

看雪论坛.珠海金山2007逆向分析挑战赛第一阶段结束

原创

[valiant1ster](#) 于 2007-08-27 21:34:00 发布 1291 收藏

文章标签: [金山 汇编 bt 算法 编程 工具](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/valiant1ster/article/details/1761193>

版权

看雪论坛.珠海金山2007逆向分析挑战赛第一阶段结束, 出了两道题, 第一题看似容易, 实际还是有点难度。开始分析那个crackme的流程并不难, 除了对字符信息如“OK!!”的隐藏比较BT; 然后定位到其中的一段代码, 只要能分析清楚, 并将其逆向之, 答案就不得而解了。但反编译是件不轻松的事情, 花了3个小时才把那段汇编代码反成C的 (后来发现其实只要汇编熟练不反也一样)。最后只要解决一个类似 $f(x) + g(y) =$ (满足某个约束条件) 的等式就OK了。由于看了一个上午的汇编代码, 头早就晕了, 于是解决那个算法还是花了一下午+一晚上。: (除了感觉自己不熟练之外, 第一次感觉到编程到最后要解决的还是数学问题。:)

第二题看似不容易, (主要以前没自己动手做过), 但做起来还不是很困难, 最后是看谁动作快, 呵呵。尤其是用现成的工具。顺利通过第一阶段, 自己庆贺一下先。。。