《漏洞利用及渗透测试基础》实验报告

姓名：孙蕗 学号：2112060 班级：信安1班

**实验名称：**

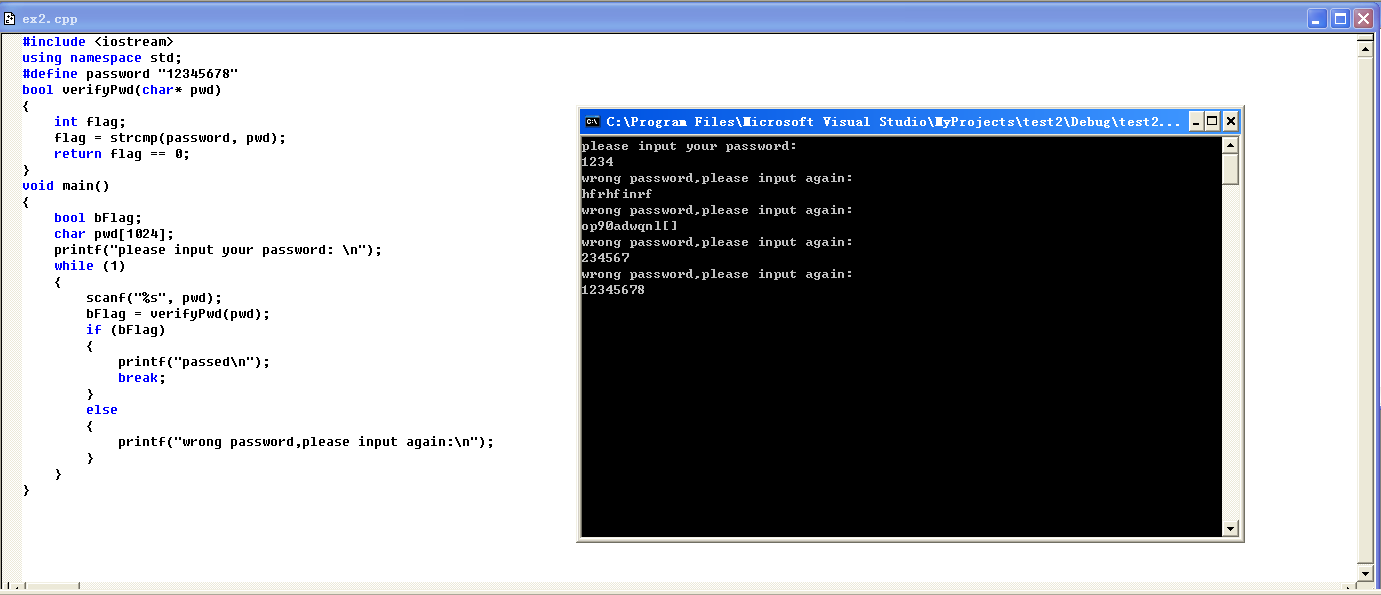
OLLYDBG软件破解

**实验要求：**

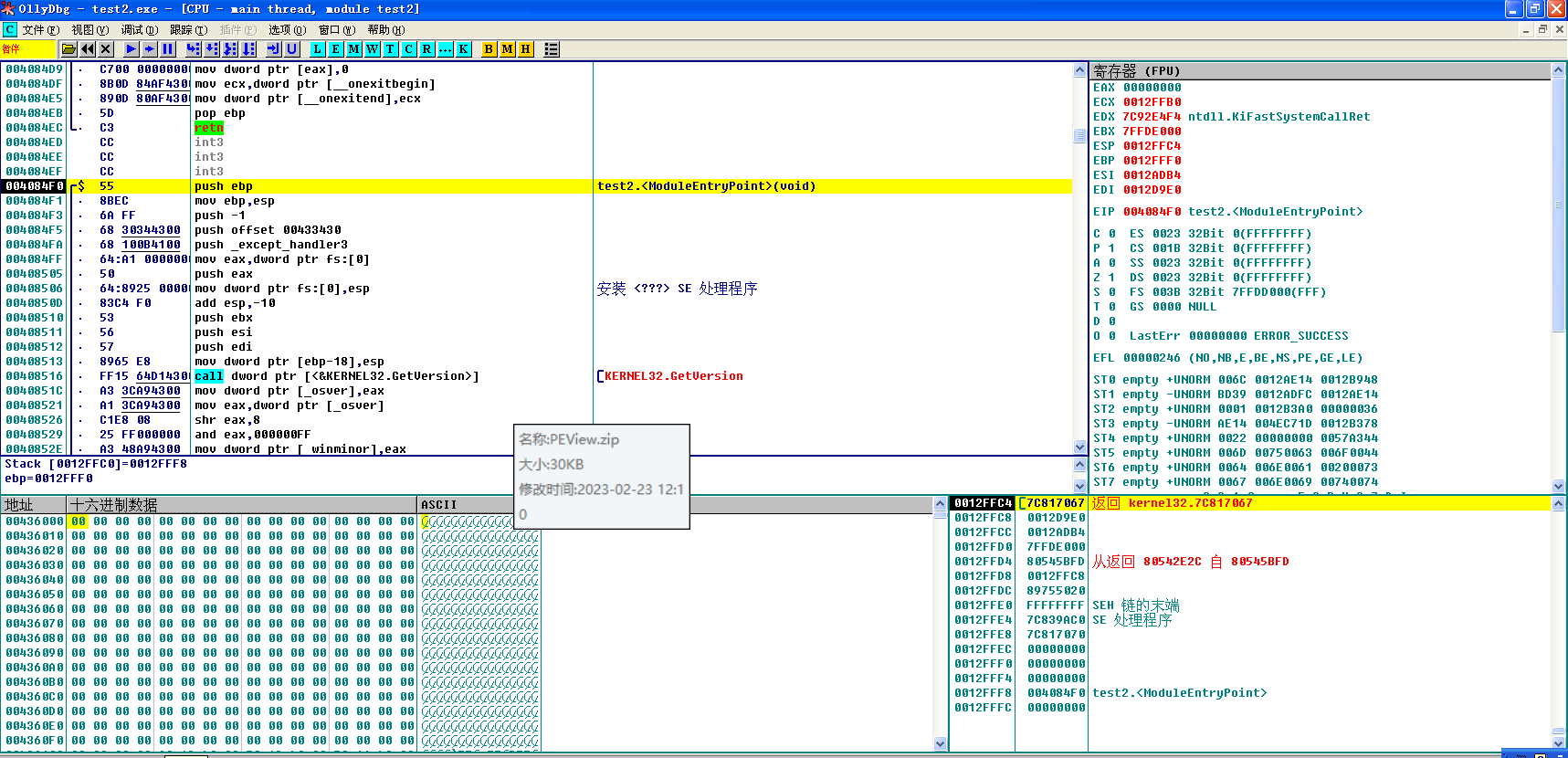
1. 请在XP VC6生成课本第三章软件破解的案例（DEBUG模式，示例3-1）。进而，使用OllyDBG进行单步调试，获取verifyPWD函数对应flag==0的汇编代码，并对这些汇编代码进行解释。
2. 对生成的DEBUG程序进行破解，复现课本上提供的两种破解方法

