CTF HACKON 2021
MISC - GLaDOS

https://www.hackon.es/
@HackOnURJC

ENUNCIADO

Al acabar la prueba podrás disfrutar de tarta y de nuestros psicólogos.

FLAG

HackOn{Th3_C4k3_1s_a_L1e}

SOLUCIÓN

Primero vemos el tipo de archivo al que nos enfrentamos.

```
/mnt/c/U/a/De/GlaDOS ls
Aperture_Science_Handheld_Portal_Device.rar

/mnt/c/U/a/De/GlaDOS file Aperture_Science_Handheld_Portal_Device.rar
Aperture_Science_Handheld_Portal_Device.rar: RAR archive data, v5
```

Un archivo RAR (versión 5). Intentamos descomprimirlo.

```
/mnt/c/U/a/De/GlaDOS unrar e Aperture_Science_Handheld_Portal_Device.rar

UNRAR 5.91 freeware      Copyright (c) 1993-2020 Alexander Roshal

Enter password (will not be echoed) for Aperture_Science_Handheld_Portal_Device.rar:
```

Oh vaya… tiene contraseña. No nos dan nada más, tiene pinta de fuerza bruta. Sacamos el hash a un archivo con rar2john.

```
/mnt/c/U/a/De/GlaDOS rar2john Aperture_Science_Handheld_Portal_Device.rar > glados.hash
```

```
/mnt/c/U/a/De/GlaDOS cat glados.hash                                    ✔ 11:28:43
       File: glados.hash
   1   Aperture_Science_Handheld_Portal_Device.rar:$rar5$16$47b9079c86881ce7d2a6ef057fde3ced$15$
       6c4ebdc166ccdefa718239f79a944beb$8$e990778a46f37819
```

Una vez hecho eso simplemente debemos de ejecutar john, indicándole como no, la lista más famosa, rockyou. Le especificamos el formato rar5 y el hash.

```
/mnt/c/U/a/De/GlaDOS john --wordlist /usr/share/wordlists/rockyou.txt --format=rar5 glados.hash
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (RAR5 [PBKDF2-SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
computer         (Aperture_Science_Handheld_Portal_Device.rar)
1g 0:00:00:00 DONE (2021-02-14 11:46) 3.333g/s 853.3p/s 853.3c/s 853.3C/s 123456..franklin
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Una vez hecho eso simplemente debemos de ejecutar john, indicándole como no, la lista más famosa, rockyou. Le especificamos el formato rar5 y el hash.

```
/mnt/c/U/a/De/GlaDOS john --wordlist /usr/share/wordlists/rockyou.txt --format=rar5 glados.hash
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (RAR5 [PBKDF2-SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
computer         (Aperture_Science_Handheld_Portal_Device.rar)
1g 0:00:00:00 DONE (2021-02-14 11:46) 3.333g/s 853.3p/s 853.3c/s 853.3C/s 123456..franklin
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Hecho, john –show para ver la contraseña.

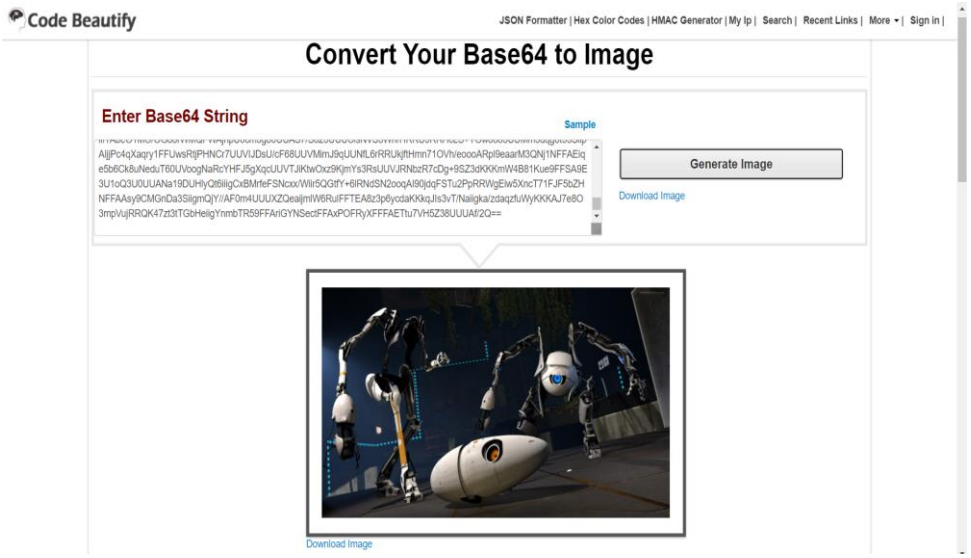
```
/mnt/c/U/a/De/GlaDOS john --show glados.hash
Aperture_Science_Handheld_Portal_Device.rar:computer

1 password hash cracked, 0 left
```

El archivo dentro del RAR es un txt. Vamos a verlo.

