Postfix: filtriranje poruka na osnovu zaglavlja i/ili sadržaja

 Kadkad baš i ne možemo biti sigurni da li ćemo pogoditi pravu metodu filtriranja neželjene pošte. U pravilu, što jače pooštrimo kriterije, veća je vjerojatnost da se iz opticaja povuče i korisna e-pošta, pa je često najbolje rješenje da se filtrirane poruke ne brišu automatski, već stave na čekanje u tzv. *hold queue*, gdje čekaju dok administrator ne odluči koje treba a koje ne treba proslijediti primatelju.

Podsjetimo prvo na ranije članke u kojima su opisana pravila, po kojima je moguće filtrirati e-poštu na osnovu primatelja (Postfix: Selektivna zaštita korisnika [1]) ili na osnovu pošiljatelja (Kako zabraniti primanje određenih dolaznih poruka? [2]).

U daljnjem tekstu bit će riječ o još dva pravila filtriranja, po zaglavlju i po sadržaju poruke a koja će se metoda ili čak kombinirane metode koristiti, ovisi o tome, s kako dovitljivim rasijačima *spam* i *phishing* poruka imamo posla.

Da bi e-poštu filtrirali po zaglavlju ili sadržaju (tijelu poruke), potrebno je imati instaliran dodatak postfixu za obradu *regularnih izraza*, najčešće se rabi ili ***regexp*** ili ***pcre***. Recimo da ste se odlučili za *pcre* (=*Perl Compatible Regular Expressions*), onda prvo provjerite da li je instaliran:

```
 dpkg -l|grep pcre
```

pa ako vidite da nije, onda ga instalirate naredbom:

```
apt-get install postfix-pcre
```

Ako želite mogućnost filtriranja i po zaglavlju (header) i po tijelu (body) poruke, onda u datoteku **/etc/postfix/main.cf** dopišite:

```
header_checks = pcre:/etc/postfix/header_checks
body_checks = pcre:/etc/postfix/body_checks
```

Kreirajte navedene datoteke (imena su proizvoljna), ako ne postoje:

```
touch /etc/postfix/body_checks /etc/postfix/header_checks
```

U datoteku **/etc/postfix/header_checks** sada možete upisati filtere poput:

```
#Format zapisa je:
#/^HEADER: .*content_to_act_on/ ACTION
#
 /^To: .*Parris/ HOLD Spam Header Rule #AMG Header Par*ris#
 /^From: .*Canadian-Pharmacy/ HOLD Spam Header Rule #Cana*dian-Phar*macy#
```

```
 /^From: .*info\Sappastudio.it/ HOLD Spam Header Rule #appas*tudio.it#
 /.*hooshmand.yazd.*/ HOLD Spam Header Rule #hoosh--mand#
 /^Subject: .*viagra/ HOLD Spam Header Rule #via*-gra#
#Pozivi na  Facebook, LinkedIn... cesto u naslovu imaju rijec "Accept?" a vrlo cesto
#su laznjaci, da bi se dobila lozinka korisnika, u slijedecem redu je definirano da s
e
# pozivima  za druzenje na drustvenim mrezama naslov zamijeni u upozorenje #OPREZ!#
/^Subject: .*ccept/ REPLACE Subject: #OPREZ!#
#Iduci redci: Naslov je SIGURNO neprihvatljiv, poruku odmah odbij (ne stavljaj na cek
anje).
 /^Subject:(.*)penis|(.*)fuck|(.*)viagra|(.*)pr0n/ REJECT Dont Bother Sending Rubbish
 Emails
 /.*free money.*/ REJECT
```

Primjetite da iza ključne riječi HOLD Spam Header Rule između dviju "taraba" (#) stoji opis o kojem se pravilu radi. To je korisno radi praćenja logova, ali treba paziti da ne bude isti kao i tekst koji se filtrira, jer će poruke logova koje daje *monit* ili OSSEC biti također zaustavljene (HOLD) ili odbačene (REJECT), (zato su ovdje stavljene zvjezdice ili crtice unutar njega!).

Unutar direktorija **/etc/postfix/** je potrebno još samo utipkati:

```
postmap header_checks
```

(eventualno se pojave opomene tipa: "record is in "key: value" format; is this an alias file?" ili "postmap: warning: header_checks.db: duplicate entry: "/^from:", no u pravilu se mogu ignorirati.)

