Ciscolaire (EASY)

Auteur(s) :

Senkei

Catégorie :

Forensic

Description :

Un élève à réussit à mettre la main sur un routeur Cisco. Il a réussit à récupérer la config mais il n'arrive pas à trouver le mot de passe admin. Quelle est le mot de passe de senkei ?

cisco.conf

Flag : UHOCTF{password0123}

Solution :

Type 7 mdp non sécu

Hoka : UHOCTF_escalope
Zyksa : UHOCTF_dragodinde
??? : UHOCTF_p@ass

On voit qu'on commence avec UHOCTF_

Ducoup je créer une wordlist custom avec rockyou:

```
sed -i -e '/s/^/UHOCTF_/' rockyou
```

Et on peux bruteforce le mdp de senkei :

`john --wordlist=./uho_wl.txt ./pass.txt`

```
┌──(kali㉿kali)-[~/UHOCTF]
└─$ john  --wordlist=./uho_wl.txt ./pass.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4×3])
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
UHOCTF_naruto    (senkei)
1g 0:00:00:00 DONE (2023-06-11 05:14) 50.00g/s 12000p/s 12000c/s 12000C/s UHOCTF_123456..UHOCTF_karina
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
$1$uWu$dVdb41eRcD.np7zCwgUgU1 => UHOCTF_naruto
```

Flag : UHOCTF{UHOCTF_naruto}