Kako umanjiti štetu nakon provale preko SASL-a?

Spamiranje s vlastitog servera smo svi doživjeli, ponajviše zahvaljujući našim vlastitim neopreznim korisnicima. Ma koliko korisnike učili i obavještavali da ne smiju slati nikome svoju zaporku (pa ni nama administratorima), uvijek netko "nasjedne". Možda najčešće "padnu" na web formulare, jer izgledaju vjerodostonije od nemuštih mailova u kojima ih se upozorava da hitno promijene lozinku jer će izgubiti podatke i slično.

Posljedice ovakvog ponašanja korisnika svi znamo: vrlo brzno stignemo na black liste, i gotovo nikome više ne možemo slati mail. Osim toga, imamo na desetke tisuća mailova u queueu koji čekaju isporuku. Njih sve treba pobrisati (na Portalu potražite skriptu delete_from_mailq.pl na stranici http://sistemac.carnet.hr/node/203 [1]). To nije problem ako spamer koristi uvijek istu odlaznu adresu, no često se događa da se adresa mijenja sa svakim poslanim mailom. Pošiljatelji tada imaju neka slučajna imena, poput:

```
pyjo@domena.hr
ruk@domena.hr
```

Sve što tada možete učiniti je pobrisati sve mailove sa:

```
# delete_from_mailq.pl \*@domena.hr
```

Ova će operacija, naravno bez ikakve obavijesti, obrisati zaista sve mailove koji su trenutno u redu čekanja, uključujući i one od vaših korisnika. Zato, da ne biste doživjeli prozivanje kod pretpostavljenih, vrijedi se malo potruditi. U ovom slučaju je svakako "bolje spriječiti nego liječiti".

Što možemo učiniti? Ne previše, ali u nekim slučajevima će to biti već zamjetna pomoć. Ideja je sljedeća: forsirati da svi mailovi korisnika autenticiranog preko SASL-a imaju istu odlaznu adresu.

Ovo će olakšati prepoznavanje korisnika kojemu je provaljen password, ali možda i u potpunosti spriječiti masovno spamiranje. Razlog je taj da će svi mailovi koji nemaju točno određen oblik biti zaustavljeni još kod primitka i neće (previše) opterećivati reusurse servera.

Nešto slično smo imali u članku http://sistemac.carnet.hr/node/388 [2], gdje smo *potiho* forsirali da svi korisnici imaju uniformne adrese. Ovdje ćemo spriječiti korisnika (ili spamere koji znaju korisnikovu lozinku) da uopće pošalju mail koji nema točno određenu odlaznu adresu. E, to je već konkretna pomoć, zar ne?

Naravno, za oblik adrese ćemo odabrati standardni oblik ime.prezime@institucija.hr, a nećemo zaboraviti i one koji vole korisnik@institucija.hr. Sve što nam treba je jedan redak u **/etc/postfix/main.cf**, jedan skripta i jedan *cron job*. Zapravo, skriptu i *cronjob* već imamo od paketa postfix-cn, samo ćemo ih iskopirati i malo prepraviti.

1. Skripta

Skriptu make-aliases-gecos.sh smo bez pitanja ukrali od CARNetovih maintainera, preimenovali u make-senders.sh (ime je proizvoljno, možete je nazvati kako želite) i prepravili je:

```
#!/bin/sh
set -e

PATH=/sbin:/usr/sbin:/bin:/usr/bin:$PATH

sasl="/etc/postfix/filtered_senders"
dom="domena.hr"
fqdn="server.domena.hr"

[ -x /usr/sbin/postmap ] || exit 0
[ -f /etc/postfix/main.cf ] || exit 0

grep -q "hash:$sasl" /etc/postfix/main.cf || exit 0

[ -d /var/lib/postfix-cn/ ] || exit 0

# Load CARNet Tools
. /usr/share/carnet-tools/functions.sh

getent passwd | awk -vm="@$dom" -vf="@$fqdn" -F: '
        $3 >= 100 && $1 != "nobody" && $1 != "bacula" && $5 \
        {
                split($5, g, ",");
                if (g[1]=="") {next};
                gsub(/ /, ".", g[1]);
                print tolower(g[1]) m" " $1 f;
                print tolower($1) m" " $1 f;
        }' | sort -u > $sasl.dpkg-tmp.$$

if ! cmp -s $sasl.dpkg-tmp.$$ $sasl > /dev/null; then
  cp_mv $sasl.dpkg-tmp.$$ $sasl
  postmap hash:$sasl
else
  rm -f $sasl.dpkg-tmp.$$
fi
```

U skripti trebate definirati domenu ($dom) i potpuno ime računala ($fqdn). Skriptu snimite gdje vam odgovara, možda u direktorij s vašim sistemskim skriptama ili ćete je staviti u **/usr/share/postfix-cn** zajedno s make-aliases-gecos.sh - svejedno je.

Skripta će generirati datoteku, odnosno bazu ovakvog sadržaja:

```
aperic@domena.hr        aperic@server.domena.hr
ante.peric@domena.hr    aperic@server.domena.hr
```

Ove unose treba citati ovako: autenticirani korisnik aperic@server.domena.hr može slati mail kao "aperic@domena.hr" i "ante.peric@domena.hr". Svi drugi oblici adrese će biti odbijeni odmah kod zaprimanja.

2. Cron job

U /etc/cron.d iskopirajte datoteku postfix-cn u primjerice "make_senders". Sadržaj je kratak:

```
#!/bin/sh
PATH=/sbin:/usr/sbin:/usr/local/sbin:/bin:/usr/bin:$PATH

0 0-23/1 * * * root if [ -x /usr/share/postfix-cn/make-senders.sh ]; then
      /usr/share/postfix-cn/make-senders.sh; fi
```

3. main.cf

U /etc/postfix/main.cf treba dodati dva retka:

```
smtpd_sender_login_maps = hash:/etc/postfix/filtered_senders
smtpd_sender_restrictions = reject_unknown_sender_domain,
   reject_authenticated_sender_login_mismatch
```

Samo još trebate napraviti bazu (dok cron ne odradi svoje) i restartati postfix (moguće da je dovoljno napraviti samo *reload*):

```
# postmap hash:/etc/postfix/filtered_senders
# /etc/init.d/postix restart
```

Ukoliko sve radi kako treba, u logovima (**/var/log/mail.log** ili **/var/log/mail/mail.log**) ne biste trebali ništa vidjeti što se i dosada nije pojavljivalo. No, ukoliko korisnik SASL-a pokuša poslati mail koji nije u bazi, to ćete moći detektirati:

```
unknown[161.53.X.Y]: 553 5.7.1 <lana@domena.hr>: Sender address rejected:
not owned by user lana@server.domena.hr; from=<lana@domena.hr> to=<pero@gmail.
proto=ESMTP helo=<domena314>
```

Možda će nekima ovo biti mala pomoć, ali znamo da će onima koji su iskusili napade i zbog toga imali probleme, ove upute značiti mnogo više.

Zdravko Rašić

sri, 2014-01-29 01:40 - Zdravko Rašić**Kuharice:** Linux [3]
Kategorije: Servisi [4]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1347

Links
[1] https://sysportal.carnet.hr/node/203
[2] https://sysportal.carnet.hr/node/388
[3] https://sysportal.carnet.hr/taxonomy/term/17

[4] https://sysportal.carnet.hr/taxonomy/term/28