

第一次小作业writeup

转载

diuzhabj9104 于 2015-01-04 15:00:00 发布 73 收藏

原文链接: <http://www.cnblogs.com/D0g3/p/4201181.html>

版权

打开运行, 文件提示keyfile, 确认就出错, 程序结束



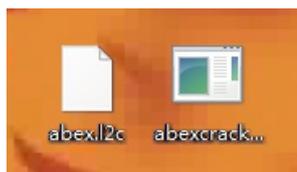
OD载入, 发现keyfile在一个名叫abex.l2c的文件中, 故在同文件夹下新建文件abex.l2c

```
00401013 . 6A 00          push 0x0
00401015 . 68 80000000    push 0x80
0040101A . 6A 03          push 0x3
0040101C . 6A 00          push 0x0
0040101E . 6A 00          push 0x0
00401020 . 68 00000000    push 0x80000000
00401025 . 68 B9204000    push abexcrac.004020B9
0040102A . E8 5E000000    call <jmp.&KERNEL32.CreateFileA>
                                     hTemplateFile = NULL
                                     Attributes = NORMAL
                                     Mode = OPEN_EXISTING
                                     pSecurity = NULL
                                     ShareMode = 0
                                     Access = GENERIC_READ
                                     abex.l2c
                                     CreateFileA
```

向下查看是否有密码算法, 结果发现只有比对了文件大小, 并没有密码比对

```
0040103B . FF35 CA204000 push dword ptr ds:[0x4020CA]
00401041 . E8 40000000    call <jmp.&KERNEL32.GetFileSize>
00401046 . 83F8 12        cmp eax,0x12
                                     hFile = NULL
                                     GetFileSize
```

所以只要密码文件长度为0x12即可, 十进制长度18



对于修改文件abex.l2c文件内容, 可用工具SublimeText3

转载于: <https://www.cnblogs.com/D0g3/p/4201181.html>