El Día a Día del Administrador de Sistemas: Webalizer Xtended

ACCESOS ERRÓNEOS

Webalizer es una herramienta para analizar los ficheros de registros de los servidores web. Un nuevo parche le proporciona a los administradores la posibilidad de ver lo que no hay. **POR CHARLY KÜHNAST**

De vez en cuando reviso los ficheros de registro de mi servidor web, aunque no es algo que me guste hacer muy a menudo. Después de todo, veo muchas cosas molestas en el trabajo. Cuando analizo mis propios registros, normalmente aparece información de depuración, pero también aparecen entradas del tipo "accesos erróneos". A veces se ven registros extraños como:

```
tharis.xxxxx.at - - ➥
[03/Dec/2005:08:24:43
+0100] "GET /LOST HTTP/1.1" ➥
404 1025 "-"
"Mozilla/4.0"
```

Aunque este mensaje parece muy ofensivo, en realidad es bastante inofensivo. En otras ocasiones, encuentro gente intentando navegar por URLs pertenecientes a aplicaciones que han sido nombradas en los avisos recientes de seguridad. En las últimas semanas, por ejemplo, he leído avisos referentes a PhpMyAdmin y PhpBB. Los intentos para acceder a ficheros con extensiones tales como *.mdb* y *.asp*, son signos evidente de fuego enemigo. El Listado 1 muestra un extracto.

Es bueno conocer exactamente qué consultas realizadas contra nuestro servidor han dado en el blanco. De hecho, esto es una forma de detectar patrones de ataque que podrían causar dolores de cabeza a otros servidores.

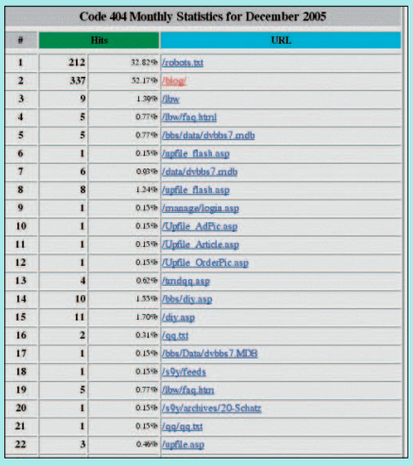
Listado 1: Accesos al Servidor Web

```
01 cncln.online.ln.cn - -
   [05/Dec/2005:22:09:04 +0100]
   "GET
   /bbs/upload.asp?action=upfile
   HTTP/1.1" 404 1025 "-"
   "InetURL:/1.0"
02 58.241.228.180 - -
   [06/Dec/2005:03:32:54 +0100]
   "GET /bbs/diy.asp HTTP/1.1"
   404 1025 "-" "Mozilla/4.0"
03 222.62.228.179 - -
   [06/Dec/2005:07:19:49 +0100]
   "GET /bbs/diy.asp HTTP/1.1"
   404 1025 "-" "InetURL:/1.0"
04 220.191.42.203 - -
   [13/Oct/2005:10:12:23 +0200]
   "GET /data/dvbbs6.mdb
   HTTP/1.1" 404 1025 "-"
   "InetURL:/1.0"
05 220.191.42.203 - -
   [13/Oct/2005:10:12:24 +0200]
   "GET /data/dvbbs7.mdb
   HTTP/1.1" 404 1025 "-"
   "InetURL:/1.0"
```

Detectando Patrones 404

Se entra en Webalizer, el amigo del administrador. Patrick Frei ha escrito un parche para Webalizer que proporciona al administrador estadísticas adicionales referentes a solicitudes que hayan provocado la respuesta *404 - File not found* en el servidor. La Figura 1 muestra estas estadísticas de mi servidor web del día 6 de Diciembre de 2005. Se puede ver de un vistazo que las entradas que descubrí no son un caso aislado. También se pueden observar un par de enlaces erróneos que tengo que eliminar.

El código fuente de Webalizer (incluido el parche ya aplicado) está disponible en [1]. Tan sólo hay que compilar e instalar:



Code 404 Monthly Statistics for December 2005

#	Hits		URL
1	212	32.82%	/robots.txt
2	337	52.17%	/blog/
3	9	1.39%	/ibw
4	5	0.77%	/ibw/faq.htm1
5	5	0.77%	/bbs/data/dvbbs7.mdb
6	1	0.15%	/upfile_flash.asp
7	6	0.93%	/data/dvbbs7.mdb
8	8	1.24%	/upfile_flash.asp
9	1	0.15%	/manage/logia.asp
10	1	0.15%	/Upfile_AdPic.asp
11	1	0.15%	/Upfile_Article.asp
12	1	0.15%	/Upfile_OrderPic.asp
13	4	0.62%	/mdqq.asp
14	10	1.55%	/bbs/diy.asp
15	11	1.70%	/diy.asp
16	2	0.31%	/qq.txt
17	1	0.15%	/bbs/Data/dvbbs7.MDB
18	1	0.15%	/s9y/feeds
19	5	0.77%	/ibw/faq.htm
20	1	0.15%	/s9y/archives/20-Schatz
21	1	0.15%	/qq/qq.txt
22	3	0.46%	/upfile.asp

Figura 1: Webalizer Xtended muestra las estadísticas erróneas para el 6 de Diciembre.

```
./configure
make
make install
```

Harán falta los paquetes Zlib, Libpng y GD, junto con los paquetes de desarrollo correspondientes. El parche que convierte el código fuente original de Webalizer en "Webalizer Xtended" está disponible en [1]. Para aplicarlo, en el directorio del código fuente de Webalizer, se teclea el siguiente comando:

```
patch -Np1 -i /Pfad
/webalizer-2.01-10-RB06-patch
```

Luego sólo hay que compilar Webalizer como se ha descrito anteriormente. El proceso completo es mucho más sencillo para los usuarios de Gentoo, ya que está disponible un Ebuild. ¡Felices accesos erróneos!

SYSADMIN

RECURSOS

[1] Webalizer Ztended: *http://www.webalizer.go.to*