UAM Reto Silicon Valley: Episodio 3 - Hispasec

Descripción

Nombre: UAM- Silicon Valley - Episodio 3 - (Related https://www.filmaffinity.com/es/film279751.html)
Fecha de liberación: 15 de noviembre de 2018
Autor: 1v4n https://unaalmes.hispasec.com/team/40
Puntuación: 350

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


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}

Objetivo

Formato de la flag: UAM{md5}

Herramientas utilizadas

Versión 70.0.3538.102 (Build oficial) (64 bits) https://www.google.com/chrome/
curl 7.61.0
file-5.34
7-Zip [64] 16.02 https://www.7-zip.org/download.html
GNU strings (GNU Binutils for Debian) 2.31.1
GNU grep
DeepSound 2.0 http://jpinsoft.net/DeepSound/
Wireshark 2.6.4 https://www.wireshark.org/docs/relnotes/wireshark-2.6.4.html
CyberChef - The Cyber Swiss Army Knife https://gchq.github.io/CyberChef
Netcat v1.10-41.1 http://netcat.sourceforge.net/
Blowfish Encryption and Decryption https://webnet77.net/cgi-bin/helpers/crypthelp.pl

Resumen:

Comenzamos por visitar el reto descargando el archivo adjunto *con el fichero de Gilfoyle* utilizando la herramienta *curl -L "https://docs.google.com/uc?export=download&id=1qTuI9VndJ24krrO8U1WF3JpS77M4M2hV" > output3*

```
curl -L
"https://docs.google.com/uc?export=download&id=1qTuI9VndJ24krrO8U1WF3JpS77M4M2hV" >
output3
root@kali:~/Desktop/uam/SiliconValley/SV-Ep3# file output3
output3: Zip archive data, at least v2.0 to extract
root@kali:~/Desktop/uam/SiliconValley/SV-Ep3# mv output3 output3.zip
```

Obteniendo un archivo comprimido que llamaremos output3.zip (MD5: 3ac8ba8cefbc6b3739bcda1ef2e956c7).

Procesado del archivo comprimido .zip

Descomprimimos el fichero *output3.zip* de 30,4 MB obteniendo un archivo de audio con el Soundtrack de la película de Vengadores: Infinity War un homenaje para el recién fallecido Stan Lee.

```
root@kali:~/Desktop/uam/SiliconValley/SV-Ep3# 7z x output3.zip

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=es_ES.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs Intel(R)
Core(TM) i7-6500U CPU @ 2.50GHz (406E3),ASM,AES-NI)

Scanning the drive for archives:
1 file, 30425943 bytes (30 MiB)

Extracting archive: output3.zip
--
Path = output3.zip
Type = zip
Physical Size = 30425943

Everything is Ok

Size:       33323015
Compressed: 30425943
root@kali:~/Desktop/uam/SiliconValley/SV-Ep3# ls -la
total 62268
drwxr-xr-x 2 root root     4096 nov 21 00:10  .
drwxr-xr-x 4 root root     4096 nov 20 19:08  ..
-rw------- 1 root root 33323015 nov 15 09:58 'Avengers Infinity War Soundtrack - DEP
Stan Lee.wav'
-rw-r--r-- 1 root root 30425943 nov 20 17:27  output3.zip
```

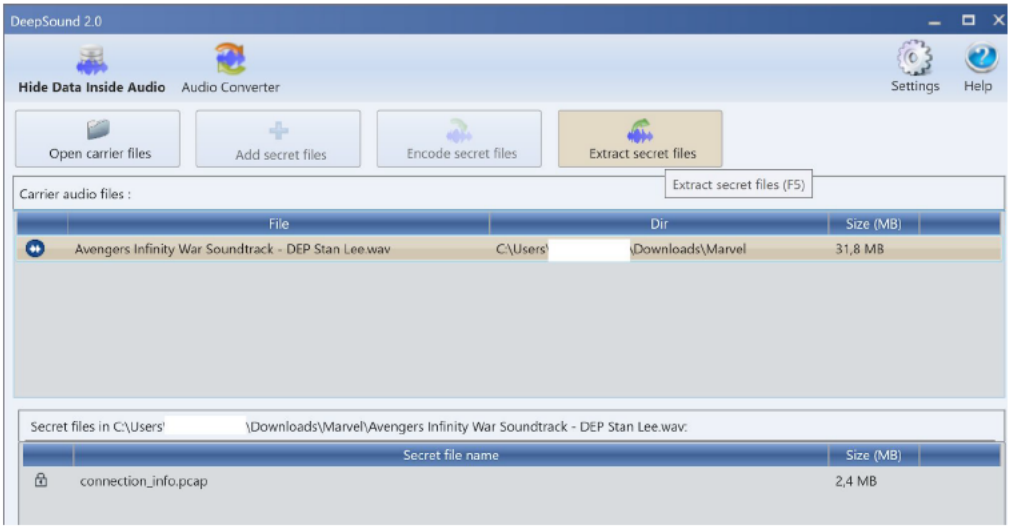
Analizado el archivo de audio .wav

Revisando el audio 'Avengers Infinity War Soundtrack - DEP Stan Lee.wav' (MD5: 10b72dee628e605dbe1f6f85362586b7) obtenemos una cadena codificada en base64 que nos aporta un consejo que nos apunta a una posible ocultación por esteganografía de fichero/s a través del programa DeepSound (Sonido Profundo)

```
root@kali:~/Desktop/uam/SiliconValley/SV-Ep3# md5sum 'Avengers Infinity War Soundtrack - DEP Stan Lee.wav'
10b72dee628e605dbe1f6f85362586b7  Avengers Infinity War Soundtrack - DEP Stan Lee.wav
root@kali:~/Desktop/uam/SiliconValley/SV-Ep3# strings 'Avengers Infinity War Soundtrack - DEP Stan Lee.wav'
RIFF
WAVEfmt
data
...
U29uaWRvUHJvZnVuZG87KQo=
root@kali:~/Desktop/uam/SiliconValley/SV-Ep3#
root@kali:~/Desktop/uam/SiliconValley/SV-Ep3# printf 'U29uaWRvUHJvZnVuZG87KQo=' | base64 -d
SonidoProfundo;)
```

