

## Bitácora de un Secuestro

=====

True or no True.

Eran las 2 de la madrugada, mi corazón palpitaba con resguardo y disminuyente, por el cansancio, estaba seco, una noche dura.

Mis ojos borrosos no distinguían la realidad de lo virtual.

Buscando objetivos con que jugar, como un niño que elige un juguete, encontré algo, y crearme era lo más similar a un juguete.

Al rato entra mi compadre, había hecho una mala elección, eligió la azul, al igual que yo :(, hechos del mismo fuego, le pedí inquietante su ayuda.

Lo primero fue averiguar todo sobre ese lugar, que hacen, que tienen, como se mueven.

Objetivo: <http://xxx.xxx.xxx>

1ª Etapa: Saltando barreras

=====

Después de remover la basura y divagar con palabras locas, encontramos un bug del tamaño de un pozo ciego.

Encontramos una falla en el soft estadístico AWSTATS, en la cual mediante el script `awstats.pl` permitía la inserción de código malicioso.

Verificamos ansiosamente la vulnerabilidad de la siguiente manera:

```
http://xxx.xxx.xxx/cgi-bin/awstats.pl?configdir=%20|%20/usr/bin/w%20|%20
```

```
Error: LogFile parameter is not defined in config/domain file
```

```
Setup (' | /usr/bin/w | /awstats.xxx.xxx.xxx.conf' file, web server or permissions) may be wrong.
```

```
See AWStats documentation in 'docs' directory for informations on how to setup awstats.
```

WUALAAA, le encontramos el fondo al pozo, no era tan ciego después de todo.

Una vez viendo lo que teníamos en nuestros monitores, decidimos tomar seria importancia en el asunto.

Mediante un exploit, nos pusimos a comandar el server.

```
http://www.k-otik.com/exploits/20050124.GHCaws.pl.php
```

Tirando piedras al pozo, logramos insertar un backdoor por lo cual, claro, luego entramos.

Alguien dijo que era mala educación entrar sin ser invitado?, pues por cierto no lo recuerdo.

/\*

*Soluciones:*

=====

*\*)AWSTATS: Actualizar a una versión >= 6.3.*

*\*) Permisos: Configurar correctamente /tmp y /var/tmp solo con permiso de escritura y lectura para usuarios y otros, evitando así ejecución de backdoor, exploits, etc.*

```
#chmod 766 /tmp /var/tmp
```

*\*) Programas comunitarios :P: Eliminar wget y nc, lo cuales sirven de gran ayuda para bajar binarios al servidor y/o hacer tecnicas como la de shell inverse.*

*\*)PHP.INI: Configurarlos correctamente.*

```
register_globals    off

log_errors          on

display_errors     off //lo que hace es que no muestre en el browser
el error y se guarde en el log, muy útil. así impedimos cosas como
que saquen el path.

error_log /var/log/php_errors //aca iria la salida de los errores producidos
magic_quotes_gpc = on // para evitar ataques de html injection

*/
```

## 2ª Etapa: Escalando Privilegios

=====

Con mi compadre, estábamos adentro, y como el lugar era demasiado grande decidimos repartirnos las actividades, el escarbaba buscando información sensible y yo, :), yo buscaba hacerme del trono.

Tras un ligero comando, llegue hasta el corazón,

\* El kernel, en versión 2.6.8 fue inmune a mis ataques.

```
http://www.k-otik.com/exploits/20050117.stackgrow2.c.php
http://www.k-otik.com/exploits/20050107.efl1bl.c.php
```

el maldito tenia , lo mas similar a un cinturón de castidad, MALDICION.

El siguiente paso fue buscar aplicaciones explotables, y probé con los siguientes xpls.

```
http://www.k-otik.com/exploits/08242004.PST_chpasswd_exp-v_b.c.php
http://www.k-otik.com/exploits/04202004.0x3142-sq-chpasswd.c.php
```

los cuales no fueron efectivos.

Mientras mi cabeza rebosaba de ideas frustradas buscando alguna falla humana, mi compadre ,mi gran compadre, me dijo,con su apastada voz, mejor dicho tecleada:

*"No te hagas problema, BRO, ellos mismos solucionaron nuestro problema"*

Mi mirada seguía sin entender a lo que se refería

```
/dit/path/backup/etc.tar.gz
```

Mis ojos seguían mirando sin asimilar, sin darme cuenta, que pasaba tiempo buscando minuciosos errores cuando había uno muy GRANDE y ESTUPIDO.

Pues así nos hicimos con mi compadre, de este sitio, reinamos un lugar mas, gracia a la ayuda

implícita de los del otro lado. No tuvimos que hacer mucho, solo ser despiertos a los errores de los demás.

/\*

*Soluciones*

=====

*\*Backups: NUNCA DEJAR BACKUPS Y MENOS DEL DIR ETC INCLUYENDO PASSWD Y SHADOW A LA VISTA Y CON PERMISO DE USUARIO. Se podría otorgar permisos especiales sobre el archivo. Leer sobre chattr,lsattr,(man chattr) su uso es muy sencillo.*

```
#chattr +i backup.tar && chown root.root backup.tar && lsattr backup.tar
```

*\*Archivos de configuración: Evitar de algún modo los datos sensibles en estos,y si lo requieren, que tengan los permisos adecuados para los usuarios adecuados.*

\*/

*Y así concluye este relato de esta Bitácora, real o no ?.*

*MySt4 – SoulBlack TEAM*