Kako se riješiti spamova s vlastitog poslužitelja?

Na Portalu za sistemce smo već u nekoliko smo navrata pisali o tome što učiniti kada nam s vlastitog poslužitelja odlaze stotine spamova. Ovi spamovi mogu vam napraviti problem, jer će vaš poslužitelj biti stavljen na razne crne liste, s kojih se kasnije teško skinuti. Uglavnom, skidanje će svakako potrajati neko vrijeme, a u međuvremenu korisnici zovu i zovu...

Kako vaš poslužitelj postaje izvor spama? Postoji nekoliko uzroka, a jedan od najčešćih je provala na vaš CMS sustav. Napadač jdnostavno pronađe sigurnosni propust u vašem CMS-u, postavi nekoliko svojih skripti i počne slati spamove na sve strane. Nekada su ti spamovi imali različite odlazne adrese koje nemaju veze s vašom domenom, a sada su to gotovo redovito mailovi s vašom domenom (iako korisnici najčešće ne postoje na sustavu). Ovo čini čišćenje nešto težim, jer sada morate paziti da ne obrišete legitimne mailove vaših korisnika.

Drugi čest način neovlaštenog pristupa vašem poslužitelju je dobijanje zaporke nekog od vaših korisnika primjenom nekih od tehnika socijalnog inženjeringa. Obično je to lažiran mail poslan na stotine korisnika, u kojem se pod nekom izlikom traži njihova zaporka. Nakon što zaporka stigne napadaču, on se spaja na poslužitelj i isporuka spamova počinje. Kako je *mail relaying* zabranjen, napadač se spaja na SASL *daemon*, a ponekad i na webmail (najčešće je to popularni Squirrelmail).

Ukoliko je neko računalo u vašo lokalnoj mreži zaraženo, napadač može slati spamove jer je adresama iz lokalne mreže *relaying* dopušten. No, srećom, sve se ove (a i druge) napade može vidjeti u logovima. Kojim? Datoteka je, kao i uvijek kada se radi o mailu /var/log/mail.log (kod nekih je to možda /var/log/mail/mail.log).

Nažalost, unatoč nizu članaka na Portalu, još nam dolaze upiti "što učiniti, kako detektirati tko šalje, kako se skinuti s black lista" i slično. Potpuno i sveobuhvatno rješenje ovog problema u vidu neke kuharice "napravite ovo, upišite ono" ne možemo ponuditi. Svaki slučaj, iako sličan, ima svoje specifičnosti. Primjerice, jedan kolega je promijenio zaporku *provaljenom* korisniku, ali problem nije nestao. Razlog? Sustav je autenticirao zaporku korisnika preko PAM-a i radiusa. Dakle, trebalo je promijeniti i tu zaporku. Drugi kolega je u žurbi mislio da je zaključao račun korisniku, ali taj korisnik je i dalje mogao slati mail (a time su i spamovi mogli prolaziti). Treći kolega je zaboravio restartati *daemon* saslauthd, pa je stara zaporka još neko vrijeme vrijedila. **Nemojte zaboraviti restartati *daemon* saslauthd, kako bi promjena zaporke bila trenutačna.**

Iz svega ovoga proizlazi da je teško predvidjeti sve moguće situacije i opisati ih u jednom kratkom dokumentu.

No, pogledajmo **što ipak možemo učiniti.**

SASL

Čini se da je tumačenje zapisa u logovima nekima malo problematično, pa ćemo se poslužiti kratkom skriptom. Skripta je vrlo jednostavna, a možete je pokretati iz crona, poput nekog *early-warning* sustava.

```
#!/bin/bash
# skripta prati logiranja preko SASL-a i javlja ukoliko se prijedju limiti
set -e
```

```
LIMIT_ALL=500

LOG=/var/log/mail.log

TOTAL=$(grep -c sasl_username $LOG)
UNIQ=$(awk '/sasl_username/ {print $9}' < $LOG | sed 's/sasl_username=//g' \
        | uniq -c | sort -rn | head -1)

if [ "$TOTAL" -gt "$LIMIT_ALL" ]; then
        echo "Ukupno logiranja: $TOTAL"
        echo "Najvise pojedinacnih logiranja: $UNIQ"
fi
```

Skripta je vrlo jednostavna i dobra je za stavljanje u cron. Lako ju je moguće prepraviti za vaše potrebe, iako je mogla biti znatno kompliciranija. No, bolje je složenije stvari prepustiti specijaliziranom softveru (OSSEC, fail2ban).

Napomena: naišli smo i na slučaj kada je u **samo 4 logiranja preko SASL-a** otišlo na stotine poruka, stoga smanjite varijablu $LIMIT_ALL ako imate problem, a skripta ništa ne izbacuje. Uobičajenija je, ipak, situacija da su zabilježene stotine logiranja, jer na ovaj način spamer pokušava raspodijeliti opterećenje mail servisa na dulji vremenski period.

