pwnable.kr-random-Writeup

转载

baikeng3674 于 2017-02-07 22:06:00 发布 26 收藏
文章标签： 运维
原文链接：http://www.cnblogs.com/WangAoBo/p/6376082.html

MarkdownPad Document

pwnable.kr-random-Writeup

- 与前几题套路相同，ssh远程登录，ls -l查看文件及权限，cat获得C代码如下：

```
#include <stdio.h>

int main(){
    unsigned int random;
    random = rand();    // random value!

    unsigned int key=0;
    scanf("%d", &key);

    if( (key ^ random) == 0xdeadbeef ){
        printf("Good!\n");
        system("/bin/cat flag");
        return 0;
    }

    printf("Wrong, maybe you should try 2^32 cases.\n");
    return 0;
}
```

> 查看random（）函数时有这样的描述：。
>
> 即该函数每次产生的随机值均为定值，自己写一个类似的程序可以得到此时产生的随机值为**1804289383**。
>
> 根据代码流程，**1804289383 ^ 0xdeadbeef**即可得到要输入的key值为**3039230856**，则可得到flag为***Mommy, I thought libc random is unpredictable...***。

2017-2-7 22:01;32