Writeup: Welcome to REV !

HACK THE PODS CTF 第2回
作問者 : 嶋田壮志

1. 説明文

Reversingへようこそ！

このジャンルでは、実行形式のファイルを解析してパスワードやプロダクトコードを推定したりするよ！

このジャンルを学ぶことで、アセンブリ言語を読めるようになったり、実行ファイルの形式に詳しくなったりして、最終的にはゲームの解析や仕様書が公開されていないソフトの改造、マルウェアの解析なんかもできたりするよ！

興味がある方はぜひこのジャンルを極めていこう！

Reversingの基本は、とにかく実行すること！

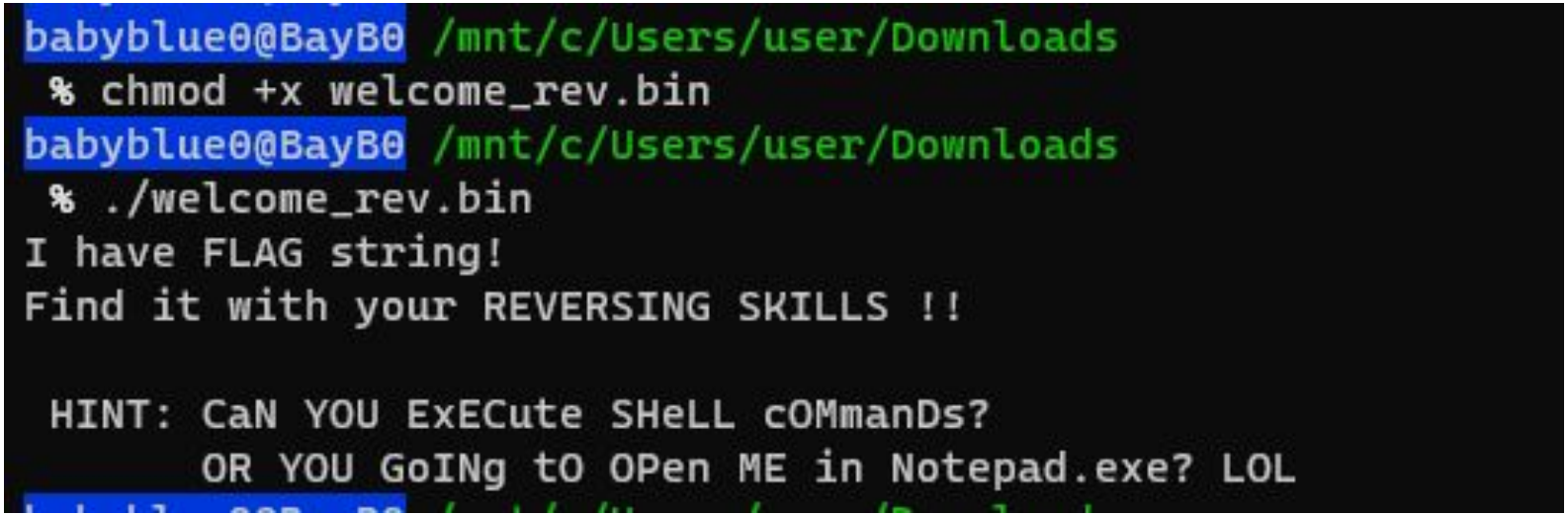
どのような出力がされるか、まずは見てみよう！

2. 共有されるファイル

- welcome_rev.bin
  - 問題のメインファイル

3. Wireup

説明文にもある通り、まずは実行してみましょう。



3. Wireup

実行ファイル自身にFLAG文字列を持っているのがわかったので、
「strings」コマンドで全文字列を出力してみる

```
babyblue0@BayB0 /mnt/c/Users/user/Downloads
 % strings ./welcome_rev.bin
/lib64/ld-linux-x86-64.so.2
libc.so.6
puts
__cxa_finalize
__libc_start_main
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[]A\A]A^A_

*=*=*=*= WATCH THIS! =*=*=*=*=
htp-ctf{W3Lc0m3_70_Und3r6R0uNd}
~*~*~*~*~*~*~*~*~*~*~*~*~*~*~*~

I have FLAG string!
Find it with your REVERSING SKILLS !!
 HINT: CaN YOU ExECute SHeLL cOMmanDs?
       OR YOU GoINg tO OPen ME in Notepad.exe? LOL
:*3$"
```

