

Unix/Linux

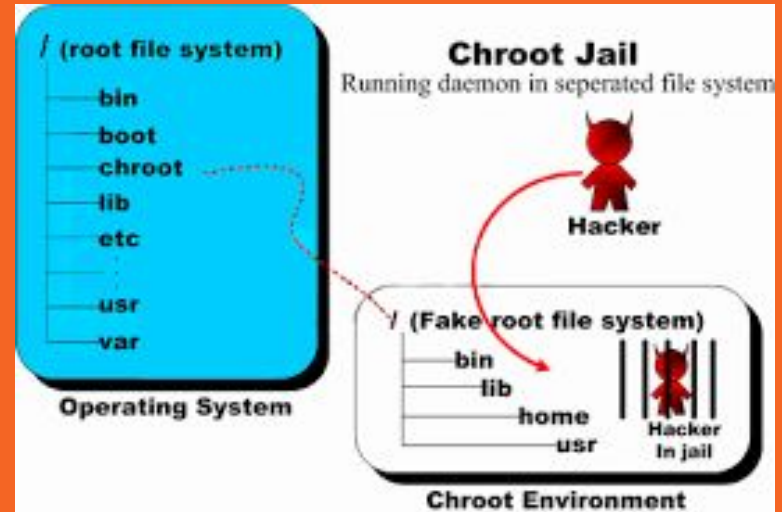
ISEN - AP4

T- TP Rep & Fichiers

2019 - J. Hochart

Objectif

- Créer un environnement chrooté pour un utilisateur spécifique qui se connectera en SSH
 - Environnement sandboxé et dupliqué
 - Pas accès au système



/dev

- Identifier les devices indispensables dans /dev au fonctionnement d'un shell
 - ls

/dev

- Créer les devices dans le /dev jailé
 - # mkdir
 - ..
 - # mknod -m 666 null c 1 3
 - # mknod -m 666 tty c 5 0
 - # mknod -m 666 zero c 1 5
 - # mknod -m 666 random c 1 8

Permissions

- Mettre les bonnes permissions au répertoire de jail
- Doit appartenir à root et ne pas pouvoir être write par d'autres utilisateurs (755)
 - Chown
 - Chmod
 - Ls -al

/bin

- Créer le /bin du jail
- Y copier bash
 - Mkdir
 - Cp -v
 -

Libs

- Identifier les libs dynamiques utilisées par bash
 - ldd
- Les copier dans le /lib jailé
 - Mkdir
 - Cp -v

Utilisateur

- Créer l'utilisateur unix qui sera jailé: prisoner
- Lui set un password simple
- Changer son shell pour bash (ou copier bash en sh)
 - Useradd
 - Passwd
 - Chsh (ou à la main)

/etc

- Créer le /etc de la jail
- Y mettre le minimum: les fichier passwd et group
 - Mkdir
 - Cp
 -

Conf SSH

- Patcher le fichier de configuration de SSHD pour chrooter l'utilisateur prisoner
- : (À la fin)
 - Match User prisoner
 - ChrootDirectory /home/jail
- Redémarrer le daemon SSH

Test

- Tester!

Bonus

- Bonus
 - Enrichir les commandes disponibles pour l'utilisateur chrooté
 - Mettre en place un /home et rendre le jail utilisable pour plusieurs users

Commandes

```
mkdir -p /home/jail
```

```
ls -l /dev/{null,zero,stdin,stdout,stderr,random,tty}
```

```
mkdir -p /home/jail/dev/
```

```
cd /home/jail/dev/
```

```
mknod -m 666 null c 1 3
```

```
mknod -m 666 tty c 5 0
```

```
mknod -m 666 zero c 1 5
```

```
mknod -m 666 random c 1 8
```

```
chown root:root /home/jail
```

```
chmod 0755 /home/jail
```

```
ls -ld /home/jail
```

Commandes

```
mkdir -p /home/jail/bin  
cp -v /bin/bash /home/jail/bin/
```

```
ldd /bin/bash  
mkdir -p /home/jail/lib64  
mkdir -p //home/jail/lib/x86_64-linux-gnu  
cp -v /lib64/{linux-vdso.so.1,libtinfo.so.5,libdl.so.2,libc.so.6,ld-linux-x86-64.so.2} /home/jail/lib64/  
cp -v /lib/x86_64-linux-gnu/{linux-vdso.so.1,libtinfo.so.5,libdl.so.2,libc.so.6,ld-linux-x86-64.so.2}  
/home/jail/lib/x86_64-linux-gnu/
```

```
useradd prisoner  
passwd prisoner
```

Commandes

```
mkdir /home/jail/etc
```

```
cp -vf /etc/{passwd,group} /home/jail/etc/
```

```
# SSHD.conf
```

```
Match User prisoner
```

```
ChrootDirectory /home/jail
```