**实验过程：**

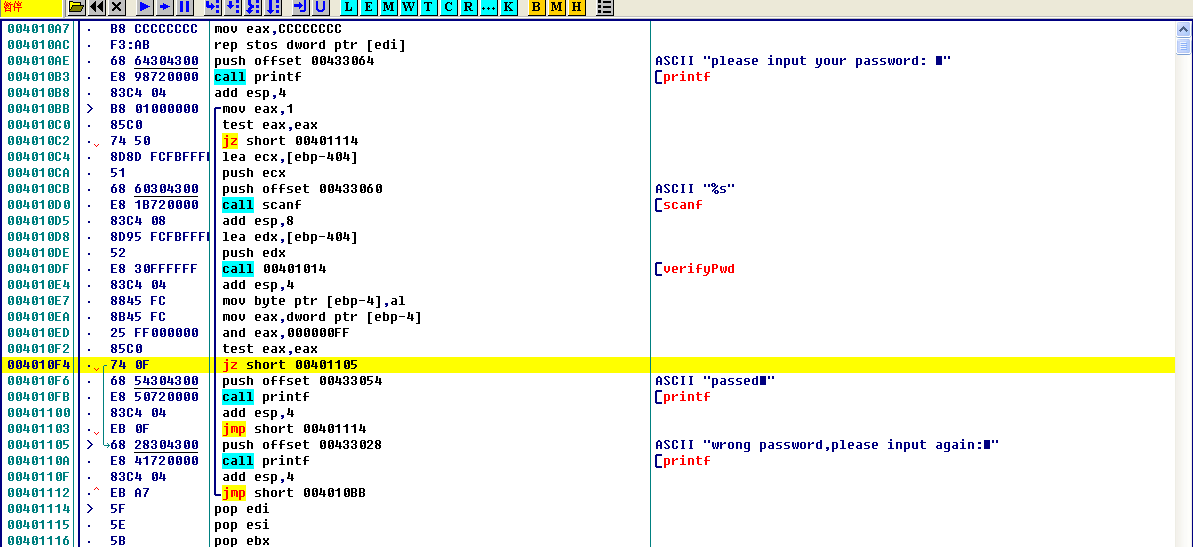
1. **要求1**
2. 在VC6上生成课本第三章软件破解的案例。示例3-1



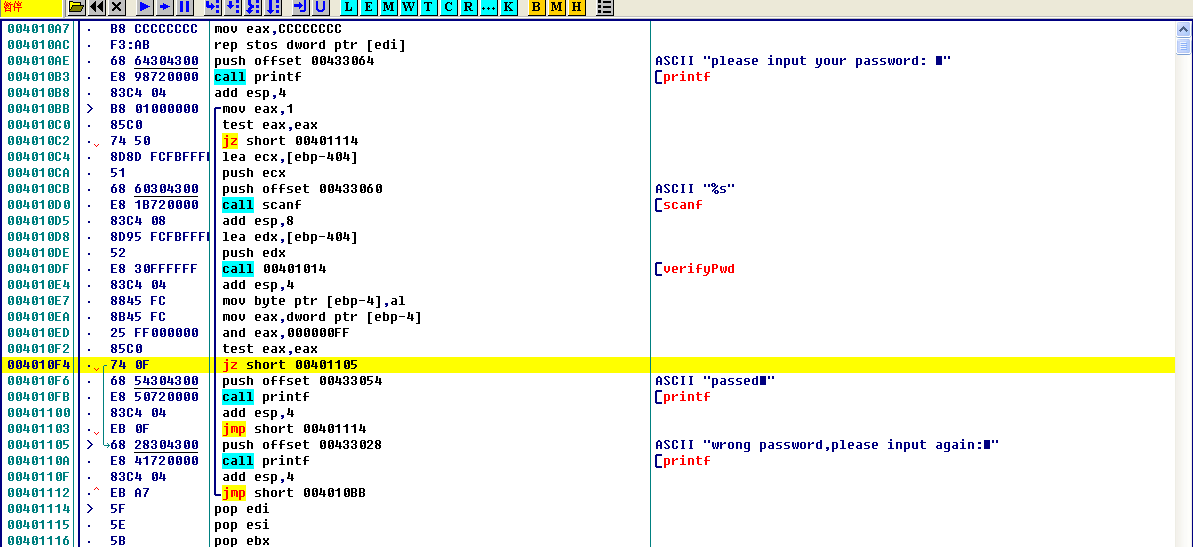
1. 在ollydbg中打开.exe文件



1. Ollydbg单步调试获取verifyPWD函数对应flag==0的汇编代码

