EPISODIO 3
350

Richard mandó a Gilfoyle montar un servicio oculto que mantuviera a flote "El Flautista" pero este ya no recuerda donde se encuentra. Gracias a dios, como buen sysadmin, siempre hace backup de todo su trabajo, pero se trata de backups un tanto peculiares... Gilfoyle guarda el trabajo que hace en archivos encriptados relacionados con temáticas que le gustan.

Tenemos el fichero que contiene información sobre el servicio. Necesitamos que extraigas la información, accedas al servicio y consigas la flag de UAM. ¡Mucha suerte!

Enlace de descarga: https://drive.google.com/open?id=1qTuI9VndJ24krrO8U1WF3JpS77M4M2hV

Info: La flag tiene el formato UAM{md5}

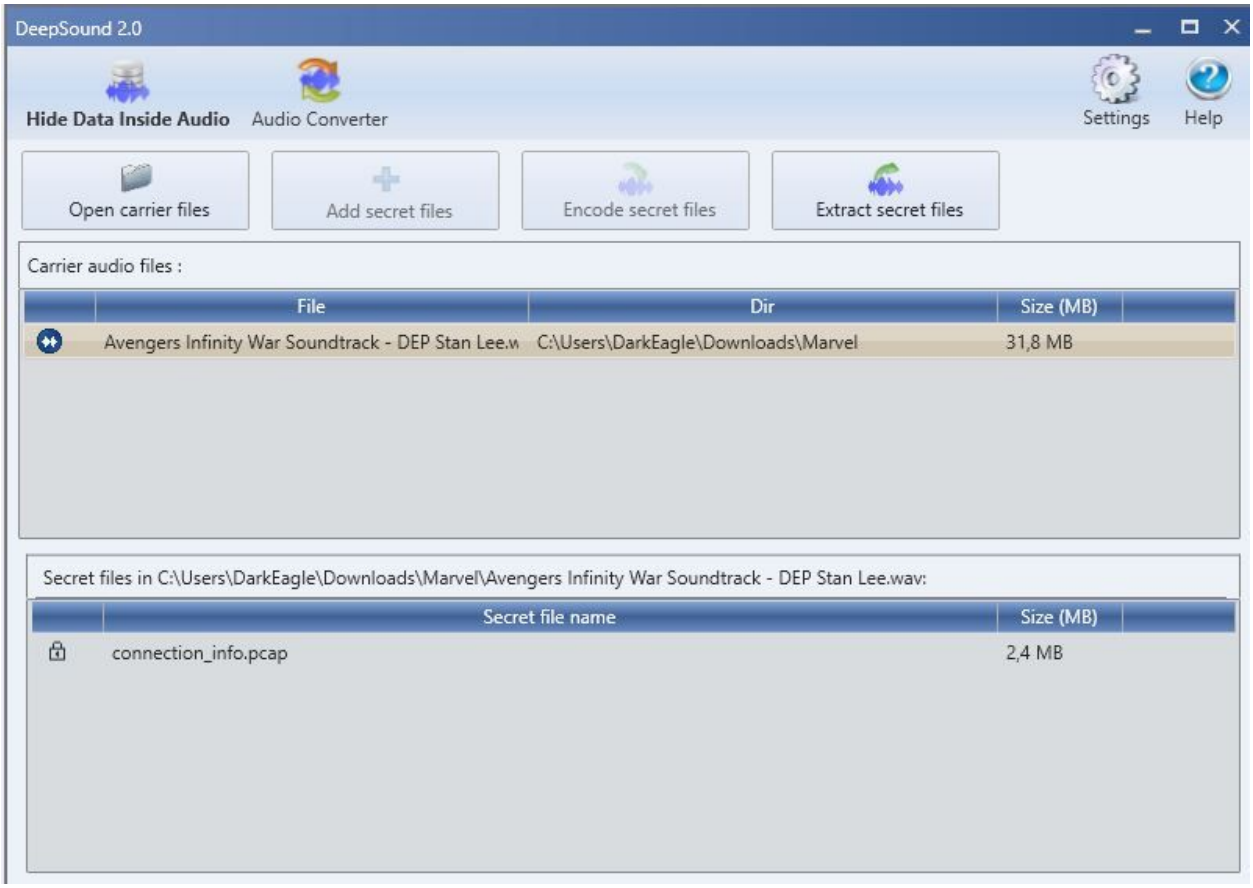
Descargamos el fichero que nos proponen, Marvel.zip de 30 MB un merecido homenaje al recientemente fallecido Stan Lee.
Al descomprimir el fichero encontramos un wav, vemos los strings, y en especial la última línea:

