DISCOGRAPHY

El siguiente contenido está publicado con fines académicos y de concienciación. No nos hacemos responsables de las actividades que se lleven a cabo con la información mostrada a continuación.

El siguiente post forma parte de una serie de posts dedicados a mostrar las soluciones a los retos presentados en el **Evento de CiberSeguridad de Secuma 2018** celebrado en **Málaga el 15 de Noviembre de 2018.**

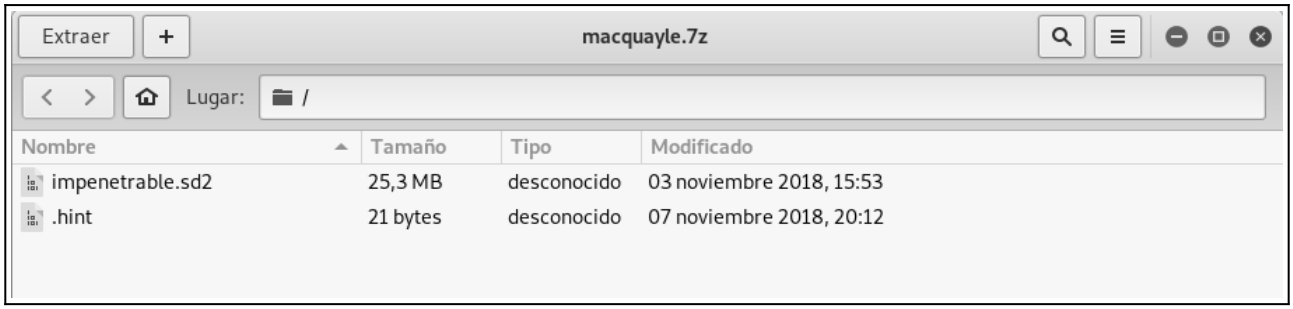
Cabe destacar que vamos a proceder a publicar el código fuente de cada uno de los retos (de los retos de Web) para que todo el mundo pueda bajarselo, modificarlo y conseguir así customizarlo a su gusto para lograr nuevas variantes procedientes del mismo reto que puedan inspirar a la creación de nuevos retos y/o soluciones. Así que estar atentos al **Gitlab**.

Tan sólo pedimos que siempre que se modifique el código se mencione al autor del mismo así como que se ponga a disposición del público el resultante. Dicho esto vamos a proceder a explicar, de forma detallada los pasos que seguimos así como consejos que puedan ayudar al lector y/o aclarar conceptos. Empecemos!

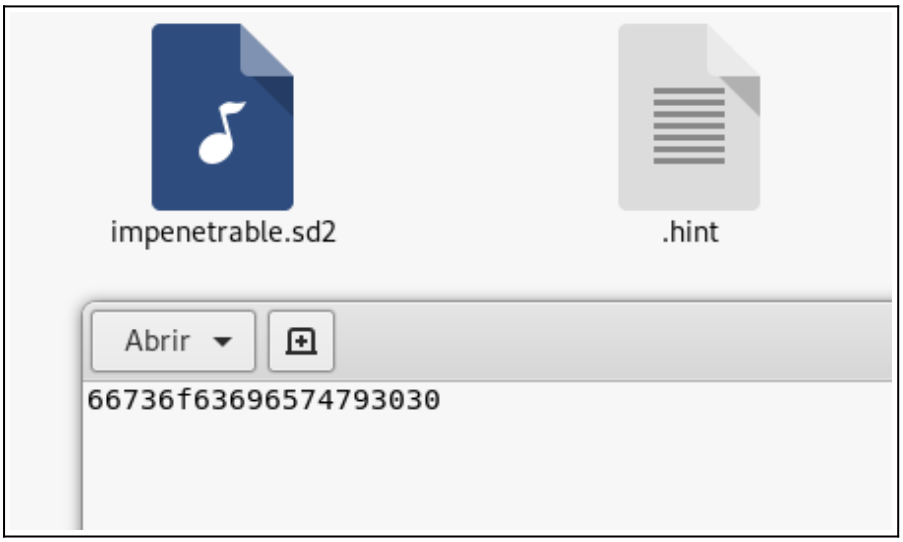
FASE DE CONTACTO.

Inicialmente nos descargamos el fichero adjunto después de leer la descripción.

Nos topamos con un **7z** (fichero comprimido) que, si inspeccionamos el contenido, nos damos cuenta que contiene dos archivos: impenetrable.sd2 y .hint (cuidado con este último, pues si lo descomprimimos automaticamente en un sistema linux, el . forzará al archivo a tomarse como **oculto**, y no se mostrará en el directorio donde se extrae).



Si inspeccionamos el **.hint** (pista) vemos el siguiente contenido (una cadena alfanumérica de longitud par):



Que, si separamos, en en grupos de **2 cifras**, nos daremos cuenta que esta codificado en **ASCII**, podemos usar la siguiente herramienta online para decodearlo y nos da el siguiente resultado:

Una vez con ese "**fsociety00**" vamos a pasar al archivo impenetrable.sd2, cuya extensión nos parece sospechosa, así que, mirando el contenido del archivo con el comando file, descubrimos que no es más que un **WAV** (en mi caso Linux ya me reconocia hasta que era un audio) que contiene una canción de la serie de mr robot.

```
root@kali:~/Descargas/scu/1/macquayle# file impenetrable.sd2
impenetrable.sd2: RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, stereo 44100 Hz
```

Un WAV y un texto (o mejor dicho, clave), ¿qué podríamos hacer? Pues mirar si tiene algún mensaje o contenido oculto, y sabiendo que nos dan una clave, lo primero que nos viene a la cabeza es la herramienta Steghide:

```
root@kali: ~/Descargas/scu/1/macquayle
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali:~/Descargas/scu/1/macquayle# ls
impenetrable.sd2
root@kali:~/Descargas/scu/1/macquayle# steghide --extract -sf impenetrable.sd2 -xf textoculto.txt
Anotar salvoconducto:
anot? los datos extra?dos e/"textoculto.txt".
root@kali:~/Descargas/scu/1/macquayle# ls
impenetrable.sd2  textoculto.txt
root@kali:~/Descargas/scu/1/macquayle# cat textoculto.txt
secuma18{Hide_your_criminal_notes}
root@kali:~/Descargas/scu/1/macquayle#
```

Y tras pasarle como salvoconducto la frase decodeada de ascii obtenemos un txt que contiene la **FLAG**!

by **@Secury**