writeup-fd

原创

charlie_heng 于 2016-11-21 20:13:34 发布 223 收藏

分类专栏： 二进制-逆向工程 文章标签： 逆向工程

本文链接：https://blog.csdn.net/charlie_heng/article/details/53263590

打开题目，给出了ssh fd@pwnable.kr -p2222 (pw:guest)，打开ubuntu，连接上去

直接cat flag 并没有成功，先cat fd.c 看下有什么东西

代码如下

```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;

}
```

看了下代码，应该是构造一个数字等于0x1234

输入 ./fd 4660 然后再输入LETMEWIN，成功拿到flag

mommy! I think I know what a file descriptor is!!