170709 逆向-CISCN总结

原创

奈沙夜影 于 2017-07-10 11:46:36 发布 912 收藏

1625-5 王子昂 总结《2017年7月9日》【连续第280天总结】

A. CISCN

B. 一整天都投入进去还是非常充实的，虽然几个同学一起想MISC却一道都没做出来，这种经历却是特别有趣
MISC方面大家的积攒都不够，开脑洞基本上能过一些小关，但是面对真正的题目就寸步难行了

这既是成长的过程也是提醒我们抓紧时间锻炼各方面知识

个人的逆向方面比较受挫。今年的逆向不同以往，大量使用了动态函数，以前的直接IDA反编译出源码通读一遍就能明白算法得到flag；今年的必须动静结合一点一点跟才能找到

而且代码极其复杂，使用了很多不常见的函数，读起来感觉寸步难行

数字游戏作为低分逆向，与maze类似，刚开始读起来因为使用了很多没见过的函数误以为加壳，导致浪费了很多时间。其实这个程序看名字就能大概猜想应该是接收数据然后与静态内存用算法比对，完成

中间APK和ELF的逆向都在IDA用F5反编译后就很难进行了，函数地址存放在寄存器中导致完全无法读下去。基本都在跟同学做MISC，包括明文攻击和文件分析逆序，然而都没找到flag

最后零点出了一个低分逆向-溯源。这个题目读起来虽然也有点吃力，但没到无法进行的地步。OD进行动态跟踪可以大概猜到值存放在什么位置，长距离变量间的联系；IDA静态反编译统领大局，比较容易

搞出来源码以后，时间所剩也不多了，突然发现需要得到的是逆算法，尝试将加减运算做逆处理也没得到正确的逆算法

最后几分钟的时候输出了log，观察发现此时的逆算法已经大体能够逆出原数据了，只是中间有少量数据还是报错了，感觉是有一步出问题了。然而没时间了，后来再找也没找到问题

总的来说，需要学习的地方还很多，虽然挫败感挺强的，不过还有很多要学习的地方啊

C.
明日计划

ZigBee学习，学习大佬的WriteUp