Dragon Ball - Episodio 2

UAM CTF 2019-9-15

El reto

https://unaalmes.hispasec.com/challenges#EPISODIO%202

api

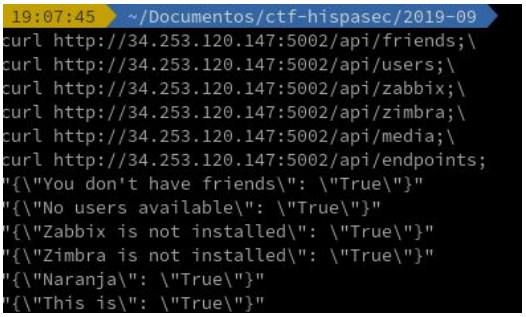
Tenemos que ver averiguar qué esconden estos servers… comenzamos con la api web:

```
curl http://34.253.120.147:5002/api/list

"[{\"http://34.253.120.147:5002/api/friends\": \"True\"},
{\"http://34.253.120.147:5002/api/users\": \"True\"},
{\"http://34.253.120.147:5002/api/zabbix\": \"True\"},
{\"http://34.253.120.147:5002/api/zimbra\": \"True\"},
{\"http://34.253.120.147:5002/api/media\": \"True\"},
{\"http://34.253.120.147:5002/api/endpoints\": \"True\"}]"
```

Este json mutante nos muestra unos cuantos endpoints

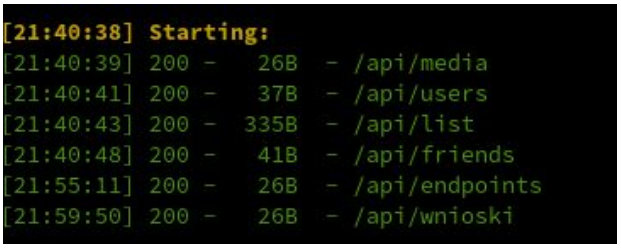
...que también nos retornan json:



Si cogemos la primera letra de cada endpoint construimos esto: **fuzzme**
Parece que quieren que hagamos fuzzing de nuevo… ¿se caerá el server esta vez?

Probando durante horas con dirsearch y algunas wordlists típicas como rockyou (demasiado bestia y la paré) y las de SecLists… encontramos algo usando raf-large-words.txt. Suponiendo que el endpoint está en /api/{LOQUESEA}:

```
python3 dirsearch.py -u http://34.253.120.147:5002/api/ -w
../Seclist/Fuzz/Web-Content/raf-large-words.txt  -e \
```



...y al ~98% encontramos eso: /api/wnioski

```
curl http://34.253.120.147:5002/api/wnioski
"{\"TrUnK5\": \"5w0RD\"}"
```

Interesante… parece que tenemos user y pass del ftp

ftp

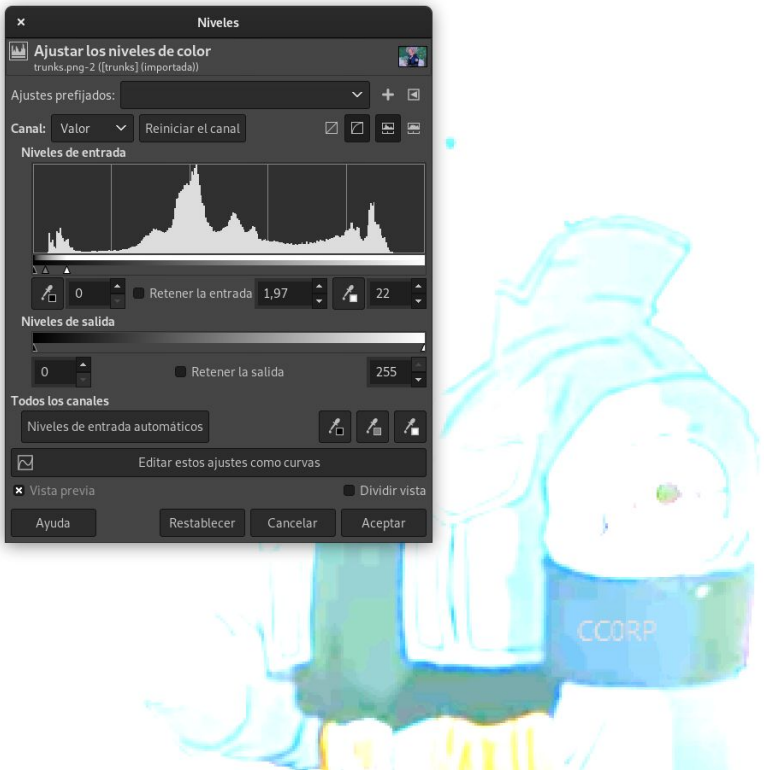
Accedemos al ftp con este usuario y password y descargamos un jpg

```
22:00:31 ~/src/other/dirsearch  master ftp 34.253.120.147
Connected to 34.253.120.147 (34.253.120.147).
220 (vsFTPd 3.0.2)
Name (34.253.120.147:j0n3): TrUnK5
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (34,253,120,147,82,108).
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp        243198 Sep 15 12:59 trunks.png
226 Directory send OK.
ftp> get trunks.png
local: trunks.png remote: trunks.png
227 Entering Passive Mode (34,253,120,147,82,116).
150 Opening BINARY mode data connection for trunks.png (243198 bytes).
226 Transfer complete.
243198 bytes received in 0,168 secs (1448,05 Kbytes/sec)
```

