

# [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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/qq\\_23026851/article/details/81167792](https://blog.csdn.net/qq_23026851/article/details/81167792)

版权

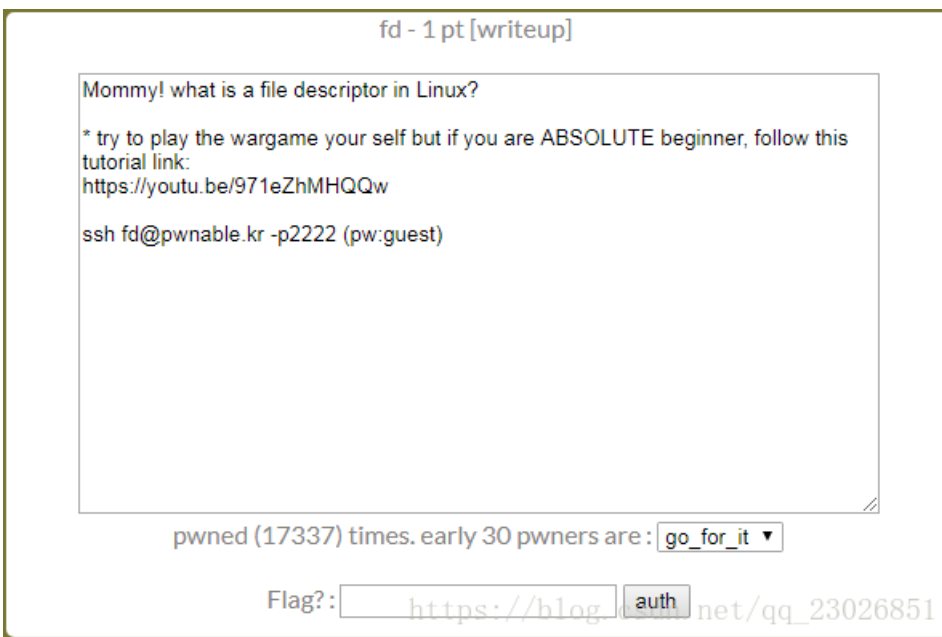


[pwnable.kr](#) 专栏收录该内容

1 篇文章 0 订阅

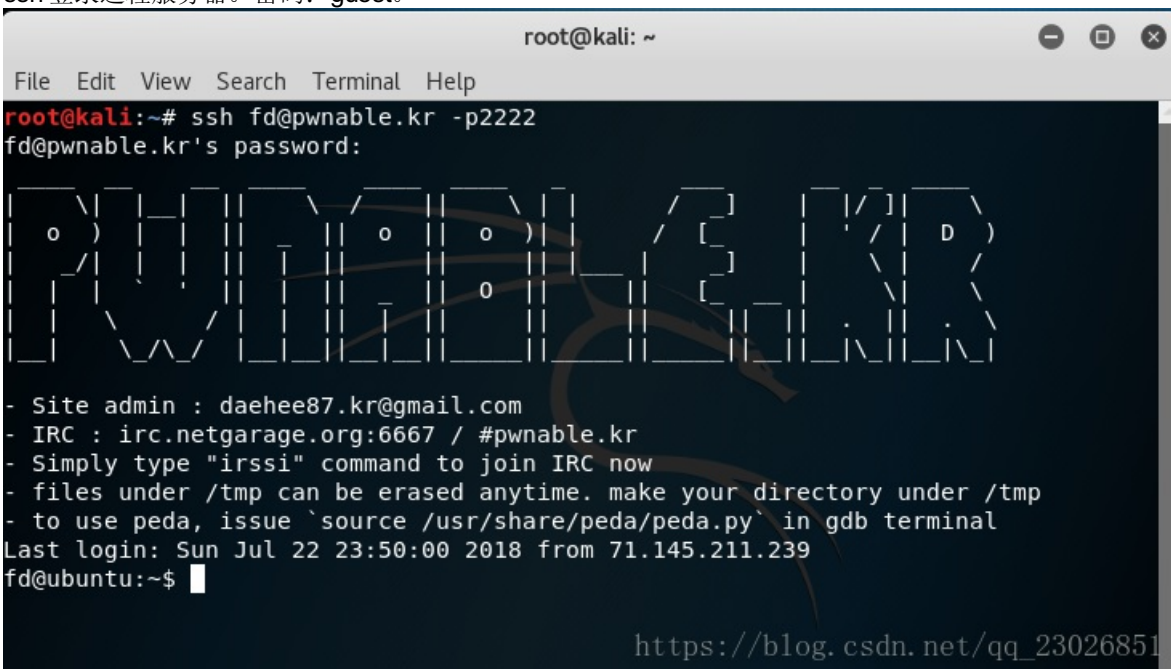
订阅专栏

题目:



解:

1. ssh 登录远程服务器。密码: `guest`。



[https://blog.csdn.net/qq\\_23026851](https://blog.csdn.net/qq_23026851)

2. `ls -al` 发现没有权限运行flag，但可以读fd的源码。如下。

```
root@kali: ~
File Edit View Search Terminal Help
fd@ubuntu:~$ cat fd.c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
char buf[32];
int main(int argc, char* argv[], char* envp[]){
    if(argc<2){
        printf("pass argv[1] a number\n");
        return 0;
    }
    int fd = atoi( argv[1] ) - 0x1234;
    int len = 0;
    len = read(fd, buf, 32);
    if(!strcmp("LETMEWIN\n", buf)){
        printf("good job :)\n");
        system("/bin/cat flag");
        exit(0);
    }
    printf("learn about Linux file IO\n");
    return 0;
}
fd@ubuntu:~$
```

[https://blog.csdn.net/qq\\_23026851](https://blog.csdn.net/qq_23026851)

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](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。

```
fd@ubuntu:~$ ./fd 4660
LETMEWIN
good job :)
mommy! I think I know what a file descriptor is!!
fd@ubuntu:~$
```

[https://blog.csdn.net/qq\\_23026851](https://blog.csdn.net/qq_23026851)