EPISODIO 2
300

Dinesh ha perdido la clave VERDADERA que usaba para abrir su zip secreto pero gracias a DIOS tiene un archivo .raw donde puede recuperarla y necesita que le echemos una mano.

A Dinesh le encantan los mensajes con doble sentido, debéis tenerlo en cuenta...

- Archivo .raw (escoged el que mejor os venga):

https://www.mediafire.com/file/piv4t8514bp5dpg/pied_piper_bak.zip/file

https://mega.nz/#!iAUDnKwA!Y2g23qnZ9rwZvzZA3Bg8cbENe_ZtASOi1NF

Info: Las pistas os servirán a partir de que tengáis la contraseña del zip adjunto (Secretos_Dinesh.zip). Recordad que flag.txt tiene dos cifrados (leed bien README).

Info: La flag tiene el formato UAM{md5}

Descargamos tanto el .raw como el .zip.

El .raw vemos que es un volcado de memoria, por lo que vamos a sacar el profile:

 # volatility -f pied_piper_bak.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/media/sf_Downloads/pied_piper_bak/pied_piper_bak.raw)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf80002a520a0L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff80002a53d00L
KUSER_SHARED_DATA : 0xfffff78000000000L

Image date and time : 2018-10-15 10:48:27 UTC+0000
Image local date and time : 2018-10-15 12:48:27 +0200

Ahora que ya tenemos el profile, vamos a sacar el listado de ficheros:

 # volatility -f pied_piper_bak.raw --profile=Win7SP1x64 filescan > fitxers.txt

En el listado de ficheros, hay uno en especial que parece interesante:

0x0000000040501860 16 0 R--rw-
\Device\HarddiskVolume2\Users\Richard\Desktop\piperdb.db

Vamos a recuperarlo:

 # volatility -f pied_piper_bak.raw --profile=Win7SP1x64 dumpfiles -Q 0x0000000040501860 --name -D ./
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x40501860 None
\Device\HarddiskVolume2\Users\Richard\Desktop\piperdb.db
SharedCacheMap 0x40501860 None
\Device\HarddiskVolume2\Users\Richard\Desktop\piperdb.db

 # file file.None.0xfffffa800273c2d0.piperdb.db.dat
file.None.0xfffffa800273c2d0.piperdb.db.dat: SQLite 3.x database, last written using SQLite version 3015002

Vamos a obtener más información del fichero:

 # sqlite3 file.None.0xfffffa800273c2d0.piperdb.db.dat

qlite> .dbinfo
database page size: 4096
write format: 1
read format: 1
reserved bytes: 0
file change counter: 6
database page count: 5
freelist page count: 0
schema cookie: 5
schema format: 4
default cache size: 0
autovacuum top root: 0
incremental vacuum: 0
text encoding: 1 (utf8)
user version: 0

```
application id:      0
software version:    3015002
number of tables:    3
number of indexes:   1
number of triggers:  0
number of views:     0
schema size:         287
data version         1
```

sqlite> .schema

```
CREATE TABLE `USERS` (
        `id`    INTEGER UNIQUE,
        `user`  TEXT,
        `pass`  TEXT,
        `age`   INTEGER,
        `md5`   INTEGER
);
CREATE TABLE `FLAG` (
        `id_flag`       INTEGER,
        `char_flag`     TEXT,
        `falso`  TEXT
);
CREATE TABLE `COMMUNICATIONS` (
        `idmsg`         INTEGER,
        `msg`   TEXT,
        `rcv`   INTEGER,
        `user`  TEXT,
        `sum`   TEXT
);
```

sqlite> select * from users;

```
1|admin|21232f297a57a5a743894a0e4a801fc3|28|21232f297a57a5a743894a0e4a801fc3
2|richard|97a53ee9f45adfe53c762a72f83f6f43||97a53ee9f45adfe53c762a72f83f6f43
3|gilfoyle|327a6c4304ad5938eaf0efb6cc3e53dc||327a6c4304ad5938eaf0efb6cc3e53dc
4|erlich|e3353512022242b52c702b4b38951356||e3353512022242b52c702b4b38951356
5|jared|ecd5c54d0956b37daff84de64e06326f||ecd5c54d0956b37daff84de64e06326f
6|ghost|71144850f4fb4cc55fc0ee6935badddf||
7|true_god|BAAABAABAAABBAAAAAAABBAABABBBAAAAAAAAAABAAAAAAAABAABBB
AABBABABAAAAAAAABBAB||3L_R3m1t0_m3j0R_Q_L4_fl4ut4
```

En este punto, dado que el enunciado decía: “Dinesh ha perdido la clave **VERDADERA** que usaba para abrir su zip secreto pero gracias a **DIOS** tiene un archivo .raw donde puede recuperarla y necesita que le echemos una mano.”

