pwnable.kr-fd-Writeup

转载

baikeng3674 于 2017-02-04 22:32:00 发布 84 收藏
文章标签： 运维
原文链接：http://www.cnblogs.com/WangAoBo/p/6366517.html

pwnable.kr-fd-Writeup

- 根据题目描述*Mommy! what is a file descriptor in Linux?* 知该题与Linux系统下的文件描述有关；
- ssh远程登录如下：
- 根据题目提示，***ls -l***查看文件及权限如下,由下图，用户fd只具有读文件fd.c的权限（尝试sudo chmod增加权限，但失败）：
- ***cat fd.c***读取fd.c中的内容，可得到如下代码：

```
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:~$
```

- 分析上述代码，执行*system("/bin/cat flag");*语句，即可获得flag;
- 执行*system("/bin/cat flag");*需要使buf == "LETMEWIN";
- 继续分析，需要buf通过read函数读入"LETMEWIN\n"，有read函数的定义，需要使fd==0；
- 则有atoi(argv[1]) == 0x1234(即十进制下的4660），由atoi函数的定义，需要argv[1] == "4660";
- 进而由LinuxC下argv[]的相应定义可以构造输入，LinuxC下argc，argv[]的意义请参考http://www.cnblogs.com/WangAoBo/p/6366600.html

```
echo "LETMEWIN" | ./fd 4660
```

如下，flag为：***mommy! I think I know what a file descriptor is!!***

2017-2-4 22:24;39

转载于:https://www.cnblogs.com/WangAoBo/p/6366517.html