# 170702 逆向-IOS（失败）

原创

奈沙夜影 于 2017-07-02 00:37:40 发布 251 收藏
分类专栏： CTF



1625-5 王子昂 总结《2017年7月1日》【连续第272天总结】

A.全国大学生信息安全竞赛-IOS

B.下载下来发现是ipa文件，赶紧下个pp助手，拖到自己的古董4S里安装试试

--需要Ios9.0以上版本

看看自己的7.0默然无语，连比赛的题目都要这么高的等级

试试静态反编译吧，拖到IDA里main函数直接显示出来，但是一堆赋值以后是一堆不明所以的函数调用

看起来是加壳了的样子

百度了一番，http://www.jianshu.com/p/4da57be23275 这个地址有比较细致的整理

找到了DumpDecrypted：https://github.com/ianisme/IANDecryptiOSApp/tree/master/dumpdecrypted

其他工具诸如Dump-Class，HommerDisassembler等等似乎都是要在mac系统下才能运行的

用越狱后的4S运行DumpDecrypted报错框架文件错误

猜测是运行不了该文件的版本问题

查了一下发现没法刷机然后越狱了……_(:3」∠)_GG

只有去年冠军队才有该题的writeup，他们用IDA查看文件后发现是DES加密，但密钥和明码都被硬编码了，然后最后真机运行，结束。OTZ

C. 明日计划

实验吧Reverse，和书理论学习