

NON-PRÉSENTÉ_CTF_SecretStory-Alex

Description du challenge : On vous a donné accès à un serveur Linux. Quelque part sur le serveur, un flag est caché dans un fichier `dot`. Utilisez vos compétences forensic pour localiser et récupérer le flag. Rappelez-vous, dans les systèmes Unix, les fichiers qui commencent par un point (.) sont des fichiers cachés.

La complexité à mettre en place ce challenge a fait qu'il n'a pas été retenu.

Configuration du défi : [à retravailler.]

Solution :

Étape 1 : Connection au serveur via SSH

Étape 2 : Utilisez la fonction `find_hidden_file` du script Python pour rechercher des fichiers cachés. Cette fonction parcourt le système de fichiers de manière récursive et imprime les chemins de tous les fichiers qui commencent par un point (.).

Brouillon du script :

```
import os

def find_hidden_file(path):
    for root, dirs, files in os.walk(path):
        for file in files:
            if file.startswith("."):
                print(os.path.join(root, file))

find_hidden_file("/home") # Commencez à rechercher à partir du
répertoire /home
```

Étape 3 : Vérifiez le contenu de chaque fichier caché trouvé. Le flag est stocké dans l'un de ces fichiers.

Flag : [NHM2I{SecretStory}]

Conclusion : Ce challenge teste la capacité du joueur à effectuer une analyse forensic de base sur un OS Linux. En comprenant comment fonctionnent les fichiers cachés dans les systèmes de type Unix et comment les localiser, les joueurs peuvent ensuite récupérer le flag.