Kako omogućiti SASL autentikaciju (SMTP AUTH) samo nekim korisnicima?

 Zaprimili smo nekoliko uznemirenih upita kolega sistemaca koji su se uplašili da su im poslužitelji provaljeni. Razlog za to su unosi u logovima, gdje se moglo vidjeti kako se pojedini korisnici autenticiraju preko SASL-a sustava s ispravnim korisničkim podacima, te šalju mailove s različitih mrežnih adresa. Provjerom je ustanovljeno da u to vrijeme ti isti korisnici nisu uopće rabili mail ili računalo.

Jednom dijelu tih poslužitelja je, s druge strane, bio zabranjen pristup nekim besplatnim davateljima mail usluga, jer je s njih bio poslan veliki broj spam poruka. Spamovi su svi kroz poslužitelj prolazili na identičan način, autenticirajući se preko SASL-a i time preskačući određene zaštite koje standardno postoje u Postfixu. Što se zapravo događalo, odakle spamerima zaporke i je li uistinu poslužitelj provaljen?

Spameri su korisničke zaporke saznavali rabeći socijalni inženjering, u većini slučajeva preko ovakvih mailova:

```
Dragi carnet.hr korisni?ki ra?un,


Ova poruka je od svog webmail usluga i održavanja vašeg ra?una e-pošte za
sve korisnike centra. Mi smo poboljšanje naše baze podataka i e-mail centra
zbog spama aktivnosti identificirane u našem sustavu e-pošte. Stoga, kako bi
se izbjeglo sve ra?une spam identificirali smo
poboljšanje i stvaranje prostora za nove.

Vi ste potrebni kako bi potvrdili svoj ra?un e-pošte putem e-pošte potvrdu
identifikacije.To ?e sprije?iti vaš korisni?ki ra?un iz zatvorena tijekom
ove vježbe.

Kako biste potvrdili svoj identitet e-mail, daju sljede?e podatke tražene u
nastavku:


* Korisni?ko Ime: (...........) (required)
* Lozinka: (...........) (required)
* Datum ro?enja: (...........) (Neobavezno)
* Država: (..............) (Neobavezno)
```

Iako nemušto preveden preko nekog od servisa za prevođenje, mail je dovoljno razumljiv i neki korisnici su poslali zaporku. Što učiniti?

Prije svega, svakako **morate** promijeniti zaporke svim korisnicima koji su ih **poslali**, a još bolja opcija baš svim korisnicima, ukoliko je to moguće. Nove im možete priopćiti usmeno ili SMS-om, ili na neki drugi siguran način (npr. preko interne dostavne službe).

Dalje imamo dva puta: jednostavno onemogućiti SASL, ili probati ostaviti ovu mogućnost samo

određenoj skupini korisnika, ukoliko je to moguće.

Onemogućiti SASL je jednostavno, i postupak je opisan u članku "SASL: Brute force napadi i kako ih onemogućiti" na Portalu za sistemce na adresi: http://sistemac.carnet.hr/node/752 [1].

Više informacija o samom SASL-u možete naći u članku "SASL SMTP autentikacija u Postfixu [2]".

Drugi put je pokušati naći rješenje koje će zadovoljiti potrebe vaših korisnika, odnosno postići da korisnici ne moraju mijenjati postavke na koje su se navikli (preko SASL autentikacije mogu bez brige slati mail iz bilo koje mreže). Konketno, zahtjev je bio da zaposlenici (odnosno samo dio zaposlenika koji već rabi SASL) mogu i dalje nastaviti uporabu SASL-a, dok bi svima ostalima SASL bio zabranjen. Time bi se postiglo da čak i ako korisnici nekome ubuduće pošalju zaporku, spameri neće moći zlorabiti vaš poslužitelj.

Naravno, sasvim je druga priča da vaši korisnici ne bi trebali nikome slati zaporku, čak i ako se čini da zahtjev dolazi od CARNeta, uprave ili direktno vas. Tu može pomoći samo obrazovanje vaših korisnika, čime ćete u konačnici sebi uštedjeti neugode i gubitak vremena.