Provjeriti da li je kreirana datoteka ***header_checks.db,*** te ponovo učitati postfix konfiguraciju:

```
postfix reload
```

Ista je procedura i za filtriranje po tijelu poruke: u datoteku **/etc/postfix/body_checks** upišemo pravila filtriranja, npr:

```
 /wants to follow you/ HOLD Body Rule #slijediti#
 /www.piramidasunca.ba/ HOLD Body Rule #pira*mide#
 /Dear Webmail Account User/ HOLD Body Rule #Dear W*ebmail..#
```

ili bilo koji tekst koji je jednoznačan za neželjenu poštu, te potom u direktoriju **/etc/postfix/** izvršite:

```
postmap body_checks #kreira ili ažurira bazu body_checks.db
postfix reload
```

Primijetite da se u gornjim primjerima maltene sva filtrirana pošta stavlja da čeka odluku administratora (ključna riječ HOLD) tj. posprema u *queue* direktorij **/var/spool/postfix/hold**.

Kad su filtrirane poruke stavljene na čekanje, može se putem zgodnog *ncurses* programčića ***pfqueue*** obaviti pregled, brisanje, isporuku pojedine ili istovremeno više poruka koje su na čekanju. Program treba pokrenuti (pod *root* ovlastima):

```
pfqueue
```

i u sučelju tipkama 1-4 se pozicionirati u odgovarajući queue direktorij (1=deffered, 2=active, 3=incoming, 4=hold). Ostale važne naredbe su: strelice gore-dolje=pozicioniranje na poruku, 'Enter'=vidi poruku, 'd'=brisanje poruke, 'l'=oslobađanje poruke s liste čekanja primatelju bez nanovog filtriranja, 'r'=oslobađanje poruke s liste čekanja, ali će ponovo proći filtriranje, 't'=(de)selektiranje više poruka, ';'=iduća naredba se odnosi na sve odabrane (selektirane) poruke, '?'=kompletan ispis naredbi.
Taj **pfqueue** je vrlo koristan, kad je u pitanju manji broj poruka (do cca 200) koje čekaju na odluku administratora. Mnogo toga je moguće napraviti i direktno iz komandne linije, treba se samo pozicionirati u direktorij **/var/spool/postfix/hold** U njemu su sve poruke pohranjene kao datoteke imena kojih su jedinstveni heksadecimalni nizovi kao npr:

```
CECB6859E
857F98B79
564157E84
1606D8AFB
930B68AA2
00AC98A9F
22CA28B7B
5C2C98B7A
A6B9E8541
```

Naredba:

```
postcat CECB6859E
```

prikazat će sadržaj poruke CECB6859E, a naredba:

```
mailq
```

poruke i njihove primatelje i pošiljatelje u svim *queue* direktorijima. Mi možemo i sami konfekcionirati naredbu, primjerice:

```
cd /var/spool/postfix/hold; for a in $(ls);do echo;postcat $a|grep 'Subject:';echo "F
ilter:  #$(zgrep $a /var/log/mail.log*|grep '#'|cut -d'#' -f2)#";read -ep "brisati=b,
 dalje=Enter " b;if [[ $b == "b" ]];then rm $a;fi;done;cd -;
```

koja će npr. izlistavati naslove svih poruka u direktoriju uz pravilo po kojemu su filtrirane (zapisano u log datoteci), pa ako vidimo da se nedvojbeno radi o smeću s 'b' možemo brisati datoteku, tj. poruku. Umjesto 'Subject' (naslov) možemo koristiti i neku drugu ključnu riječ, 'From', 'Reply-To' i sl. Poruke, koje nismo obrisali odnosno, za koje znamo da nisu smeće, možemo proslijediti kome su upućene tipkom 'l', kad se pozicioniramo u *hold queue* tipkom '4' u programu **pfqueue**. Za one koji hoće još više mogućnosti iz komandne linije prložena je skripta **hold.sh** pri dnu ovog članka - daje mogućnost pregledavanja, brisanja, proslijeđivanja, kopiranja itd.

Testiranje efikasnosti pojedinih pravila za filtriranje (zar to treba reći ☺) je slanje poruke s kompromitirajućim sadržajem i/ili zaglavljem - samom sebi.

Prilog	Veličina
hold.sh_.txt [3]	2.3 KB

- Logirajte [4] se za dodavanje komentara

čet, 2013-07-04 14:11 - Luka Ćavara**Kuharice:** Linux [5]
Kategorije: Servisi [6]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1289

Links
[1] https://sysportal.carnet.hr/node/943
[2] https://sysportal.carnet.hr/node/735
[3] https://sysportal.carnet.hr/system/files/hold.sh_.txt
[4] https://sysportal.carnet.hr/sysportallogin
[5] https://sysportal.carnet.hr/taxonomy/term/17
[6] https://sysportal.carnet.hr/taxonomy/term/28