Foremost – Recuperando archivos php borrados en servidor

Introducción

Bien en este post vamos a mostrar como recuperar archivos php borrados accidentalmente (situación a la que no se debe llegar, puesto que se tiene que contar con un sistema de backup). Para ello utilizaremos Foremost. Lo mas importante llegados a este punto es no usar dicho almacenamiento!!!! Los datos continúan estando en el disco a menos que grabemos un nuevo dato en el mismo sector, en ese caso no habrá posible recuperación. Tampoco podemos tomar esto como la solución a todos nuestros males, el uso de esta herramienta no es garantía de recuperar nuestros datos.

Foremost

Es un programa para hacer carving (rescate selectivo de ficheros).

¿Cómo funciona? Foremost trabaja con imágenes generadas con dd o particiones directamente, y se basa en el análisis de encabezados y footers de los archivos para 'extraer' lo que se pueda salvar. Esto se realiza mediante el encabezado hexadecimal de un fichero, por ejemplo:

- jpg
- gif
- png
- bmp
- avi
- exe
- mpg
- wav

- riff
- wmv
- mov
- pdf
- ole (PowerPoint, Word, Excel, Access y StarWriter)
- doc
- zip
- rar
- htm
- cpp

Instalando Foremost

sudo apt-get install foremost

Configurando Foremost para recuperar archivos php

Vamos a explicar poco la estructura del archivo de configuración. Este consta de líneas en las que se especifican búsquedas

Cada linea tiene la siguiente estructura:

- Extensión del archivo (php, cpp) que se quiera buscar
- Definir si se debe hacerse búsqueda case-sensitive «y» o no «n»
- Tamaño máximo del archivo.
- Encabezado: cadena de texto a buscar en los encabezados de los archivos; puede ser especificado en texto o hexadecimal.
- Footer: cadena de texto a buscar al final de los archivos; puede ser especificado en texto o hexadecimal.

Bien deberemos editar el archivo de configuración

sudo vi /etc/foremost.conf

y añadir la siguiente línea

php y 100000 \x3C\x3F\x70\x68\x70/

Bien para empezar con la recuperación ejecutaremos el siguiente comando:

foremost -t php -i /dev/sda1 -o /dev/sda2/recover/

Teniendo en cuenta que:

- -t especifica el tipo de archivo a buscar (si no se usa por defecto busca todos los que esten configurados en foremost.conf)
- Deberemos substituir /dev/sda1 por la ruta al disco del cual se quiera recuperar datos
- Deberemos modificar /dev/sda2/recover/ por la ruta donde queremos guardar los archivos recuperados (esta carpeta debe estar vacía)
- Los archivos recuperados no conservaran el nombre original. Nos encontraremos con archivos tipo 6856758.php
- Se debe tener mucha paciencia este proceso no durará segundos

Observaciones
Espero que esto pueda servir de ayuda. Normalmente esto ocurre cuando se no se tiene un sistema de backups. Se debe tener cuidado, hacer periódicamente backups incrementales puede evitar encontrarnos en la tediosa situación de utilizar este tipo de programas. Que si, deben estar, se agradecen y mucho, pero no son garantía de recuperación y entramos en un terreno delicado nunca es bueno.

Ruben.