CTF Una-al-mes

SILICON VALLEY. Episodio 2.

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_ZtASOi1NFgrgfL8sg

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}

Resolución

Descargamos el fichero y descomprimimos, nos encontramos con un archivo raw.

El fichero parece un volcado de memoria, por lo que vamos a utilizar **volatility**

Primero identificar el sistema.

volatility -f pied_piper_bak.raw imageinfo

Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418

Una vez identificado, visualizamos los procesos activos.

volatility --profile=Win7SP1x64 -f pied_piper_bak.raw pslist

Si nos fijamos en la lista de procesos encontramos algunos que nos llaman la atención:

0xfffffa80012d9b30 DB Browser for	***1836***	***1464***	***9***	***345***	***1***
0xfffffa8001355060 notepad.exe	***2616***	***1464***	***1***	***62***	***1***
0xfffffa80013286e0 notepad.exe	***1520***	***1464***	***1***	***62***	***1***

Buscamos los ficheros abiertos por el proceso "***DB Browser"***

volatility --profile=Win7SP1x64 -f pied_piper_bak.raw -p 1836 handles -t File

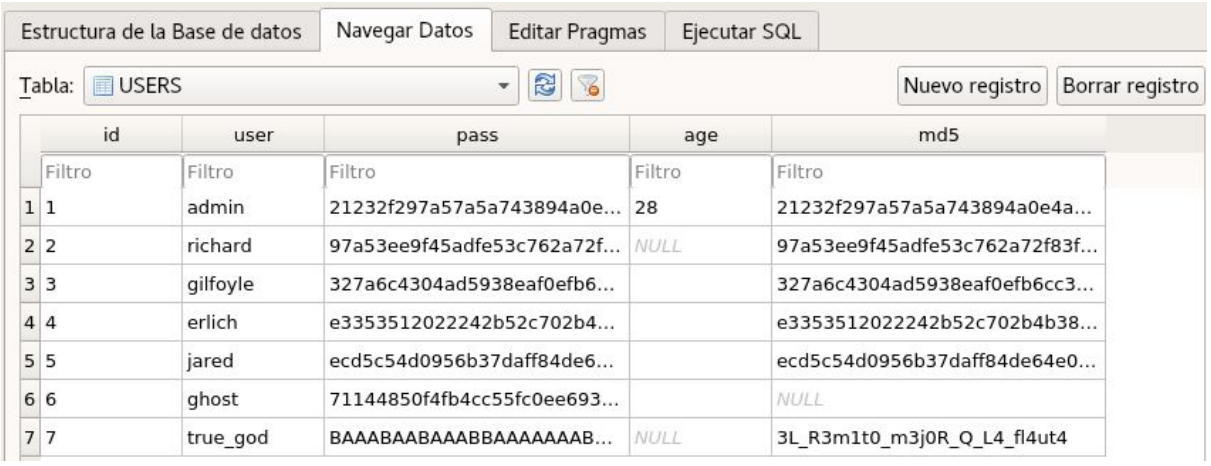
Entre todos los ficheros, encontramos un fichero, ***piperdb.db*** que parece interesante…

0xfffffa800103a8d0 1836 0x668 0x12019f File \Device\HarddiskVolume2\Users\Richard\Desktop\piperdb.db

Volcamos el fichero piperdb.db

volatility --profile=Win7SP1x64 -f pied_piper_bak.raw dumpfiles -i -r piperdb -n -D T/

Nos encontramos con base de datos SQLite, con tres tablas, la interesante, “USERS”



	id	user	pass	age	md5
	Filtro	Filtro	Filtro	Filtro	Filtro
1	1	admin	21232f297a57a5a743894a0e...	28	21232f297a57a5a743894a0e4a...
2	2	richard	97a53ee9f45adfe53c762a72f...	NULL	97a53ee9f45adfe53c762a72f83f...
3	3	gilfoyle	327a6c4304ad5938eaf0efb6...		327a6c4304ad5938eaf0efb6cc3...
4	4	erlich	e3353512022242b52c702b4...		e3353512022242b52c702b4b38...
5	5	jared	ecd5c54d0956b37daff84de6...		ecd5c54d0956b37daff84de64e0...
6	6	ghost	71144850f4fb4cc55fc0ee693...		NULL
7	7	true_god	BAAABAABAAABBAAAAAAAB...	NULL	3L_R3m1t0_m3j0R_Q_L4_fl4ut4

El último no sigue el formato, y si nos fijamos en la descripción del reto tenemos dos palabras en mayúsculas VERDADERA Y DIOS (true_god). Vamos bien…….

