Silicon Valley - Episodio 3

UAM CTF 2018-11-15

El reto

https://unaalmes.hispasec.com/challenges#EPISODIO%203

Vamos a ver qué nos tienen preparado en este reto :)

Audio

Descargo y descomprimo el zip y veo que contiene un wav:

Avengers Infinity War Soundtrack - DEP Stan Lee.wav

Homenaje obligado al recientemente difunto Stan Lee y supongo que esconde alguna sorpresa pero... ¿dónde está la sorpresa?

Si lo escuchamos, es el tema aparentemente normal (ni pitiditos con morse ni Bella Ciaos). Audacity no muestra nada relevante a la vista salvo, quizá un poco de ruido… ¿sospechoso?

A veces con un simple head o tail podemos ver cosas relevantes y en este caso, al hacer un tail, vemos algo al final:

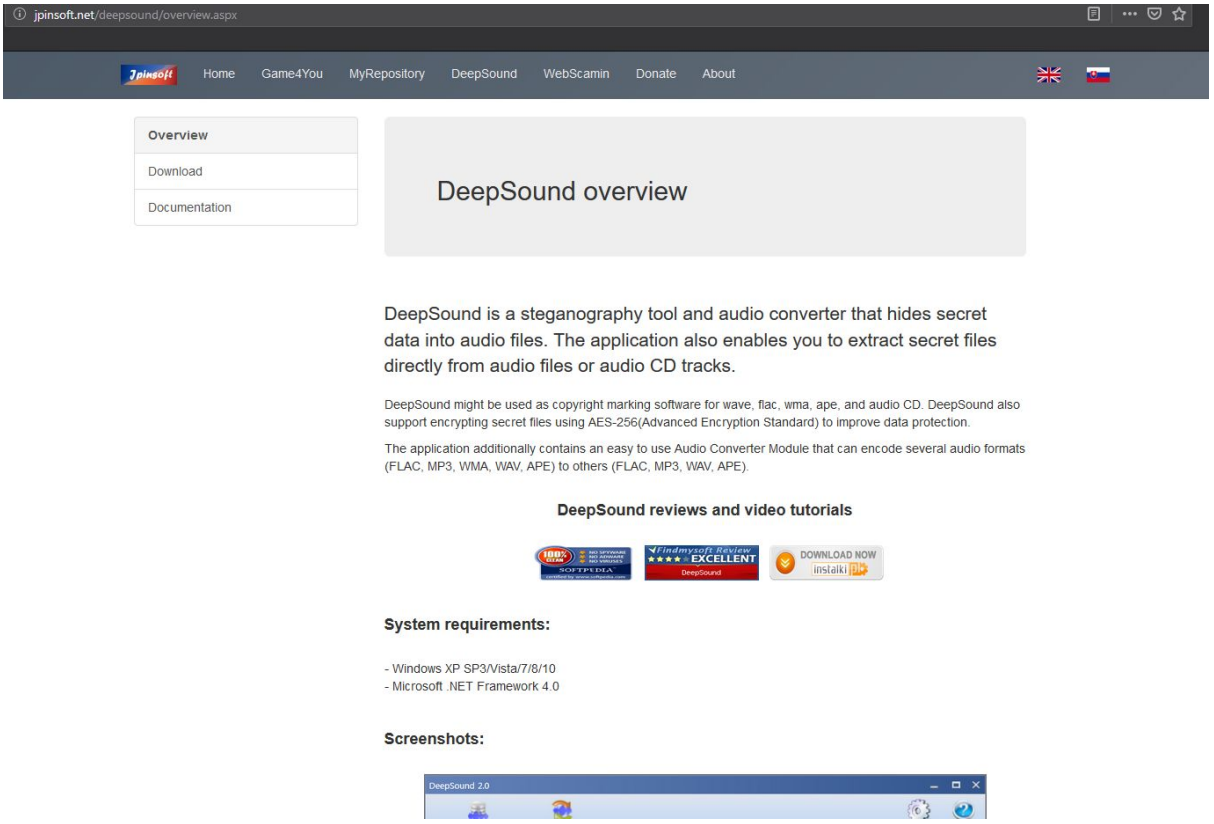
tail Avengers Infinity War Soundtrack - DEP Stan Lee.wav