Stego

Es una imagen en la que aparece trunks

Jugando con gimp y los niveles encontramos CCORP claramente, aunque también se distingue a simple vista… Cualquier herramienta que nos permita modificar el brillo y contraste nos valdrá.



Metadatos

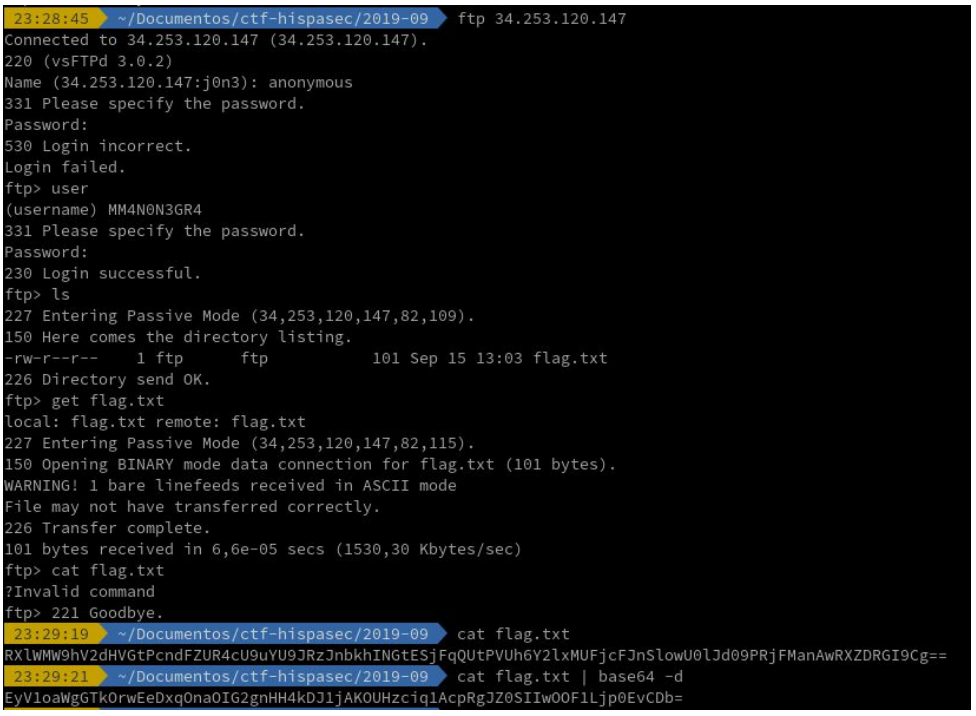
Y buscando metadatos con exiv2 veo algo interesante también:

```
22:16:05 ~/Documentos/ctf-hispasec/2019-09 exiv2 -pa trunks.png
Xmp.dc.rights                                LangAlt     1  lang="x-default" MM4N0N3GR4
```

