TSCTF2017

。MISC。

1．Logo

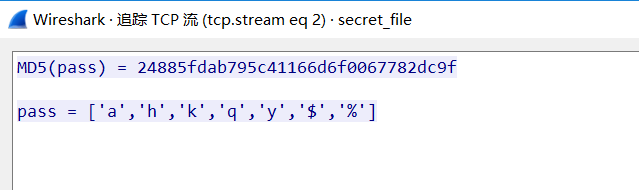
用Hex查看 图片信息结束后是一串字符 结尾是== 用base64解密得到flag

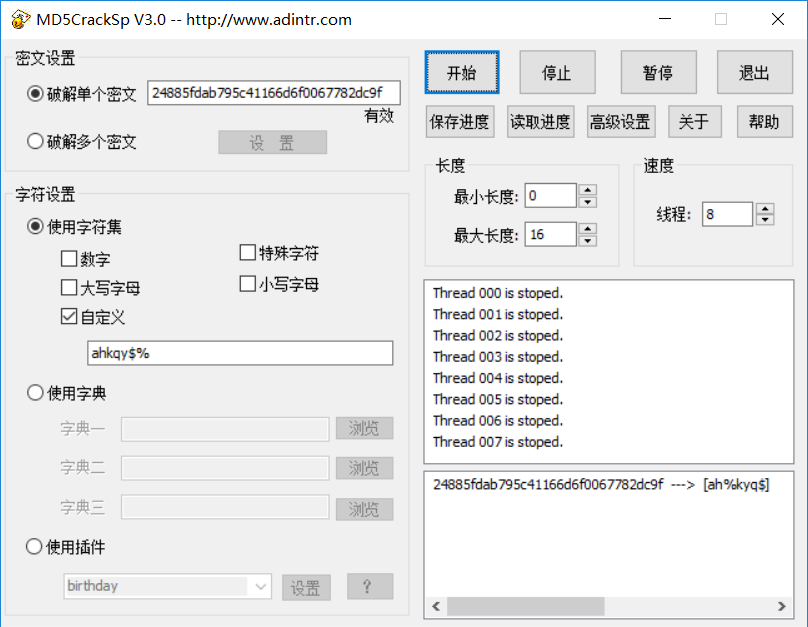
2．神秘的文件

pcapng格式 百度得知是wireshark文件

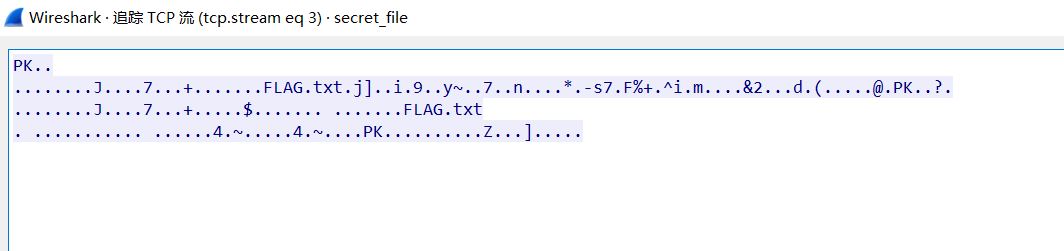
现学现卖 follow tcp流 总共有4组

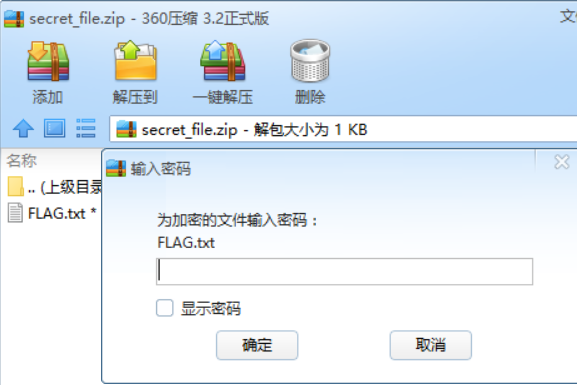
1. Stream2是Md5密文 带有字典 MD5Crack得密码ah%kyq$





