**Write-Ups FCSC 2020**

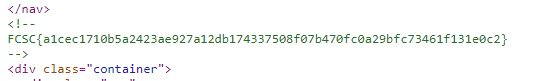
Catégorie welcome (les plus simples haha 😂😂😂😂) :

* Welcome : FCSC{Bienvenue\_et\_bonne\_chance!}
* Discord : FCSC{Flag\_de\_bienvenue\_sur\_Discord}

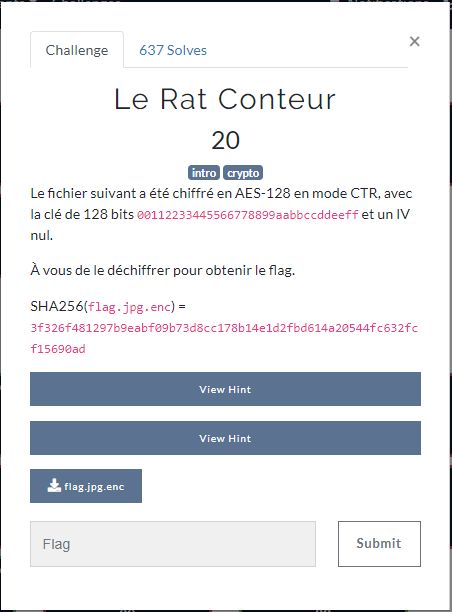
Catégorie intro :



Une fois arriver sur la page web du challenge je consulte la page puis effectue un clic droit afficher le code source de la page le flag est en commentaire dans le code source :



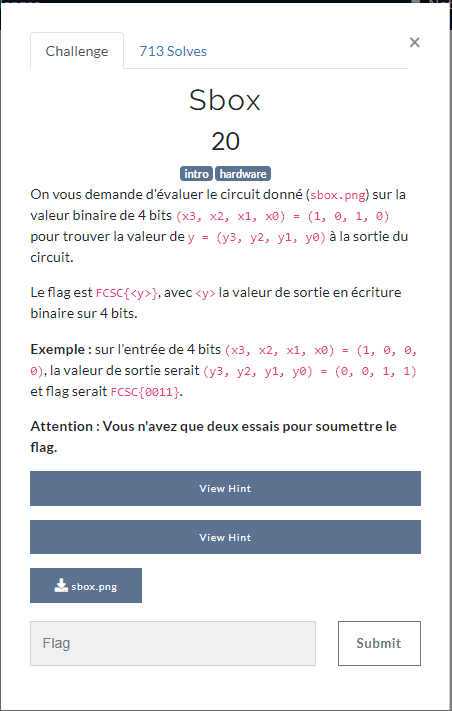
Le flag est : FCSC{a1cec1710b5a2423ae927a12db174337508f07b470fc0a29bfc73461f131e0c2}



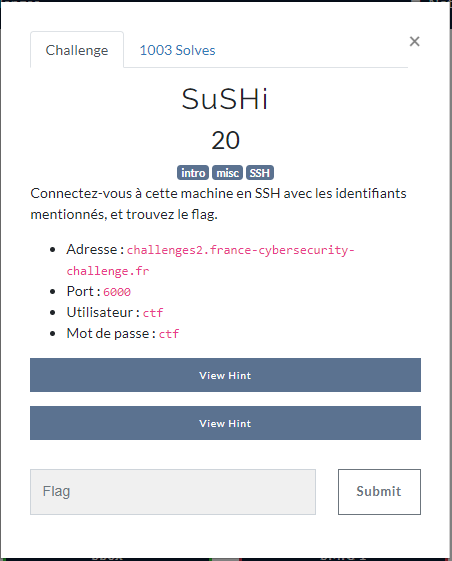
Je télécharge le fichier flag.jpg.enc consulte les Hints et fais des recherches sur openssl et sur la structure de la commande openssl enc -aes-128-ctr et réaliser la commande suivante openssl enc -aes-128-ctr -d -K 00112233445566778899aabbccddeeff -iv 00000000000000000000000000000000 -in flag.jpg.enc -out flag.jpg et j’ouvre le fichier image JPG ci-dessous contenant le flag avec notre cher et tendre Maître YODA.

Une image contenant assis, bébé, petit, tenant

Description générée automatiquement



Ayant consulter les hints et imprimer l’image j’ai pu savoir à quel type d’opérateurs logiques correspondait chaque porte et j’ai ensuite fait le calcul pour obtenir le résultat des différentes valeurs des y et trouver le flag FCSC{0101}.



