【逆向学习】还是代码 writeup

原创

charlie_heng 于 2017-12-22 11:44:01 发布 620 收藏

分类专栏： 二进制-逆向工程

本文链接：https://blog.csdn.net/charlie_heng/article/details/78871641

二进制-逆向工程 专栏收录该内容

34 篇文章 3 订阅

订阅专栏

这是jctf2014的一道题

首先用工具查出来关键的函数是sub_401430

看了下，大概逻辑是用pass1对在0x422000地址一顿操作，具体操作是

1. 取两个字节，比如说第三四个字节，0xc3，0x2
2. 将0x2左移八位，然后加上0xc3，得到的结果传进sub_4011A0
3. sub_4011A0的参数有三个，第一个是上面得到的结果，第二个是pass1，第三个是1517
4. 函数的代码如下

```
int __cdecl sub_4011A0(int a1, int a2, int a3)
{
  int result; // eax
  int v4; // ecx

  result = 1;
  if ( a2 != 0 )
  {
    v4 = a2;
    do
    {
      --v4;
      result = a1 * result % a3;
    }
    while ( v4 );
  }
  return result;
}
```


5. 写段pythonn代码，然后让0x422000的前两个字节变为0x55,0x8b，也就是push ebp
6. 解出来pass1是233 （做题都被出题人嘲讽。。。。

解出0x422000的代码之后，跟进去会发现他硬编码了flag，所以直接扒出来就行了

但是交到i春秋那么蜜汁提示回答错误。。。。算了，有收获就行