XCTF攻防新手区逆向writeup（1）csaw2013reversing2

原创

酸酸菜鱼 于 2020-07-07 14:11:54 发布 305 收藏 1

分类专栏： 逆向工程 CTF

本文链接：https://blog.csdn.net/lhk124/article/details/107151802

逆向工程 同时被 2 个专栏收录

12 篇文章 1 订阅

订阅专栏

CTF

41 篇文章 1 订阅

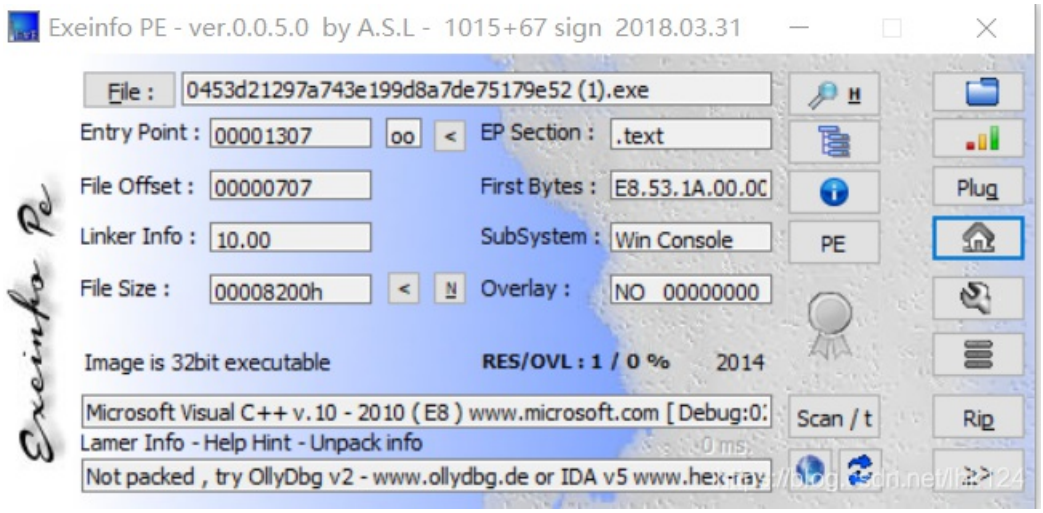
订阅专栏

题目1 csaw2013reversing2

题目来源： Source: CSAW CTF 2014

题目描述：听说运行就能拿到Flag，不过菜鸡运行的结果不知道为什么是乱码

exeinfo查壳，无壳



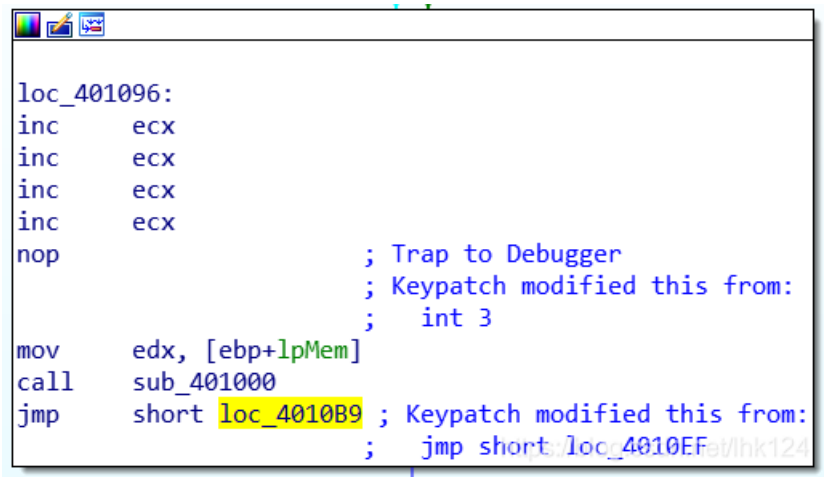
丢ida里自行分析。

3种解决方法

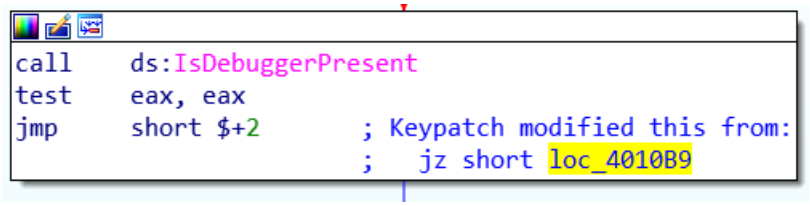
1.用ida keypatch打补丁，改变程序流程。

顺序如下：

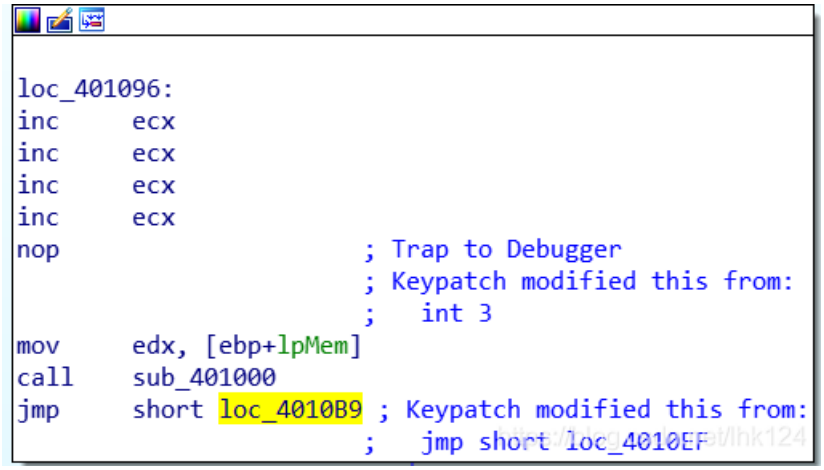
int3时IsDebuggerPresent触发后的中断操作，将其nop



```
loc_401096:
inc     ecx
inc     ecx
inc     ecx
inc     ecx
nop                     ; Trap to Debugger
                        ; Keypatch modified this from:
                        ;   int 3
mov     edx, [ebp+lpMem]
call    sub_401000
jmp     short loc_4010B9 ; Keypatch modified this from:
                        ;   jmp short loc_4010EF
```



```
call    ds:IsDebuggerPresent
test    eax, eax
jmp     short $+2       ; Keypatch modified this from:
                        ;   jz short loc_4010B9
```



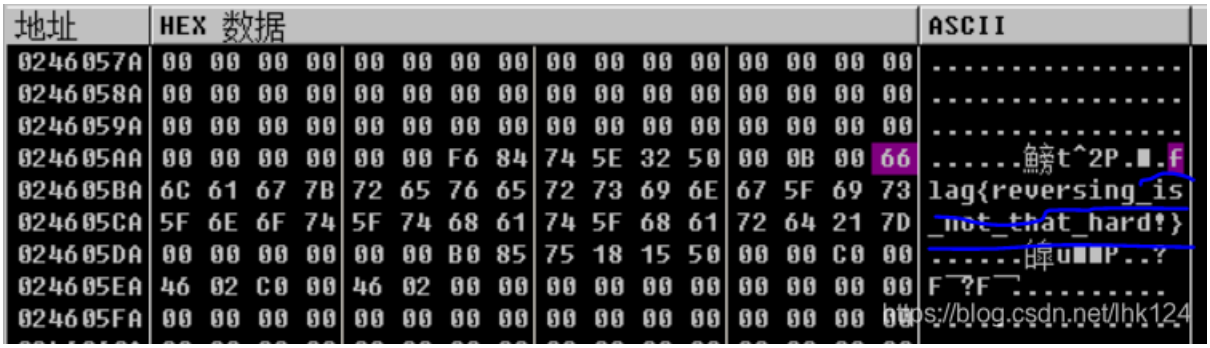
```
loc_401096:
inc     ecx
inc     ecx
inc     ecx
inc     ecx
nop                     ; Trap to Debugger
                        ; Keypatch modified this from:
                        ;   int 3
mov     edx, [ebp+lpMem]
call    sub_401000
jmp     short loc_4010B9 ; Keypatch modified this from:
                        ;   jmp short loc_4010EF
```

其余两处改变跳转顺序，使得程序走过计算字符串的函数401000后，再让其调用MessageBox函数。实现弹窗是flag的效果。

存在问题：改变keypatch的顺序时，会出现某处Keypatch failed to process this input的报错。

方法2：
既然已知程序的最终结果是在401000中中跑出来的，那么就在程序末端查看寄存器

看到flag了。缺了个f。在edi处->右键->在数据窗口中跟随



方法3：在OD中动态调试，与方法一相同，改变程序执行流程。并且不会有方法1的问题，所以可以更直接的修改指令，比如修改跳过IsDebuggerPresent。