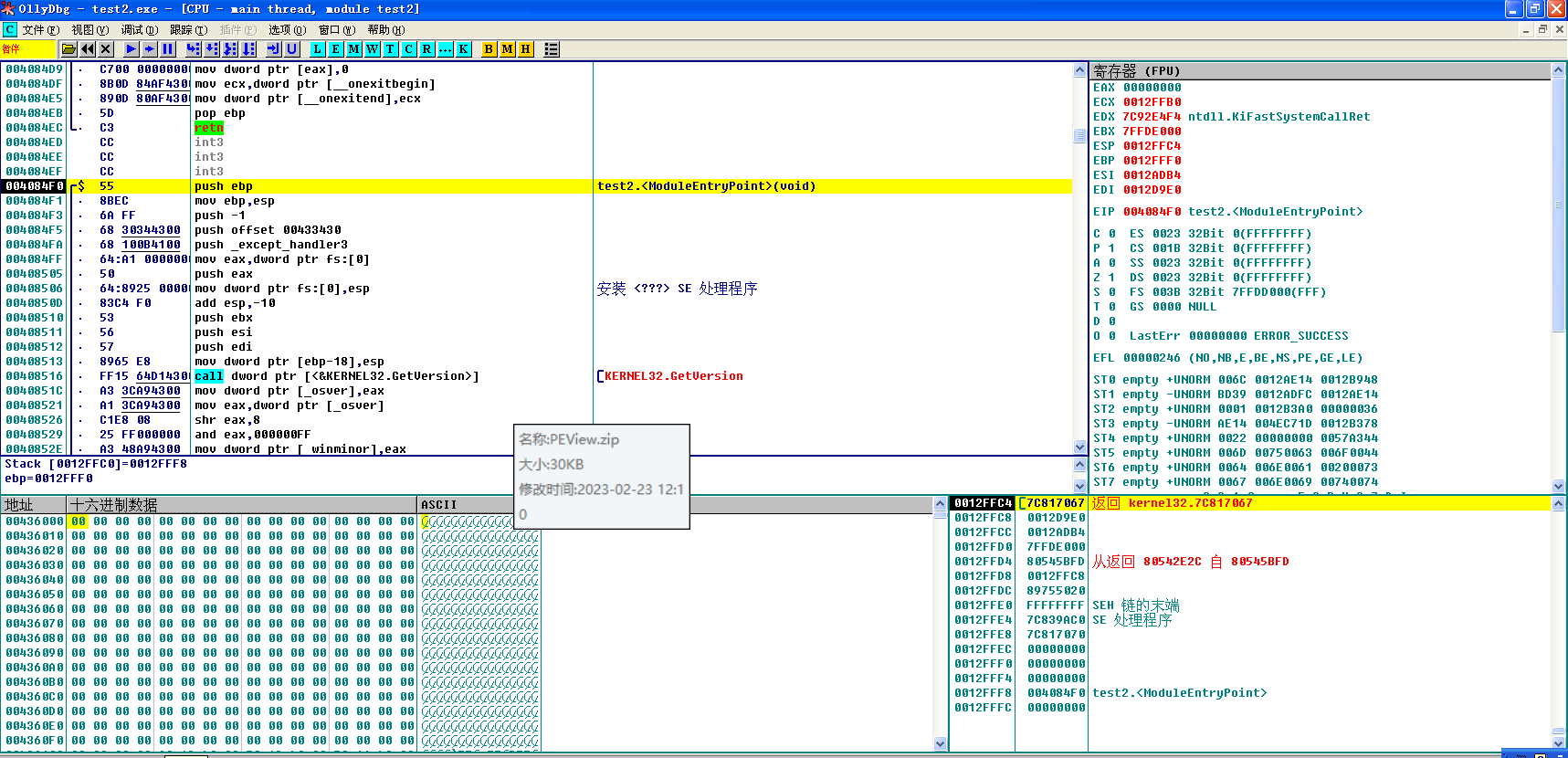


1. 解释

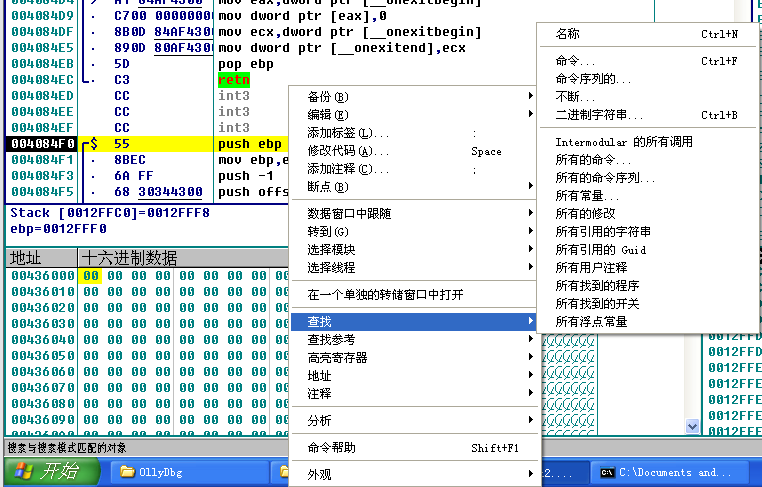


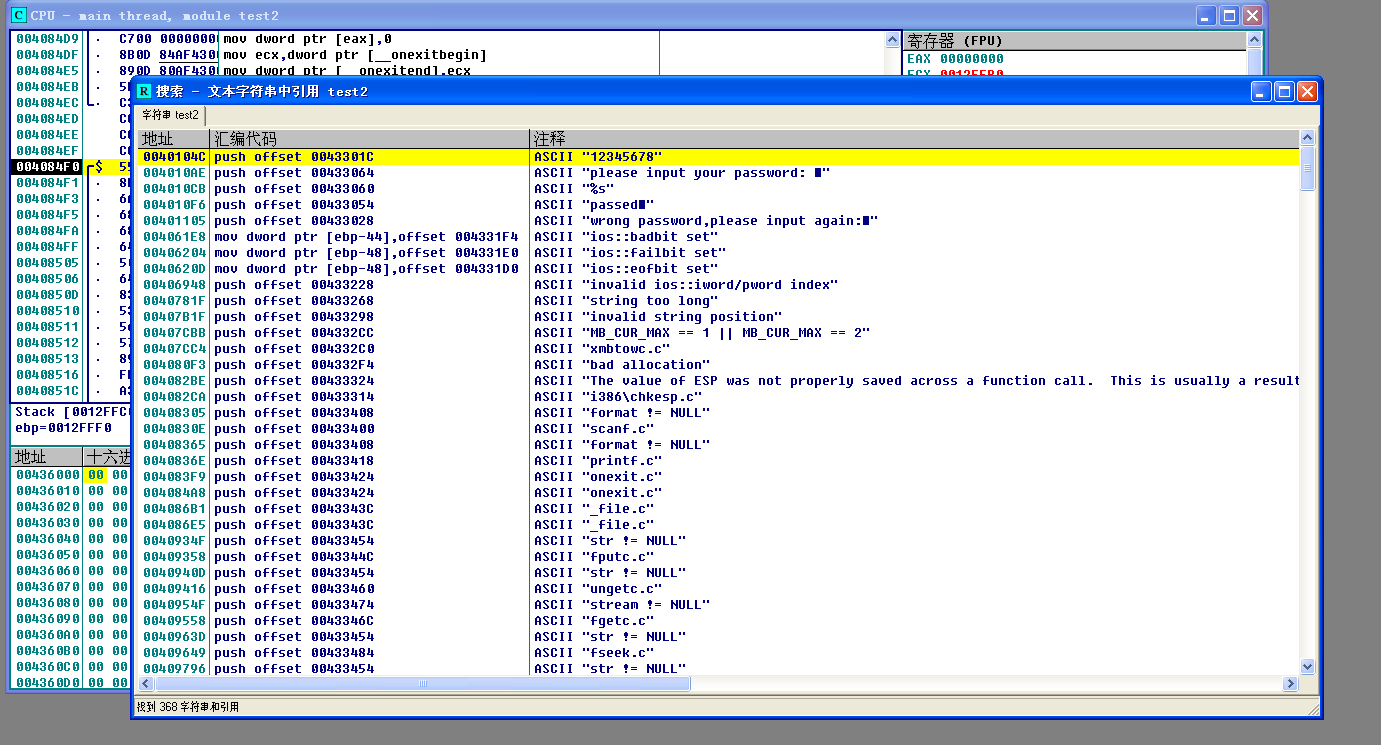
如果条件成立，即密码错误，则跳转到00401105执行，最终会输出“wrong password,please input again: ”；如果条件不成立，即密码正确，则执行下一行指令，最终会输出“passed”。

