

[writeup]360-ctf-2014-re123

原创

hellotaqini 于 2016-03-13 20:28:24 发布 824 收藏

分类专栏: [ctf](#) 文章标签: [逆向 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/hellotaqini/article/details/50879818>

版权



[ctf](#) 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

2014年360 CTF 逆向分析 三道简单的题目

re1

输入错误密码后会提示Done

正确的会提示success

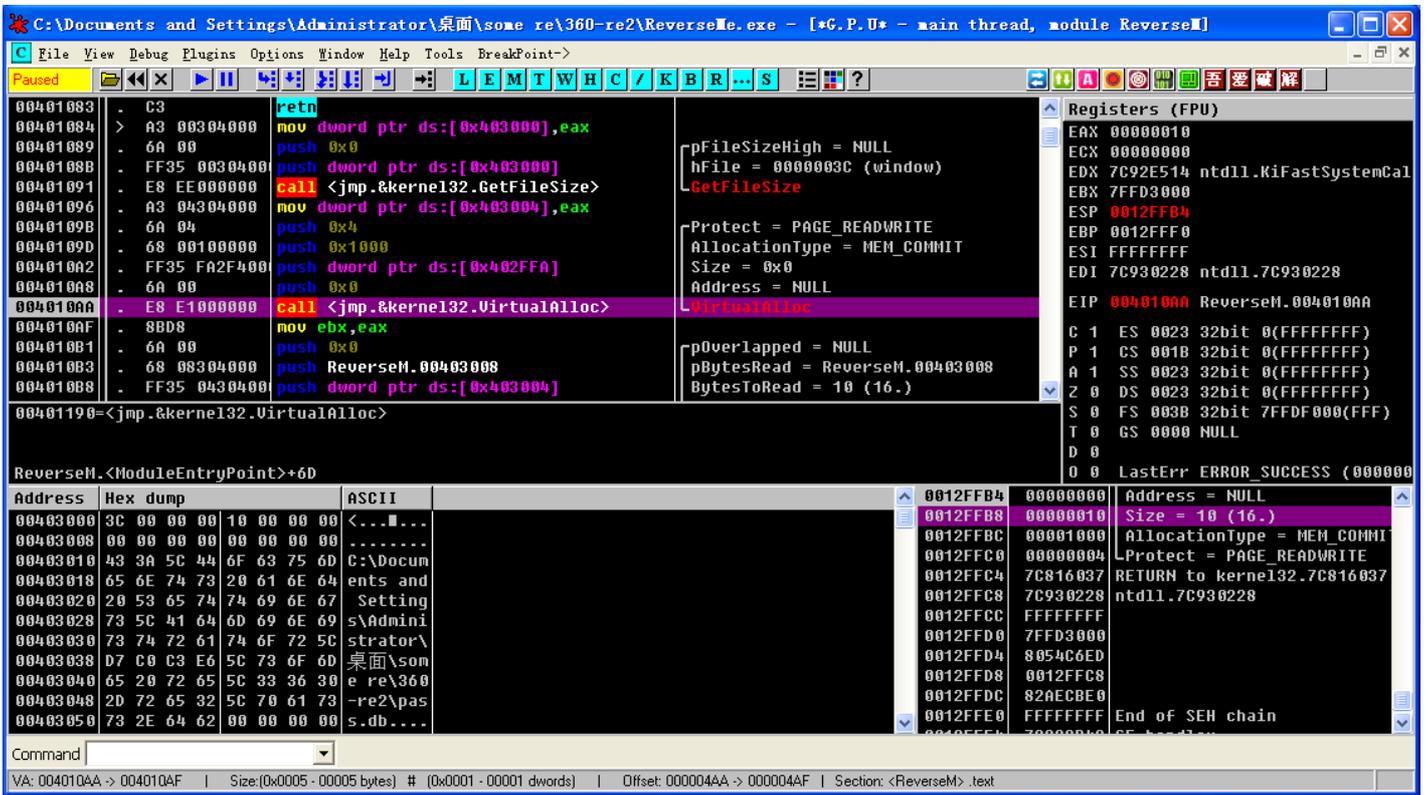
定位到success, 发现是明文比较 ==

The screenshot shows a debugger window for CrackMe.exe. The assembly window is paused at address 004014C6, which contains the instruction `cmp dl, byte ptr ds:[esi+0x1]`. The registers window shows EAX=009639F0, ECX=00000024, EDX=00962824, EBX=00000001, ESP=0012F8E0, EBP=0012F90C, ESI=00963950, EDI=0012FEA4, and EIP=004014C6. The memory dump shows the string "1234567890" at address 004014B5 and "K\$q*a_+@xt" at address 004014C6. The command window shows the command `!s:[00963951]=32 ('2')` and `!l=24 ('$')`.

