SASL: Brute force napadi i kako ih onemogućiti

U članku http://sistemac.carnet.hr/node/747 [1] smo opisali jako praktičan sustav za sigurnu autentikaciju korisnika u svrhu slanja e-maila s bilo koje mreže - SASL. On je automatski uključen prilikom instalacije CARNetovog paketa postfix-cn. No, primili smo nekoliko upita kako navedeni sustav isključiti. Zašto bi netko uopće htio isključiti ovaj sustav?

Razlog su *brute-force* napadi, slični kao i oni na SSH. Napadači pomoću gotovih skripti pokušavaju pronaći zaporku za određene korisnike, i na taj način provaliti na sustav. Kako su korisnici obično nemarni sa zaporkama, ovo im može uspjeti, iako ste najosjetljiviji dio sustava (udaljeni pristup preko SSH) možda na neki način već zaštitili.

Napadi preko SASL-a, odnosno njegovog pripadajućeg *daemona* **saslauthd** se lako mogu detektirati u logovima:

```
Jun  5 11:41:37 server postfix/smtpd[14726]: warning:
  unknown[67.23.228.80]: SASL LOGIN authentication failed:
  authentication failure
Jun  5 11:41:37 server saslauthd[3022]: do_auth         : auth
  failure: [user=postmaster] [service=smtp]
  [realm=neki.server.hr] [mech=pam] [reason=PAM auth error]
Jun  5 11:41:35 server saslauthd[3023]: do_auth         : auth
   failure: [user=postmaster] [service=smtp]
...
```

U navedenom primjeru, može se vidjeti kako netko s IP adrese 67.23.228.80 pokušava pronaći odgovarajuću zaporku za korisnika "postmaster". No, nemojte odmah u iptables tablice upisivati ovu adresu, vjerojatno se radi o zaraženom računalu i vlasnik vjerojatno nema pojma da njegovo računalo služi za ilegalne svrhe. Sljedeći dan ovu adresu može dobiti sasvim drugi korisnik. No, svakako biste trebali prijaviti slučaj CERT, onome nadležnom za taj mrežni raspon, ili ukoliko ne možete naći tko je odgovoran za taj raspon, CARNetovom CERT-u.

Ukoliko rabite fail2ban, ipt_recent modul ili OSSEC, ne bi se trebali uzrujavati zbog ovakvih napada, ali ima situacija kada možete razmotriti druga rješenja.

Prvi slučaj

Prvi problem koji nam je stigao se odnosio na slanje spama preko određenog korisničkog računa. Netko je negdje uspio uhvatiti korisnikovu zaporku i tu činjenicu iskoristio kako bi slao spam na tisuće adresa, a polazne adrese su bile iz Saudijske Arabije i Španjolske. Kolega sistem-inženjer je ispravno zaključio da bi trebalo promijeniti zaporku tom korisniku, no to nije "upalilo", i dalje su mailovi prolazili. Ni potpuno brisanje korisnika sa sustava nije pomoglo. Problem je što **saslauthd** *cacheira* korisnikove podatke, i potrebno ga je restartati kako bi se obrisao taj *cache*, i počela vrijediti nova zaporka. Iako iskusan, kolega je bio iznenađen s ovom činjenicom:

```
Izgleda da je ipak kljucno bilo restartati saslauthd sto mi nije bilo ni u
peti. Kada te uhvati panika onda zaboravis na osnovne stvari. Restartao
sam mail + amavis par puta ali da mi sasl nije ni pao na pamet????
```

Dakle, zaključak je: trebate restartati **saslauthd** ukoliko korisnicima mijenjate zaporke:

```
# /etc/init.d/saslauthd restart
```

Drugi slučaj

U drugom primjeru, kolega je imao sličan problem, no kako njegovi korisnici nemaju potrebe slati mail preko AUTH SMTP-a, nego rabe webmail, odlučio je ugasiti SASL u cijelosti. U ovom slučaju je riječ o posebnoj situaciji i maloj instituciji, pa iako ne savjetujemo da u potpunosti gasite SASL, i to se može učiniti. Potrebno je učiniti sljedeće korake:

U datoteci /etc/postfix/main.cf treba ugasiti uporabu SASL-a:

```
smtpd_sasl_auth_enable = no
```

Potrebno je restartati Postfix (u ovom slučaju dovoljno je napraviti reload):

```
# /etc/init.d/postfix reload
```

Sada treba ugasiti sam saslauthd proces. U datoteci /etc/default/saslauthd upišite:

```
START=no
```

te zaustavite servis:

```
# /etc/init.d/saslauthd stop
```

Ukoliko rabite monit, potrebno je onemogućiti automatsko restartanje procesa saslauthd:

```
# update-monit.d
```

Naredba update-monit.d će onemogućiti startanje procesa koji su trenutno neaktivni. Alternativno, možete ručno ugasiti automatsko restartanje **saslauthd** servisa:

```
# cd /etc/monit.d
# mv saslauthd.conf saslauthd.conf.disabled
# pkill monit
```

Gornji recept je isto ono što će napraviti naredba update-monit.d.

Nadamo se da nećete imati toliko problema sa SASL-om da ćete ga morati ugasiti, no dobro je znati da se i to može. Samo pripazite da kod nadogradnje ne "zgazite" konfiguracijske datoteke i vratite se na početno stanje (dakle, da vaš sustav rabi SASL).

pon, 2010-06-14 15:16 - Željko Borš**Kuharice:** Linux [2]
Kategorije: Servisi [3]

Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

Source URL: https://sysportal.carnet.hr./node/752

Links
[1] https://sysportal.carnet.hr./node/747
[2] https://sysportal.carnet.hr./taxonomy/term/17
[3] https://sysportal.carnet.hr./taxonomy/term/28