

bugkuCTF平台逆向题第三道游戏过关题解

原创

iqiqiya 于 2017-12-27 21:02:51 发布 7408 收藏

分类专栏: [-----bugkuCTF 我的CTF进阶之路](#) 文章标签: [CTF 游戏过关](#) [writeup](#) [bugku](#) [reverse](#)

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/xiangshangbashaonian/article/details/78916412>

版权



-----bugkuCTF 同时被 2 个专栏收录

9 篇文章 0 订阅

订阅专栏

我的CTF进阶之路

108 篇文章 18 订阅

订阅专栏

题目链接:

<http://123.206.31.85/files/cd2487de0516fa77d5fa911cdf2582c9/ConsoleApplication4.exe>

tips

游戏过关

60

作者: Docupa



Key

SUBMIT

查壳发现无壳 (截图略)

OD载入

发现有两个重要的段

0x001

```
0132E8EE CC int3
0132E8EF CC int3
0132E8F0 -> 55 push ebp
0132E8F1 . 8BEC mov ebp,esp
0132E8F2 . 81EC C00000 sub esp,4C0
0132E8F3 . 53 push ebx
0132E8F4 . 56 push esi
0132E8F5 . 57 push edi
0132E8F6 . 8B80 40FFFFFF lea edi,[local.40]
0132E8F7 . B9 30000000 mov ecx,4C0
0132E8F8 . BB C0C0C0C0 mov eax,4C0C0C0C0
0132E8F9 . F3:00 rep stos dword ptr es:[edi]
0132E8FA . 68 50AE3E01 mov ConsoleA.013AE50
0132E8FB . E8 060EFFFF call ConsoleA.0130A70E
0132E8FC . 83C4 04 add esp,4
0132E8FD . 5F pop edi
0132E8FE . 5E pop esi
0132E8FF . 5B pop ebx
0132E900 . 81CA C00000 add esp,4C0
0132E901 . 3BEC cmp ebp,esp
0132E902 . E8 069EFFFF call ConsoleA.0130A801
0132E903 . 8BES mov esp,ebp
0132E904 . 5D pop ebp
0132E905 . C3 ret
0132E906 CC int3
```

0x002

```

0133E93E CC      int3
0133E93F CC
0133E940 55      push ebp
0133E941 8BEC   mov  ebp,esp
0133E943 81EC 58010001 sub  esp,0x158
0133E949 53      push ebx
0133E94A 56      push esi
0133E94B 57      push edi
0133E94C 8DBD A8FEFF lea  edi,[local.86]
0133E952 B9 56000000 mov  ecx,0x56
0133E957 B8 CCCCCCCC mov  eax,0xC0000000
0133E95C F3:AB  rep  stos dword ptr es:[edi]
0133E95E A1 04204101 mov  eax,dword ptr ds:[0x1412004]
0133E963 33C5   xor  eax,ebp
0133E965 8945 FC   mov  [local.1],eax
0133E968 68 F8B83E01 push ConsoleA.013EB0F0
0133E96D E8 4CBEFFFF call ConsoleA.0133A7BE
0133E972 83C4 04   add  esp,0x4
0133E975 C645 BC 12  mov  byte ptr ss:[ebp-0x44],0x12
0133E979 C645 BD 40  mov  byte ptr ss:[ebp-0x43],0x40
0133E97D C645 BE 62  mov  byte ptr ss:[ebp-0x42],0x62
0133E981 C645 BF 05  mov  byte ptr ss:[ebp-0x41],0x5
0133E985 C645 C0 02  mov  byte ptr ss:[ebp-0x40],0x2
0133E989 C645 C1 04  mov  byte ptr ss:[ebp-0x3F],0x4
0133E98D C645 C2 06  mov  byte ptr ss:[ebp-0x3E],0x6

```

ConsoleA.<ModuleEntryPoint>

done!!! the flag is

分析处0x001每次输入n的值都会有只有那一个跳转调向它

那么我们直接修改跳转地址指向我们的0x002的段首试一下

成功跳转后直接F8单步向下跟

如果遇到向上跳转 就F4下面的下一行

把它拷贝出来 发现提交正确

堆栈地址=004FF7B4, (ASCII "zscft{T9is_tOpic_1s_v5ry_int7resting_b6t_others_are_n0t}")

eax=00000038

跳转来自 0133EB77