Cryptoxore (MEDIUM)

Auteur(s) :

Hokanosekai

Catégorie :

Crypto

Description :

Lors d'un cours de réseau, vous retrouvez une capture d'écran du résultat d'une commande linux. Vous trouvez également un fichier python qui semble être un script de chiffrement.

```
hoka@hoka N/c/U/U/C/C/src (main)> python3 chall.py
bytearray(b'>ZCt\xf8j\x7f9a\xe3\xdeX`9\x06\xd8\x1d73W\xe2\xfa4Qd\x03\x9d\x
1d7\x02h\xe1\xd5')
hoka@hoka N/c/U/U/C/C/src (main)>
```

cryptoxore.py

Flag - UHOCTF{??????????????????????ng3}

Solution

On remarque que le script python utilise un chiffrement XOR, or on ne voit pas la clé utilisée.

En effet la clé est générée aléatoirement a chaque tour de boucle, et le caractère utilisé pour XOR est le n'ième caractère de la clé, avec le n'ième caractère du message.

On peut aussi remarquer que le message a encrypter doit faire 33 caractères, et que la clé générée est constituée de 3 fois 11 caractères aléatoires.

De plus, nous possédons une partie du message chiffré, et nous savons que le message original commence par UHOCTF{??????????????????????ng3}.

Si l'on compte le nombre de caractères connus, on obtient 11 caractères, ce qui correspond à la taille d'une partie de la clé.

On peut donc compléter les 11 premier caractéres du message originel en faisant un XOR entre les 4 derniers de la première partie du message originel, les 4 derniers et 4 premiers du message chiffré.

```
FLAG = bytearray(b'UHOCTF{??????????????????????ng3}')
CIPHER =
```

```
bytearray(b'>ZCt\xf8j\x7f9a\xe3\xdeX`9\x06\xd8\x1d73W\xe2\xfa4Qd\x03\x9d\x
1d7\x02h\xe1\xd5')

FLAG[7] = CIPHER[7] ^ FLAG[29] ^ CIPHER[29]
FLAG[8] = CIPHER[8] ^ FLAG[30] ^ CIPHER[30]
FLAG[9] = CIPHER[9] ^ FLAG[31] ^ CIPHER[31]
FLAG[10] = CIPHER[10] ^ FLAG[32] ^ CIPHER[32]
```

On peut ensuite réitérer le même procédé sur les 11 caractères suivants, puis enfin sur les 7 permiers de la dernière partie du message originel.

```
for i in range(11):
    FLAG[11 + i] = CIPHER[11 + i] ^ FLAG[i] ^ CIPHER[i]

for i in range(7):
    FLAG[22 + i] = CIPHER[22 + i] ^ FLAG[11 + i] ^ CIPHER[11 + i]
```

On obtient donc le message originel : `UHOCTF{Un1v3r51t13_X0R_Ch4113ng3}`

Flag `UHOCTF{Un1v3r51t13_X0R_Ch4113ng3}`