

EASY MODE

800

Vamos a ver la información que podéis conseguir de un dominio. Reto nivel fácil para no saturaros tras la uad360 :P

La flag os va a gustar...

Dominio: lesaleapagar.e96e7c910b.com

Flag

Submit

Lo que hago primero es hacer un whois al dominio:

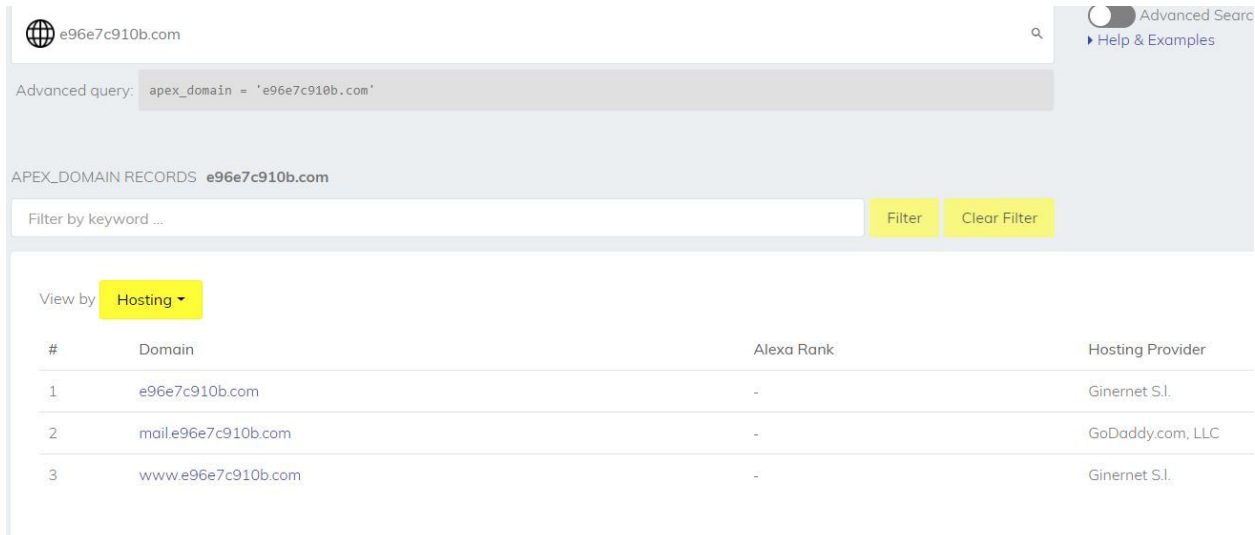
```
root@kali:~/unaalmes/uad360# whois e96e7c910b.com
Domain Name: E96E7C910B.COM
Registry Domain ID: 1832447186_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2018-10-26T10:16:34Z
Creation Date: 2013-10-25T07:22:25Z
Registry Expiry Date: 2019-10-25T07:22:25Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS33.DOMAINCONTROL.COM
Name Server: NS34.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2019-06-16T20:17:47Z <<<
```

Vemos que es un dominio registrado con godaddy. Se me ocurre tirar para ver si hay algo de OSINT, así que investigo un poco el historial de ese dominio.

En <https://crt.sh> no encuentro nada referente a este dominio.

En https://securitytrails.com/list/apex_domain/e96e7c910b.com

Puedo ver que ha tenido 3 subdominios:



Advanced query: apex_domain = 'e96e7c910b.com'

APEX_DOMAIN RECORDS e96e7c910b.com

Filter by keyword ... Filter Clear Filter

View by Hosting

#	Domain	Alexa Rank	Hosting Provider
1	e96e7c910b.com	-	Ginernet S.L.
2	mail.e96e7c910b.com	-	GoDaddy.com, LLC
3	www.e96e7c910b.com	-	Ginernet S.L.

Como vemos, el dominio que nos propone el enunciado no está aquí, de todas formas en <https://web.archive.org/> podemos encontrar un snapshot del 7 de agosto de 2018 del dominio principal ... pero no nos sirve de nada.