3. Wireup

親切にフラグ文字列が浮き出てますね

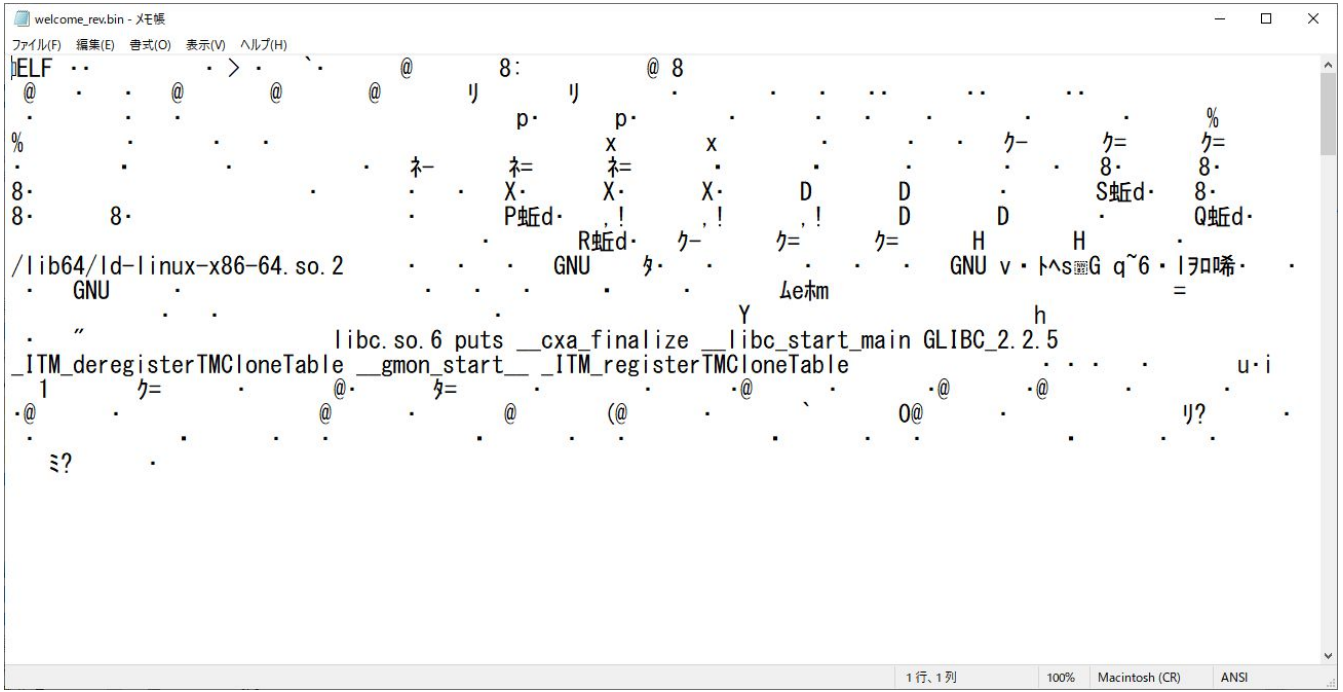
flag: **htp-ctf{W3Lc0m3_70_Und3r6R0uNd}**

