**leak**

Account : stanleymusic

Writeup:

Step 1:

Get Secret

Use brute force to get the secret, since buf size is 8 byte and read() with 0x10 bytes we can overflow it

Step 2:

Get Canary and Stack

Use Grill and overflow the Buf to print Canary and old rbp.

We need to overflow 0x208 Bytes.

Since the first byte of Canary in little endian is \x00 we need to send one more “B” to overflow it.

The last two bytes of old rbp in little endian are \x00.

After getting canary and old rbp, need to overflow it again and change the first byte of canary back to \x00. Otherwise the program will crashed.

The Stack value is &s2 by looking at IDA pro, Thus we need to minus old rbp by 0x70.

Step 3:

Get ListMessage address

We can get return address by minus old rbp by 0x20 and add 0x08.(By using gdb)

Then send ‘C’\*0x20 + return\_address + ‘B’\*0x20 + ‘\x00’ in Grill to overflow ListMessage[1].

After sending the upper payload, use ShowMessage again to get the address of return address and we can use gdb to get the ListMessage address. Since the difference between them are fixed. We can get the ListMessage address by adding 0x2447 to address of return address.

Step 4:

Get system address

It’s similar to step 3.

The difference is that this time we don’t send return address we send address of GOT\_system, then the return value will be address of system.

To get address of GOT\_system, we minus ListMessage address by 0x88(According to the ppt from TA)

Step 5:

Send All the answers we get and get flag

