




BCTF总结

原创

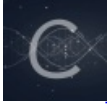
 于 2014-03-14 22:40:37 发布  2142  收藏

分类专栏: [杂谈](#) 文章标签: [BCTF Writeup Sigma](#)

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/I0g1n/article/details/21256161>

版权



[杂谈](#) 专栏收录该内容

19 篇文章 0 订阅

订阅专栏

缘由

上周, 我们小组Sigma参加了“百度杯”BCTF比赛, 经历了难忘的双休, 这次的BCTF跟以前参加的国内类似的安全比赛有些不同, 时间只有48小时, 题目不多, 但难度大, 完全跟国际接轨(我自己的感觉)。

反思

我完成了两个题目, 都是与逆向有关:

- 1、题目简单, nop掉MessageBox, 下个断点, 跑起来就出来KEY了。
- 2、很明显的考查了算法的逆向, 回想起来是很简单的算法逆向, 只是除以10, 对余数和商做些简单计算。

对这个题目, 多说一些, 我用了一天半的时间在做这个题目, 中途两次想放弃, 在队友的鼓励下, 艰难的完成了。

对我自己暴露的问题: 逆向分析不扎实、耐心不足, 在使用IDA进行分析时, 没考虑到栈空间复用的问题, 导致出现错误;空间想像能力也差一些, 多次循环之后就会晕了。每当出现问题, 并在努力解决问题的时候, 才是水平真正提高的时间, 如果一些题目, 一看就搞出来了, 对自身能力是不会有提高的, 在这里警示自己, 遇到问题, 放弃了, 你就输了, 输的很彻底。对逆向, 多加练习, 理解栈、堆、代码各部分的联系, 不能太理所当然, 出现问题, 通过调试来解决。

对一些溢出和其它的逆向题目, 基本无从下手, 原因是Linux平台、Arm平台下的, gdb基本不会, 是软肋, 现在Writeup出来了, 题目还有, 后面的需要学习一下gdb, 和一些狸奴x下调试技巧。

Writeup

放上线上赛前8名所有的Writeup, 大家可以对比一下, 看哪里是自己欠缺的地方。

<http://download.csdn.net/detail/I0g1n/7042787>