Write-up - Un fichier enigmatique

Auteur : Wa0k CTF Flag'Malo 2022

L'énoncé évoque un certain Alan… Le challenge est situé dans la catégorie cryptographie, Alan fait référence au célèbre Alan Turing ! Cette information sera importante par la suite du challenge.

1. Déchiffrement de l'archive

Tout d'abord, essayons de déchiffrer l'archive secret.zip pour lire son contenu. Pour cela, nous pouvons utiliser l'outil JohnTheRipper sur Linux.

1.1. Calculer le hash de l'archive

Avec la commande zip2john, nous allons pouvoir récupérer le hash de l'archive .zip dans un fichier, ici hash.txt.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l
total 4
-rw-rw-rw- 1 kali kali 453 Oct 31 12:32 secret.zip

┌──(kali㉿kali)-[~/Desktop]
└─$ zip2john secret.zip > hash.txt
ver 2.0 secret.zip/settings.txt PKZIP Encr: TS_chk, cmplen=98, decmplen=173, crc=A24935C5 ts=BB4F cs=bb4f type=8
ver 2.0 secret.zip/secret.txt PKZIP Encr: TS_chk, cmplen=33, decmplen=19, crc=70C6E36D ts=7A1D cs=7a1d type=8
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
```

Le contenu du fichier "hash.txt" est le suivant :

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat hash.txt
secret.zip:$pkzip$2*1*1*0*8*24*bb4f*657ed9480f89edc16997ebb1e609706a8deb5120dab25a546e4da688164ee7e2c4184387*2*0*21*13*70c6e3
6d*9c*28*8*21*7a1d*4fc38afcc279634a38f26100c312edbe3281cbffdbbf687bff281955b3f8acf597*$/pkzip$::secret.zip:secret.txt, settin
gs.txt:secret.zip
```

1.2. Casser le chiffrement avec une attaque par dictionnaire

Pour ce faire, nous utilisons donc l'outil JohnTheRipper et la wordlist rockyou, très utilisé dans le monde des CTFs. La commande est john hash.txt –wordlist=/usr/share/wordlists/rockyou.txt et le résultat ci-dessous :

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.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
vfrvgybgtbhu     (secret.zip)
1g 0:00:00:00 DONE (2022-10-31 12:36) 2.777g/s 8066Kp/s 8066Kc/s 8066KC/s vhvhvhvh..vetnames1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

L'outil a réussi à trouver le mot de passe de l'archive : **vfrvgybgtbhu**.

2. Déarchivage et déchiffrage

Maintenant que nous avons le mot de passe, nous pouvons accéder aux fichiers de l'archive. Nous avons alors : un fichier secret.txt, et un fichier settings.txt.

Parmi ces deux fichiers, le plus intéressant est le fichier settings.txt car en analysant son contenu, celui-ci ressemble énormément à du braille…

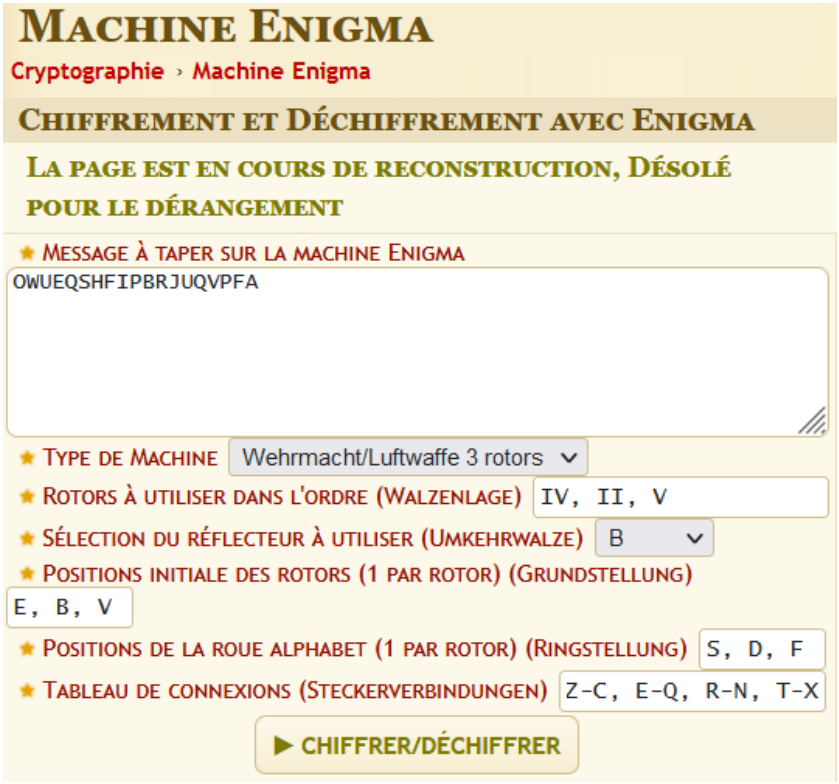
Avec dcode.fr, nous pouvons décoder le fichier pour obtenir le message :

M3
IV, II, V
B E, B, V
S, D, F
A-T, Z-C, E-Q, R-N, T-X

Bon, et si nous repensions à l'énoncé du challenge : "D'après un certain Alan…" fait référence à Alan Turing… qui est le célèbre ~~inventeur~~ mathématicien et cryptologue britannique ayant déchiffré le code Enigma.

Et si le fichier secret.txt contenait un message chiffré avec la machine Enigma, dont les paramètres de chiffrement sont ceux dans le fichier settings.txt ? Hypothèse plus que convaincante, essayons !

Avec dcode.fr (une fois de plus), nous avons un outil en ligne de déchiffrement de la machine Enigma.



Bingo, cela nous renvoie : ALANTURINGISAGENIUS.

Nous obtenons donc le flag : FMCTF{ALANTURINGISAGENIUS}.