re2

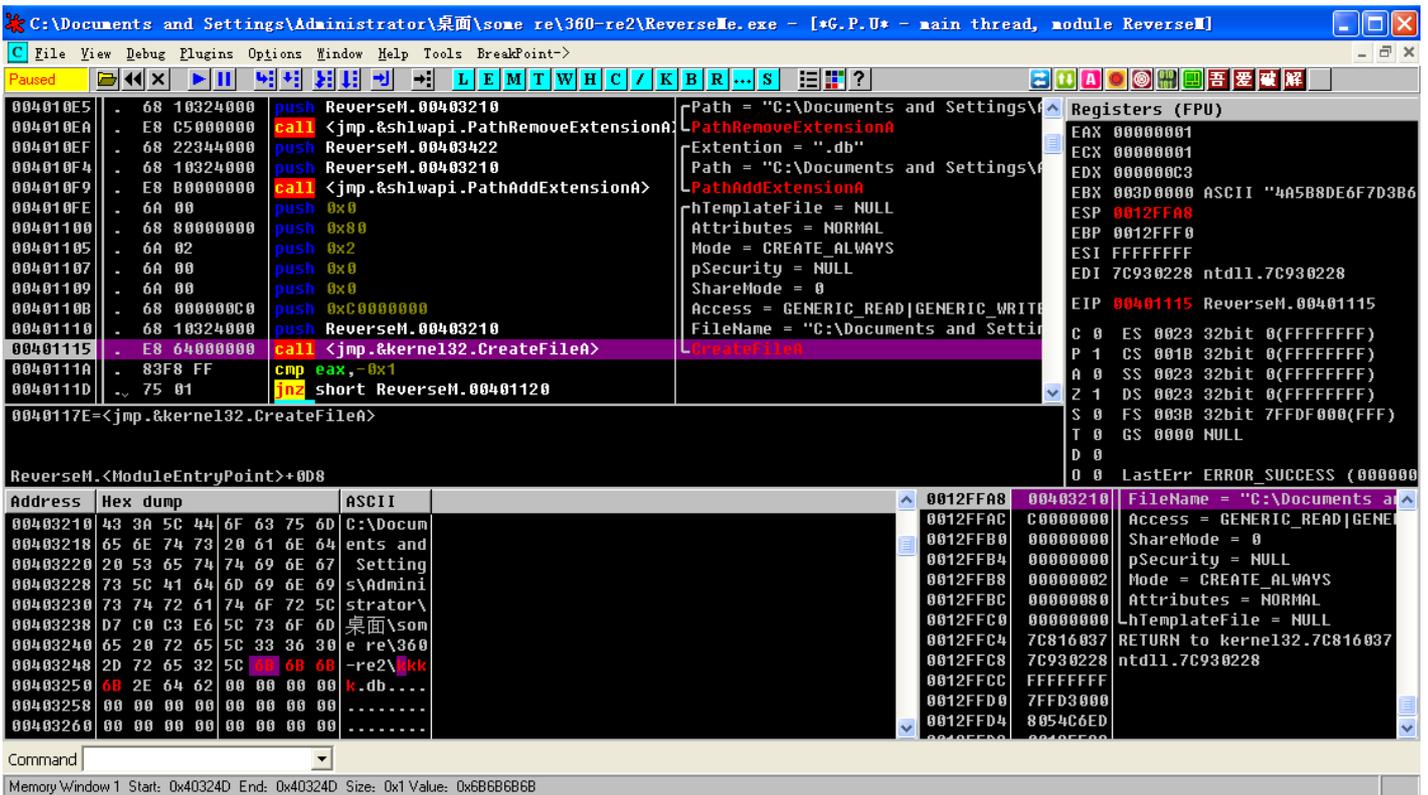
设置参数为pass.db, 用od载入

单步执行到VirtualAlloc, 发现函数没调用成功。



根据pass.db长度把size改为0x10(16)，函数成功调用

继续单步执行，又碰到一个CreateFileA，文件名还是pass.db，修改文件名



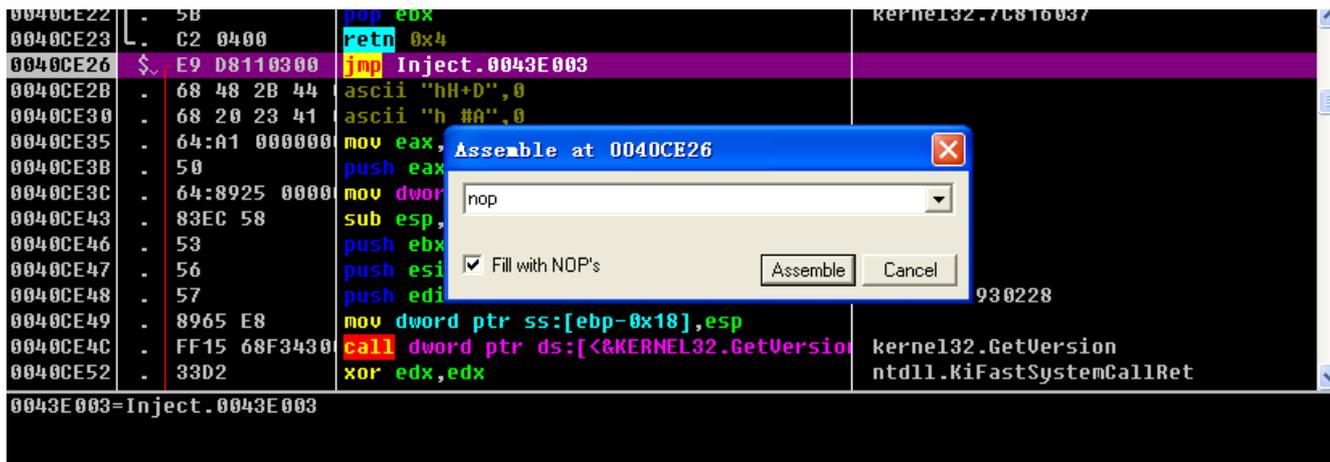
继续执行程序

打开生成的kkkk.db发现密码

...说是被病毒感染了

od载入程序后发现进入点有个jmp

直接nop掉



运行程序即可看到密码