2．Stream3开头为PK… Zip格式 用winhex拉出来得到加密的zip





3．输入密码得到flag.txt base64解密得flag

3.四维码（未完成）

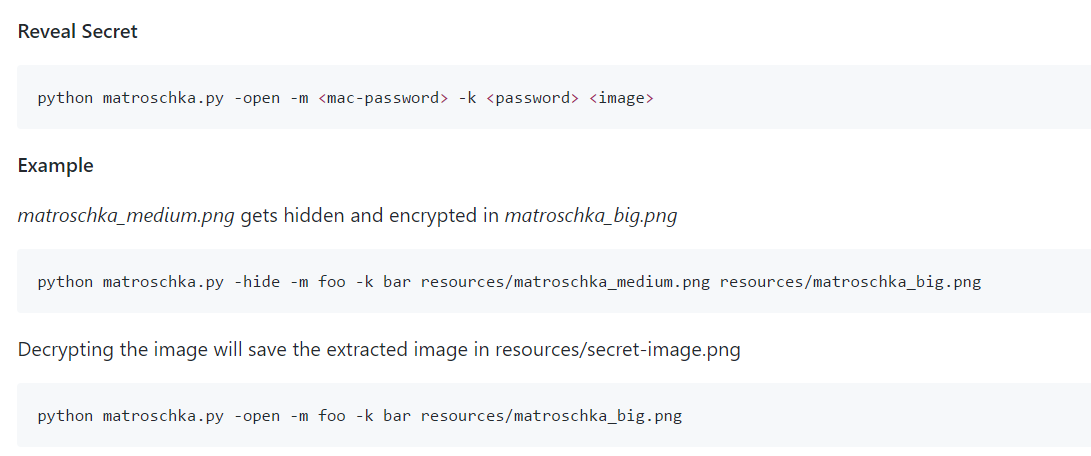
你听说过四维码么？听说每拿到一个新码你就离成功进了一步哦！  
HINT 1:Base32  
HINT 2:如果脑洞不够大，多用搜索引擎搜搜看！  
HINT 3:谷歌搜图？

1．图1为13帧的二维码gif 每帧扫码得两位 组合[www.twitter.com/pinkotsctf](http://www.twitter.com/pinkotsctf) 得图2

2．扫套娃的二维码得NNSXSPLROJRW6ZDF

根据hint2 3 谷歌搜图搜到玄武实验室 再跳转到github上的matroschka加密算法

<https://github.com/fbngrm/Matroschka> 需要password

3．图三可看出是二维码 用stegsolve加深后可得一串二进制 共231位

000000000011010010000111101110101001110110010010011110110010111001010011000010011110100100110000101100100111011000010100101001100001101000111011000101110100001011001001110110010000100110101100100001111010010011000111010110000000000

猜想1：33\*7 补一位转换ascii 一堆控制符 gg

猜想2：新的二维码 经百度二维码最小的version1为21\*21 gg

猜想3：条形码 做不下去 gg（结果就是条形码）

。Coding。

1. Python & Socket

Py3中sock.send()只能传输bytes ，而答题格式应为sock.send(String+”\n”)，故选用py2。

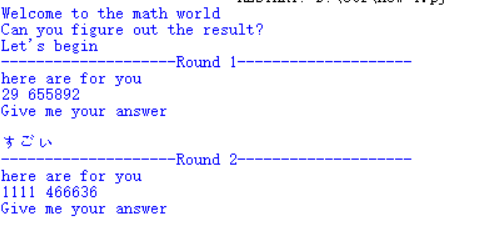
答题有时间限制，需在算法和sleep的时间上优化。题目大部分可通过搜索引擎得到c语言的解法，加以理解后改为python。若sleep时间过短，rec不到全部的数据，需按需求变更。有时算法多跑几次就能跑出来，对sock理解不够，不知道原因\_(:з)∠)\_

