

MachineHackeeExemple

Exemple d'une machine hackée

Un petit exemple d'une machine bien hackée:

```
# ps auxw
nobody 8889 47.8 1.6 13140 2092 ? R Dec08 2711:09 /usr/local/apache/bin/httpd
nobody 7208 0.0 0.2 2100 260 ? T Dec09 0:00 ./telek
nobody 20546 0.0 0.0 0 0 ? Z Dec09 0:00 telek
nobody 14831 20.4 1.8 11556 2332 ? R Dec10 600:46 /usr/local/apache/bin/httpd
nobody 9472 20.5 1.8 10288 2296 ? R Dec10 600:48 /usr/local/apache/bin/httpd

nobody 19874 0.0 0.1 1352 212 ? T Dec10 0:00 /tmp/c
nobody 18338 0.0 0.0 0 0 ? Z Dec10 0:00 c
nobody 18390 0.0 0.1 1352 212 ? T Dec10 0:00 /tmp/c
nobody 590 0.0 0.0 0 0 ? Z Dec10 0:00 c
nobody 1486 0.0 0.1 1352 212 ? T Dec10 0:00 /tmp/c
nobody 11311 0.0 0.0 0 0 ? Z Dec10 0:00 c
nobody 2231 0.0 0.1 1356 216 ? T Dec10 0:00 /tmp/c
nobody 16076 0.0 0.0 0 0 ? Z Dec10 0:00 c
nobody 21115 19.6 0.2 1348 252 ? R Dec11 178:08 ./kmod
nobody 27214 0.0 0.1 1360 212 ? S 02:15 0:00 ./x0x
nobody 15064 0.0 0.2 2104 288 ? S 03:03 0:00 getty
```

On peut penser que la machine est MachineSemiHackee, mais ...

```
# netstat -tanpu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:2600 0.0.0.0:* LISTEN 11133/psync
tcp 0 0 0.0.0.0:6668 0.0.0.0:* LISTEN 31528/psync
```

Tiens 2 bounceurs IRC.

```
#ps auxw |grep 11133
root 23763 0.0 0.5 1832 672 pts/5 S 12:18 0:00 grep 11133
```

Le process n'est pas vu par la commande **ps**.

```
# cd /proc/11133/
#ls -l
total 0
-r--r--r-- 1 nobody nobody 0 Dec 12 12:19 cmdline
lrwxrwxrwx 1 nobody nobody 0 Dec 12 12:19 cwd -> /var/tmp/psync
-r-- 1 nobody nobody 0 Dec 12 12:19 environ
lrwxrwxrwx 1 nobody nobody 0 Dec 12 12:19 exe -> /var/tmp/psync/psync
dr-x-- 2 nobody nobody 0 Dec 12 12:19 fd
-r--r--r-- 1 nobody nobody 0 Dec 12 12:19 maps
```

```

-rw- 1 nobody nobody 0 Dec 12 12:19 mem
-r-r-r- 1 nobody nobody 0 Dec 12 12:19 mounts
lrwxrwxrwx 1 nobody nobody 0 Dec 12 12:19 root -> /
-r-r-r- 1 nobody nobody 0 Dec 12 12:19 stat
-r-r-r- 1 nobody nobody 0 Dec 12 12:19 statm
-r-r-r- 1 nobody nobody 0 Dec 12 12:19 status
# cat stat
11133 (psybnc) S 1 10133 21624 0 -1 134217792 1052 0 790 0 3107 1321 0 0 9 0 0 0 173526992 2871296
253 4294967295 134512640 135116556 3114546144 3114545452 134716030 0 0 4096 28367 3223080614 0
0 17 0

#cat cmdline
./psybnc

```

Alors que le process existe bien, **ps** est donc modifié et donc le hackeur a pu être root.

La machine est foutue, mais on va regarder en profondeur.

```

# lsattr /bin/
suSiadAc- /bin/login
suSiadAc- /bin/ls
suSiadAc- /bin/netstat
suSiadAc- /bin/ps

```

Les hackers font toujours cette manipulation: ils mettent en place leur commande et ils changent les droits sur les exécutions pour éviter les mises à jour.

```

# chattr -suSiadAc /bin/*
# rpm -qf /bin/ps
procps-2.0.7-11
# rpm -Uvh ftp://rpmfind.net/linux/redhat/7.3/en/os/i386/RedHat/RPMS/procps-2.0.7-12.i386.rpm
Retrieving ftp://rpmfind.net/linux/redhat/7.3/en/os/i386/RedHat/RPMS/procps-2.0.7-12.i386.rpm
Preparing... 100%
1:procps error: unpacking of archive failed on file /usr/bin/top: cpio: rename failed - Opération non permise
# chattr -suSiadAc /usr/bin/top
# rpm -Uvh --force
ftp://rpmfind.net/linux/redhat/7.3/en/os/i386/RedHat/RPMS/procps-2.0.7-12.i386.rpm
Retrieving ftp://rpmfind.net/linux/redhat/7.3/en/os/i386/RedHat/RPMS/procps-2.0.7-12.i386.rpm
Preparing... 100%
1:procps 100%

```

Maintenant on pourra regarder mieux

```

# ps auxw
nobody 8889 47.7 1.6 13140 2092 ? R Dec08 2713:27 /usr/local/apache/bin/httpd
nobody 7208 0.0 0.2 2100 256 ? T Dec09 0:00 ./telek
nobody 20546 0.0 0.0 0 0 ? Z Dec09 0:00 telek
nobody 14831 20.4 1.8 11556 2332 ? R Dec10 603:04

