NON-PRÉSENTÉ_CTF _DockerDiver- Alex

Conception de l'épreuve de Capture The Flag (CTF) - DockerDiver

Introduction

"Docker Diver" est épreuve de CTF qui implique l'exploitation d'un conteneur Docker en cours d'exécution pour attaquer via une commande malveillante. L'objectif est de tester les attaquants sur un environnement Docker. Ce document explique la conception du challenge et sa solution.

La mise en place Docker, ainsi que l'apprentissage de l'environnement a fait que ce challenge n'a pas été retenu.

Description du Défi

Le défi invite les joueurs à se connecter à un client Docker, via CTFd, puis d'attaquer le docker. Le nom du conteneur est donné et le flag se trouve dans un document `flag.txt`.

Déroulement du Défi

Étape 1

La première étape consiste à se connecter au client Docker en utilisant la bibliothèque Docker pour Python. Ceci peut être réalisé avec le code suivant :

```
import docker

# Connexion au client Docker
client = docker.from_env()
```

Étape 2

Ensuite, le participant doit obtenir une référence au conteneur en cours d'exécution :

```
# Obtention du conteneur en cours d'exécution

```

Étape 3

Enfin l'attaquant exécute une commande malveillante sur le conteneur :

```
# Envoi de la commande malveillante pour exécuter du code arbitraire
```

Cette commande vise, *in fine*, à lire le contenu du fichier flag.txt situé dans le répertoire racine du conteneur.

Étape 4

Enfin, le participant doit afficher la sortie de la commande pour obtenir le flag :

```
# Affichage de la réponse
print("...")
```

Flag

Le flag est [NHM2I{marin-d-eau-douce}].

Conclusion

"Docker Diver" est un défi qui teste les compétences de l'utilisateur en matière d'exploitation de conteneurs Docker. Il nécessite une compréhension du fonctionnement de Docker à travers des scripts Python.