1. **要求2**
2. 在ollydbg中打开.exe文件

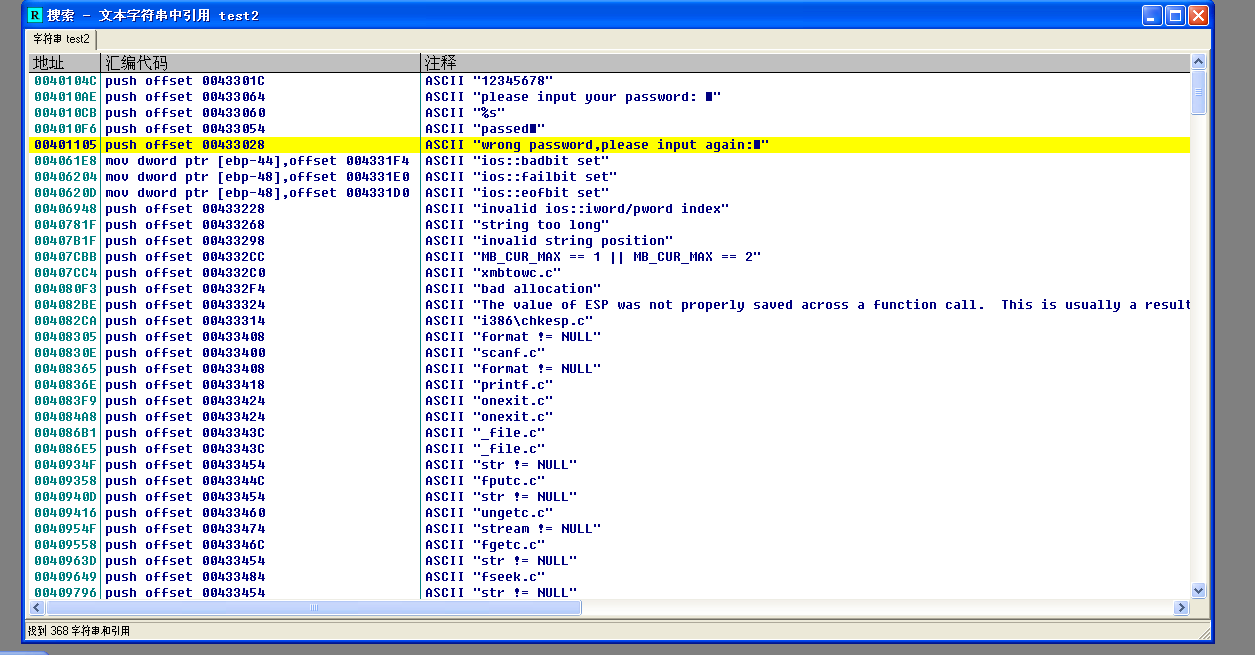


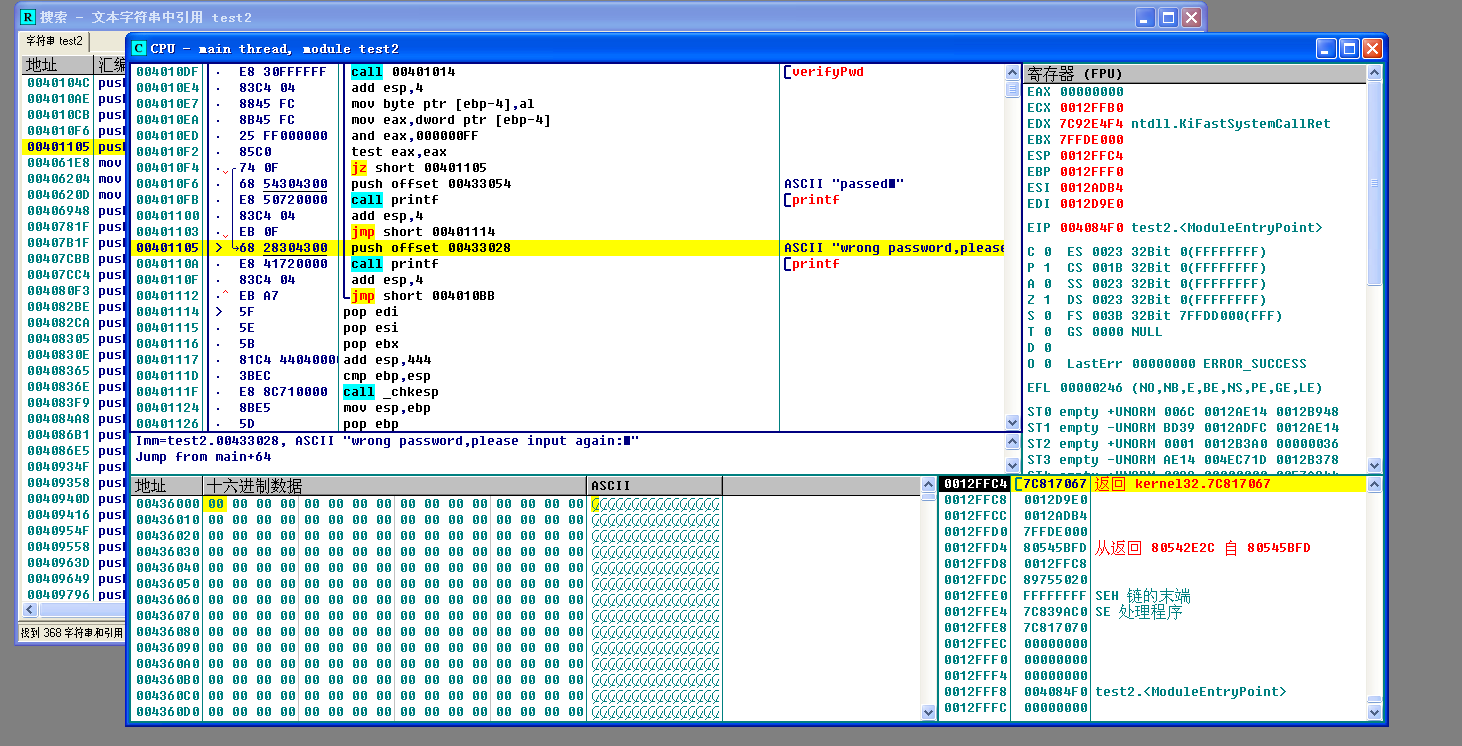
1. 右键->查找->所有引用的字符串进入搜索-文本字符串中引用，显示了所有的字符串常量信息



