Document Astuce CTF Moyen

Etape 1

- Indice 1 : Quel est le nom du service et de la commande qui permet de voir les ports ouverts sur une machine distance ?

Solution :

```
nmap -sV -sC IP_distante
```

- Indice 2 : Quels services semblent être attaquables ?

Solution : Deux services sont présent ssh et mysql

Etape 2

- Indice 1 : Un des deux services ne semblent pas être bruteforcable, l'un d'entre eux vous bloque lequel faudrait t'il attaquer selon vous ?

Solution : Il faut attaquer le service ssh

- Indice deux : Pour faire un bruteforce il existe un outils, le nom de cet outils est celui d'une créature mythologique grecque , quel est son nom ?

Solution : Il faut utiliser hydra avec des listes de nom et d'utilisateurs .

Etape 3

- Indice 1 : Une fois sur le home de l'utilisateur une image est présente cela est étrange, quelle est la manière la plus classique de caché des informations dans une image ?

Solution : C'est d'encoder l'information sur les LSB de l'image il faut décoder cela

- Indice 2 :

Etape 4

- Indice 1 : Vous avez désormais récupéré une string de 20 caractère alphanumérique. Quelle méthode de hashage très connue donne ce genre de string

Solution : Le hashage est en SHA-1

- Indice 2 : A quoi pourrait service ce hashage, quel service à été non exploité ?

Solution : Utiliser les rainbown table pour trouver un mot de passe pour utiliser le service mysql

Etape 5

- Indice 1 : Que faire en premier lorsque l'on se connecte en remote mysql ?

Solution : Regarder les databases présente et les tables via une requête mysql

- Indice 2 : Vous avez vu que dans votre terminale une commande s'exécutait chaque minute, quel service linux permet d'automatiser des tache de telle manière ?

Solution : Cron est un service linux d'automatisation des taches, visiblement ici cron exécute automatiquement des script présent dans un dossier

- Indice 3 : Comment faire depuis mysql pour écrire un script dans le dossier que cron Exécute ?

Solution : Il y a une database de script, il faut faire une requête sur le bon script avec en sortie INTO OUTFILE dans le dossier afin que cron l'exécute automatiquement

Etape 6

- Indice 1 : Vous avez récupréer un mot de passe que serait-il judicieu de faire avec la connection ssh ?

Solution : tester ce mot de passe avec plusieurs utilisateur comme root/superuser/admin etc ... afin de voir si cela correspond !