<http://pwnable.kr/play.php第二个collision>

题目内容：

Daddy told me about cool MD5 hash collision today.

I wanna do something like that too!

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

显然是要求我们用SSH远程连入获取信息

SSH的默认端口是22，也就是说，你的登录请求会送进远程主机的22端口。使用p参数，可以修改这个端口。

　　使用 ssh -p 2222 user@host 可以直接连入主机的2222端口

在Linux中打开终端，输入ssh -p2222 col@pwnable.kr

然后输入密码guest进入主机

用ls指令可以看到主机中的文件，共有col、col.c、flag三个

用cat指令看col.c的代码如下：

#include <stdio.h>

#include <string.h>

unsigned long hashcode = 0x21DD09EC; //关键数字

unsigned long check\_password(const char\* p){

int\* ip = (int\*)p; //这里将输入的字符串指针转换为整型指针

int i;

int res=0;

for(i=0; i<5; i++){

res += ip; //这里累加5个数

}

return res; //返回累加和

}

int main(int argc, char\* argv[]){

if(argc<2){ //没有输入参数的过滤

printf("usage : %s [passcode]\n", argv[0]);

return 0;

}

if(strlen(argv[1]) != 20){ //从这里知道我们的参数字符串长度为20个字符

printf("passcode length should be 20 bytes\n");

return 0;

}

if(hashcode == check\_password( argv[1] )){ //如果累加和相等就能够执行对应的命令，输出flag

system("/bin/cat flag");

return 0;

}

else

printf("wrong passcode.\n"); //输出错误

return 0;

}

代码要求构造一个长度为20的字符串，然后每4位转换为int相加之后的值为0x21DD09EC

经大佬尝试，已知一个符合的字符串为 ah\_mah\_lah\_mam\_mhc\_m

执行./col ah\_mah\_lah\_mam\_mhc\_m，得到flag：

daddy! I just managed to create a hash collision :)