

Servidor atacado por un hacker

Introducción

Diariamente se producen ataques y hacks (entradas no permitidas) en servidores conectados a Internet.

En el caso del alojamiento compartido, OVH le garantiza que no se produzcan estos accesos y si usted utilizara un foro o un portal no seguro y sufriera un ataque, el ataque sería sólo en esos elementos no seguros y no en todo el servidor.

En el caso del servidor dedicado es usted, el administrador del servidor quien debe gestionar la seguridad.

Recuerde:

- Un servidor es accesible desde Internet y está al alcance de todos.
- Un ataque es siempre posible.
- No sucede sólo a los demás. Tome precauciones

¿Por qué una máquina ha sido hackeada?

Los orígenes del problema son múltiples, pero se puede resumir en una frase: **el administrador no ha sido usted lo bastante paranoico.**

Algunos de los fallos habituales :

- Si utiliza telnet, su login y contraseña viajan por internet en claro y pueden ser capturados en cualquier momento. Hay que utilizar ssh.
- Si utiliza ftp, su login y contraseña viajan por internet en claro y es la misma contraseña que root. Sftp es la solución.
- Si utiliza pop3/imap con la contraseña (que viaja en claro) y es la contraseña root. Utilice APOP o POP3S/IMAPS.
- Si no actualiza el servidor regularmente con nuevas versiones actualizadas y seguras, corre el riesgo de sufrir un ataque fácilmente. (En una red como la de OVH se efectúan aproximadamente 250 scans diarios para detectar fallos de seguridad).

Soluciones OVH para la seguridad de su servidor

En OVH intentamos (hasta donde llegan nuestras posibilidades) impedir los scans a nuestros clientes

OVH

Si utiliza una distribución Release de OVH (basadas en Red-Hat/Gentoo), puede usar nuestro **sistema de Releases** para mantener el servidor siempre al día.

Si utiliza una distribución de Debian (stable/testing), puede utilizar el sistema **security.debian** para mantener el servidor siempre al día.

Consulte la guía ReleasePatchSeguridad

Igualmente OVH le proporciona un sistema de monitorización en tiempo real para detectar cualquier fallo y limitar la indisponibilidad al mínimo.

Este sistema de seguridad tiene 3 componentes principales : los kernels GR-Security, la SSH Key y la monitorización RTM

Más información en la guía SeguridadDedicado

¿Cómo saber que un servidor ha sido atacado?

Un vistazo a las MRTG del servidor (disponibles en el Manager) no se equivoca nunca:

y en el servidor encontramos:

```
root 3632 0.0 1.0 2368 1320 pts/0 S 10:51 0:00 -bash
root 6310 0.0 0.1 476 248 pts/0 S 11:27 0:00 ./ipv6fuck 213.186.34.196
192.88.99.1 2002:d5ba:22c4:: 2001:6b8:0:400
[...]
root 6360 0.0 0.1 476 244 pts/0 S 11:27 0:00 ./ipv6fuck 213.186.34.196
192.88.99.1 2002:d5ba:22c4:: 2001:6b8:0:400
```

Luego, visiblemente el hacker ha podido lanzar procesos en root.

Se ha tomado el control de la máquina y debe ser reinstalada.

```
# netstat -tanpu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
udp 0 0 0.0.0.0:9875 0.0.0.0:* 28823/xc
udp 0 0 0.0.0.0:1052 0.0.0.0:* 28823/xc
udp 0 0 0.0.0.0:6770 0.0.0.0:* 28823/xc
# ps auxw | grep 28823
root 7117 0.0 0.5 1796 748 pts/1 S 11:38 0:00 grep 28823
```

Servidor atacado por un hacker

Hay procesos lanzados que tienen un pid y que no son vistos por **ps**.

Seguramente porque **ps** ha sido reemplazado por un **ps** hackeado que filtra todos los procesos del hacker para confundirnos.

En este caso no hay arreglo posible. Paramos la máquina inmediatamente:

```
# halt
```

```
Broadcast message from root (pts/1) Thu Nov 20 11:39:22 2003...
```

```
The system is going down for system halt NOW !!
```

Y pensamos en la reinstalación.

Con suerte, otras veces, si el hacker no ha modificado nada en el sistema, podemos tener un Servidor Semi-Hackeado? y basta con borrar la carpeta y los datos de los usuarios afectados.

Consulte la guía ServidorSemiHackeado

¿ Qué hacer ?

Una vez que el servidor ha sido hackeado, sólo queda una solución: **reinstalar**.

Puede realizar esta operación desde su Manager. Puede pasar su servidor en modo rescue para recuperar el máximo de información posible (aquella que el hacker no ha borrado / modificado).

Más información en nuestra guía ReinstalarServidor.

Utilice el espacio **Backup FTP** para guardar los ficheros que desee conservar

Más información

: 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)

: ReinstalarServidor :: Reinstalar el servidor

: SeguridadDedicado :: Herramientas OVH para asegurar su dedicado

: SshSobreServidorDedicado ::

: ReleasePatchSeguridad ::

OVH

: SmtPop3Imap ::