# WRITE-UP UAD360 – CTF UAM - HISPASEC

# EPISODIO-3

## *ELABORADO POR: ARSENICS*

**Misión:**

EASY MODE

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

Tools:

-Url encoder characters: https://www.degraeve.com/reference/urlencoding.php

-John: https://github.com/magnumripper/JohnTheRipper

-Cewl: https://github.com/digininja/CeWL

-Exiftool: https://github.com/exiftool/exiftool

### Primera fase: Information Gathering – Dominios

Empezamos la búsqueda de información con el dominio que se nos ha proporcionado. Hay varias técnicas que podemos utilizar. Recursos: nslookup, dnsenum, theharvester, recondns, dig. Búscando opciones he encontrado esta web que está bastante bien: https://centralops.net/co/ aunque no me haya failitado en este caso lo que necesitaba.

En este caso me ha sido de utilidad:

dnsrecon -d lesaleapagar.e96e7c910b.com – D /usr/share/wordlists/dnsmap.txt -t std –xml dnsrecon.xn

```
root@kali:~# dnsrecon -d lesaleapagar.e96e7c910b.com -D /usr/share/wordlists/dnsmap.txt -t std --xml dnsrecon.xm
[*] Performing General Enumeration of Domain:lesaleapagar.e96e7c910b.com
[-] DNSSEC is not configured for lesaleapagar.e96e7c910b.com
[*]      SOA ns33.domaincontrol.com 97.74.106.17
[-] Could not Resolve NS Records for lesaleapagar.e96e7c910b.com
[-] Could not Resolve MX Records for lesaleapagar.e96e7c910b.com
[*]      TXT lesaleapagar.e96e7c910b.com https|3a2f2f|drive|2e|google|2e|com|2f|open|3f|id|3d|1Qsbr5NdE|2d|FsX9JIZeFzvpKDJ1OOxzgj7|0a|
[*] Enumerating SRV Records
[-] No SRV Records Found for lesaleapagar.e96e7c910b.com
[+] 0 Records Found
[*] Saving records to XML file: dnsrecon.xm
```

Vemos un txt con una url de un drive. ¿Que contiene? Procedo recolocar los datos de la url para que el navegador los pueda interpretar con ayuda del url encoder podemos sustituir los valores por los reales:

https://www.degraeve.com/reference/urlencoding.php


## Segunda Fase: Fuerza bruta contra el zip

Obtenemos una web de la noticia del congreso de la uad360 y un zip que contiene una imagen que solita contraseña para su extracción. Incialmente pruebo con varias uad360, teatinos, ctfuad360, 7y8dejunio sin éxito. Dado que hoy no es mi dia creativo decido crear una lista personalizada para esta prueba con cewl y crackeo la pass.

Cewl -v –depth 2 --write /usr/share/wordlists/listauam.txt https//unaaldia.hispasec.com/2019/03/una-al-dia-tendra-su-propio-congreso-de-seguridad-informatica-uad360.html

```
root@kali:~# cewl -v --depth 2 --write /usr/share/wordlists/listauam.txt https://unaaldia.hispasec.com/2019/03/una-al-dia-tendra-su-propio-congreso-de-seguridad-informatica-uad360.html
CeWL 5.4.3 (Arkanoid) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Starting at https://unaaldia.hispasec.com/2019/03/una-al-dia-tendra-su-propio-congreso-de-seguridad-informatica-uad360.html/
Visiting: https://unaaldia.hispasec.com/2019/03/una-al-dia-tendra-su-propio-congreso-de-seguridad-informatica-uad360.html referred from https://unaaldia.hispasec.com/2019/03/una-al-dia-tendra-su-propio-congreso-de-seguridad-informatica-uad360.html/, got response code 200
Attribute text found:
  Una al Día » Feed Una al Día » RSS de los comentarios Una al Día » Una Al Día tendrá su propio congreso de seguridad informática – UAD360 RSS de los comentarios RSD banner-uad360-01 banner-uad360-01 Haz clic para compartir en Twitter Haz clic para compartir en Facebook Haz clic para compartir en LinkedIn Haz clic para compartir en Reddit Haz clic para compartir en Telegram Haz clic para compartir en WhatsApp Una Al Día tendrá su propio congreso de seguridad informática &#8211; UAD360

Visiting: https://unaaldia.hispasec.com:443/ referred from https://unaaldia.hispasec.com/2019/03/una-al-dia-tendra-su-propio-congreso-de-seguridad-informatica-uad360.html, got response code 200
Attribute text found:
    Una al Día » Feed Una al Día » RSS de los comentarios RSD thunderbird e2212-exim_logo adobe-security vim goldbrute

Visiting: https://unaaldia.hispasec.com/secciones/auditoria referred from https://unaaldia.hispasec.com/2019/03/una-al-dia-tendra-su-propio-congreso-de-seguridad-informatica-uad360.html, got response code 200
Attribute text found:
Una al Día » Feed Una al Día » RSS de los comentarios Una al Día » Auditoría RSS de la categoría RSD

Visiting: https://unaaldia.hispasec.com/secciones/eventos referred from https://unaaldia.hispasec.com/2019/03/una-al-dia-tendra-su-propio-congreso-de-seguridad-informatica-uad360.html, got response code 200
Attribute text found:
Una al Día » Feed Una al Día » RSS de los comentarios Una al Día » Eventos RSS de la categoría RSD
```

