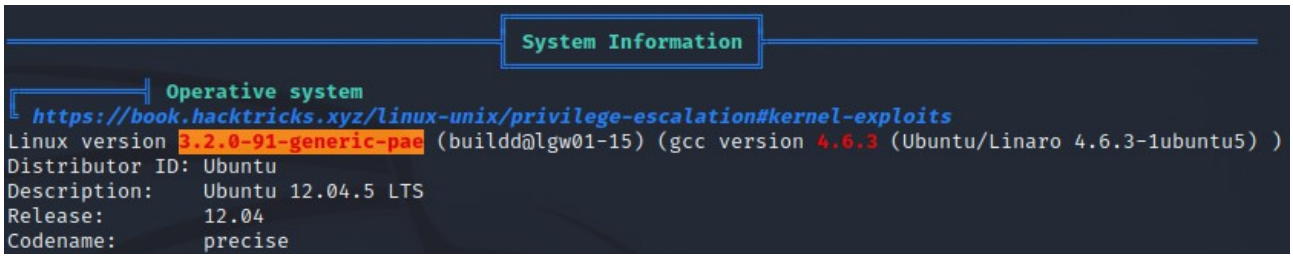
DIRTY COW

Boot2root writeups

Lorsqu'on se connecte en tant que l'utilisateur **laurie**, on a en réalité une manière de devenir root assez facilement, en lançant simplement un exploit **dirtycow**.

En effet, **linpeas** nous informe que la version du kernel est vraiment ancienne :



Et qu'il est très probable que le système soit vunérable à dirtycow :

On commence par télécharger le code source de l'exploit (disponible dans le dossier `scripts/dirty`) :
https://github.com/FireFart/dirtycow/blob/master/dirty.c

> Pour les librairies x32 :

```
apt-get install gcc-multilib
```

> Pour libcrypt en 32 bits :

```
dpkg --add-architecture i386
apt-get update
apt install libc6-dev:i386
```

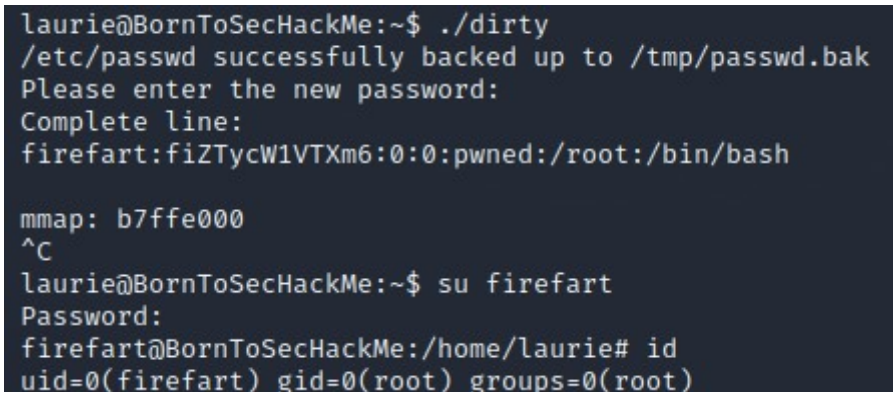
> Maintenant on peut compiler en statique notre exploit :

```
gcc -m32 -static -pthread dirty.c -o dirty -lcrypt
```

Une fois le binaire compilé en statique, on le transfert sur la machine cible (par exemple avec un scp) :

```
scp dirty laurie@192.168.1.7:/home/laurie/dirty
```

Il ne nous reste plus qu'à l'exécuter en indiquant le mot de passe de notre choix, puis en nous connectant sur l'utilisateur **firefart** avec ce même mot de passe ; on a ensuite les privilèges **root** :



On a donc bien **l'utilisateur root**.