Parece que hay algo justo al final y tiene toda la pinta de ser un base64, así que decodifico:

```
> echo U29uaWRvUHJvZnVuZG87KQo= | base64 -d
SonidoProfundo;)
```

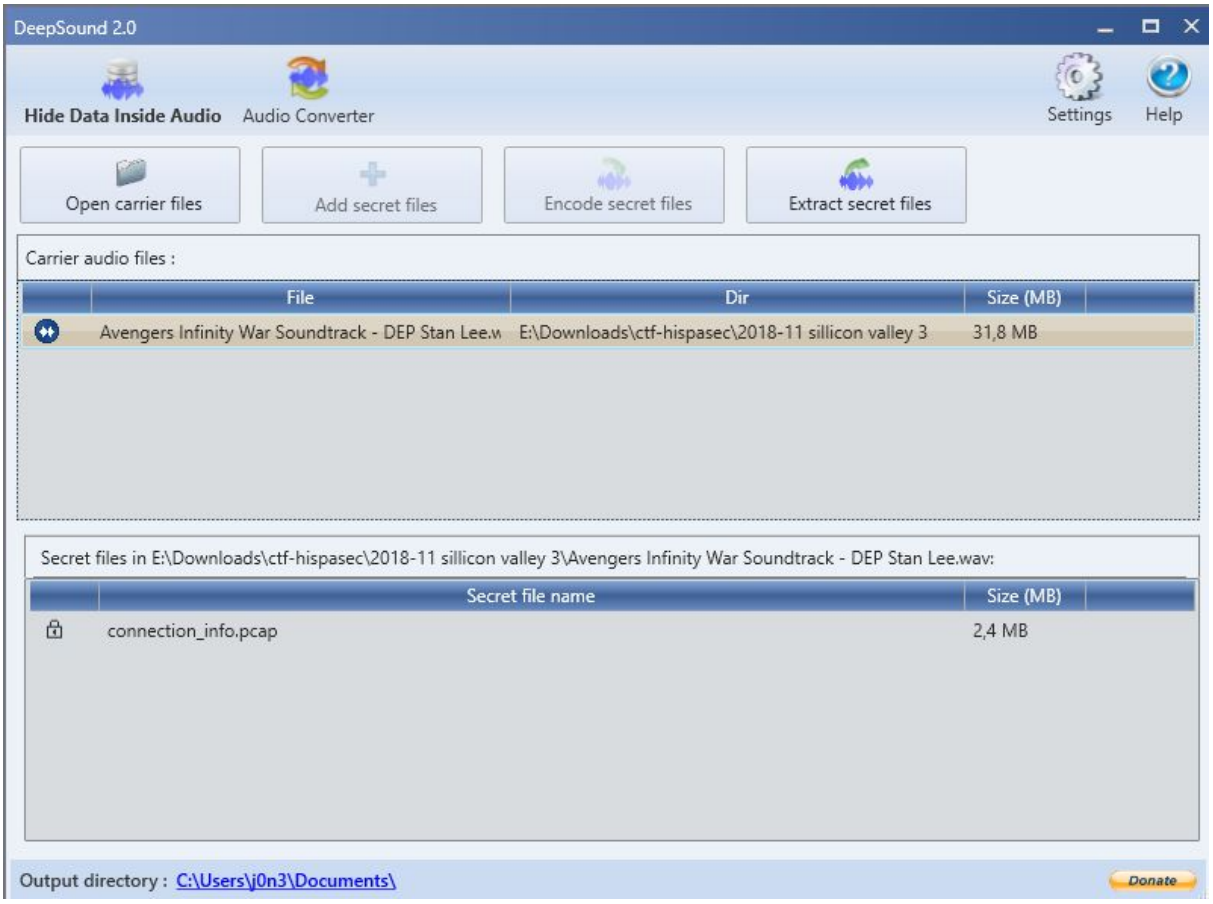
¿SonidoProfundo? Quizá sea alguna técnica o algoritmo… no sé, no me suena… si fuera un algoritmo seguro que lo encuentro en inglés antes que en castellano, como casi todo :/

Busco “DeepSound crypto” en google y el primer resultado es:



Me parece que sigo bien las pistas y creo que he acertado con el programa ;)

Descargar, instalar, ejecutar, abrir wav.

