# Créer un Challenge Pwn avec et sans Docker

Ce guide explique comment créer un challenge de type 'pwn' pour un CTF en utilisant un programme vulnérable, en exposant le service avec xinetd ou yinetd, et en l'isolant 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 xinetd socat docker.io

## 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. Configurer le service avec xinetd

1. Créez un fichier de service pour xinetd dans /etc/xinetd.d/ :

sudo nano /etc/xinetd.d/pwn_challenge

2. Ajoutez la configuration suivante dans le fichier :

```
service pwn_challenge
{
   port = 1337
```

```
    socket_type = stream
    protocol = tcp
    wait = no
    user = root
    server = /path/to/your/vuln
    log_on_failure += USERID
}
```

3. Redémarrez le service xinetd pour appliquer la configuration :

```
sudo systemctl restart xinetd
```

## 4. Configurer le service avec Docker

1. Créez un Dockerfile pour isoler le challenge dans un conteneur :

```
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
```

## 5. Tester le challenge

Testez le challenge en vous connectant au port 1337 via nc :

```
nc <ip_du_serveur> 1337
```

## 6. Sécuriser le challenge

Assurez-vous que le challenge est sécurisé en suivant ces étapes :

1. Limitez l'accès au service en configurant un pare-feu avec `iptables` ou `ufw`.

2. Utilisez un conteneur Docker ou une VM pour isoler le challenge.

3. N'exécutez pas le programme vulnérable avec des privilèges élevés (éviter `root`).

## 7. Description du challenge

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

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