Examinamos pass:

BAAABAABAAABBAAAAAAABBAABABBBAAAAAAAAAABAAAAAAAABAABBBAABBABABAAAAAAAAABBAB

Cifrados AB => Beacon. Desciframos utilizando alfabeto de 26 letras:

https://mothereff.in/bacon

REMAZOABACONIAN

Ya tenemos password de “*Secretos_Dinesh.zip*”

En el zip tenemos dos ficheros, README y flag.txt

README:

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...

flag.txt

2Dd!E2(^as/MoI>2)$U91G(::/MJn20JtF90J+t:/N#@:2)?gA1+b1>/N#772)Hm=2D$U>/N#@:0OcUk1+b@B/MK+82)Hm=2D$U?/MJk12)[$D1bCCA/N#=90KC^B1+b1:/MJn21hIk2@<3Q#Bk;05+F.B<FCcS7F_,)I+Dk\-Df[N

El primer punto nos destaca “DATE” y un video:
USA for Africa - We Are The World - 1985

Luego examinando la codificación, y con la primera pista, tras probar **Base85**, obtenemos:

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.

Decodificación en CyberChef

Parece que tenemos 37 caracteres hexadecimales:

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

du|IP.....TSR.QT..T.RW.T...VT S R..O

Dispone de caracteres no imprimibles, lo que nos hace sospechar de alguna transformación tipo XOR

Probamos en CyberChef con un XOR Bruteforce y para la clave 31h (1)

Key = 31: UDMxa220417ebc9`e75e:cf6e741ge8b8c50~.Ûßë?

Parece que tenemos un formato UAM{MD5} (37 caracteres) UAM{ } 5 + 32 (MD5)

Con esto, y tras algunas pruebas, podemos deducir las cuatro primeras letras de la pass.

31 34 31 32 (**1412**)

UAM{a723447fbf9ce25f:ff5e242g`8a8f53~.ÛÜë:

Pero la cosa no es tan sencilla, parece que es una clave de mayor longitud.

La segunda pista, tampoco me ayuda mucho,

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

Nada de corazón, ni de fechas de Telegram, que empiece por 14, bueno si, la fecha de 14 Agosto del 2013, pero tampoco va, …….14 Diciembre…….

En este punto, empecé a trabajar en la posibilidad de realizar un script que reduzca el espacio de claves para un ataque de fuerza bruta al XOR. Disponemos una limitación importante en la salida sólo 0-9, a-f. Luego no pueden existir tantos caracteres diferentes en la clave.

texto:

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

pass:

31 34 31 32 31 31 31 31 31 30 31 31 31 31 31 32 31 31 31 31 32 31 31 31 31 31 31 31 30 31 31 31 31 31 31 31 32

14121111101111121111211111111011111112

UAM{a220407ebc9ce75e9cf6e741fe8b8c50}

No progreso demasiado por aquí, y pasan los días, decido tirar del HINT 2

Hint
Los grupos de Telegram pueden durar mucho tiempo pero no todo el mundo sobrevive a un XOR.

Esto nos confirma lo del XOR, y también menciona “Los grupos de Telegram pueden durar mucho tiempo…..

Un momento “grupo Telegram, mucho tiempo, UAM, comienzos”… No puede ser ……

Buscamos la fecha inicial del grupo de UAM, BINGO!!!!! (14 de diciembre 2017) **1412.**

Nos faltaba el año en la pass; **14122017**

Solución: CyberChef

UAM{b326447fab9fe25f9bf0e242dd8d8f53}

@bicacaro