Créer un Challenge Pwn avec Docker

Ce guide explique comment créer un challenge de type 'pwn' pour un CTF en utilisant un programme vulnérable et en isolant l'environnement avec Docker.

1. Préparer l'environnement

1. Assurez-vous que votre serveur Ubuntu est à jour et installez les outils nécessaires :

sudo apt update && sudo apt install gcc gdb libc-dev docker.io socat

2. Configurez Docker pour permettre l'isolation des services liés au challenge.

2. Écrire le programme vulnérable

Créez un programme C vulnérable, par exemple un débordement de tampon :

```
#include <stdio.h>
#include <string.h>

void vuln() {
   char buffer[64];
   printf("Enter your input: ");
   gets(buffer); // Vulnérabilité : fonction non sécurisée
   printf("You entered: %s\n", buffer);
}

int main() {
   printf("Welcome to the pwn challenge!\n");
   vuln();
   return 0;
}
```

Compilez le programme avec les protections minimales :

gcc -m32 -fno-stack-protector -z execstack -o vuln vuln.c

3. Créer un environnement Docker

1. Créez un fichier Dockerfile pour isoler le challenge :

```
FROM ubuntu:20.04

RUN apt update && apt install -y socat
```

```
WORKDIR /challenge

COPY vuln /challenge/vuln

RUN chmod 750 /challenge/vuln

CMD socat TCP-LISTEN:1337,reuseaddr,fork EXEC:/challenge/vuln
```

2. Construisez l'image Docker :

```
docker build -t pwn_challenge .
```

3. Lancez un conteneur basé sur l'image :

```
docker run -d -p 1337:1337 pwn_challenge
```

4. Tester et sécuriser

1. Testez le challenge en vous connectant au port 1337 :

```
nc <ip_du_serveur> 1337
```

2. Fournissez les fichiers nécessaires (binaire, libc, etc.) aux participants.

3. Ajoutez des règles pare-feu pour sécuriser le serveur.

5. Description du challenge

Dans votre plateforme CTF, ajoutez une description du challenge. Par exemple :

Nom : Stack Overflow 101
Description : Un petit programme vous attend... Saurez-vous en prendre le contrôle ?
Port : 1337