Dodatna sigurnost za SSH - pam_access

Dopuštanje pristupa na poslužitelj putem protokola SSH (a prije i preko TELNET-a) je u sigurnosnom smislu oduvijek bilo problematično . Iako ste (možda) vjerovali svojim korisnicima, nikada niste mogli znati je li zaporka *provaljena* i tko je zaista prijavljen na sustav. Jednom kad je prijavljen, napadač ima širom otvorena vrata da pokuša "provaliti" korisnika root, a time i cijeli sustav. Na ovaj način mu je znatno olakšan posao, jer je probiti sustav (pa makar i preko neprivilegiranoh korisnika) daleko teže kada se radi udaljeno.

Neki su problem riješili na način da pristup shellu preko SSH-a nema nitko, odnosno samo nekolicina korisnika koje je tako daleko lakše pratiti i provjeravati što rade na sustavu. To je dobro rješenje, ako ga smijete upotrijebiti. Neki su samo pokušali otežati *brute-force* napade na slabe zaporke premještajući port na kojem sluša SSH daemon, ili su preko iptablesa ograničili mreže s kojih se može pristupiti (recimo, samo iz Hrvatske, gdje se u slučaju potrebe možemo obratiti providerima i njihovim CERT timovima).

Problem s iptablesom je što ne diskriminira po korisničkom imenu, nego pušta sve korisnike, bitno je samo da dolazi iz dopuštenih mreža. U konfiguraciji SSH daemona je, pak, moguće ograničavati korisnike, ali ne i adrese s kojih dolaze.

Postoji elegantno rješenje za ovu kombinaciju, moguće je ograničiti SSH pristup shellu na razini korisnika. Ovo otvara zanimljive mogućnosti, da jedan korisnik može pristupiti samo iz Hrvatske, a drugi može samo iz inozemstva, ali nikako ne iz Hrvatske (recimo, radi se o nekom vanjskom suradniku koji sasvim sigurno neće pristupati iz Hrvatske i svaka aktivnost na tom računu je odmah sumnjiva ako dolazi iz mreža HR ISP-ova).

Mi ćemo se pozabaviti ovim problemom uz pomoć dobrog starog PAM-a i modula **pam_access.so**.

Modul pam_access.so se nalazi u paketu libpam-modules, koji ćete instalirati na uobičajen način ukoliko slučajno nije instaliran. Konfiguracija se radi pomoću direktiva u datoteci **/etc/security/access.conf**, ali prije toga potrebno je omogućiti ovaj modul u datoteci **/etc/pam.d/sshd:**

```
server$ grep pam_access /etc/pam.d/sshd
# account  required     pam_access.so
```

Samo obrišite znak '#' na početku retka. Provjerite također postoji li redak "**UsePAM yes**" u /etc/ssh/sshd_config. Ukoliko ga nema, dopišite ga ili promijenite vrijednost iz "**no**" u "**yes**".

Vratimo se na /etc/security/access.conf. Konfiguracija će vas možda podsjetiti na konfiguraciju libwrap biblioteke (odnosno TCP wrappera):

```
+ : root : 161.53.X.
```

Format zapisa je sljedeći:

```
dozvole : korisnik : lokacija
```

U polje "dozvole" upisuje se jednostavno "+" (pristup dopušten) ili "-" (pristup zabranjen).

U polje "korisnik" upisujemo korisnika ili grupu korisnika na koje se dozvola odnosi. Možemo upisati ključnu riječ "ALL", koja znači ono kako glasi: **svi** korisnici ili grupe.

U treće polje, polje "lokacija" upisujemo adresu s koje će se korisnik spajati. Ova adresa može biti u više različitih oblika, a mi preporučujemo standardnu notaciju CIDR:

193.198.X/24 - korisnik se može spojiti samo iz navedene mreže
161.53.X.Y - korisnik se može spojiti samo s te adrese
.domena.hr - korisnik se može spojiti samo iz navedene domene

Primjerice, pravilo:

```
+ : root : 161.53.X.0/24
```

dopušta spajanje korisniku root iz navedene mreže (ako je dopušteno spajanje korisnika root u /etc/ssh/sshd_config).