Seguimos con los procedimientos standard para ver que tiene el subdominio, y lo siguiente a probar es consultar el DNS. Con una simple consulta de los registros TXT del subdominio, tenemos lo que nos interesa:

```
root@kali:~/unaalmes/uad360# dig -t TXT lesaleapagar.e96e7c910b.com
```

```
>>> DiG 9.11.5-P4-5-Debian <<>> -t TXT lesaleapagar.e96e7c910b.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42736
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;lesaleapagar.e96e7c910b.com.      IN      TXT
```

;; ANSWER SECTION:

lesaleapagar.e96e7c910b.com. 1782 IN TXT

"https|3a2f2f|drive|2e|google|2e|com|2f|open|3f|id|3d|1Qsbr5NdE|2d|FsX9JIZeFzvpKDJ1OOxzgj7|0a|"

Vemos que la URL esta parte en HEX, por lo que la reescribimos correctamente:

<https://drive.google.com/open?id=1Qsbr5NdE-FsX9JIZeFzvpKDJ1OOxzgj7>

Si accedemos a la URL tenemos otra serie de links:

<https://unaaldia.hispasec.com/2019/03/una-al-dia-tendra-su-propio-congreso-de-seguridad-informatica-uad360.html>

<https://drive.google.com/file/d/1xRnh8JNhHR6MEdW8bysC9YL1KkcgV3c5/view?usp=sharing>

El primer LINK es la noticia de hispasec y el congreso de uad360 realizado.

En el segundo link, tenemos un fichero ZIP con contraseña, el interior del cual tiene una imagen. Parece claro que la contraseña del ZIP debe ser alguna palabra que hay en la noticia del primer enlace.

Descargamos el ZIP.

```
root@kali:~/unaalmes/uad360# zipinfo imagen.zip
```

```
Archive: imagen.zip
```

```
Zip file size: 58577 bytes, number of entries: 1
```

```
-rw----- 3.0 unx 58707 BX defN 19-Jun-14 15:01 ctf.jpg
```

```
1 file, 58707 bytes uncompressed, 58385 bytes compressed: 0.5%
```

Si quisiéramos hacer fuerza bruta, tendríamos que usar john, puesto que hashcat **NO NOS SIRVE**, ya que no tiene soporte para **PKZIP2**.

```
root@kali:~/unaalmes/uad360# zip2john imagen.zip > petar.txt
```

```
ver 2.0 efh 5455 efh 7875 imagen.zip/ctf.jpg PKZIP Encr: 2b chk, TS_chk, cmplen=58397, decmplen=58707, crc=2B267DFF
```

Generamos un diccionario para bruteforzar el ZIP, usando el link de la noticia, sin profundidad, para que solo utilice la URL que le pasamos para crear el diccionario.

```
root@kali:~/unaalmes/uad360# cewl -d 0
```

```
https://unaaldia.hispasec.com/2019/03/una-al-dia-tendra-su-propio-congreso-de-seguridad-infor-  
matica-uad360.html -w diccionario.txt
```

```
root@kali:~/unaalmes/uad360# john --wordlist=diccionario.txt petar.txt
```

Using default input encoding: UTF-8

Loaded 1 password hash (PKZIP [32/64])

Will run 6 OpenMP threads

Press 'q' or Ctrl-C to abort, almost any other key for status

locomotora (imagen.zip/ctf.jpg)

1g 0:00:00:00 DONE (2019-06-16 22:46) 33.33g/s 11666p/s 11666c/s 11666C/s Una..RSD

Use the "--show" option to display all of the cracked passwords reliably

Session completed

```
root@kali:~/unaalmes/uad360# unzip -P locomotora imagen.zip
```

Archive: imagen.zip

inflating: ctf.jpg

```
root@kali:~/unaalmes/uad360# exiftool ctf.jpg
```

ExifTool Version Number : 11.16

File Name : ctf.jpg

Directory : .

File Size : 57 kB

File Modification Date/Time : 2019:06:14 15:01:00+02:00

File Access Date/Time : 2019:06:14 15:12:30+02:00

File Inode Change Date/Time : 2019:06:15 15:30:32+02:00

File Permissions : rw-----

File Type : JPEG

File Type Extension : jpg

MIME Type : image/jpeg

JFIF Version : 1.01

Exif Byte Order : Big-endian (Motorola, MM)

X Resolution : 1

Y Resolution : 1

Resolution Unit : None

Artist : UAM{4ddcb848b6433e0649b69077a47da93c}

Y Cb Cr Positioning : Centered

Image Width : 702

Image Height : 395

Encoding Process : Progressive DCT, Huffman coding

Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Image Size : 702x395
Megapixels : 0.277

Como vemos, la flag se encuentra en los metadatos.

Flag: UAM{4ddcb848b6433e0649b69077a47da93c}

En <https://md5online.es/> encontramos la solución del md5

Found : **VimEsMejorQueNano**
(hash = 4ddcb848b6433e0649b69077a47da93c)

DarkEagle