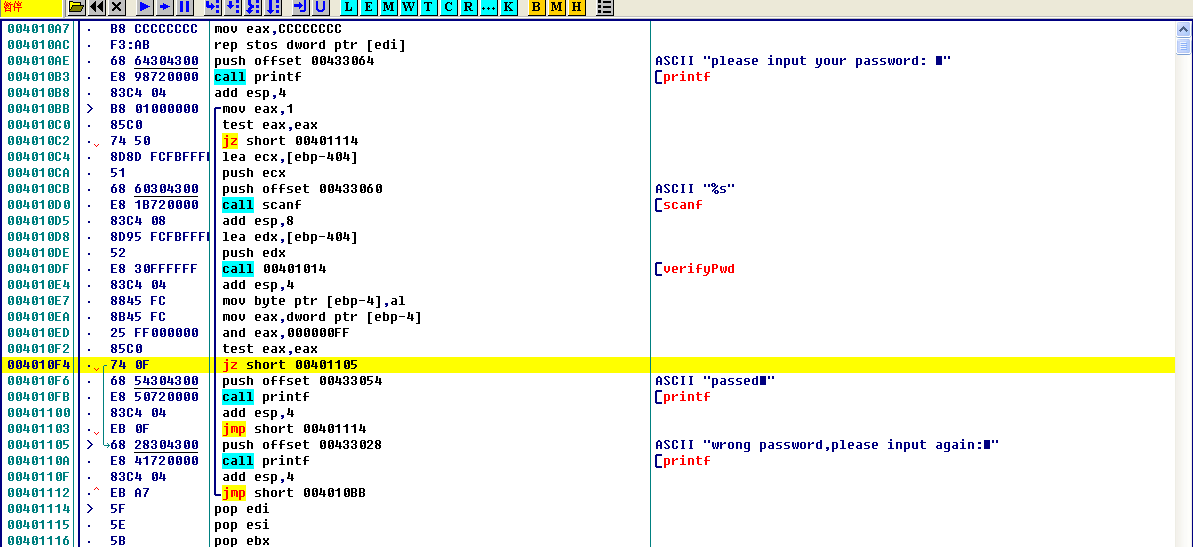


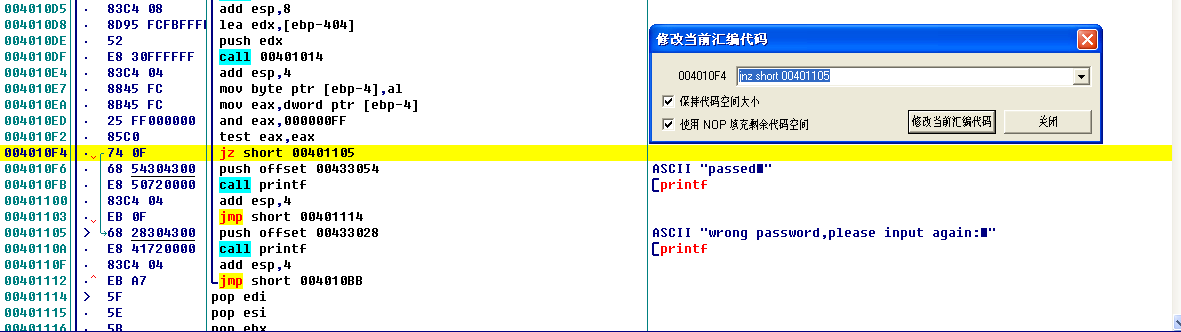
1. 双击ASCII“wrong password,please input again:”这一行，进入反汇编区域