root@kali:~/unaalmes# strings Avengers\ Infinity\ War\ Soundtrack\ -\ DEP\ Stan\ Lee.wav | tail -1
U29uaWRvUHJvZnVuZG87KQo=

Lo decodificamos de base64:

root@kali:~/unaalmes# strings Avengers\ Infinity\ War\ Soundtrack\ -\ DEP\ Stan\ Lee.wav | tail -1 | base64 -d
SonidoProfundo;)

Ok, tenemos una pista .. probamos las típicas cosas de stego en audio .. Sonic Visualizer, Audacity .. y es usando DeepSound (Sonido Profundo) donde tenemos un resultado.



Extraemos el fichero y lo analizamos con Wireshark.

Analizando las tramas TCP en el stream 35 vemos algo curioso:

Pasamos el morse a texto:

Convert morse code to text

Input data

```
...-- ....- .-. ..- -. - --- ..--- ....- --... .-. ..- -. - ---
-.... ----. .-. ..- -. - --- ---.. -.... -.. --- ... .-. ..- -. -
--- ... .---- ...-- ...-- --...
```

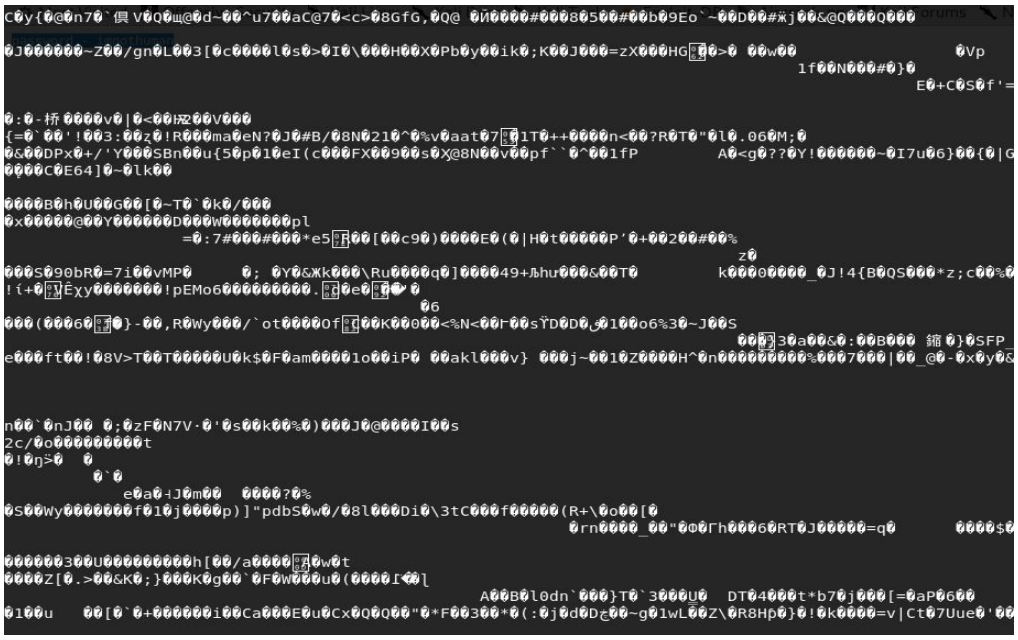
Convert: morse_code to text

Output:

```
34punto247punto69punto86dospuntos1337
```

Ok, vemos que hay en la ip y puerto que nos indican.