MM4N0N3GR4

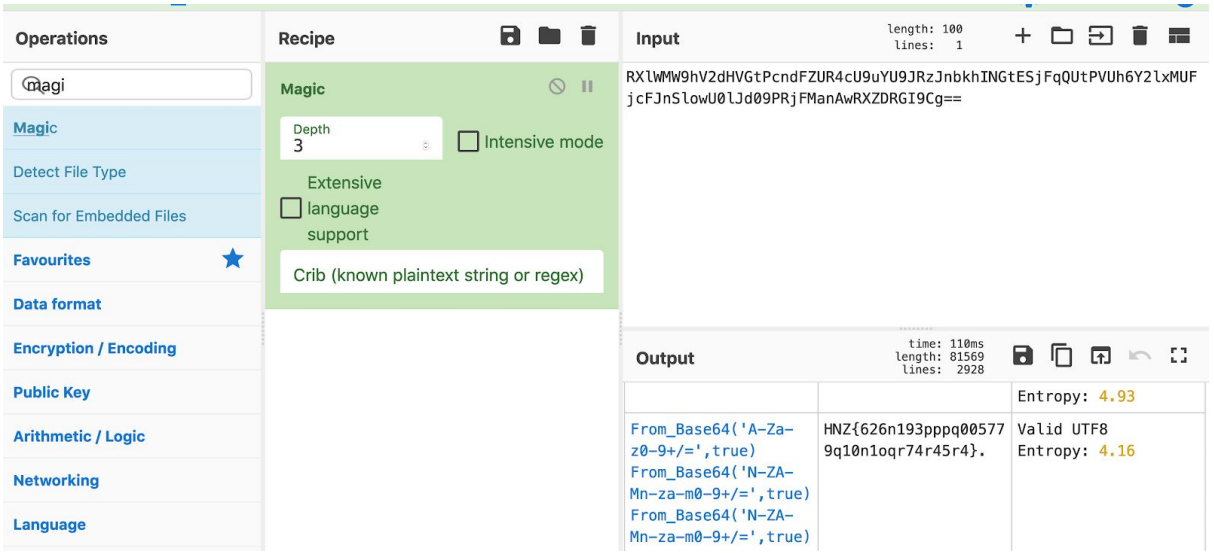
ftp otra vez

probando incontables combinaciones al final di con el user:pass MM4N0N3GR4:CC0RP



bajo el fichero y parece algo codificado en base64...

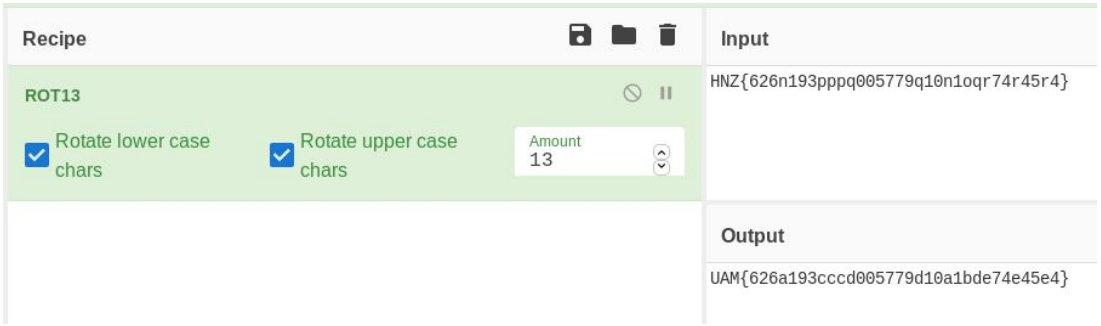
Probando combinaciones en cyberchef encuentro cosas con el maravilloso plugin magic:



HNZ{626n193pppq005779q10n1oqr74r45r4} ¡Parece que está cerca!

Flag

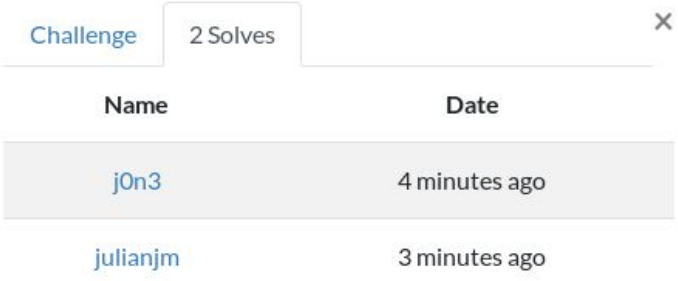
Tras probar algunas cosas, si hacemos un rot 13 a lo anterior...



UAM{626a193cccd005779d10a1bde74e45e4}

Meto la flag en la plataforma y… Gol! pero uff, julianjm ha estado a un minuto de quitarme la satisfacción de coronar xD

Conclusión



Parece que los admins no se resignan y han hecho los deberes para crear un servicio capaz de soportar nuestro fuzzing sin pestañear, ¡bravo!. El stego no ha sido muy complicado pero me ha costado un rato encontrar la combinación de user y pass para el ftp ¯_(ツ)_/¯

Cyberchef ha vuelto a ser una herramienta esencial para encontrar la flag.

Rockyou.txt es una lista enorme y no contiene lo que buscábamos, pero en las wordlists de SecList aparece en varias ocasiones, así que solo era dar con la lista adecuada y tener paciencia:

```
✘ 10:09:26 ~/src/other/SecLists  master grep -R -e "^wnioski$" .
./Passwords/openwall.net-all.txt:wnioski
./Discovery/Web-Content/raft-large-words.txt:wnioski
./Discovery/Web-Content/raft-large-words-lowercase.txt:wnioski
./Discovery/Web-Content/raft-large-directories-lowercase.txt:wnioski
./Discovery/Web-Content/raft-large-directories.txt:wnioski
./Discovery/DNS/dns-Jhaddix.txt:wnioski
./Discovery/DNS/shubs-subdomains.txt:wnioski
```

José Ángel Sánchez
@_j0n3