Write-up

暨第三届北邮TSCTF2017——第一次参加CTF比赛记录。

* Coding题，学了一上午的socket编程（时序总是不时地出现问题）。程序和运行结果都在附件中

1. 小明二进制

模拟，转化为求每个数的MAX｛个位，十位，百位……｝求解

1. 泽哥的算术

快速幂，求pow（a,b）%10000

1. LV

博弈论入门，每次拿a%（b+1）个，直至拿完

1. 修路

并查集

* MISC题：除签到外，只会做接近于Coding类型的题目。程序和运行结果都在附件中

1. 签到
2. 密码学枚举攻击（RSA加密，高次剩余问题）

枚举遍历私钥d，

求m1=pow(c1,d)%n

M2=pow(c2,d)%n

E=(m1^m2)%p

使得pow(m1,e)%n=c1

Pow(m2,e)%n=c2

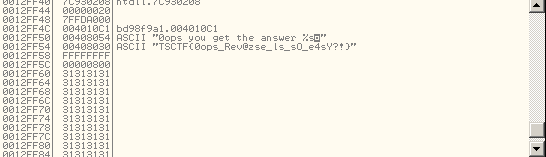
1. EasyCrypto（加密解密）

根据加密算法，编写解密算法，得到原文

* RE&APK题：边学边做，试着分析汇编代码，只会简单的，很好玩，以后会进步的

1. Checkin

跟踪OD，找到flag



1. Babyandroid

利用安卓逆向工具，得到源码，根据源码逻辑写出flag（源码很乱，看着感觉像是个加密过程，把a-f转成10-15，0-9照抄，其他忽略，按这个逻辑往回解，还真对了。）

1. Easy

跟踪OD，理出逻辑，拿到两个关键数据段，写了一小段C语言程序完成异或和移位操作得到flag

* PWN题：

1. asci

见exp.py

1. again

见exp.py

1. Fsb

见exp.py