Wa0k 13/11/2022

Write-up - Make a splash !

Auteur : Wa0k CTF Flag'Malo 2022

Pour ce challenge, l'énoncé ne nous donne pas énormément d'informations.

Le fichier n'a pas d'extension, donc une première étape serait d'essayer de déterminer le type de fichier. Pour ce faire, la commande file sous Linux permet d'identifier le type d'un fichier en se basant sur l'header.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ file file
file: data
```

Le résultat retourné est data : cela signifie que le type n'a pas été identifié.

Intéressons nous alors à l'header du fichier, visible via un éditeur hexadécimal comme par exemple hexed.it.

file ×

```
00000000  00 00 00 00 00 00 00 00  00 00 68 73 71 73 55 06  ..........hsqsU.
00000010  00 00 CD DA 6A 63 00 00  02 00 4A 00 00 00 01 00  ..=┌jc....J.....
00000020  11 00 C0 00 01 00 04 00  00 00 77 12 64 32 00 00  ..└.......w.d2..
00000030  00 00 C9 52 AF 00 00 00  00 00 C1 52 AF 00 00 00  ..╔R».....┴R»...
00000040  00 00 FF FF FF FF FF FF  FF FF D2 C9 AE 00 00 00  ..          ╥╔«...
00000050  00 00 90 01 AF 00 00 00  00 00 C0 47 AF 00 00 00  ..É.».....└G»...
```

L'header d'un fichier correspond aux premiers octets de celui-ci. Ici, nous remarquons une répétition de valeur hexadécimale (00) ce qui est anormal.

Par conséquent, nous pouvons essayer de supprimer ces octets supplémentaires et tenter à nouveau d'identifier le type du fichier.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ file file
file: Squashfs filesystem, little endian, version 4.0, zlib compressed, 11489993 bytes, 1621 inodes,
 blocksize: 131072 bytes, created: Tue Nov  8 22:40:13 2022
```

Cette fois-ci, nous obtenons un type de fichier : squashfs.

Pour information : SquashFS est un système de fichiers compressé en lecture seule sous Linux.

Ainsi, nous pouvons donc essayer de décompresser le fichier avec la commande unsquashfs.

```
┌──(kali㉿kali)-[~/Desktop/system]
└─$ unsquashfs file
Parallel unsquashfs: Using 2 processors
1283 inodes (1045 blocks) to write

[=============================================================================================] 2328/2328 100%

created 997 files
created 338 directories
created 286 symlinks
created 0 devices
created 0 fifos
created 0 sockets
created 0 hardlinks
```

La décompression est un succès et nous obtenons une arborescence similaire à celle d'un système de fichier sous Linux.

```
┌──(kali㉿kali)-[~/Desktop/system]
└─$ cd squashfs-root

┌──(kali㉿kali)-[~/Desktop/system/squashfs-root]
└─$ ls
bin  dev  etc  home  init  lib  linuxrc  mnt  opt  proc  root  run  sbin  sys  tmp  usr  var
```

Un réflexe au fur et à mesure des CTFs est de chercher un fichier flag.txt dans cette arborescence. La commande ls -R | grep flag.txt serait une façon de faire.

```
┌──(kali㉿kali)-[~/Desktop/system/squashfs-root]
└─$ ls -R | grep flag
flag
./home/flag:
flag.txt
```

Nous obtenons donc le flag : FMCTF{Mak3_A_Spl@$h!!!!}.