16].

Lista de enlaces de este artículo:

1. http://spamassassin.apache.org/
2. http://projects.puremagic.com/greylisting/
3. http://projects.puremagic.com/greylisting/whitepaper.html
4. http://www.postfix.org/
5. http://isg.ee.ethz.ch/tools/postgrey/
6. http://www.debian.org/
7. http://www.debian.org/releases/unstable/
8. http://www.debian.org/releases/testing/
9. http://packages.debian.org/postgrey

10. http://www.debian.org/releases/stable/
11. http://packages.debian.org/stable/mail/postgrey
12. http://volatile.debian.net/
13. http://bulma.net/body.phtml?nIdNoticia=2143
14. http://packages.debian.org/greylistd
15. http://www.exim.org/
16. http://www.internostrum.com/navegar.php

E-mail del autor: bulma _ARROBA_ pirispons.net