Zip2john imagen.zip >hashuam.txt

```
root@kali:~/Downloads# zip2john imagen.zip > hashuam.txt
ver 2.0 efh 5455 efh 7875 imagen.zip/ctf.jpg PKZIP Encr: 2b chk, TS_chk, cmplen=58397, decmplen=58707, crc=2B267DFF
```

```
root@kali:~/Downloads# john -wordlist=/usr/share/wordlists/listauam.txt hashuam.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 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 12:07) 16.66g/s 60283p/s 60283c/s 60283C/s que..WordPressBarra
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Voilà! Pues ya la tengo, si os digo la verdad no se me hubiese ocurrido nunca jaja. Introducimos locomotora como pass y se nos abre la imagen.

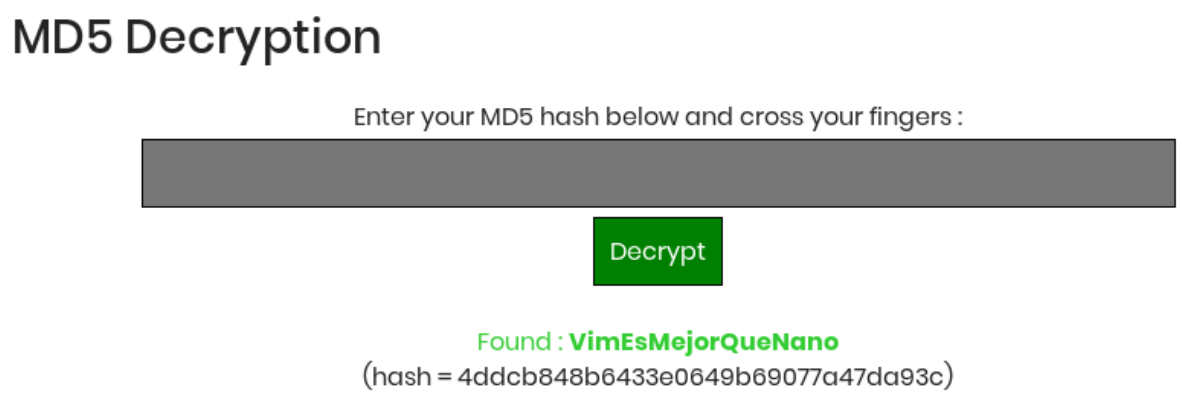
## Tercera Fase: Esteganografía

Hay varias herramientas de estego para esta prueba he utilizado un clásico. Exiftool

```
root@kali:~/Desktop# exiftool ctf.jpg
ExifTool Version Number         : 11.16
File Name                       : ctf.jpg
Directory                       : .
File Size                       : 57 kB
File Modification Date/Time     : 2019:06:14 06:01:00-07:00
File Access Date/Time           : 2019:06:16 12:15:22-07:00
File Inode Change Date/Time     : 2019:06:16 12:12:23-07:00
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
```

Pero como me gusta el nombre del artista de la foto!!

Decodeamos el md5 de la flag




Parece que nuestros admins no están deacuerdo con el resultado de los hispadebates jejeje No siempre se puede ganar, la diversidad de opiniones es enriquecedora. Si todos pensasemos igual no hubieramos tenido una semanita de debates tan divertida.

Flag: UAM{4ddcb848b6433e0649b69077a47da93c}

***Autoría: Arsenics***