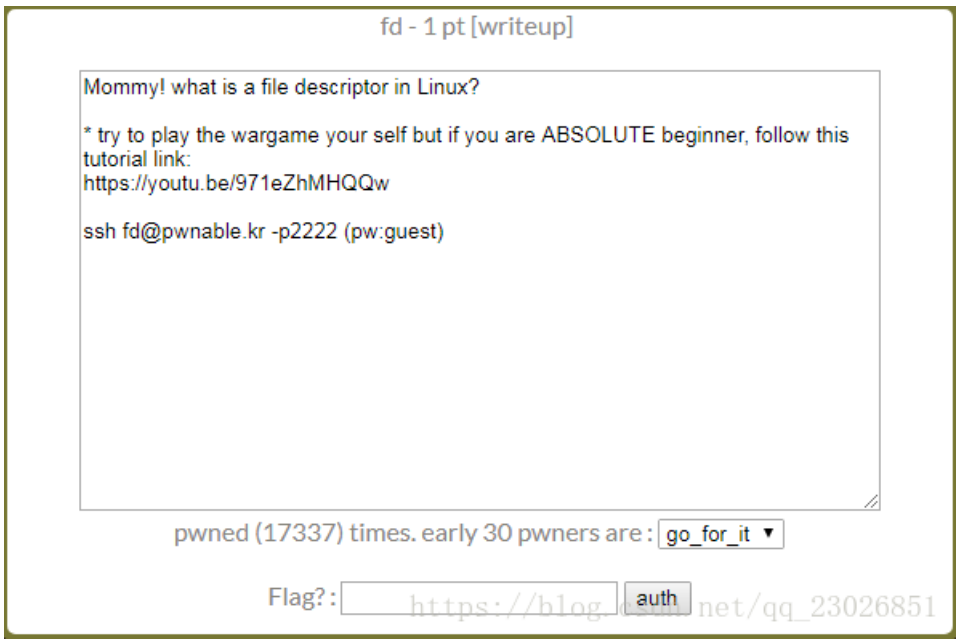
[WriteUp] pwnable.kr -- [fd]

原创

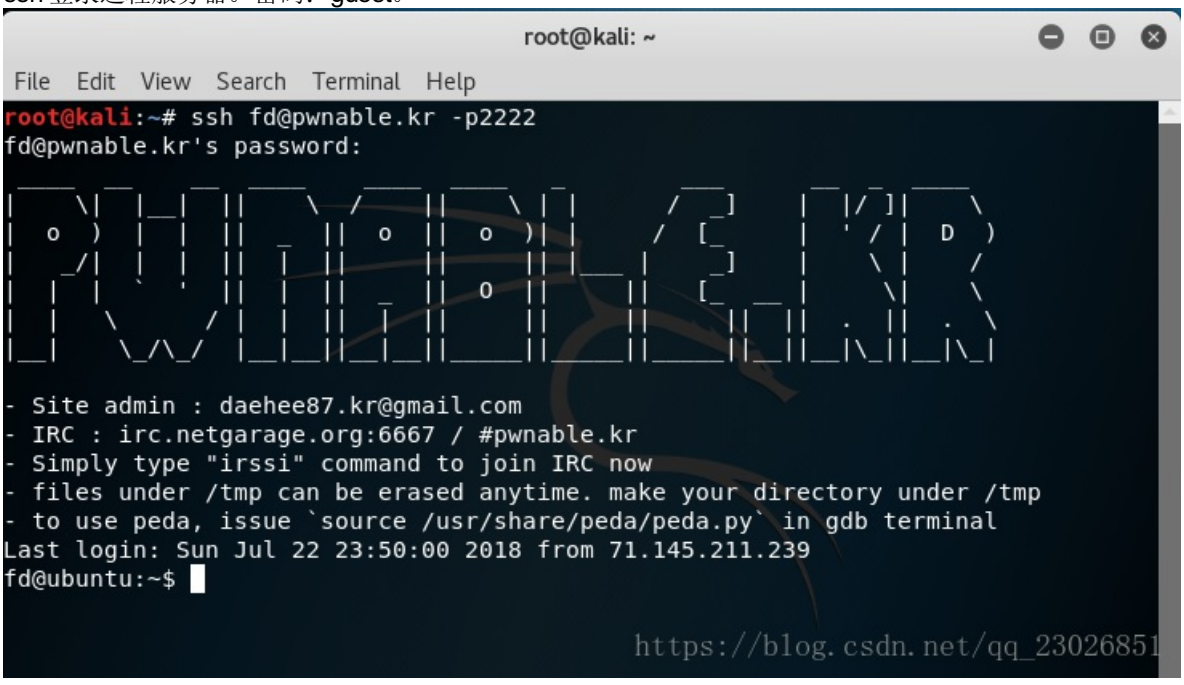
ShinJoe 于 2018-07-23 15:27:32 发布 249 收藏
分类专栏： pwnable.kr 文章标签： pwn CTF 安全 Linux

