Chroot login di Linux dengan menggunakan sudo

Asfihani (asfik@cakraweb.com) dan Agung Ud (agung@mawarbiru.net)

24 Februari 2003

Pendahuluan

Tujuan dari *chroot* terhadap suatu *login(account/user)* adalah untuk "memenjarakan" *user* tersebut ke *home* direktorinya sendiri sehingga *user* yang bersangkutan tidak bisa "naik" ke direktori yang lebih tinggi diatasnya. Hal ini mungkin bisa meminimalisir usaha pembajakan terhadap suatu account yang lain (misalnya *root*) ataupun pencurian data *user* maupun data penting lainnya pada suatu sistem operasi linux.

Langkah yang pertama adalah membuat *fake shell* yang akan dijadikan *login shell* terhadap *user* yang akan di*chroot,* disini kita misalkan *shell* tersebut diberi nama **/bin/chroot-sh** isinya adalah :

```
#!/bin/bash
if [ "$1" = "-c" ]; then
i=0;
PARAMS="";
for param in $*; do
if [ $i -gt 0 ]; then
PARAMS="$PARAMS $param";
fi
let i++;
done;
sudo /usr/sbin/chroot /home/$USER /bin/su - $USER -c "$PARAMS"
else
sudo /usr/sbin/chroot /home/$USER /bin/su - $USER
fi;
```

Ubah mode menjadi *executable* :

```
[root@suro root]# chmod +x /bin/chroot-sh
```

Buat *user* baru yang akan di*chroot* sekalian kita set *password*nya :

```
[root@suro root]# useradd -d /tmp -s /bin/chroot-sh suminten
[root@suro root]# passwd suminten
Changing password for user suminten
New password:
Retype new password:
passwd: all authentication tokens updated successfully
```

Buat direktori **etc,dev,bin,lib,usr,usr/bin,home,home/suminten**didirektori **/home/suminten** :

```
[root@suro root]# mkdir -p /home/suminten/{etc,dev,bin,lib,usr/bin,home/suminten}
```

Buat *entry* untuk *user* **root** dan **suminten** di file **/home/suminten/etc/passwd**dan **/home/suminten/etc/group** :

```
[root@suro root]# grep ^root /etc/passwd | sed -e 's{/root{/{g' > /home/suminten/etc/passwd
[root@suro root]# grep ^suminten /etc/passwd | sed -e 's{/tmp{/home/suminten{g;s{chroot-sh{bash{g' >> /home/suminten/etc/passwd
[root@suro root]# grep ^root /etc/group > /home/suminten/etc/group
[root@suro root]# grep ^suminten /etc/group >> /home/suminten/etc/group
```

Install *bash* dengan menyalin file **/bin/bash** ke **/home/suminten/bin**:

```
[root@suro root]# cp /bin/bash /home/suminten/bin
```

Salin file *library* yang digunakan oleh *bash* (anda bisa memeriksanya dengan perintah *ldd*) :

```
[root@suro root]# ldd /bin/bash
```

```
libtermcap.so.2 => /lib/libtermcap.so.2 (0x4001d000)
libdl.so.2 => /lib/libdl.so.2 (0x40021000)
libc.so.6 => /lib/i686/libc.so.6 (0x40025000)
/lib/ld-linux.so.2 => /lib/ld-linux.so.2 (0x40000000)
[root@suro root]# cp /lib/libtermcap.so.2 /home/suminten/lib
[root@suro root]# cp /lib/libdl.so.2 /home/suminten/lib
[root@suro root]# cp /lib/i686/libc.so.6 /home/suminten/lib
[root@suro root]# cp /lib/ld-linux.so.2 /home/suminten/lib/
```

Atau bisa juga dengan menggunakan perintah ini :

```
[root@suro root]# for a in $(ldd /bin/bash | awk '{print $3}'); do cp $a /home/suminten/lib/; done
```

Install program **su** yang termasuk dalam paket **sh-utils** (pada saat dokumen ini ditulis versi yang paling terbaru adalah *sh-utils-2.0.15.tar.gz*, namun anda bisa melihat *source* yang paling baru di http://www.gnu.org/software/shellutils/shellutils.html) :

```
[root@suro root]# wget ftp://alpha.gnu.org/gnu/sh-utils/sh-utils-2.0.15.tar.gz
[root@suro root]# tar -xzvf sh-utils-2.0.15.tar.gz
[root@suro root]# cd sh-utils-2.0.15
[root@suro sh-utils-2.0.15]# ./configure
[root@suro sh-utils-2.0.15]# make
[root@suro sh-utils-2.0.15]# cp src/su /home/suminten/bin
[root@suro sh-utils-2.0.15]# chmod +s /home/suminten/bin/su
```

Salin *library* yang diperlukan oleh **su** (ldd /home/suminten/bin/su) :

```
[root@suro sh-utils-2.0.15]# cp /lib/libcrypt.so.1 /home/suminten/lib
```

Untuk Redhat 7.x, salin pula file **/lib/libnss_files.so.2, /lib/libnsl.so.1**dan **/lib/libnss_compat.so.2** :

```
[root@suro root]# cp /lib/libnss_files.so.2 /home/suminten/lib
[root@suro root]# cp /lib/libnsl.so.1 /home/suminten/lib
[root@suro root]# cp /lib/libnss_compat.so.2 /home/suminten/lib
```

Jika diperlukan juga, install *file-utils* (**ln,ls,rm,mv,cp,du,mkdir**):

```
[root@suro root]# cp /bin/{ln,ls,rm,mv,cp,mkdir} /home/suminten/bin
[root@suro root]# cp /usr/bin/du /home/suminten/bin
```

Periksa kembali *library* yang akan digunakan oleh file-file tersebut dengan menggunakan perintah *ldd* (misalnya: **ldd /bin/ls** dan seterusnya), kemudian salin ke direktori **lib** pada home direktori *user* yang bersangkutan.

Ganti kepemilikan **/home/suminten** (kecuali file **su**) ke *user* **suminten**:

```
[root@suro root]# chown -R suminten.suminten /home/suminten
[root@suro root]# chown root.root /home/suminten/bin/su
```

Jika anda menginginkan agar *user* yang bersangkutan tidak bisa menghapus file/direktori yang digunakan dalam *chroot*, anda bisa menggunakan perintah *chattr* :

```
[root@suro root]# chattr -R +i /home/suminten/{bin,etc,lib}
```

Tambahkan pada file **/etc/sudoers** (anda bisa menggunakan perintah **visudo**) *entry* untuk *user* yang bersangkutan :

```
suminten ALL= NOPASSWD: /usr/sbin/chroot /home/suminten /bin/su - suminten*
```

Jika segalanya berhasil dengan baik anda bisa mencoba *ssh* ke *localhost* dengan menggunakan *user* yang bersangkutan :

```
[root@suro root]# ssh suminten@localhost
suminten@localhost's password:
Last login: Mon Feb 24 10:37:51 2003 from localhost
bash-2.05$ pwd
/home/suminten
```

Referensi

- http://www.tjw.org/chroot-login-HOWTO