

Una-al-mes: Silicon Valley - Episodio#1 - Hispasec

Enunciado CTF:

Alguien ha denunciado a "El Flautista" por hacer actividades empresariales en una vivienda personal. Necesitamos encontrar a la persona en cuestión para convencerlo de que retire la denuncia o se nos caerá el pelo. El problema es que ha habido un apagón en la incubadora de Erlich y todos los discos duros han muerto menos el de Gilfoyle. En ellos estaban las credenciales de acceso (encriptadas) a la plataforma de la empresa y la única pista del denunciante. Debes conseguir las credenciales de alguno de los archivos de Gilfoyle para entrar y poder encontrar la dirección de la persona que ha montado todo este lío.

Disco duro de Gilfoyle (escoged el enlace que mejor os venga):

<http://www.mediafire.com/file/31pj2a5umpfm345/GILFOYLE-HELLDD.zip>

https://mega.nz/#!3IkWISiK!MkrFlvvt7JBWm-_vrhlv-JFLoNFVh8_dDvFCE-qjKuc

Login: <http://34.247.69.86/siliconvalley/episodio1/login.php>

Resolución:

Accedemos a la URL que nos facilita el reto y vemos que es un formulario para introducir un usuario y su password:

<http://34.247.69.86/siliconvalley/episodio1/login.php>



Si analizamos el código fuente de la página no encontramos nada relevante.

Descargamos el archivo *GILFOYLE-HELLDD.zip* y lo descomprimos. Se trata de un archivo .raw, un dump de memoria.

Para analizarlo hacemos uso de la herramienta **Volatility**:

Usamos **imageinfo** para ver el profile que tenemos que utilizar para su análisis:

```
$ python vol.py --plugins=plugins/
--filename=/home/rafamartos/Documentos/CTF/Silicon Valley/GILFOYLE-HELLDD.raw
imageinfo
Volatility Foundation Volatility Framework 2.6
INFO      : volatility.debug      : Determining profile based on KDBG search...
           Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64,
Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000,
Win7SP1x64_23418 (Instantiated with Win2008R2SP0x64)
           AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
           AS Layer2 : FileAddressSpace
(/home/rafamartos/Documentos/CTF/Silicon Valley/GILFOYLE-HELLDD.raw)
           PAE type  : No PAE
           DTB       : 0x187000L
```

```

KDBG : 0xf800029f00a0L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xffffffff800029f1d00L
KUSER_SHARED_DATA : 0xffffffff7800000000L
Image date and time : 2018-09-15 09:56:27 UTC+0000
Image local date and time : 2018-09-15 11:56:27 +0200

```

Usando un profile de la lista procedemos a su análisis, por ejemplo Win2008R2SP0x64.

Analizamos los posibles hashes de usuarios del sistema con **hashdump**:

```

$ python vol.py --plugins=plugins/
--filename=/home/rafamartos/Documentos/CTF/Silicon\ Valley/GILFOYLE-HELLDD.raw
--profile=Win2008R2SP0x64 hashdump
Volatility Foundation Volatility Framework 2.6
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
unaalmes:1001:aad3b435b51404eeaad3b435b51404ee:777e926012b1c652e8866847b1bd64fa:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:211d6fd0a9f90f4967f52f09d9770038:::


```

Haciendo uso de **crackstation** (<https://crackstation.net/>) buscamos las claves para los usuarios encontrados:


```

31d6cfe0d16ae931b73c59d7e0c089c0
777e926012b1c652e8866847b1bd64fa
777e926012b1c652e8866847b1bd64fa
211d6fd0a9f90f4967f52f09d9770038

```



No soy un robot



reCAPTCHA
Privacidad · Condiciones

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
31d6cfe0d16ae931b73c59d7e0c089c0	NTLM	
777e926012b1c652e8866847b1bd64fa	NTLM	hispasec
777e926012b1c652e8866847b1bd64fa	NTLM	hispasec
211d6fd0a9f90f4967f52f09d9770038	Unknown	Not found.

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Si intentamos hacer log in en el formulario con ellas, no tenemos un resultado positivo.

Vemos los procesos que hay en ejecución con **pslist**. De la lista hay uno que me llama la atención:

```

$ python vol.py --plugins=plugins/
--filename=/home/rafamartos/Documentos/CTF/Silicon\ Valley/GILFOYLE-HELLDD.raw
--profile=Win2008R2SP0x64 pslist
Volatility Foundation Volatility Framework 2.6
(Salida truncada)
0xffffffff8002d24b30 soffice.exe          1756    1900        1        66        1 1
2018-09-15 09:48:13 UTC+0000

```

Se trata de la aplicación de ofimática LibreOffice.

