

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。

```
babyblue0@BayB0 /mnt/c/Users/user/Downloads
% chmod +x welcome_rev.bin
babyblue0@BayB0 /mnt/c/Users/user/Downloads
% ./welcome_rev.bin
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. 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

[illegible]

3. Wireup

親切にフラグ文字列が浮き出てますね

flag: **http-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、、、

welcome_rev.bin - メモ帳

ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)

```
ELF .. > . @ 8: @ 8  
@ . @ @ @ リ リ . . . .  
%  
. . . . p· p· . . . . %  
x x . . . . k= k=  
. . . . X· X· X· D D S蚯d· 8·  
8· 8· . . . . P蚯d· R蚯d· クー ク= ク= H H Q蚯d·  
/lib64/ld-linux-x86-64.so.2 GNU タ· 木和 GNU v · トゝs G q~6 · 口唏·  
GNU . . . . Y h  
" libc.so.6 puts __cxa_finalize __libc_start_main GLIBC_2.2.5  
_ITM_deregisterTMCloneTable __gmon_start__ _ITM_registerTMCloneTable u·i  
1 ク= @. ぢ= @. @. @. @. O@ . @ . ?  
ミ? . . . . . . . . . .
```

1行、1列 100% Macintosh (CR) ANSI

4. おまけ

スクロールしてくと、、、

```
welcome_rev.bin - メモ帳
```

ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)

.
***== WATCH THIS! ==** http-ctf
[W3Lc0m3_70_Und3r6R0uNd] ~~~~~
with your REVERSING SKILLS !! HINT: CaN YOU ExECute SHeLL cOMmanDs? I have FLAG string! Find it
Notepad.exe? LOL ...;@ . . . t . . . \$. . I 4 . . ¥ . . フ t . . . 落 . . 4 . .
.zR .x...▲... ミ . / D.. \$ 4 xF..J..w.. ?.:*3\$” . ¥ p . .
. t h . . . I . K E . C
. B▲.. D ヤ . e F...I...E·E·(・D・O・H・8・G・@n・8A・OA・(B・B・・B・・B・・・ i . .

2行、8126列 | 100% Macintosh (CR) ANSI

5. ちょっとした疑問

私自身英語が苦手なのですが、
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、
どれなのでしょう？

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