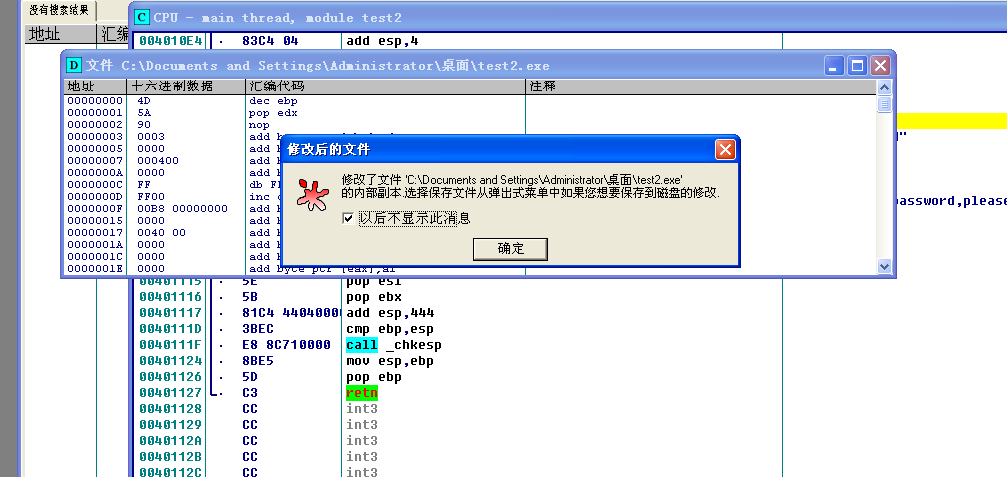


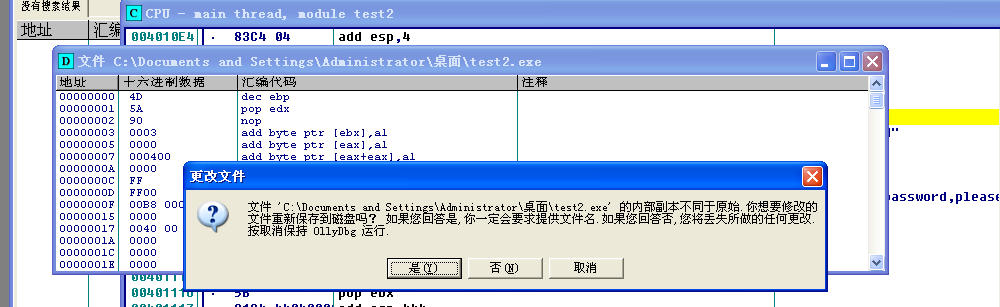
1. 双击修改这一行，修改汇编代码，将jz short 00401105修改为jnz short 00401105。变成本应该跳转到输出wrong的条件在代码更改后会变成正确的passed的条件；本应该是正确的是passed的条件在代码更改后会变成输出wrong的条件。

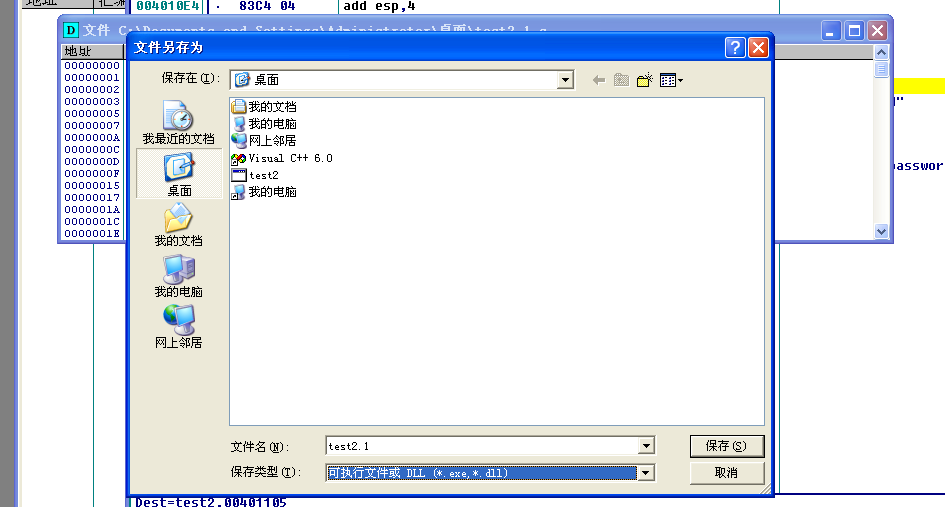




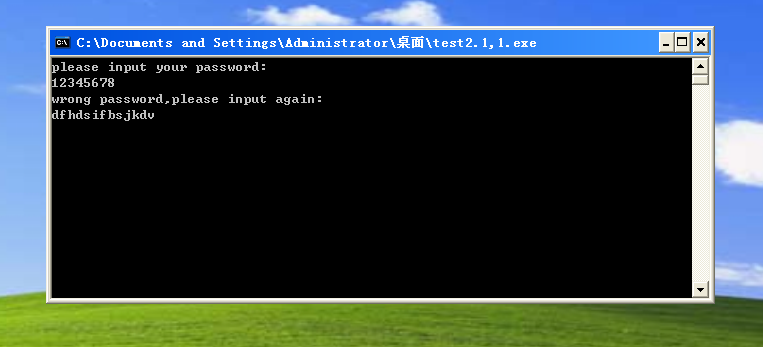
1. 右键->编辑->复制所有修改到可执行文件，然后右键->保存文件，保存为可执行文件或dll。



