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

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

前言

非常简单的获取shell

1.checksec走一下

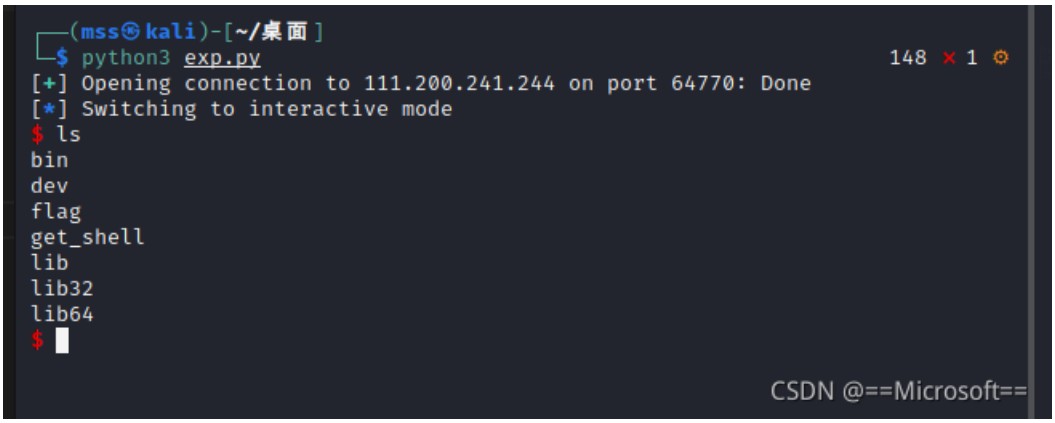
2.IDA看一眼

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

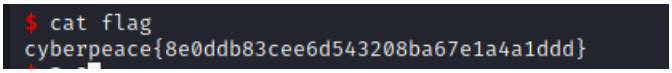
确实只要运行就能获取flag

3.直接连接服务器

```
nc 111.200.241.244 54762
```



直接cat flag




```
cyberpeace{8e0ddb83cee6d543208ba67e1a4a1ddd}
```

题目下载地址

点击下载