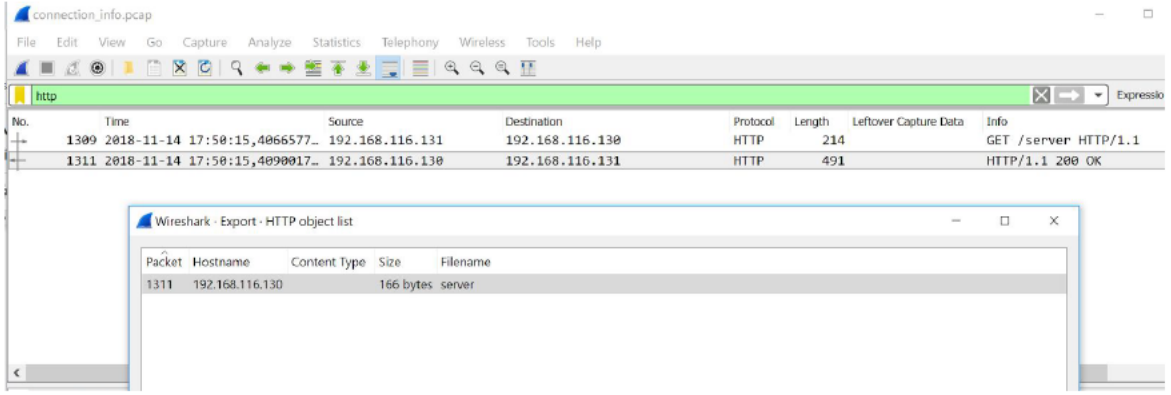
Extracción del archivo .pcap con DeepSound

Ejecutamos el programa en Windows OS de DeepSound 2.0 y pasamos a extraer un archivo de captura de tráfico que posiblemente nos desvele el *servicio oculto* llamado *connection_info.pcap* (MD5: 644274589c1ede9caa531319cf363907)



Obtención del servicio

Abrimos el archivo con Wireshark 2.6.4 el archivo *connection_info.pcap* obteniendo una lista de varios paquetes, estamos interesados en los http, antes de analizarlos, verificaremos si podemos exportar archivos de datos *File->Export Objects->Http*



Conseguimos exportar un archivo llamado *'server'* (MD5: 575970d942b076a1e60281097d0b9aef) que nos arroja la siguiente string en Morse

```
root@kali:~/Desktop/uam/SiliconValley/SV-Ep3# cat server
...-- ....- .--. ..- -. - --- ..--- ....- -.... .--. ..- -. - --- -.... ----. .--. ..-
-. - --- ---.. -.... -.. --- ... .--. ..- -. - --- ... .---- ...-- ....- -....
```

Lo decodificamos obteniendo 34PUNTO247PUNTO69PUNTO86DOSPUNTOS1337 y nuestro servicio será ***34.247.69.86:1337***

Acceso al servicio

Pasados unos minutos escuchando el netcat al servicio generamos un archivo de salida. Al cual filtramos con strings y con un grep con el término UAM.

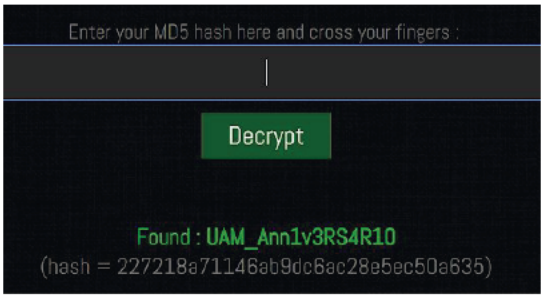
```
root@kali:~/Desktop/uam/SiliconValley/SV-Ep3/output3# nc 34.247.69.86 1337 > output

root@kali:~/Desktop/uam/SiliconValley/SV-Ep3/output3# strings output | grep UAM
'd
UAM:OWY5MTBhNjNiMGRlNWMzNjM4YTA3MTg4MzFiN2JkODk0MGYxN2EyZjZjYTQ4MTE2MDVlYmU0NGMwZjNkYjJi
NmI2YzQzZjU1NmZhYjYwMWZ8a2V5OjFZRUFS
```

Decodificación y obtención de la Flag

Pasamos a decodificar la cadena que identificamos como base64 utilizamos la herramienta online de CyberChef y obtenemos una cadena con cifrado Blowfish ***'9f910a63b0de5c3638a0718831b7bd8940f17a2f6ca4811605ebe44c0f3db2b6b6c43f556fab601f\|key:1YEAR'***.

Posiblemente un cifrado con la key: 1YEAR. Encontramos despúes buscar decodificadores el servicio online https://webnet77.net/cgi-bin/helpers/blowfish.pl que nos arroja el resultado de la FLAG.

Y la solución es ***UAM{227218a71146ab9dc6ac28e5ec50a635}***



Autor: MXY0bg== a.k.a. 1v4n
Twitter: https://twitter.com/Hackers4f // https://twitter.com/1r0Dm48O