Kako ograničiti usera na njegov $HOME direktorij - SFTP

 Uz vlastite korisnike (profesore, studente i ostale djelatnike), na poslužitelj ponekad moramo dodati i vanjske korisnike (primjerice, web developere). Kako vanjskim (a niti 'domaćim') korisnicima ne bismo trebali u potpunosti vjerovati, želja nam je onemogućiti im pristup izvan njihova $HOME direktorija.

Malo googlanja i dobit cemo rješenje pod nazivom 'chroot jail'.

Pristup na poslužitelj obično imaju preko FTP-a, SFTP-a ili SSH-a. Neki sistem-inženjeri odavno ni svojim korisnicima ne daju SSH pristup (a ostali čim prije napravite isto), pa SSH u principu nije problem.

FTP je prastari standard koji se i dalje itekako koristi, ali ima svoje mane, koje ponekad znaju zasmetati. Najveća mana je što prijenos nije enkriptiran, pa mnogi pribjegavaju SFTP-u. Postali smo svjesni da podatke treba štiti i koristiti samo 'sigurne' kanale komunikacije.

Vratimo se FTP-u. O ograničavanju korisnika FTP-a je već bilo pisano na Portalu u članku "**VSFTP: Ograničenje korisnika na njegov $HOME**" na adresi https://sysportal.carnet.hr/node/1034 [1]

Opis je i dalje točan, ali vrijedi samo za FTP. A kako smo mi odlucili implementirati SFTP, pri testiranju smo uočili da se nije ništa promijenilo. Nakon nekoliko sati googlanja otkrijete da od distribucije Debian 7 (wheezy) trebate napraviti još jedan dodatni korak. :)

$HOME direktorij moramo uzeti korisniku i dati korisniku root:

```
# chown root:root /home/korisnik1
# chown root:root /home/korisnik2
# ...
```

Kreirajte folder unutar korisničkog $HOME, nad kojim user ima full ovlasti. To ujedno može biti i public_html koji je već tamo, ili neki novi.

```
# mkdir /home/korinik1/ftpdir
# chown korinsik1:student /home/korinik1/ftpdir
# chmod 755 /home/korinik1/ftpdir
```

Svi direktoriji iznad njega također moraju biti u vlasništvu roota, ali to je za direktorije "/home" i "/" ionako slučaj, pa ne moramo raditi nikakve dodatne intervencije.

S obzirom da se spajamo preko protokola SFTP (ovdje mislimo na kvazi-FTP u sklopu protokola SSH), morat ćemo podesiti SSH daemon.

Ove retke treba dodati na kraj datoteke /etc/ssh/sshd_config (obavezno na kraj!):

---- /etc/ssh/sshd_config ----

```
Subsystem sftp internal-sftp

Match Group sftpuser
     ChrootDirectory %h
     ForceCommand internal-sftp
     AllowTcpForwarding no
```

---- /etc/ssh/sshd_config-----

Ove postavke određuju da će svi korisnici u grupi "sftpuser" kada pristupaju preko protokola SFTP biti zaključani na svoj vlastiti korisnički direktorij. Neće moći vidjeti datotečni sustav izvan svog $HOME.

Nadalje, moramo pripremiti ostatak sustava, prvo ćemo kreirati grupu "sftpuser" i dodati korisnike u nju:

```
# groupadd sftpuser
# usermod korisnik -g sftpuser
```

Opcija "-g" naredbe usermod određuje da se radi o novoj primarnoj grupi, te će sve datoteke unutar $HOME biti dodijeljene novoj grupi (ne i datoteke izvan kućnog direktorija!).

Ukoliko želite da korisnik ima pristup nekom drugom direktoriju (u uobičajeni /home/korisnik), ne zaboravite promijeniti i taj podatak:

```
# usermod korisnik -d /neki/drugi/direktorij
```

Ne zaboravite na pravilo o vlasništvu svih direktorija iznad, koji moraju biti u vlasništvu roota!

Na kraju je potrebno restartati servis SSH, kako bi promjene bile vidljive:

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

Ukoliko želimo (a želimo) u potpunosti zabraniti korisnički pristup ljusci (shellu), potrebno je korisniku promijeniti osnovnu ljusku. Najbolje je to napraviti tako da odredimo da je login ljuska naredba /bin/false:

```
# usermod korisnik -s /bin/false
```

Kako bi ta naredba bila uvažena kao login ljuska, potrebno ju je dodati u datoteku /etc/shells (ako već nije tamo od prije):

```
# cat /etc/shells
# /etc/shells: valid login shells
/bin/ash
/bin/csh
/bin/sh
/usr/bin/es
/usr/bin/ksh
/bin/ksh
/usr/bin/rc
/bin/sash
/usr/bin/esh
/usr/bin/screen
```

```
/bin/bash
/bin/rbash
/bin/zsh
/usr/bin/zsh
/bin/dash
/bin/tcsh
/usr/bin/tcsh
/bin/mksh
/bin/mksh-static
# echo "/bin/false" >> /etc/shells
```

Ukoliko ste sve ispravno podesili, korisnik se neće moći logirati preko SSH, ali će moći pristupiti preko FTP-a i SFTP-a, te će biti ograničen samo na svoj kućni direktorij.

Ukoliko ste pažljivo čitali, nismo spominjali ograničavanje korisnika na svoj kućni direktorij preko SSH pristupa (samo smo ga u potpunosti blokirali).

Također, ukoliko ste ranije dobro planirali, pa su vam korisnički računi (studenti, djelatnici, ..) kod kreiranja bili dodjeljivani u zasebne GUID-e, onda vam je posao uvelike olakšan. Jer s jednom skriptom možete pokupiti samo te korisnike i promijeniti im GUID, shell, $HOME vlasništvo, ... (ali to je za drugu kuharicu).

Ovakav način rada nije trivijalno ostvariti, niti je takav ***chroot jail*** posebno siguran (to mu ni nije prava namjena), pa ga nećemo ovaj put obraditi.

pet, 2016-09-30 14:10 - Domagoj Vuković**Kuharice:** Linux [2]
Kategorije: Servisi [3]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1684

Links
[1] https://sysportal.carnet.hr/node/1034
[2] https://sysportal.carnet.hr/taxonomy/term/17
[3] https://sysportal.carnet.hr/taxonomy/term/28