Une Histoire de Config

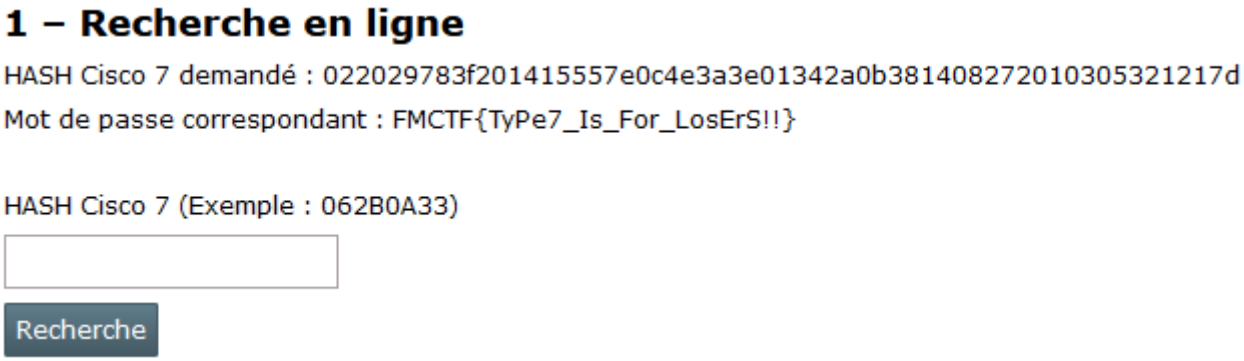
Auteur: bWlrYQ

1. Partie 1

Nous devons d'abord récupérer le mot de passe d'administration du routeur à savoir le mot de passe 'enable'. On voit ici qu'il est "chiffré" en Type 7. Fort heureusement pour nous le chiffrement de type 7 sur IOS est basé sur le chiffrement de Vigenère.

> En réalité, le chiffrement de “Type 7” est connu depuis 1995 et n’a pour d’autre but que de se protéger d’attaques contre des regards indiscrets (“eavesdropping”). L’algorithme Cisco “Type 7” est une implémentation de l’algorithme de Vigenere. (https://cisco.goffinet.org/ccna/gestion-infrastructure/chiffrement-des-mots-de-passes-locaux-cisco-ios/)

Il est donc aisément réversible, on peut utiliser un outil en ligne:



Nous avons notre premier flag !

2. Partie 2

Il faut ensuite récupérer le mot de passe de l'ancien administrateur réseau, cette fois-ci la tâche est plus ardue. Il y a cette ligne dans la configuration: `username Franck secret 5 $1$pdQG$WzDpPL3KpZb/HcC3u8z1f.`. Le prénom de l'ancien administrateur est donc `Franck`, son mot de passe est cette fois-ci chiffré en type 5 (plus connu sous le nom de md5crypt). On peut essayer de le casser à l'aide d'une liste de mot de passes telle que rockyou.

```
hashcat -m 500 -a 0 -w rockyou.txt hash.txt
[............SNIPPED.................]
$1$pdQG$WzDp...HcC3u8z1f.:Hello123
```

Le flag est donc FMCTF{Hello123}