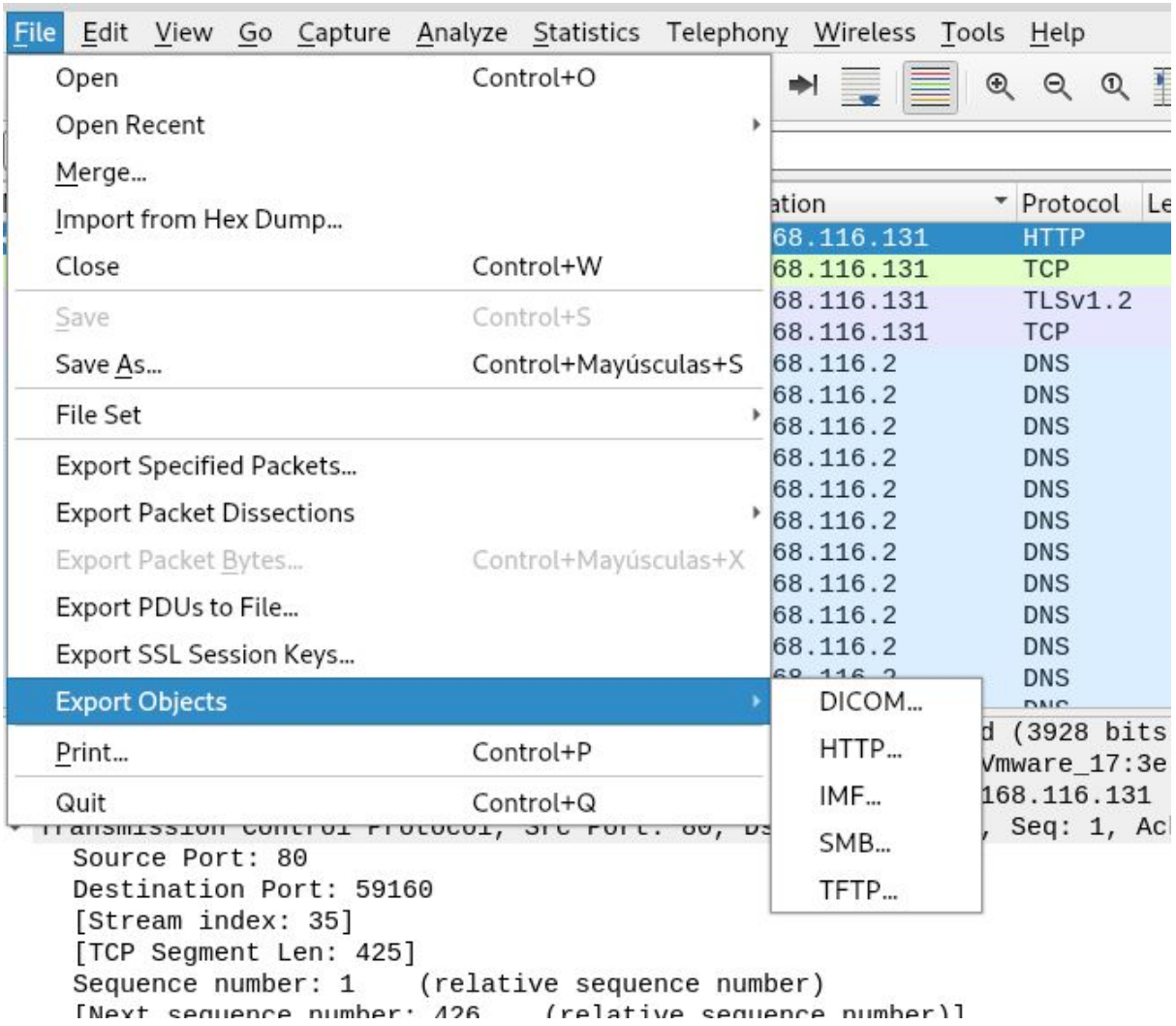


Parece que tenemos un archivo secreto.