题目：

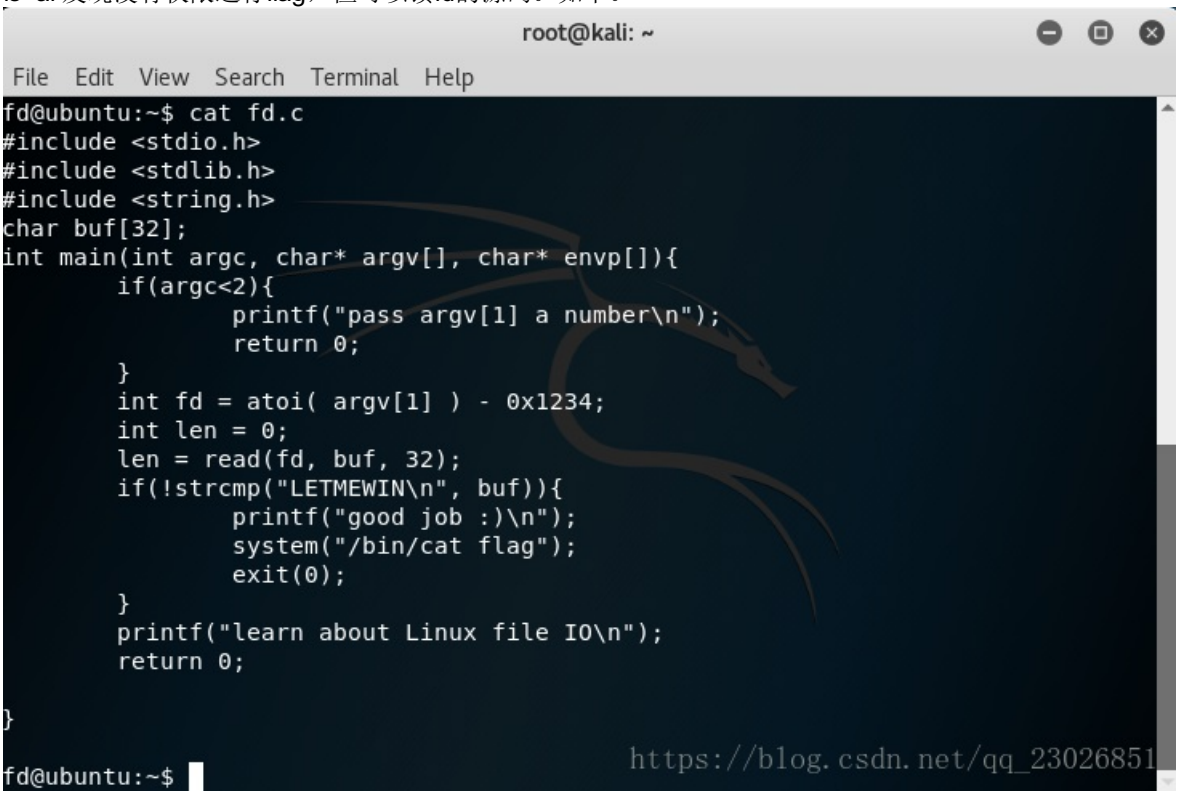


解：

1. ssh 登录远程服务器。密码：guest。



2. ls -al 发现没有权限运行flag，但可以读fd的源码。如下。



3. 显然，这里的目标就是想办法让buf的值等于“LETMEWIN\n”。如何做到？我注意到有read(fd, buf, 32)这个函数，作用是读取fd所代表的文件，并把其中一定量的字符（这里是32个）放到buf中。OK，所以我只要构造出内容为“LETMEWIN\n”的文件不就好了嘛！
4. emmm...但是先创建文件再获取fd好像很麻烦，有没有更方便的方法？我查询了文件描述符（file descriptor）的定义：https://en.wikipedia.org/wiki/File_descriptor 发现fd=0代表了standard input，也就是键盘输入。
5. 如此就很容易了，最后一步把0x1234转成十进制（4660），并作为第二个参数输入即可。