NON-PRÉSENTÉ_CTF Hamzat's Hidden Malware-Alex

Conception de l'épreuve de Capture The Flag (CTF) - Hamzat's Hidden Malware

Introduction

Un fichier Python est fourni qui semble exécuter une fonction mystérieuse codée en C et rendue exécutable en Python à l'aide de la bibliothèque `ctypes`. Votre mission, si vous l'acceptez, est de faire du reverse engineering sur ce code pour découvrir ce qu'il fait et trouver le flag

La complexité à finir ce challenge a fait qu'il n'a pas été retenu.

Titre du challenge : [Hamzat's Hidden Malware]

Instructions de configuration : Le joueur récupère un fichier Python via la plateforme CTFd qui contient le code fourni. Le code C est un shellcode qui exécute une commande Unix cachée pour afficher le flag.

Solution :

1. Étape 1 : Identifier le shellcode

Le joueur doit d'abord identifier que le code dans la variable `code` est un shellcode, c'est-à-dire une séquence d'instructions de langage machine qui sont utilisées comme charge utile dans une exploitation de logiciel.

2. Étape 2 : Décoder le shellcode

Ensuite, le joueur doit utiliser un outil de désassemblage pour transformer le shellcode en langage d'assemblage lisible. Cela révélera que le shellcode exécute une commande Unix.

3. Étape 3 : Identifier la commande Unix

En examinant le code d'assemblage, le joueur devrait être capable d'identifier la commande Unix exécutée par le shellcode. Dans ce cas, la commande pourrait être quelque chose comme `echo 'Flag : [NHM2I{H4MZ4T}]'`.

4. Étape 4 : Exécuter la commande

Enfin, le joueur peut exécuter la commande Unix dans un terminal pour afficher le flag.

Flag : [NHM2I{H4MZ4T}]

Conclusion : [Ce défi est conçu pour introduire les joueurs aux concepts de base du reverse engineering et du shellcode. En désassemblant le shellcode et en déterminant la commande Unix qu'il exécute, les joueurs peuvent découvrir le flag caché.]