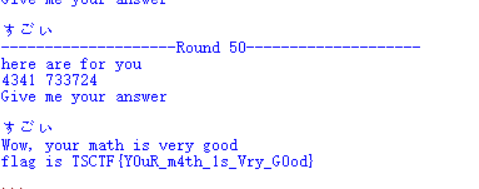
Rec后得到数据，需用正则表达式(?)得到所需的数字进行运算。

1．小明二进制

小明发现，有些整数，它们十进制表示的时候，数的每一位只能是0或者1。例如0，1，110，11001都是这样的数，而2，13，900不是，因为这些数的某些位还包含0、1以外的数。小明将这些各位只为1或者0的数，命名为“小明二进制”。 现每轮给出一个整数n，计算一下最少要用多少个“小明二进制”数相加才能得到n，总共50轮。 如13可以表示为13个1相加，也可以13=10+1+1+1，或者13=11+1+1，所以13最少需要3个“小明二进制”数相加才能得到。

解：最大的数码即为所需的n

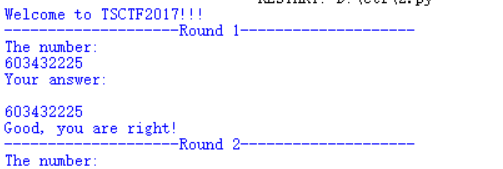


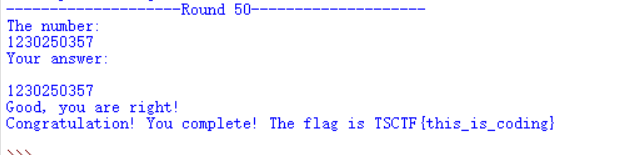


2．泽哥的算术

泽哥的数学不是很好，有一天老师给泽哥布置了五十道数学题，要求他在10s内给出A的B次幂的后四位，你能算的出来吗？ example input : 123 234 output : 6809

解：快速幂算法

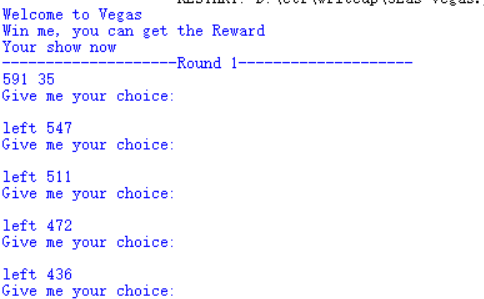


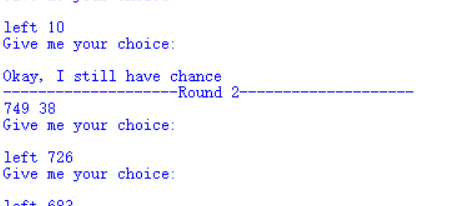


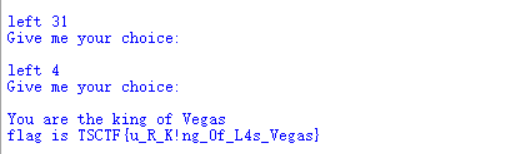
1. Las Vegas

在Las Vegas，霸哥想跟我们玩个简单的取石子游戏，规则如下：游戏给出数字A B,双方轮流从A个石子中取走石子，每次不能超过B个，谁能取走最后一个石子谁就算赢。双方需要完成50轮游戏

解：取石子游戏







1. 修路

市政府决定在1000个村子(1,2,3,4....1000)间修些路来方便大家出行，市长决定在录用你之前进行一次考察，题目给出800条连通道路信息，再做1000次询问，要求给出村子A与B之间是否连通，是回答"yes"，否回答"no"。

解：并查集 获取800条数据时需rec(7\*1024)才能一次读完