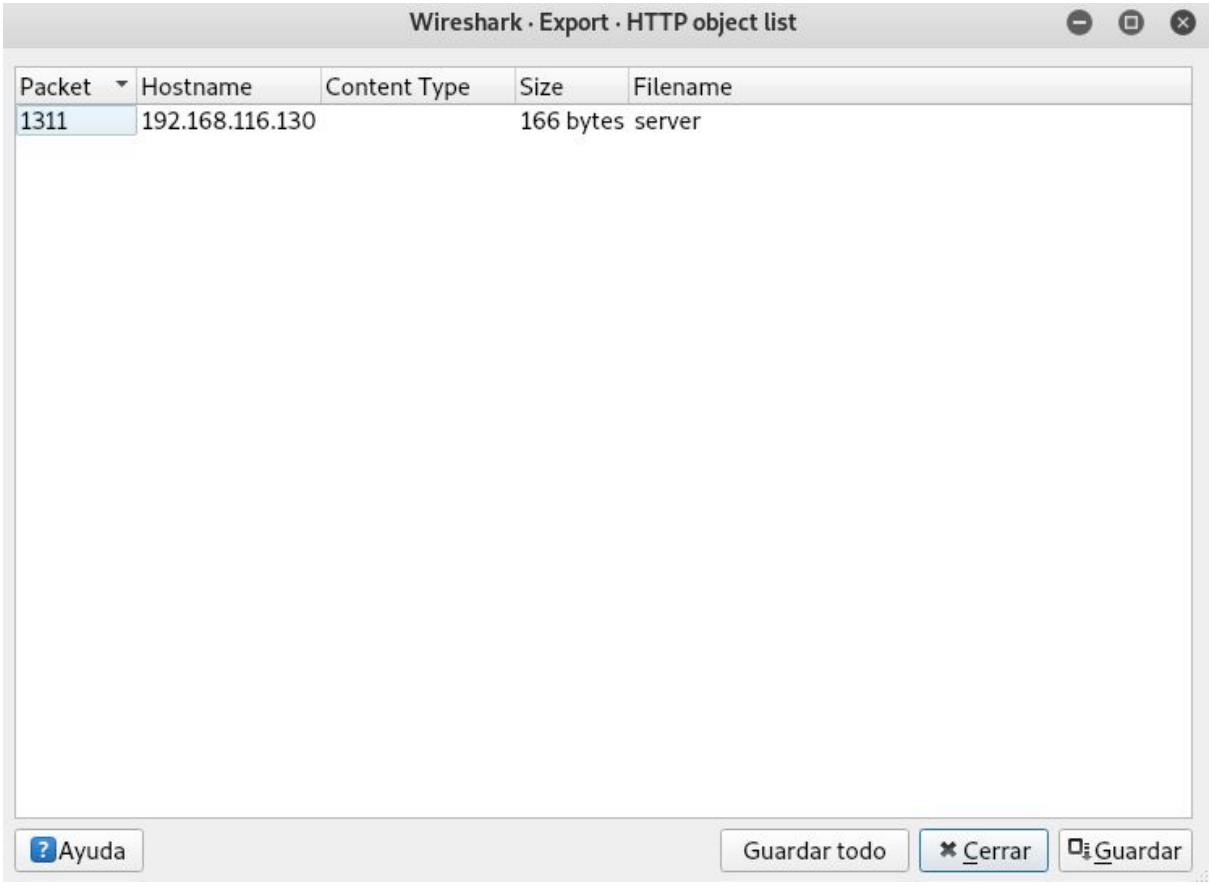
connection_info.pcap

Aunque nunca he hecho análisis de pcap sí que recuerdo haberlo leído o visto por ahí (youtube, otros writeups de retos…). Sé que es un archivo que contiene una muestra de capturas de paquetes de tráfico de red y wireshark será nuestra herramienta. Exportarmos el pcap escondido en el wav y lo metemos en wireshark para analizarlo.

Tras un rato haciendo búsquedas de texto, mirando ip's y demás, descubro esto: si exportamos los objetos HTTP...