Vratimo se na osnovni problem. Daemon program saslauthd ne podržava nikakvo filtriranje korisnika po nekom kriteriju, primjerice grupi, ali podržava uporabu sustavske (/etc/shadow) ili vlastite baze podataka (/etc/sasldb) o korisnicima. Metodom pokušaja i pogreške, došli smo do zaključka kako bismo mogli postići traženo ukoliko rabimo bazu podataka u /etc/sasldb. Na ovaj način korisnici upisani u bazu u datoteci /etc/sasldb moći će rabiti SASl, dok oni koji nisu neće. Oni koji nisu upisani u /etc/sasldb morat će mail slati iz internih mreža (ili onih navedenih u /etc/postfix/main.cf u parametru mynetworks). Naravno, uvijek im ostaje i webmail, bilo lokalni bilo onaj na adresi http://webmail.carnet.hr).

Prvo što trebamo učiniti da bismo napravili ovaj način autentikacije je napraviti promjene u /etc/default/saslauthd:

```
MECHANISMS="sasldb"
```

Zatim treba dodali "privilegirane" korisnike u bazu:

```
# saslpasswd2 -c korisnik1 -u fqdn.ime.stroja.hr -f /etc/sasldb2
# saslpasswd2 -c korisnik2 -u fqdn.ime.stroja.hr -f /etc/sasldb2
# saslpasswd2 -c korisnik3 -u fqdn.ime.stroja.hr -f /etc/sasldb2
...
```

Provjera konzistentnosti i sadržaja baze:

```
# sasldblistusers2
korisnik1@fqdn.ime.stroja.hr: userPassword
...
```

Ukoliko se kasnije ukaže potreba, korisnika možete obrisati pomoću naredbe:

```
# saslpasswd2 -d korisnik3 -u fqdn.ime.stroja.hr -f /etc/sasldb2
```

Sada treba restartati saslauthd (kao uostalom i poslije svake izmjene baze!):

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

Korisnici koji su upisani i ukucaju dobru zaporku ostavljaju ovakav zapis u logovima:

```
Sep 14 11:22:43 po postfix/smtpd[2686]: D2745135951:
  client=fqdn.ime.stroja.hr[161.53.xx.yyy], sasl_method=PLAIN,
  sasl_username=korisnik1@fqdn.ime.stroja.hr
```

Ako korisnik ne postoji ili je slučajno ukucao pogrešnu zaporku, zapis će izgledati ovako:

```
Sep 14 11:20:21 po postfix/smtpd[3230]: warning: SASL authentication failure:
  Password verification failed
Sep 14 11:20:21 po postfix/smtpd[3230]: warning:
  korisnik_izvan_sasldb@fqdn.ime.stroja.hr [1.2.3.4]: SASL PLAIN
  authentication failed: authentication failure
```

Ako nešto ne radi, možete ugasiti saslauthd i dobiti više informacija u *debug* načinu rada, tako da saslauthd pokrenete sa:

```
# /usr/sbin/saslauthd -d -a sasldb -c -m /var/run/saslauthd -n 5
```

Ne zaboravite pri tome ugasiti servis saslauthd u monitu (ukoliko rabite monit)!

Napomene:

- korisnici koji nisu u bazi neće moći rabiti SMTP AUTH, i dobit će poruku da su ukucali pogrešnu zaporku, što ih može zbuniti

- korisnici u bazi /etc/sasldb ne moraju uopće postojati na sustavu, a moći će slati mail

- *realm* je ime stroja, ali ako ne radi probajte staviti domenu

- također, korisnici i dalje mogu lažirati ime u MAIL FROM, ako ne napravite dodatne mjere, npr: http://sistemac.carnet.hr/node/388 [3]

- ako vam poslužitelj odbija konekciju nakon par provjera u kratkom vremenu, provjerite imate li uključen fail2ban ili neki drugi vid aktivne zaštite (iptables ipt_recent modul!)

Ukoliko vam ovakve negativne posljedice ne smetaju, probajte ovakav način autenticiranja, ali ne zaboravite - obrazovanje vlastitih korisnika nema zamjene, ma koliko se činilo da uzima previše vremena. Uvijek se na kraju isplati.

- Logirajte [4] se za dodavanje komentara

uto, 2010-11-23 12:45 - Željko Boroš**Kuharice:** Linux [5]
Kategorije: Software [6]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr./node/794

Links
[1] https://sysportal.carnet.hr./node/752
[2] https://sysportal.carnet.hr./node/747
[3] https://sysportal.carnet.hr./node/388
[4] https://sysportal.carnet.hr./sysportallogin
[5] https://sysportal.carnet.hr./taxonomy/term/17
[6] https://sysportal.carnet.hr./taxonomy/term/25