CTF Una-al-mes

SILICON VALLEY. Episodio 3.

Richard mandó a Gilfoyle montar un servicio oculto que mantuviera a flote "El Flautista" pero este ya no recuerda dónde 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}

Resolución

Descargamos el fichero Marvel.zip y descomprimimos. Obtenemos el fichero *"Avengers Infinity War Soundtrack - DEP Stan Lee.wav".*

Analizamos con file

Avengers Infinity War Soundtrack - DEP Stan Lee.wav: RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, stereo 44100 Hz

Comprobamos cadenas existentes con strings, y en la última línea aparece:

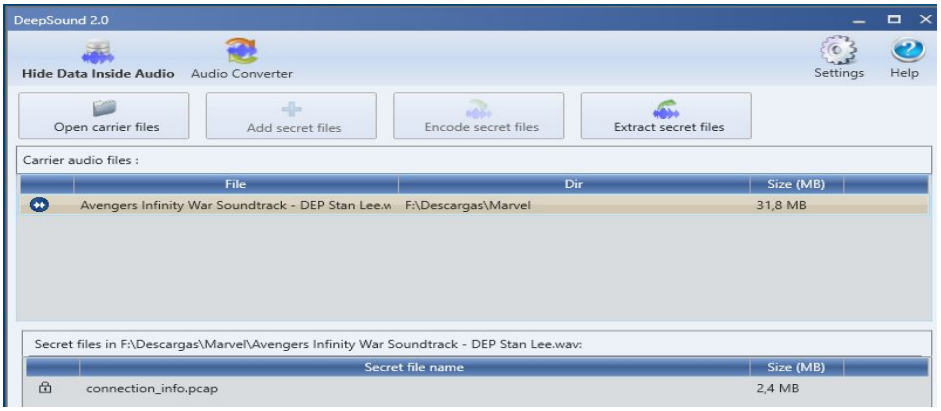
U29uaWRvUHJvZnVuZG87KQo=

echo "U29uaWRvUHJvZnVuZG87KQo=" | base64 -d

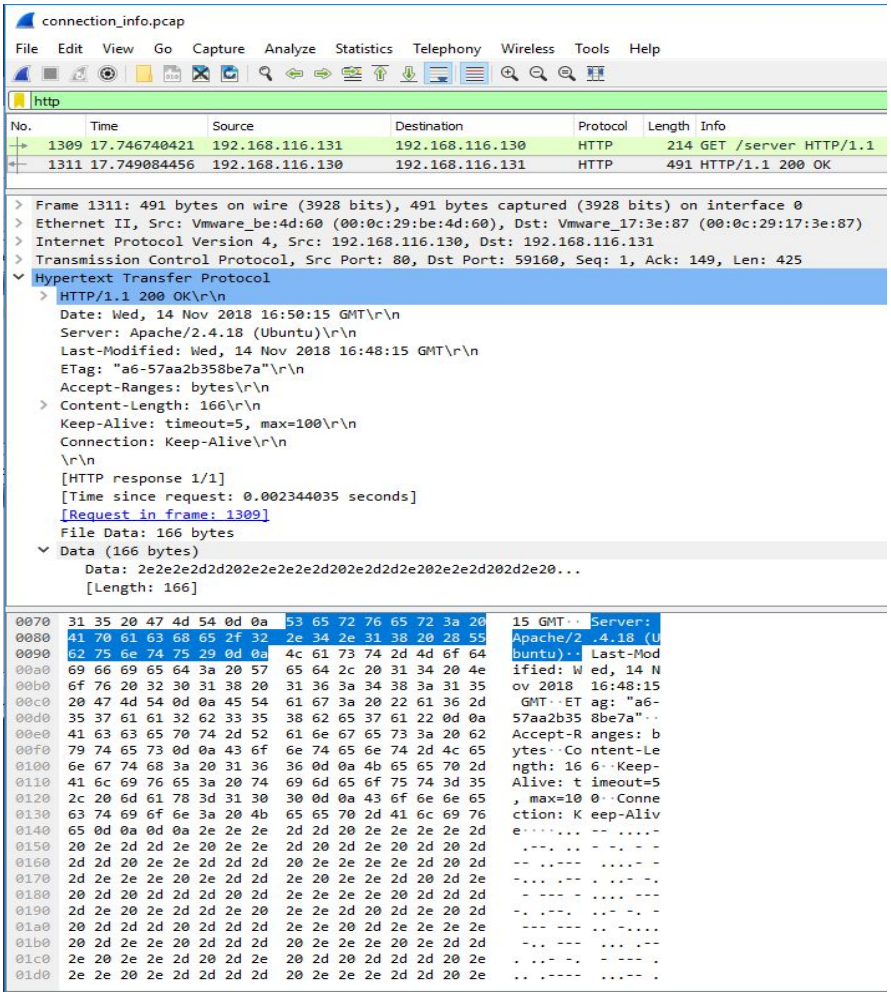
SonidoProfundo;)

Una búsqueda de "DeepSound" y nos aparece un software de stego… vamos bien….

Descargamos e instalamos, nos aparece un fichero oculto. “connection_info.pcap”



Extraemos el fichero y analizamos con Wireshark. Filtramos por HTTP.



Observamos algo que parece morse

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

Traducimos en https://morsecode.scphillips.com/translator.html

34PUNTO247PUNTO69PUNTO86DOSPUNTOS1337

Parece que ya tenemos el servicio oculto.

nc 34.247.69.86 1337

y el servicio devuelve un bucle con caracteres aparentemente aleatorios. Probamos introduciendo caracteres como entrada, pero siempre resultados diferentes.

Para realizar un análisis estático, volcamos sobre un fichero, dejando el proceso algunos minutos….

nc 34.247.69.86 1337 > a.raw

Buscamos cadenas que tengan lo que puede ser la flag “UAM” sobre el fichero.

grep -a -e UAM a.raw

UAM:OWY5MTBhNjNiMGRlNWMzNjM4YTA3MTg4MzFiN2JkODk0MGYxN2EyZjZjYTQ4MTE2MDVlYmU0NGMwZjNkYjJiNmI2YzQzZjU1NmZhYjYwMWZ8a2V5OjFZRUFS

decodificamos en base64:

9f910a63b0de5c3638a0718831b7bd8940f17a2f6ca4811605ebe44c0f3db2b6b6c43f556fab601f|key:1YEAR

En Hex:
..
c°Þ\68 q.1·½.@ñz/l¤...ëäL.=²¶¶Ä?Uo«`. 320 bits

Clave: 1YEAR 40 bits

Parece un cifrado en bloque, no parece un cifrado clásico, alfabeto A-Z…..
Tras muchos intentos con distintas herramientas y algoritmos de cifrado, y descartando algunos por el tamaño de la clave, llegamos a una web que utilizando BlowFish con la clave “1YEAR” nos devuelve la flag.

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

UAM{227218a71146ab9dc6ac28e5ec50a635}

Found : UAM_Ann1v3RS4R10
(hash = 227218a71146ab9dc6ac28e5ec50a635)

@bicacaro