Write-up: HackTheBox - Stego - Beatles

Sebastián Sepúlveda @piblack
11 de mayo de 2019

Información: Categoria Stego, puntuacion 20.

Descripción: John Lennon send a secret message to Paul McCartney about the next music tour of Beatles... Could you find the message and sumbit the flag?

WRITEUP
El desafio nos entrega 2 archivos, un `.txt` y un `.zip`. El archivo de texto se ve algo así

```
root@retro:~/Descargas/beatles# cat m3ss@g#_f0r_pAuL
Url Cnhy,
Zl Sbyqre unf cnffcuenfr jvgu sbhe (4) punenpgref.
Pbhyq lbh spenpx vg sbe zr???
V fraq lbh n zrffntr sbe bhe Gbhe arkg zbagu...
Qba'g Funer vg jvgu bgure zrzoref bs bhe onaq...
–Wbua Yraaba
CF: Crnpr naq Ybir zl sevraq... Orngyrf Onaq sbe rire!
```

Código 1. Revision de mensaje

Hacemos el tipico paso para descifrar el cifrado que se ocupa. Ocupamos MTH911 para saber de que se trata.

Obtenemos que es un cifrado Patristocrat, así que nos movemos al Cipher Patristocrat para descifrarlo. Nos devuelve:

Hey Paul,
My Folder has passphrase with four (4) characters.
Could you fcrack it for me???
I send you a message for our Tour next month...
Don't Share it with other members of our band...
-John Lennon
PS: Peace and Love my friend... Beatles Band for ever!

Una gran ayuda para descifrar la clave del archivo `.zip`. Nos indican que tenemos que obtener el password utilizando fcrackzip por tanto seguimos con la operación. Nos lanzará un mensaje así:

```
fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt BAND.zip PASSWORD FOUND!!!!: pw == pass
```

Lo ocupamos para descifrar el `.zip` y obtenemos la imagen del disco `HELP!` de los Beatles:

Figura 1. Imagen obtenido después de descomprimir el zip

Luego tenemos que saber que es lo que tiene escondido esta imagen. Ocupamos Strings, Binwalk, pero no son los que nos sirven. Finalmente ocupamos `steghide extract -sf BAND.JPG`, lo que nos pide un salvaconducto, usamos THEBEATLES:

» Anotar salvoconducto:
» anot- los datos extra-dos e/"testabeatle.out".

Revisamos que tipo de archivo es:

» file testabeatle.out
» testabeatle.out: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked,
» interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=ca68ea305ff7d393662ef8ce4e5eed0b478c8b4e, not stripped

Lo analizamos con un `strings testabeatle.out` y nos un chorrón de texto donde se destaca:

```
##########Challenge################
Tell me PAul! The result of  5+5?
Ok!ok! it was easy... Tell me now... The result of: 5+5-5*(5/5)?
Last one! The result of: (2.5*16.8+1.25*10.2+40*0.65+1.5*7.5+1.25*3.2):40
Hey Paul! nice!!! this is  the message
VGhlIHRvdXIgd2FzIGNhbmNlbGVkIGZvciB0aGUgZm9sbG93aW5nIG1vbnRoLi4
ulQ0KDQpJJ2xsIGdvIG91dCBmb3IgZGlubmVyIHdpdGggbXkgZ2lybGZyaWVuZC
BuYW1lZCBZb2NvISA7KQ0KDQplVEJ7UzByUnlfTXlfRllxM25EfQ0K
WTF! You are not Paul!! SOS SOS SOS HACKER HERE!! I will call the police someone
    want to steal my data!!!
##########END OF CHALLENGE#################
```

Código 2. bash version

Decodeamos el texto en base64 The base64 strings is just the flag: `The tour was canceled for the following month...!`
`I'll go out for dinner with my girlfriend named Yoco! ;)`
`HTBS0rRy_My_FR13nD`

Flag: HTB{S0rRy_My_FR13nD}