L’épreuve la plus facile selon moi je me connecte sur le serveur SSH avec la commande ssh ctf@challenges2.frances-cybersecurity-challenges.fr -p 6000 tape le mot de passe ctf , réalise la commande ls -al visualise le fichier .flag puis effectue la commande cat .flag pour afficher le contenu du fichier ;

ctf@SuSHi:~$ ls -al

total 24

drwxr-xr-x 1 ctf-admin ctf 4096 Apr 25 10:39 .

drwxr-xr-x 1 ctf-admin ctf 4096 Apr 25 10:38 ..

-rw-r--r-- 1 ctf-admin ctf 220 May 15 2017 .bash\_logout

-rw-r--r-- 1 ctf-admin ctf 3526 May 15 2017 .bashrc

-r--r--r-- 1 ctf-admin ctf 71 Apr 25 10:38 .flag

-rw-r--r-- 1 ctf-admin ctf 675 May 15 2017 .profile

ctf@SuSHi:~$ cat .flag

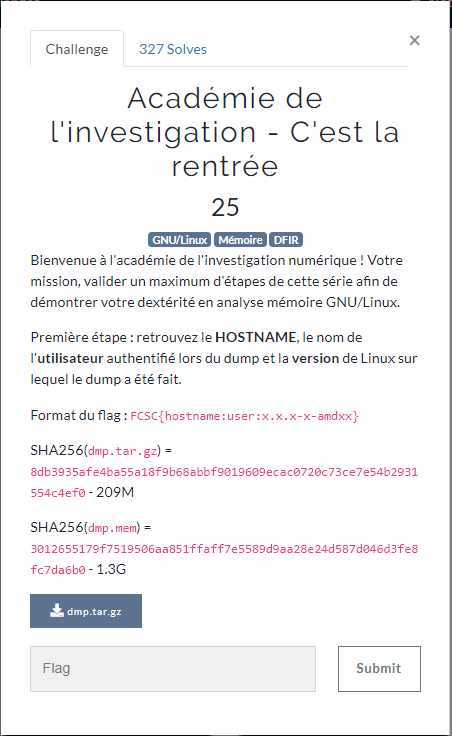
FCSC{ca10e42620c4e3be1b9d63eb31c9e8ffe60ea788d3f4a8ae4abeac3dccdf5b21}



Alors dans ce challenge il fallait analyser un fichier rapport des événements clavier (keylogger) afin de retrouver le flag j’ai la regarder la valeur KEY saisie et voir si sa valeur équivaut à 1 à l’action press et la valeur 0 l’action release afin de ne pas ressaisir 2 fois la même lettre.

Ce qui donne le flag FCSC{UNEGENTILLEINTRODUCTION}

Catégorie Forensics :



Alors ce challenge j’ai tout d’abord essayé de trouver son profile en utilisant volatility avec la commande volatility -f dmp.mem imageinfo, mais sans succès du coup j’ai utilisé la commande strings dmp.mem | more qui m’a permis de trouver de façon longue et fastidieuse le flag FCSC{eedesktop :Lesage :5.4.0-4-amd64}.



Outils utilisés : volatility

Détermination du profil du fichier mémoire : Volatility -f memory.dmp imageinfo

Résultats : Win7SP1x86

Listage fichier présent dans la MFT : Volatility -f memory.dmp --profile=Win7SP1x86 mftparser

Visualisation de deux fichiers intéressants : key.txt et flag.txt.enc

Récupération adresse physique des fichiers:

* Key.txt = volatility -f memory.dmp --profile=Win7SP1x86 filescan | grep key.txt
* Flag.txt.enc = volatility -f memory.dmp --profile=Win7SP1x86 filescan | grep flag.txt.enc

Extraction des fichiers avec le plugin Dumpfiles de volatility:

* volatility -f memory.dmp --profile=Win7SP1x86 dumpfiles -Q 0x000000003e6fa100 -D dumpfiles/ -u -n -S summary.txt
* volatility -f memory.dmp --profile=Win7SP1x86 dumpfiles -Q 0x000000003ed139f0 -D extract\_files/ -u -n -S summary.txt

Je n’ai mal malheureusement pas réussi à déchiffrer le fichier flag.txt.enc mais grâce à ce CTF j’ai pu voir mes évolutions et ce dont je dois encore travailler afin de pouvoir m’améliorer afin de me préparer pour ma future formation d’Expert en Sécurité Digitale afin de pouvoir exercer cette passion comme Métier. Ayant atteint l’âge limite l’année prochaine j’y participerais encore afin de voir mon évolution.

Je tiens à vous remercier pour ce challenge qui permet d’éprouver mes connaissances et qui me pousse à aller chercher plus loin.

Merci d’avoir lu mon Write-Up.

Je vous demander au passage quels sont les ouvrages et site web que vous me conseillez afin d’apprendre d’avantage sur la Sécurité Informatique, sur le Forensic etc. hors Udemy et OpenClassrooms et root-me vous remerciant d’avance de pouvoir m’aider à ce niveau.

sKillseries.