...vemos un archivo:



Interesante. Lo guardamos con cualquier nombre y vemos que es un fichero de texto con un morse:

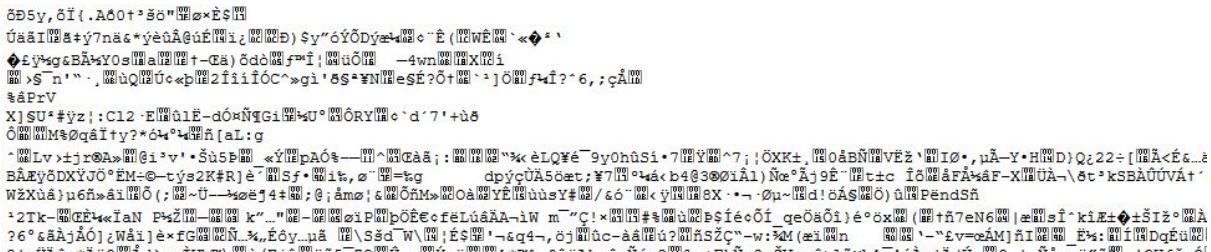
Morse

...-- ....- .-. ..- -. - --- ..--- ....- --... .-. ..- -. - --- -.... ----. .-. ..- -. - --- ---.. -.... -.. --- ... .-. ..- -. - --- ... .---- ...-- ...-- --...

Cualquier herramienta online nos sirve para verlo.