Pravilo:

```
+ : pperic : .hr
```

dopušta spajanje korisniku od bilo kuda, sve dok adresa završava s ".hr". Ovo znači da DNS mora savršeno funkcionirati, pa iako to nekad može biti problem, nema drugog načina da dopustite samo jednoj zemlji ili domeni pristup (jer danas i mali ISP-ovi imaju nekoliko mreža - CARNet ima 5, T-com 17 i tako dalje).

Postoje još neke ključne riječi, primjerice "NONE", što je zapravo negacija "ALL", i ne dopušta pristup nikome. Postoji i ključna riječ "LOCAL", koja ograničava pristup na lokalno računalo (dakle, ime računala ne može sadržavati nijednu točku, npr. "server.nekadomena.hr").

Ugrađen je jedan operator, "EXCEPT", koji dopušta inznimke od pravila navedenog prije, primjerice:

```
+ : ALL EXCEPT pperic : ALL
```

Gornje će pravilo dopustiti spajanje svima osim korisniku pperic. Slično tome, možemo zabraniti pristup grupi korisnika:

```
- : (studenti) : ALL
```

Grupa se piše u zagradama, da se razlikuje od korisničkih računa istog imena (iako nije obavezno).

Koja je logika pronalaženja i izvršavanja pravila, koji se prvi poklopi, rezultantni skup ili nešto treće? Odgovor je ovo prvo, vrijedi prvo pravilo koje zadovoljava kombinaciju korisnika i lokacije. Sva daljnja pravila s istom kombinacijom se ne izvršavaju. No, nije loše na kraju staviti neko restriktivno pravilo. Primjerice želite li korisniku "pero" dopustiti spajanje s adrese 161.53.X.Y. Napravili ste pravilo:

```
+ : pero : 161.53.X.Y
```

Ovom ste korisniku dopustili spajanje s određene adrese (što ste i htjeli), ali ste napravili i mnogo više od toga, jer se korisnik može spojiti od bilo kuda. Jednostavno, nema pravila da mu to spriječi. Trebate dodati još jedan redak:

```
+ : pero : 161.53.X.Y
- : pero : ALL
```

ili jednostavnije:

```
- : pero : ALL EXCEPT 161.53.X.Y
```

Još jedna zgodna stvar je korištenje grupa. Tada ne morate navoditi (potencijalno) na desetke korisnika u drugom polju, dovoljno je staviti korisnike u neku grupu (primjerice, "**sshallow**") i napraviti redak:

```
# groupadd -r sshallow
# usermod -a -G sshallow pero
# usermod -a -G sshallow marko...

+ : (sshallow) : ALL
```

U logovima ćete moći pratiti neuspješne pokušaje prijave (i eventualno napraviti fail2ban ili OSSEC pravila po njima?):

```
Apr 30 00:09:31 server sshd[1306]: pam_access(sshd:account): access denied for
   user `pero' from `server.domena.hr'
Apr 30 00:09:31 server sshd[1306]: Failed password for pero from 161.53.X.Y
   port 58497 ssh2
```

U datoteci /etc/security/access.conf ćet pronaći mnogo primjera koji će vam pomoći. Osmislite svoju matricu pristupa, dokumentirajte je i time ćete dobiti sigurniji poslužitelj.

Ukoliko vam je palo na pamet da bi pam_access mogli koristiti i drugi servisi koji znaju raditi s PAM-om, u pravu ste. Bilo koji servis (ftp, primjerice) bi mogao koristiti ovu kontrolu pristupa. Zgodno, ali možda vam SSH korisnici ne trebaju istu razinu pristupa preko ftp-a. U tom slučaju možete koristiti slične mehanizme unutar samog servisa. Uglavnom, sve ovisi o vašim trenutnim potrebama.

Na kraju, nemojte zaboraviti da ste uopće uveli ovu dodatnu razinu zaštite, jer bi vam rješavanje problema korisnika "*zašto se ne mogu prijaviti na server?*" moglo potrajati koji sat.

uto, 2013-04-30 01:00 - Marko Jukić**Kuharice:** Linux [1]
Kategorije: Servisi [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1257

Links
[1] https://sysportal.carnet.hr/taxonomy/term/17

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