《Strawberry》解题思路		
类型		PWN
实验名称		Strawberry
实验目的与要求		1） scanf 触发 malloc_conlidate 2） 利用 malloc_conlidate 巧妙 unlink 3） _fileno 的相关知识
实验环境	实验靶机	1）操作系统：ubuntu16.04
	访问要求	netcat 访问
	实验环境	客户端 pc
	测试工具	1 python 脚本 2 ida

		3.gdb
预备知识		1) 堆的基础 2) Scanf 触发 malloc_consolidate 3) Unlink 4) _fileno 相关知识
实验步骤		具体细节请参考Strawberry.md 文件 1.程序中一共存在着两个漏洞，一个是 off by null,但是我们申请的 size 最大只能申请 0x58，如果直接进行 off by null 会将下一堆块的 size 域踩掉，程序会直接 crash,而且不放进 unsorted bin 的话，我们也无法泄露地址，那么如何将 chunk 放入 unsorted bin 呢？我们知道当 topchunk 不够时，或者申请了一个 large bin，也就是 size 大于 0x400 的 chunk 就能触发 mallocconsolidate，使得 fastbin 合并，并且放入 unsorted bin 中，这里用到了 scanf 的一个缓冲机制，当 scanf 的缓冲区不够用时，就会 malloc 一块更大的chunk 来充当新的缓冲区，然后使用完之后在free 掉，当我们的输入大于 0x400的内容时，便会申请一块大于 0x400 的 chunk 来当缓冲区，正是这个申请可以触发 malloc_consolidate 1. 程序中还存在着一个漏洞点就是往任意地址写数据，那我们该往哪里写呢？我们注意到程序的开头

	打开了 flag 文件，并且将文件描述符改为 666，因此我们可以劫持 stdin 中的_fileno 为666 这样在后面使用 scanf 时就可以读取 flag 文件的内容并在后面输出 3. 综上我们可以先使用unlink 来造成chunk overlapping,然后劫持malloc_hook 为666 满足backdoor 的使用条件，然后向 stdin 的_fileno 写666，最后输出 flag
原理知识	Scanf 可以触发 malloc_consolidate,利用 malloc_consolidate 巧妙 unlink,_fileno 的相关知识
防护方法	要小心 0 字节溢出
分析与思考	Scanf 可以触发 malloc_conlidate 可以很轻易的创建一个 unsortedbin，当_fileno 为文件描述符时可以读取相应文件的内容