Skriptu možete dodati u cron, ali pazite da se izvršava prije rotiranja logova. U suprotnom, nećete imati potpunu sliku, odnosno broj logiranja zabilježen u logovima bi mogao biti premalen da ih skripta detektira. Vrijeme rotiranja mail logova možete pronaći u datoteci /etc/crontab. Logovi sustava se ne rotiraju preko programa logrotate, nego preko naredbe savelog. Ona se pokreće iz skripte /etc/cron.daily:

```
# grep cron.daily /etc/crontab
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-
parts --report /etc/cron.daily )
```

Na ovom sustavu, cron se pokreće u 6:25, pa stavite da se naša skripta izvršava prije tog vremena. Dodajte sljedeće u rootov crontab (ne zaboravite napraviti stvari koje se podrazumijevaju, poput **chmod a+x sasl-count.sh**):

```
20 6    * * *   /root/bin/sasl-count.sh
```

Skripta će se pokretati svakog dana u 6:20 i javit će vam ukoliko se broj prijava preko SASL-a popeo preko 500. Ovaj broj, naravno, neće odgovarati svima, pa *grepajte* svoje logove i saznajte koliki je broj logiranja u "normalnom" radu. Taj broj onda pomnožite s 2, 3 ili već kojim brojem mislite da bi u vašem slučaju odgovarao. Neki poslužitelji, odnosno korisnici, uopće ne rabe SASL, dok ga neki rabe intenzivno. YMMV.

Skriptu je poželjno modificirati kako bi u potpunosti odgovarala vašim potrebama.

MAILQ

Neki korisnici su predložili sličan sustav "ranog obavještavanja". Ovaj put mjerio bi se broj mailova koje je udaljeni poslužitelj odbio, te se stoga nalaze u queueu *deferred*. Broj odbijenih poruka možete saznati pomoću naredbi:

```
# find /var/spool/postfix/deferred -type f | wc -l
```

ili

```
# mailq | grep -- ^-- | awk '{print $5}'
```

Ove dvije naredbe zapravo nisu istoznačne (mailq će pokazati i sve druge queueove), ali za naše potrebe će biti sasvim u redu. Novu skriptu ćemo još pojednostaviti, jer nas zapravo samo zanima imamo li povećan broj neisporučenih poruka na sustavu ili ne:

```
#!/bin/bash
# skripta prati broj neisporu?enih mailova i javlja ukoliko se prijedju limiti
set -e

LIMIT_ALL=500

TOTAL=$(mailq | grep -- ^-- | awk '{print $5}')

if [ "$TOTAL" -gt "$LIMIT_ALL" ]; then
        echo "Ukupno mailova u queueu: $TOTAL"
fi
```

I ova se skripta može, pod istim uvjetima, staviti u cron. Promijenite je, molimo, po svojim potrebama.

Postfix

Na kraju, bilo je prijedloga da se problem velikog broja spama pokuša ublažiti nekim načinom *throttlinga*. Ideja je možda sasvim u redu, jer ograničiti korisnicima broj mailova u sekundi ili minuti, ograničiti broj primatelja i slično može umanjiti problem, ali ga ne može riješiti ili preduhitriti.

Vjerujemo da je uspjeh ove metode kao načina kontrole mail sustava pomalo ograničen, te da uvelike ovisi o karakteristikama poslužitelja i potrebama korisnika. Postfix svakako ima mogućnosti ovakvog tipa, i svakao bi ih trebalo razmotriti. No, možda će biti bolje takve mogućnosti pogledati u svjetlu bolje raspodjele resursa poslužitelja.

Zaključak

Ponudili smo neka rješenja u borbi protiv spama, te dali neke konkretne i opipljive skripte. Namjerno smo ih napravili rudimentarnim, kako bi vam bilo lakše promijeniti ih. Ukoliko ih poboljšate, podijelite ih s drugim kolegama.

Pogledajte svakako i naše stare članke na ovu temu:

1. Spam kao posljedica phishinga [1]

2. Kako se maknuti s crnih lista? [2]

3. Skripta 'delete_from_mailq.pl' - brisanje mailova iz reda (queuea) po e-mail adresi [3]

4. Kako pronaći spamera u vlastitim redovima [4]

5. Squirrelmailov dodatak Squirrel Logger [5]

sri, 2013-09-18 10:30 - Željko Boroš**Vijesti:** Linux [6]
Sigurnost [7]
Kuharice: Linux [8]
Kategorije: Servisi [9]
Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

Source URL: https://sysportal.carnet.hr/node/1322

Links
[1] https://sysportal.carnet.hr/node/1145
[2] https://sysportal.carnet.hr/node/1261
[3] https://sysportal.carnet.hr/node/240
[4] https://sysportal.carnet.hr/node/925
[5] https://sysportal.carnet.hr/node/906
[6] https://sysportal.carnet.hr/taxonomy/term/11
[7] https://sysportal.carnet.hr/taxonomy/term/13
[8] https://sysportal.carnet.hr/taxonomy/term/17
[9] https://sysportal.carnet.hr/taxonomy/term/28