File: GLaDOS.txt

```
1  
   ARRHVja3kAAQAEAAAAUAAA/9sAQwACAQECAQECAgICAgICAgMFAwMDAwMGBAQDBQcGBwcHBgcHCAkLCQgICggHBwoNCgoLDAwMDAc
   JDg8NDA4LDAwM/9sAQwECAgIDAwMGAwMGDAgHCAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwM
   DAwM/8AAEQgEOAeAAwEiAAIRAQMRAf/EAB8AAAEFAQEBAQEBAAAAAAAAAAABAgMEBQYHCAkKC//EALUQAAIBAwMCBAMFBQQEAAABf
   QECAwAEEQUSITFBBhNRYQcicRQygZGhCCNCscEVUtHwJDNicoIJChYXGBkaJSYnKCkqNDU2Nzg5OkNERUZHSElKU1RVVldYWVpjZG
   VmZ2hpanN0dXZ3eHl6g4SFhoeIiYqSk5SVlpeYmZqio6Slpqeoqaqys7S1tre4ubrCw8TFxsfIycrS09TV1tfY2drh4uPk5ebn6On
   q8fLz9PX29/j5+v/EAB8BAAMBAQEBAQEBAQEAAAAAAAABAgMEBQYHCAkKC//EALURAAIBAgQEAwQHBQQEAAECdwABAgMRBAUhMQYS
   QVEHYXETIjKBCBRCkaGxwQkjM1LwFWJy0QoWJDThJfEXGBkaJicoKSo1Njc4OTpDREVGR0hJSlNUVVZXWFlaY2RlZmdoaWpzdHV2d
   3h5eoKDhIWGh4iJipKTlJWWl5iZmqKjpKWmp6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NXW19jZ2uLj5OXm5+jp6vLz9PX29/j5+v
   /aAAwDAQACEQMRAD8A/BOiiiugzCiiigAooooEFFFFNK4BketFLsNLsqkrCuGVpfm9qPm9qPm9qYg+b2o+b2o+b2o+b2oEHze1Hze
   1Hze1Hze1AB83tR83tR83tR83tQAfN7UfN7UfN7UfN7UDDYKWiigoKljf5aip0bbW9qTVwJqKRW3UtKIBT/m9qZQuf/1VQh/ze1MY
   bqN3aigkanSnU0ffp1AC/eNIPlFFKy76AHfN7UfN7U1PvU75varTuQ1Yapw1TK2ahT71TfN7VA5Enze1Ojk2tUUXan/N7VS1EjoNB
   1Y8RSHj+E/0rZrj7Vv3fHB7VqabrEq4V2yvTNcsoa6HRGRuUVWWVm2nf16Gori4kTkNkHocD8qzLL1LsNZS30m7iXPsRQL64XoUNV
   ysDVaOlX94vuvUVjtq1yvUD8qRtWmXBDL+VHKxcxs+XSbDWUNemxyqn3FPXXC3fb+FHKxmn5dHl1m/2o7fdkQ0f2lOv900cjC5pMt
   Y/iDSz/rkHI6/Sp/7Um9FpG1J5FwdvNUotMl2aMLcGFC4x81T31r5cm4dD1qGtDER/u0fN7UtJ83tTSuAnl010Zl4p6fdpcUgGR52
   4PUU75vakkG37tLnjNADMU/5valxSce1AC0ifdpfK9Go8r2oK5gpvl07y9/epo9LaRdwl4PtQBX8ul+b2qwdHk7SL+tJ/Y039+OjQ
   OVkG35fu0fN7VP/AGPJ/wA9Eo/sab+/HRoPUrsu5fl69q0dPma1xu4B4/GoI9LljlB3ocVo3FkLi1XPUDnHrXLipKyQ0mR6xfLDbk
   ttPrVLS9TE/BVVYelOuNK/dkk5C+prOtVaG6+XcQDzXLGnHlshx3sbc1x5fPr0rOb/AEqYsRgZ4NXY1+0MB/DUmpXH9lxp+6RtwwK
   mErOy3HU00GW7yQgKkmYzzg/yqzb6e+oJJJBG7mJS7KASdoxlhgYwMjP+9mqVjfLP8pTbnpSTLOswWKR0KliCHIwSMHHpkda0jHmn
   qCl0Zb+1MvyksvqKy9QhDSbxznrVqCG6jXBVG9Mn/DFOaO4kXDRpj6//AF66nHSxUtShZqYZht65FaU1w8U4ZRtPXFVVt3jnwyNjt
   3rYsdPS4t2LMisBnDYyMenPtXPs7smMW1YxNUzdN5hXB7jtU2kzqtm8bMq4HAPfHJ6VNNavMWBTK9Ac81DcaLLZsHRfMjbowqpKzH
   y9UQW9nFcMysWVTnB9/wD69Vbqz+zvgFTj0rYbQzJb+aHQDuD69x9KrR2bHP7veB0I4B/WtNJPRjcHb3kZi/3s1r2mpH7OuVbI9Kr
```

Claramente se ve que es una imagen en base 64. Vamos a cualquier página de internet que te convierta de base64 a jpeg y descargamos la imagen.



Ya tenemos nuestra imagen.

Espero que nadie haya perdido el tiempo en hacer forense a la imagen jeje. La flag está arriba a la derecha algo escondida :D