pwn进阶

一.堆基本的思路

1. 了解如何将以释放堆块的fd 指向libc
2. 了解如何修改stdout
3. 了解如何伪造vtable

一般目前常见的做题方式都是，伪造fastbin 或者tcache 的 fd,使之指向stdout 结构体，修改stdout 结构体的writebase 和flag ， 泄漏libc,之后再去修改mallochook 或者 freehook

二.堆常用技巧

1. 将bss 和 tcache 结合

   题目特征，没有任何输出函数，libc 为2.27及以上版本，没有开pie或者可以泄漏程序的地址： 利用方式，free tcache，修改tcache 的fd 使之指向 bss 上的stdout 指针，之后连续malloc ，取出stdout 结构体，修改 flag 和 writebase 的低字节，泄漏libc 最后修改free_hook

2. 爆破二分之一字节

   题目特征：没有任何输出函数，libc 为2.23 或2.27,开了pie，存在悬挂指针或者可以off by null ，总之可以UAF 利用方式：利用unsorteb bin 切割，在某一个已经free 的 fastbin 的 fd 伪造出指向unsortedbin 的指针，因为unsortedbin 和 stdout 结构体的地址很近，所以只有后面2个字节不同，故只需要爆破16分之一的概率（stdout 前面有一个0x40合法块），之后修改stdout，泄漏Libc 最后修改malloc*hook 或者 free*hook

3. house of orange

三.栈高级技巧

1. ret to dlresolve

   常用于程序没有输出，或者程序的libc版本未知

2. 伪造link map

   也是ret to dlresolve 的一种，用于64位程序，因为64位的程序在进行ret to dlresolve 时，需要将link*map+0x1c8处修改为0，如果没有办法泄漏link*map 则无法使用。通过伪造linkmap，依旧可以实现调用任意函数的效果

3. 侧信道

常见于程序没有任何输出，而且关闭文件描述符1，此时可以利用侧信道的方式，将flag 文件读出