writeup-random

原创

charlie_heng 于 2016-11-22 22:07:13 发布 290 收藏

分类专栏： 二进制-逆向工程

本文链接：https://blog.csdn.net/charlie_heng/article/details/53292543

Daddy, teach me how to use random value in programming!

ssh random@pwnable.kr -p2222 (pw:guest)

题目如上，惯例先看下题目的代码

```c
#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;
}
```

很明显是伪随机，执行一下得到伪随机数是 6b8b4567 再和 deadbeef（死牛。。。） 异或一下 得到答案为-1255736440

输入后拿到flag

Mommy, I thought libc random is unpredictable…