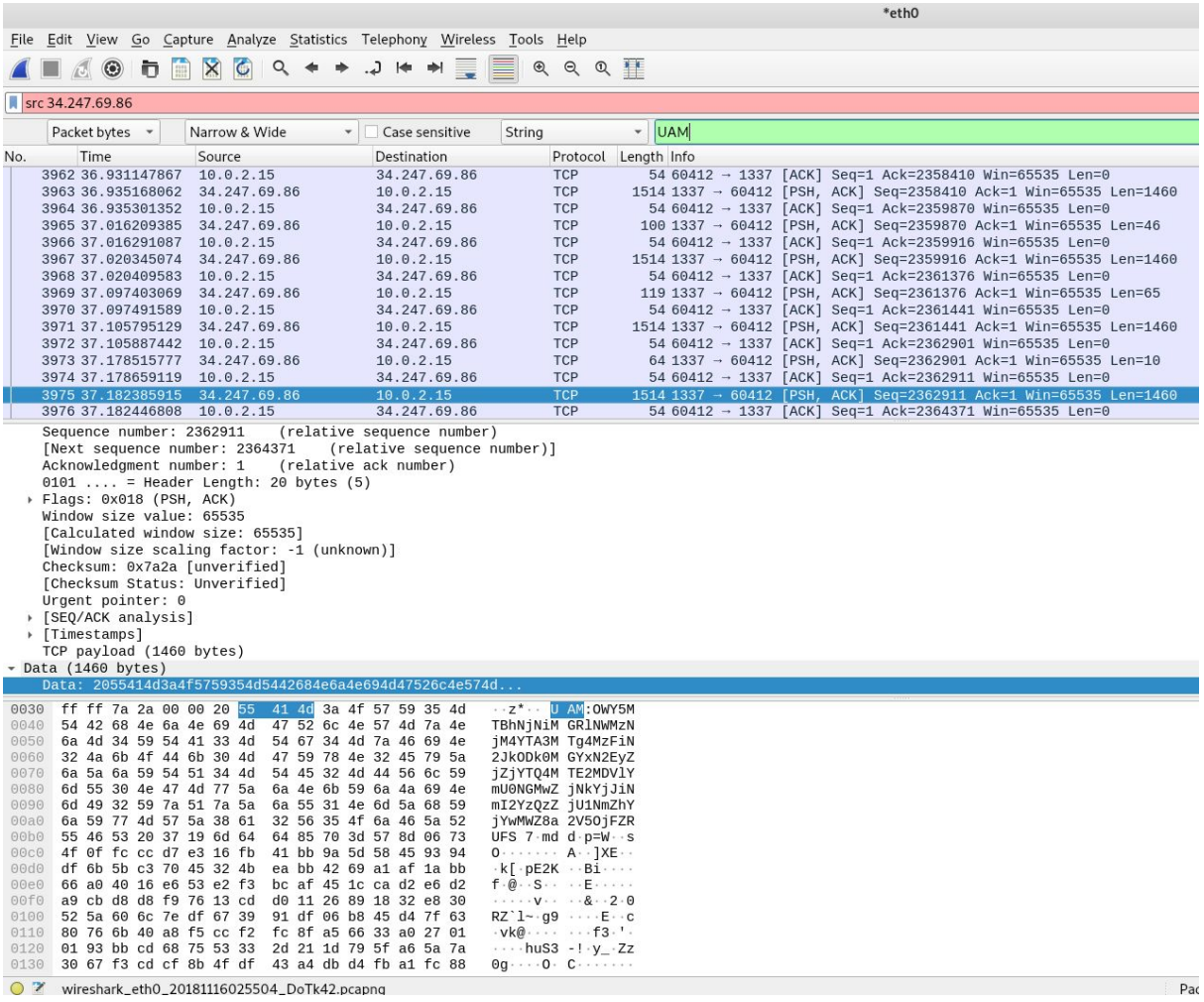
El servidor esquizofrénico

El morse corresponde a una IP y entro para ver si hay alguna página:
http://34.247.69.86:1337



El servidor nos envía un stream de datos pero no consigo saber qué es. Pruebo con vlc para ver si es vídeo o audio y nop, pero como ya tengo abierto wireshark, voy a esnifar algunos paquetes filtrando esta dirección mientras sigo recibiendo datos…

...y tras un rato capturando, buscando por 'uam' encuentro un paquete sospechoso.



Extraigo la cadena completa y con dcode (decodify) pruebo si es algo que conozca y parece que es un base64

Al decodificarlo tenemos un hash y una key:

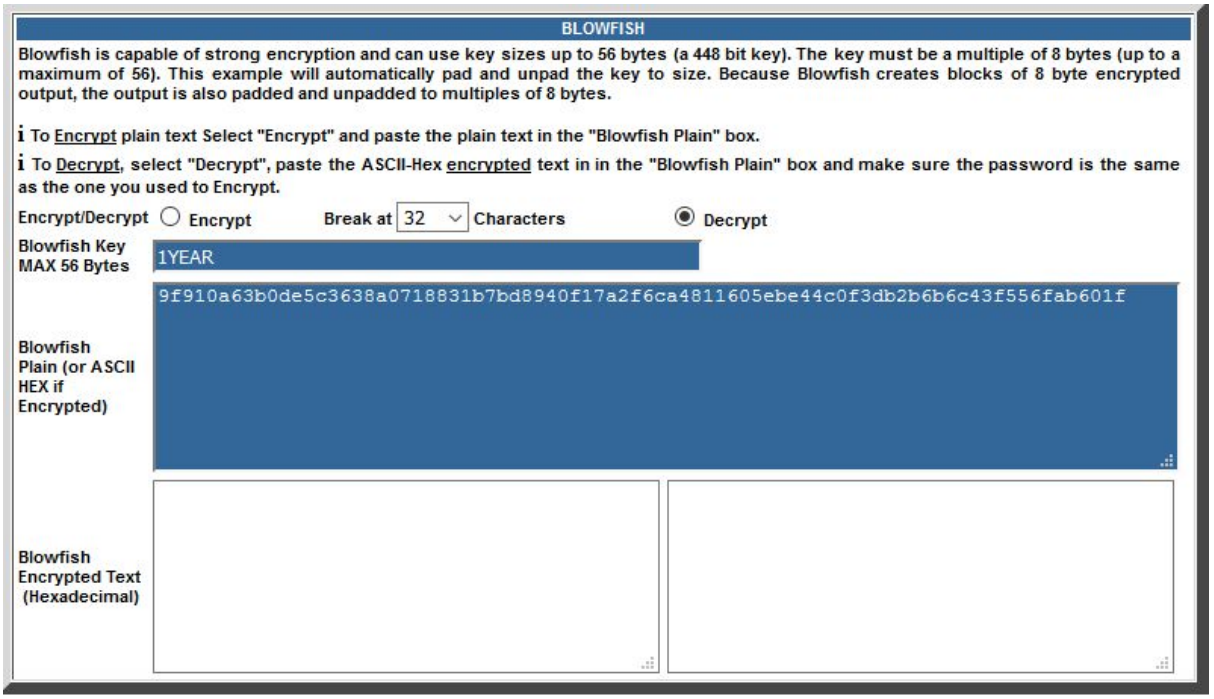
9f910a63b0de5c3638a0718831b7bd8940f17a2f6ca4811605ebe44c0f3db2b6b6c43f556fab601f|key:1YEAR