ちなみに、、、

フラグの内容は、Leet文字で書かれています。（ギャル文字と似たようなもの）
内容は、「Welcome_to_Underground」です。REV沼へようこそ！

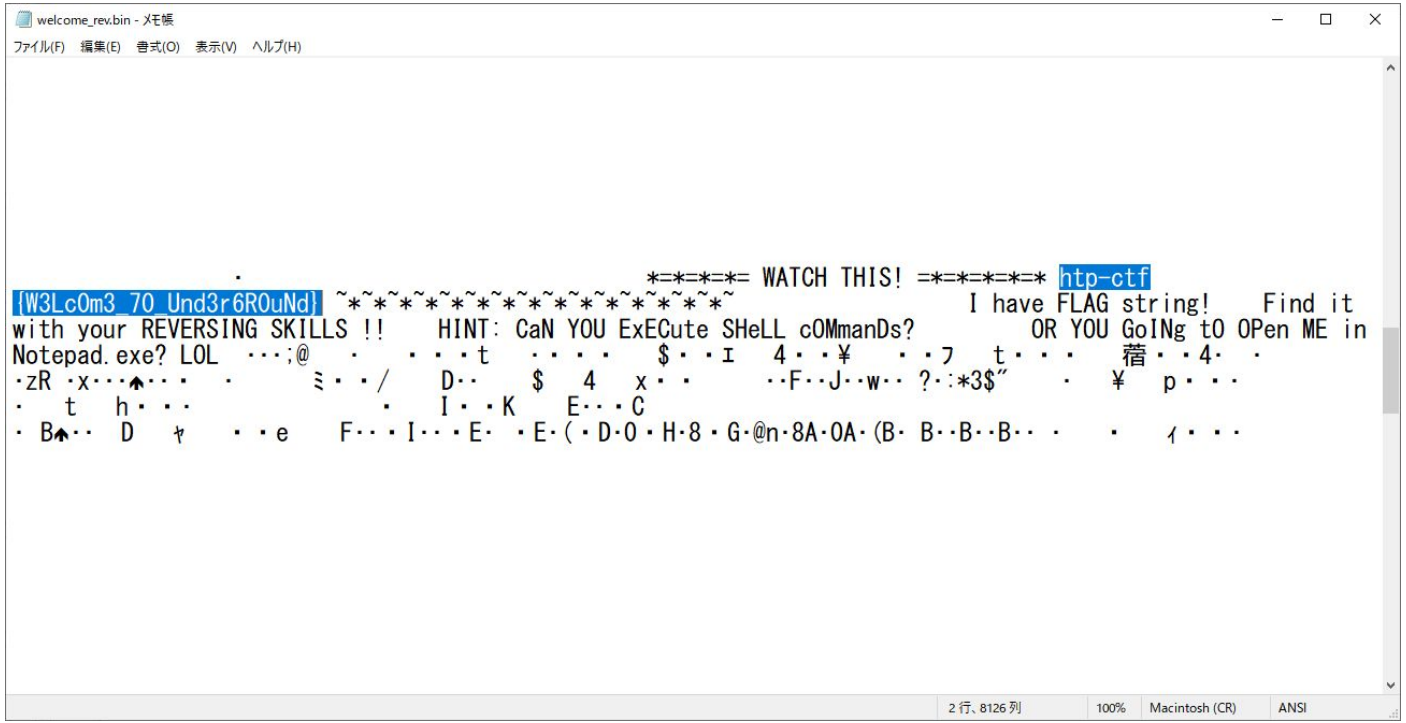
4. おまけ

Hintの最終行にあるように、notepad.exeで確認してみると、、、



4. おまけ

スクロールしてくと、、、



5. ちょっとした疑問

私自身英語が苦手なんですが、
実行したときに表示されるこの文、
「YOU GoINg tO OPen ME in Notepad.exe? LOL」

この場合、「going to」なのか、「will」なのか、「planning to」なのか、
どれなんでしょう？

その場の思いつきって感じで、私は「will」だと思ったんですが、
google翻訳だと「going to」を使ってたのでこの問題ではその表現を使いました