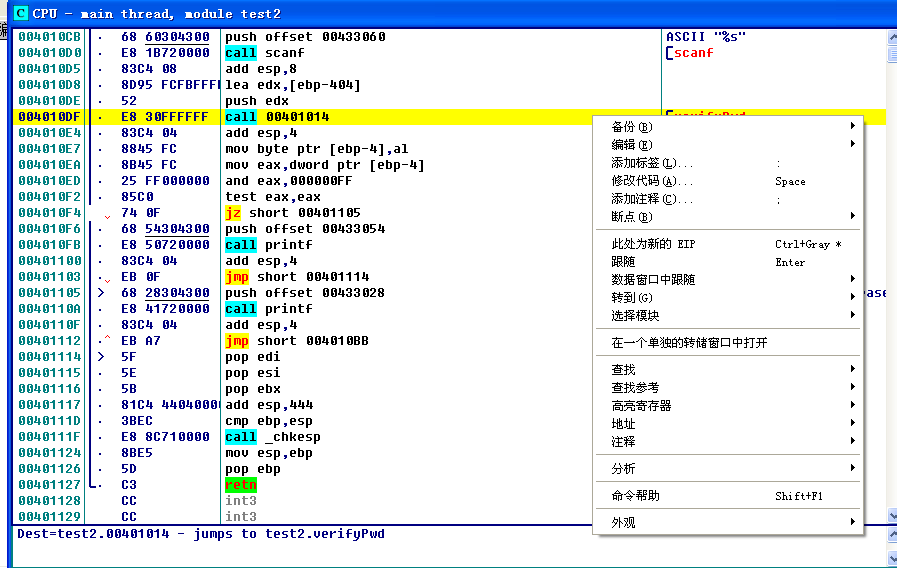


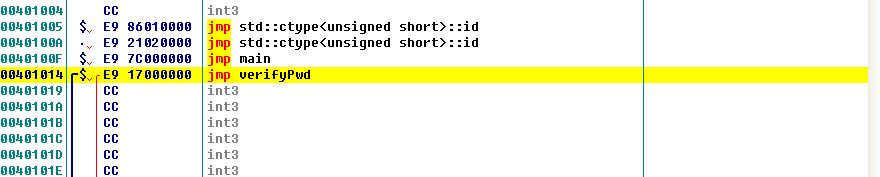


1. 运行破解方法1的.exe文件，正确的密码提示的信息是错误的，错误的密码输入后一闪而过进入，提示的信息为正确的密码。



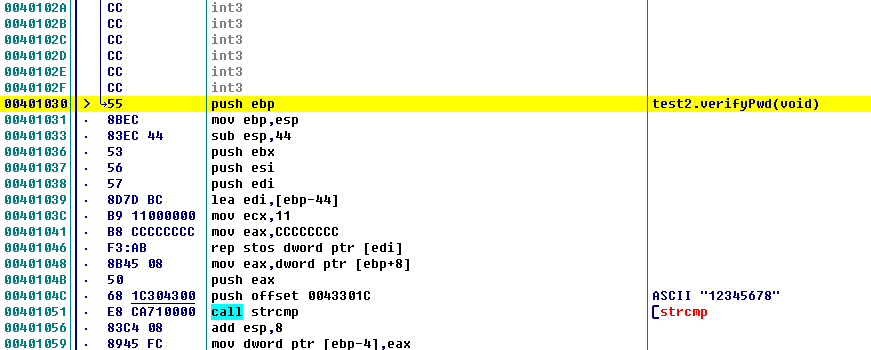
1. 恢复汇编代码，call 00401014语句右键->跟随





1. jmp verifyPwd语句右键->跟随





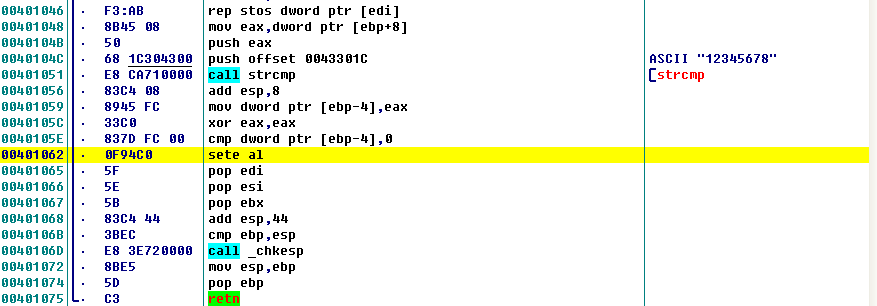
1. 返回值状态存在al中，相等可能设al为1，不相等不设al，可能为0，试图强制更改al的值。即不管什么状态，al的值总为1。

Mov dword ptr[ebp-4],eax 将strcmp函数调用后的返回值（存在eax中）赋值给变量flag

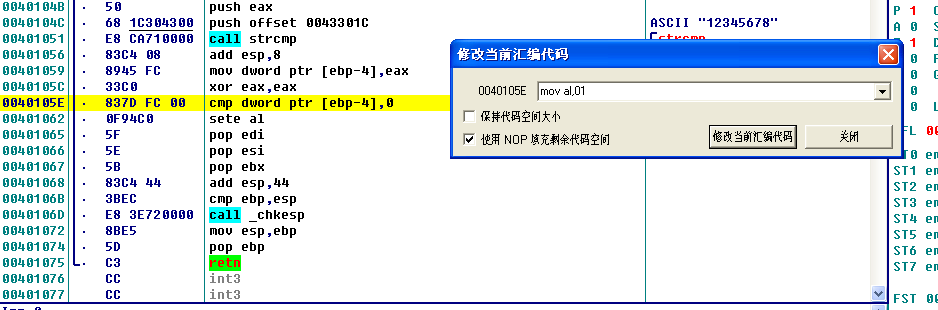
Xor eax,eax 将eax的值清空

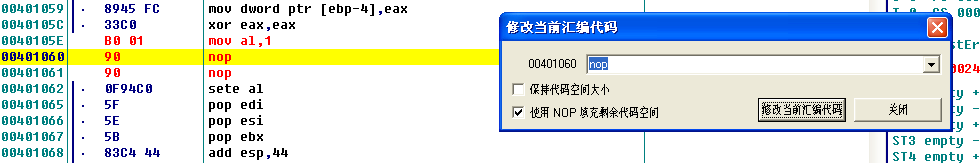
Cmp dword ptr[ebp-4],0 将flag的值与0进行比较，即flag==0；

Sete al sete是根据状态寄存器的值，如果相等，则设置，如果不等，则不设置

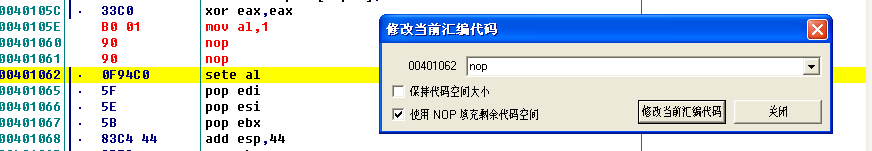


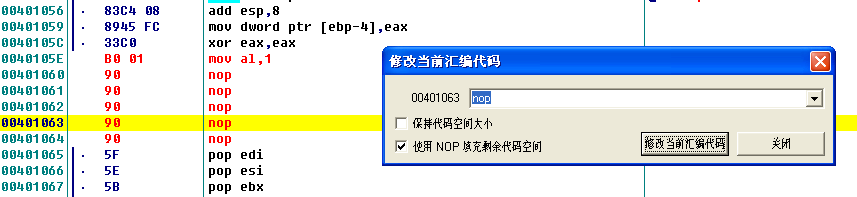
1. 双击修改语句sete al前的语句cmp dword ptr[ebp-4],0 为mov al,01，即强制更改al的值，不保存代码空间大小。如果新代码超长，将无法完成更改