root@kali:~/unaalmes# nc 34.247.69.86 1337



Parece un socket lanzando basura, pero claro .. tiene que haber algo .. así que vamos a guardarlo en un fichero

root@kali:~/unaalmes# nc 34.247.69.86 1337 > prova.txt

Hago varias pruebas, de diferente duración para estar seguro y buscar patrones .. busco uam, UAM y cosas así dentro de los ficheros.

root@kali:~/unaalmes# strings prova2.txt | grep UAM

UAM:OWY5MTBhNjNiMGRlNWMzNjM4YTA3MTg4MzFiN2JkODk0MGYxN2EyZjZjYTQ4MTE2MDVlYmU0NGMwZjNkYjJiNmI2YzQzZjU1NmZhYjYwMWZ8a2V5OjFZRUFS
UAM:OWY5MTBhNjNiMGRlNWMzNjM4YTA3MTg4MzFiN2JkODk0MGYxN2EyZjZjYTQ4MTE2MDVlYmU0NGMwZjNkYjJiNmI2YzQzZjU1NmZhYjYwMWZ8a2V5OjFZRUFS

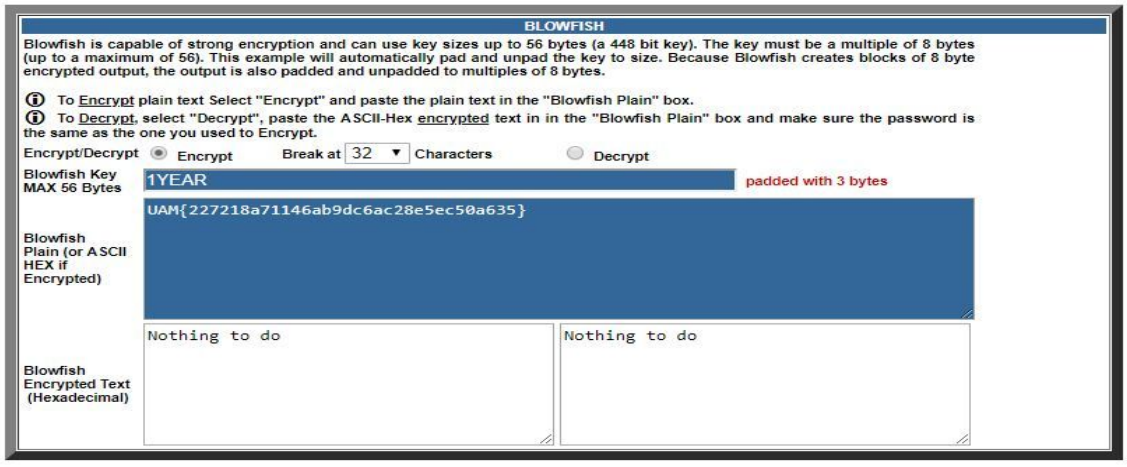
Como vemos, cada cierto tiempo el socket manda esta cadena.

root@kali:~/unaalmes# echo -n "OWY5MTBhNjNiMGRlNWMzNjM4YTA3MTg4MzFiN2JkODk0MGYxN2EyZjZjYTQ4MTE2MDVlYmU0NGMwZjNkYjJiNmI2YzQzZjU1NmZhYjYwMWZ8a2V5OjFZRUFS" | base64 -d && echo

9f910a63b0de5c3638a0718831b7bd8940f17a2f6ca4811605ebe44c0f3db2b6b6c43f556fab601f|key:1YEAR

Hasta aquí, había sido todo muy rápido y fácil … pero se ha complicado. No encontraba el tipo de cifrado de la cadena … Al final de mucho buscar, y volver a probar .. doy con una web que me da el resultado esperado:

https://webnet77.net/cgi-bin/helpers/blowfish.pl



FLAG: UAM{227218a71146ab9dc6ac28e5ec50a635}

Found : UAM_Ann1v3RS4R10
(hash = 227218a71146ab9dc6ac28e5ec50a635)

Felicidades a j0n3 por su first y también a BICACARO por el second ! Unos cracks todos !

Muchas gracias a los organizadores felicidades por el AÑAZO y esperemos que sean muchos muchos más !!!

DarkEagle