Welcome to PWN !

CTFd	☑
Created	@June 14, 2021 2:28 PM
Done	☑
Hint	
author	 baby blue
field	Pwn Welcome
placement	placed
progress	Completed
value(50-200)	100
writeup	☑

概要

ncコマンドで問題サーバーへ接続するとフラグが帰ってくる

ソースコードと実行ファイルも共有しておく（ソース内でflag.txtを読み込むコードが書かれるため、フラグ自体は提供されない）

問題サーバーに関しては、xinetdを使う予定、

https://moraprogramming.hateblo.jp/entry/2020/12/21/232357

問題文

PWNへようこそ！

このジャンルでは、実行ファイルを解析して脆弱性を見つけ出し、その脆弱性を使って実際に攻撃を行うよ！

このジャンルを学ぶことで、自分が書いているプログラムでどのへんが脆弱性になりやすいかが分かるのでセキュアコーディングの癖がついたり、他人のコードの脆弱性な部分を発見できるようになり、オープンソースソフトウェア（OSS）の脆弱性を見つけたりすることができるよ！

興味がある方はぜひこのジャンルを極めていこう！

PWNの導入は、実行ファイルを実行し動作を確認してから、ソースコードを読んでバグを見つけるんだ。

その後は、見つけたバグを使って手元の環境で攻撃を再現できたら、実際に問題サーバーへ攻撃を行ってみよう！

問題サーバーへのアクセス方法:
以下のコマンドをshellに入力してください
`nc xxx.xxx.xxx.xxx 60000`

サーバー構築用

ポート番号は適当に60000使ってます

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/381e44fc-229d-48c0-9ecc-25a7b5df074a/Welcome_to_pwn.zip

問題ファイル

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/cfd64b29-61fa-4552-80ae-d9790d35e784/welcome_pwn.bin

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/485b862f-e58d-4e03-80ab-ba7e3df440a5/welcome_pwn.c

Flag

`htp-ctf{Kitty_on_your_lap}`

解法ざっくり

詳細はWriteUpで