Como vemos, el usuario numero 7 se llama true_god por lo que vamos a examinar más detenidamente este usuario

Inmediatamente los caracteres AB … me suenan a una codificación que ya había visto anteriormente, **Baconian Cipher Decoder**, por lo que voy a intentar decodificarlo. Vamos a: https://www.dcode.fr/bacon-cipher y insertamos el texto codificado. El resultado obtenido es:

↑ ↓	↑ ↓
A=A,B=B (αß2)	REMAZOABACONIAN

Con este password podemos descomprimir el .zip

En dicho .zip tenemos dos ficheros, un fichero llamado flag.txt y otro llamado README.
El flag.txt está cifrado, y no podemos entender lo que contiene, mientras que README nos da una serie de pistas:

1. "We are the DATE" https://www.youtube.com/watch?v=tYIYRRLj-n4

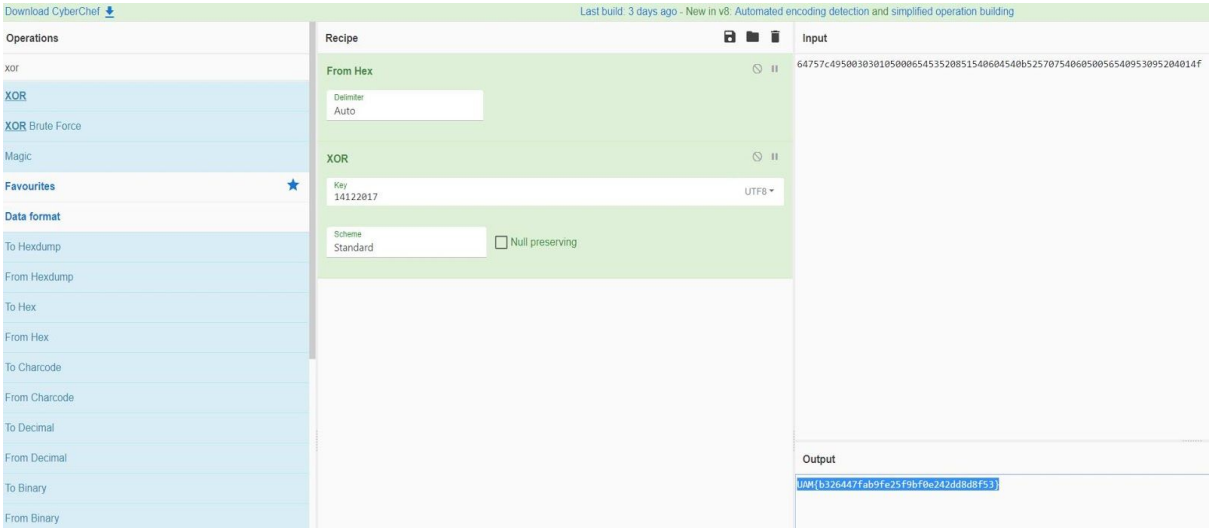
2. La clave final de todo está en el corazón de Telegram, en sus comienzos...

Como ya sabemos por el enunciado, flag.txt está doblemente cifrado, y en el README tenemos dos pistas, así que vamos a por la primera.

La DATE del video youtube que hace referencia el README es: 1985.
Recordamos la existencia de la codificación ASCII85 así que vamos a ver qué pasa si deciframos el contenido de flag.txt con este tipo de codificación. https://www.dcode.fr/ascii-85-encoding

64-75-7c-49-50-03-03-01-05-00-06-54-53-52-08-51-54-06-04-54-0b-52-57-07-54-06-05-00-56-54-09-53-09-52-04-01-4f Vas bien, ya te queda menos.

Ok, vamos bien … así que a por la segunda parte del README …
Aquí he de decir que ha sido algo duro … he probado muchísimas cosas …
Eso de Telegram … y lo de sus comienzos … me tenía muy despistado. El caso está en que alguna operación teníamos que hacer con los caracteres hexadecimales que nos dan .. y una muy común es XOR.
Haciendo brute force he podido descubrir un patrón … es decir .. podía llegar a hacer que haciendo XOR saliera como resultado UAM{
El "código" para conseguir esto era: 1412. Lo de Telegram que me tenía muy despistado … al final ha sido la clave, y he ido a mirar la fecha en que se creó el canal de @unaalmes en Telegram, y la fecha era: 14122017.



Así pues, el FLAG es: **UAM{b326447fab9fe25f9bf0e242dd8d8f53}**

DarkEagle