```

OVH

```
nobody 9472 20.5 1.8 10288 2296 ? R Dec10 603:07 /usr/local/apache/bin/httpd
nobody 19874 0.0 0.1 1352 212 ? T Dec10 0:00 /tmp/c
nobody 18338 0.0 0.0 0 0 ? Z Dec10 0:00 c
nobody 18390 0.0 0.1 1352 212 ? T Dec10 0:00 /tmp/c
nobody 590 0.0 0.0 0 0 ? Z Dec10 0:00 c
nobody 1486 0.0 0.1 1352 212 ? T Dec10 0:00 /tmp/c
nobody 11311 0.0 0.0 0 0 ? Z Dec10 0:00 c
nobody 2231 0.0 0.1 1356 212 ? T Dec10 0:00 /tmp/c
nobody 16076 0.0 0.0 0 0 ? Z Dec10 0:00 c
nobody 11133 0.0 0.8 2804 1012 ? S Dec10 0:44 ./psybnc
nobody 11598 0.0 0.7 2500 948 ? S Dec10 0:13 ./psybnc
nobody 31528 0.0 1.2 3788 1504 ? S Dec11 1:04 ./psybnc
nobody 25517 0.0 0.5 2304 712 ? S Dec11 0:01 ./psybnc
nobody 21115 19.6 0.2 1348 252 ? R Dec11 180:27 ./kmod
nobody 27214 0.0 0.1 1360 212 ? S 02:15 0:00 ./x0x
nobody 15064 0.0 0.2 2104 284 ? S 03:03 0:00 getty
nobody 27439 0.0 2.6 13552 3292 ? S 10:10 0:07 /usr/local/apache/bin/httpd
```

On voit des choses. **kmod** notamment lancé en ligne de commande ! C'est probablement un soft qui essaie d'exploiter une faille sur ptrace sur le noyau < 2.4.20. Sauf que le noyau est 2.4.21. Et sur ce noyau il existe une autre faille. Il faut passer en 2.4.23.

```
# rpm -qf /bin/netstat
```

```
net-tools-1.60-3
```

```
# rpm -Uvh ftp://rpmfind.net/linux/redhat/7.3/en/os/i386/RedHat/RPMS/net-tools-1.60-4.i386.rpm
```

```
Retrieving ftp://rpmfind.net/linux/redhat/7.3/en/os/i386/RedHat/RPMS/net-tools-1.60-4.i386.rpm
```

```
Preparing... 100%
```

```
1:net-tools error: unpacking of archive failed on file /sbin/ifconfig: cpio: rename failed - Opération non permise
```

```
# chattr -suSiadAc /sbin/ifconfig
```

```
# rpm -Uvh ftp://rpmfind.net/linux/redhat/7.3/en/os/i386/RedHat/RPMS/net-tools-1.60-4.i386.rpm
```

```
Retrieving ftp://rpmfind.net/linux/redhat/7.3/en/os/i386/RedHat/RPMS/net-tools-1.60-4.i386.rpm
```

```
Preparing... 100%
```

```
1:net-tools 100%
```

```
# netstat -tanpu | grep psybnc
```

```
tcp 0 0 0.0.0.0:2600 0.0.0.0:* LISTEN 11133/psybnc
```

```
tcp 0 0 0.0.0.0:6667 0.0.0.0:* LISTEN 11598/psybnc
```

```
tcp 0 0 0.0.0.0:6668 0.0.0.0:* LISTEN 31528/psybnc
```

```
tcp 0 0 0.0.0.0:3323 0.0.0.0:* LISTEN 25517/psybnc
```

```
tcp 0 0 xx:3799 195.47.220.2:6667 ESTABLISHED 25517/psybnc
```

```
tcp 0 0 xx:3960 195.204.1.130:6667 ESTABLISHED 31528/psybnc
```

```
tcp 0 0 xx:6667 xx:4683 ESTABLISHED 11598/psybnc
```

```
tcp 0 0 xx:2142 61.6.39.100:6667 ESTABLISHED 11133/psybnc
```

```
tcp 0 0 xx:6667 81.192.224.22:2075 ESTABLISHED 11598/psybnc
```

```
tcp 0 0 xx:2082 209.123.150.208:6667 ESTABLISHED 31528/psybnc
```

```
tcp 0 0 xx:4054 61.6.39.100:7000 ESTABLISHED 11598/psybnc
```

```
tcp 0 0 xx:2866 213.221.189.3:6667 ESTABLISHED 31528/psybnc
```

```
tcp 0 0 xx:4683 213.186.38.215:6667 ESTABLISHED 11598/psybnc
```

```
tcp 0 0 xx:1549 61.6.39.100:6667 ESTABLISHED 11133/psybnc
```

On arrete là. La machine part en reinstallation.

#halt

Broadcast message from root (pts/5) Fri Dec 12 12:37:54 2003...

The system is going down for system halt NOW !!

Comment la machine a été hackée ?

Le hackeur a d'abord trouvé une faille dans un script php. Il a donc pu avoir l'accès shell en nobody. Puis avec le bug de sécurité sur noyau < 2.3.23 il a pu passer root grâce aux exploits qu'on peut trouver sur l'internet. Le noyau de la machine est 2.4.21.