

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](#)

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/lhk124/article/details/107151802>

版权



[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

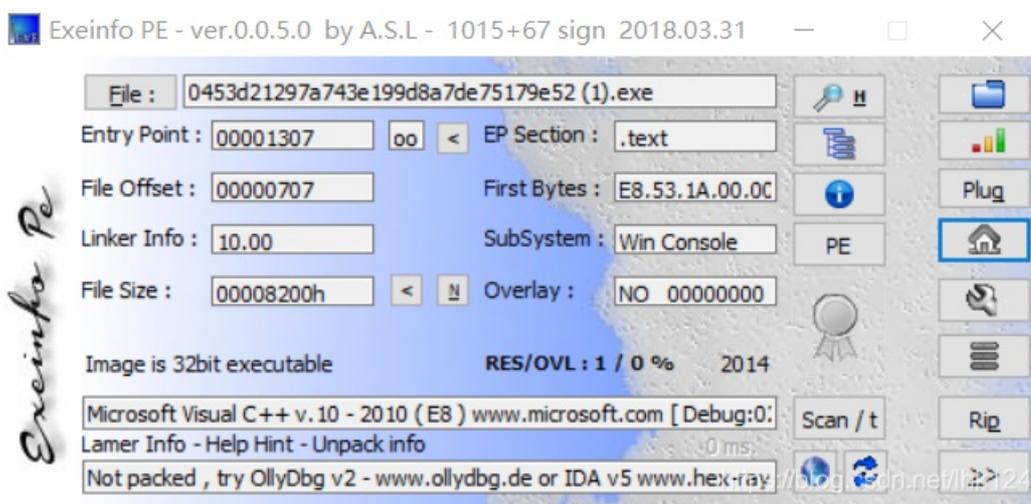
订阅专栏

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\lhk124
```

```
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\lhk124
```

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

```
023 | . 3BC8 | cmp ecx, eax | EBP 0019FF28
025 | . 72 F8 | short 0453d212.0076101F | ESI DDCCABBB
027 | > 5F | mov esi, edi | EDI 025605BA ASCII "lag{reversing_is_not_that_hard!}"
028 | . 5E | pop esi | EIP 0076101F 0453d212.0076101F
```

看到flag了。缺了个f。在edi处->右键->在数据窗口中跟随

地址	HEX 数据	ASCII
0246057A	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0246058A	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0246059A	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
024605AA	00 00 00 00 00 00 F6 84 74 5E 32 50 00 0B 00 66 鯨^2P. .f
024605BA	6C 61 67 7B 72 65 76 65 72 73 69 6E 67 5F 69 73	lag{reversing_is
024605CA	5F 6E 6F 74 5F 74 68 61 74 5F 68 61 72 64 21 7D	not_that_hard!}
024605DA	00 00 00 00 00 00 B0 85 75 18 15 50 00 00 C0 00 啤uMP..?
024605EA	46 02 C0 00 46 02 00 00 00 00 00 00 00 00 00 00	F?F.....
024605FA	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	https://blog.csdn.net/lhk124

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。



[创作打卡挑战赛](#)

[赢取流量/现金/CSDN周边激励大奖](#)