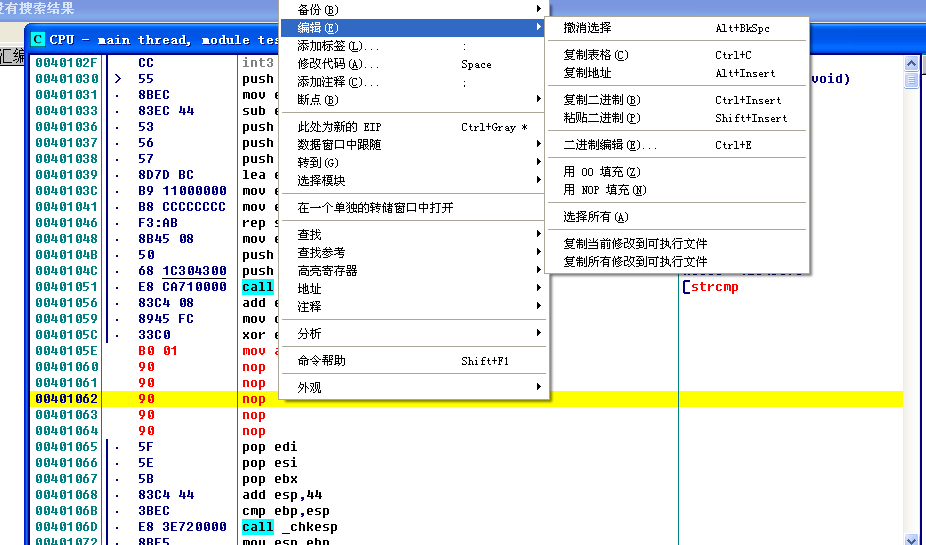


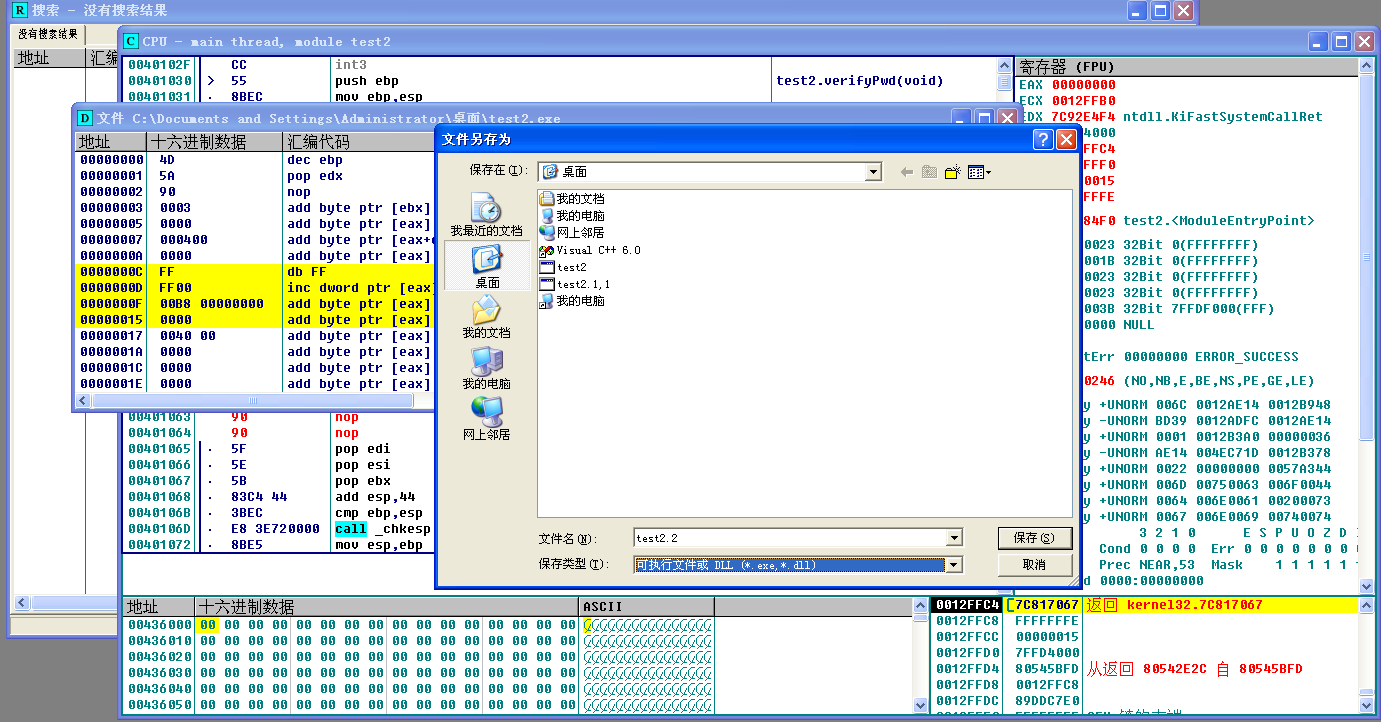
1. 把sete al语句改成空指令nop



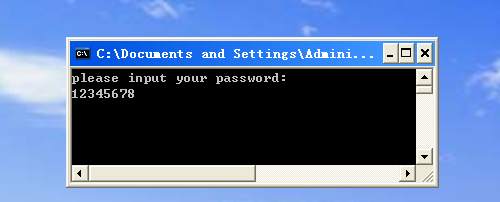


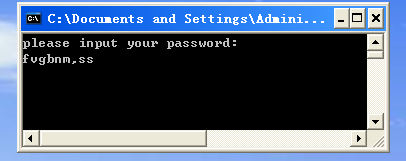
1. 右键->编辑->复制所有修改到可执行文件，然后右键->保存文件，保存为可执行文件或dll。





1. 运行破解方法2的.exe文件,原本正确的密码提示信息为正确的密码，原本错误的密码提示信息也是正确的密码





**心得体会：**

通过OllyDBG进行单步调试，获取verifyPWD函数对应的汇编代码，使用了两种方法破解密码，破解程序。初步尝试软件破解，熟悉ollydbg的一些操作，为后续实验建立基础。