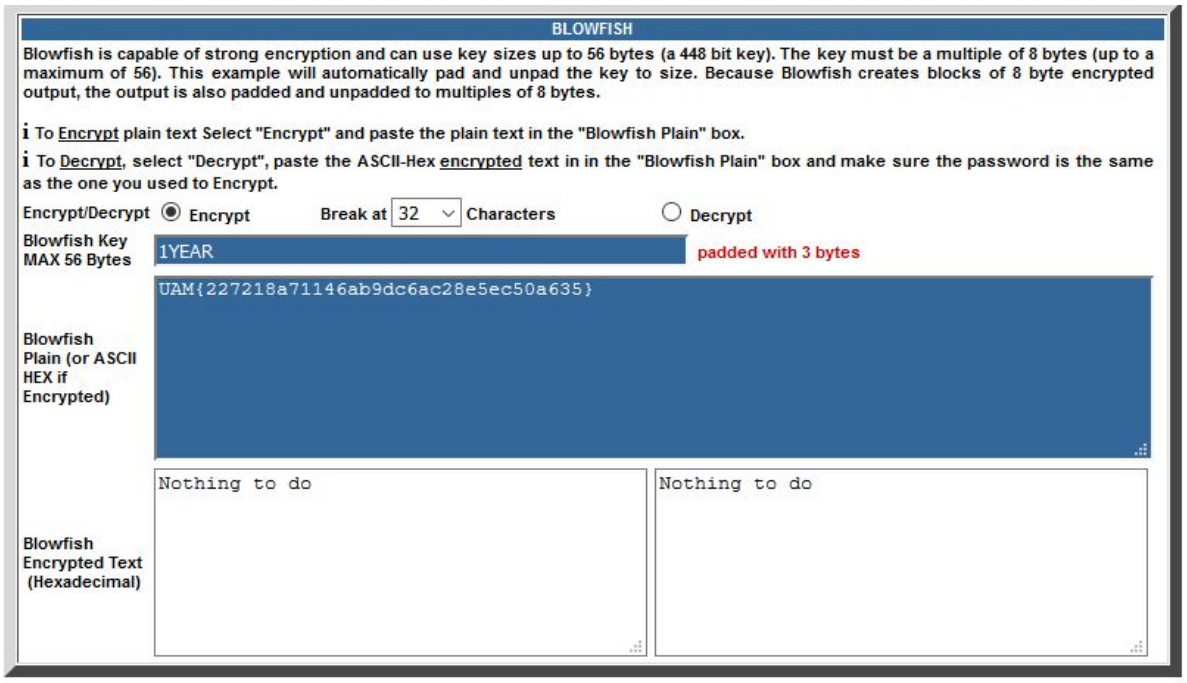
Probablemente sea un algoritmo de cifrado y 1YEAR sea la clave

blowfish

Tras muchas muchísimas vueltas, probando con decodificadores y encriptaciones varias, doy con ello. El método para encontrarlo fue buscar y probar todas y cada una de las herramientas que conozco y buscar unas cuantas más hasta dar con esta web de más abajo. Cybercheff no desencriptaba blowfish como esta:
https://webnet77.net/cgi-bin/helpers/blowfish.pl

Con casi cualquier herramienta de identificación de hashes dirá que coincide con RIPEMD320 pero por ahí no conseguí nada, así que seguí buscando herramientas hasta dar con esa. Si hubiera sabido que era blowfish me habría ahorrado varias horas de búsqueda de herramientas y prueba-error puesto que “blowfish decrypt” en google nos hubiera dado como primer resultado esta web… grrr





Flag

UAM{227218a71146ab9dc6ac28e5ec50a635}

Lo meto en la plataforma y… ¡First blood! ¡Yujuuu!

Conclusión

Ha sido un ctf muy variado, con esteganografía, cifrados, análisis y captura de tráfico de red de servidores indiscretos... y un crypto traicionero que me ha costado horas por confiar en mis herramientas habituales. He aprendido a analizar un pcap con wireshark, a no confiar ciegamente en las herramientas y a volver a probar lo que ya estaba probado. Parece que a veces caminar en círculos no es tan mala idea ;)

Gracias a @mrb0b0t y @devploit por este ctf tan currado :D

José Ángel Sánchez
@_j0n3