Table des matières

Forkbomb 3
SELinux 3
pam_tally 3

Forkbomb

Voir la définition sur Wikipedia. Sous linux avec un simple compte on peut planter la machine en quelques secondes en lançant la commande suivante (en Bash) :

```
:(){ :|:& };:
```

En général un *ulimit -u* indique le nombre de process max par user. Si ce nombre est trop élevé la machine est susceptible de planter avec une *forkbomb*. Pour éviter ça on peut utiliser le fichier **/etc/security/limits.conf** et ajouter les lignes suivantes :

- Pour un user en particulier :

```
testuser        hard    nproc           50
```

- Pour un groupe en particulier :

```
@testgroup      hard    nproc           50
```

On peut vérifier (si on utilise PAM) que la ligne suivante n'est pas commentée dans **/etc/pam.d/system-auth** (Les chemins et les noms de fichiers présentés peuvent différer d'une distribution à une autre) :

```
session     required      /lib/security/$ISA/pam_limits.so
```

Dans ce cas tous les users du groupe *testgroup* qui se loggent seront soumis aux limites. Si on veut que ces limites fonctionnent dans le cas d'un *su* il faut également décommenter la ligne contenant *pam_limits.so* dans le fichier *su*.

Au prochain login des users concernés on doit avoir :

```
ulimit -u
50
```

On peut relancer la forkbomb sans avoir peur

SELinux

Parfois on peut avoir besoin de désactiver SELinux qui peut bloquer le boot de la machine. Il suffit de breaker le grub et de rajouter *selinux=0* sur la ligne commençant par **kernel**. On peut également faire cette modification dans le fichier */etc/fstab*.

D'autres infos ici.

pam_tally

Voir à quels niveaux le module est utilisé (login, su, auth, etc). La commande pam_tally permet de gérer les comptes lockés (entre autres) :

```
root@server9000157:/etc/pam.d# pam_tally --user root
User root       (0)     has 0

pam_tally: [--file rooted-filename] [--user username] [--reset[=n]] [--quiet]
```

La commande *faillog* permet aussi de voir/éditer les infos.

From:
https://unix.ndlp.info/ - **Where there is a shell, there is a way**

Permanent link:
https://unix.ndlp.info/doku.php/informatique:nix:linux:linux_secu

Last update: **2009/08/13 12:49**