Re1

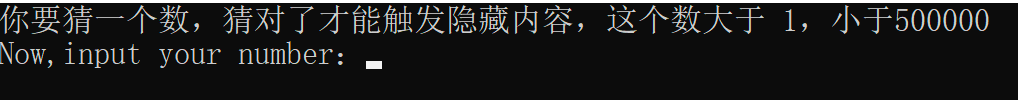
题目名：来玩个游戏吧

分值：很简单，你随便定个最低的分数

简介：来玩个游戏吧，但你别用自己的电脑运行这个程序喔，不然到时候你会得到一个文件，flag的格式是flag{通讯ip:通讯端口}

题解：

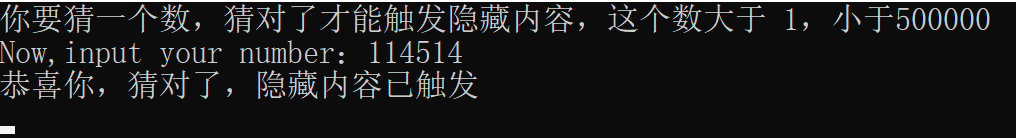
直接运行程序可以知道是个猜数字游戏



但程序是go写的，而且打乱了符号表，不容易定位，这里可以尝试用IDA强行逆向，也可以手动用二分的办法去收敛到结果，时间也用不了多久。

最后得到数字是114514

再输入之后隐藏程序运行



隐藏程序实际上是一段后门shellcode，shellcode运行后会往服务端进行通讯，shellcode运行前有简单的反调试和反沙箱，需要在一个进程数大于██的系统上才能正常运行，至于进程数是多少，大家可以去探索一下。

其中可通过很多办法捕获到通讯地址，这里选择用火绒剑



得到通讯地址。

flag：flag{42.194.141.234:30081}