

Servidor semihackeado – caso 29/09/2004

Introducción

¿Qué significa semi hackeado? Esto quiere decir que la máquina no tiene por qué ser reinstalada porque el hacker no ha podido conectarse en root en la máquina. Podemos arriesgarnos a pensar con cierta seguridad que si el hacker no ha podido entrar por el root no habrá podido tampoco modificar el sistema.

¿Por qué el ejemplo 'del 29/09/2004' ?

Simplemente porque ese día, los servidores semi-hackeados generaron un ataque conjunto de 1Gbps y el afectado no tiene que estar muy contento.

¿Cómo verlo?

En este caso bastaba con echar una ojeada a los procesos del sistema (directorio /proc).

```
# ls -aul /proc/*/exe 2>/dev/null | grep deleted
lrwxrwxrwx 1 nobody nobody 0 sep 29 11:24 /proc/5910/exe -> /tmp/upxCKRKOKLAPA4 (deleted)
```

O también :

```
# find /proc -name exe -ls 2>/dev/null | grep deleted
lrwxrwxrwx 1 nobody nobody 0 sep 29 11:24 /proc/5910/exe -> /tmp/upxCKRKOKLAPA4 (deleted)
```

Vemos que hay un proceso lanzado con el user nobody, grupo nobody, marcado en deleted, por tanto el binario original ha sido borrado.

Si este comando no tiene ningún resultado, eso significa usted no esta siendo hackeado con este método. Puede también que nuestros técnicos ya hayan verificado su servidor y la hayan dejado limpio. Vaya al grep de logs apache para confirmarlo.

```
# cat /proc/5910/cmdline
/usr/local/apache/bin/httpd
```

El truco del hacker es que ha renombrado su proceso '/usr/local/apache/bin/httpd' para no ser detectado.

El ataque ese fue llevado desde la ip :

```
# host 210.169.91.66
66.91.169.210.in-addr.arpa is an alias for 66.64.91.169.210.in-addr.arpa.
66.64.91.169.210.in-addr.arpa domain name pointer january.medical9.gr.jp.
```

Para encontrar su script que es el origen del fallo de seguridad, haga un grep de esta dirección IP en sus logs de apache (atención, algunos servidores son hackeados desde hace mucho tiempo (habrá que revisar también los log en .gz)).

Nota : si ya se ha depurado todos los ficheros afectados del servidor, solamente viendo los logs le permitirá ver el paso del hacker.

Error de origen

Este hack se basa en un error de programación en PHP. Un 'include' toma un parámetro que es el fichero a incluir. El 'include' por tanto busca el fichero y lo ejecuta sobre el servidor.

El fallo es que PHP permite buscar ese fichero a una URL y el programador no lo ha tenido en cuenta con una verificación.

Nota : un fallo de seguridad no quiere decir forzosamente un bug.

Esta variable se rellena a partir de una información que se pasa durante la llamada de la página. El hacker simplemente debe rellenar esa variable con un link a su script de ataque, el cual puede estar en cualquier sitio – en un sitio distante.

Limpieza

Para realizar la limpieza de este caso, basta seguir la guía : [ServidorSemihackeado](#).

Más información

: [ServidorHackee](#) :: Cuando el servidor sufre el ataque de un hacker.

: [ServidorInfectado](#) :: Cuando el servidor se contagia con un troyano o un virus.

: [ServidorHackeadoEjemplo](#) :: Ejemplos de servidores hackeados.

: [ServidorSemiHackeado](#) :: Servidor semi-hackeado (no afecta al sistema y no es necesaria la reinstalación)