Buscamos archivos de LibreOffice con **filescan** y hacemos un **grep** con su extensión:

```
$ python vol.py --plugins=plugins/
--filename=/home/rafamartos/Documentos/CTF/Silicon\ Valley/GILFOYLE-HELLDD.raw
--profile=Win2008R2SP0x64 filescan | grep odt
Volatility Foundation Volatility Framework 2.6
0x000000007fca5580      2      0 RW-rw-
\Device\HarddiskVolume2\Users\unaalmes\Desktop\~lock.info.odt#

0x000000007fcabd50      1      1 RW-r--
\Device\HarddiskVolume2\Users\unaalmes\Desktop\info.odt
```

Y procedemos a hacer el dump del archivo info.odt con **dumpfile**:

```
$ python vol.py --plugins=plugins/
--filename=/home/rafamartos/Documentos/CTF/Silicon\ Valley/GILFOYLE-HELLDD.raw
--profile=Win2008R2SP0x64 dumpfiles -Q 0x000000007fcabd50 -D
/home/rafamartos/Documentos/CTF/Sillycon\ Valley/ -n
```

Obteniendo como resultado el archivo: file.None.0xfffffa8001acdf10.info.odt.dat

Dentro del archivo encontramos lo que parece un texto en base64. Guardo su contenido en un archivo .txt y procedo a descifrarlo:

```
$ cat info_contenido.txt | base64 -d
(Salida truncada)
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\sys base64: entrada
inválida
```

Parte del contenido se puede descifrar, pero se detiene por un error al encontrar un carácter inválido.

Analizamos la cadena en base64 del archivo para ver qué caracteres no se encuentran dentro del alfabeto de esta codificación, para ello hago uso de una expresión regular:

```
[^A-Za-z0-9+\/=] | [=] | [=]{3,}$
```

(Fuente: <https://stackoverflow.com/questions/475074/regex-to-parse-or-validate-base64-data>)

Y de la herramienta online <https://regex101.com/>



Vemos que resalta en azul unos corchetes que delimitan lo que parece un hash MD5:

```
[ 448333920e12dc9fd9c5e8c30e6b1ea2 ] : [ b3f894165d6166da47d52ffb77b5d87 ]
```

Buscamos el texto que ha generado esos hashes usando <https://md5online.org//md5-decrypt.html>

[Gilfoyle:Satan]

Son las credenciales para hacer log in en el formulario del denunciado.

Denuncia recibida: https://drive.google.com/open?id=10iguWjRmx3mB0Y4g9iRrJOIXZ1HIJ_zC

Descargamos una imagen del enlace que aparece en pantalla y obtenemos el documento "denuncia.jpg"

JUZGADO DE INSTRUCCION N° 2

PLAZA CASTILLA, 1
Teléfono: _____ Fax: _____
Número de Identificación Único: _____

DILIGENCIAS PREVIAS PROC. ABREVIADO

Procurador/a: SIN PROFESIONAL ASIGNADO
Representado: _____

PROVIDENCIA DEL MAGISTRADO-JUEZ

SR. _____

En _____, a _____

Vista la anterior diligencia se tiene por personado y parte en las mismas al _____ bajo la dirección letrada de D. _____ en nombre y representación de _____ y al propio tiempo, dese traslado de las actuaciones al Procurador por medio de copia de las mismas, para que, conforme a lo dispuesto en el artículo 784, 1° de la Ley de Enjuiciamiento Criminal, presente escrito de defensa en el plazo de **diez días** frente a las acusaciones formuladas, con la prevención de que en caso de no verificarlo se entenderá que se opone a las actuaciones y seguirá su curso el procedimiento sin perjuicio de la responsabilidad en que pueda incurrir.

MODO DE IMPUGNACION: mediante interposición de recurso de reforma en el plazo de tres días ante este órgano judicial.

Lo mandó y firma S.S^a. Doy fe.-

Si analizamos los metadatos del archivo con **exiftool**, encontramos unas coordenadas:

```
$ exiftool denuncia.jpg
```

(Salida truncada)

Location : 37.436712, -122.137837

Buscando las coordenadas en Google Maps, vemos el número de la vivienda: **2126**



Por tanto, haciendo el MD5 de **2126** tenemos el flag:

MD5 hash for 2126 is : 3b92d18aa7a6176dd37d372bc2f1eb71

UAM{3b92d18aa7a6176dd37d372bc2f1eb71}

Rafa Martos
@elbuenodefali