《漏洞利用及渗透测试基础》实验报告

**实验名称：**

OLLYDBG软件破解。

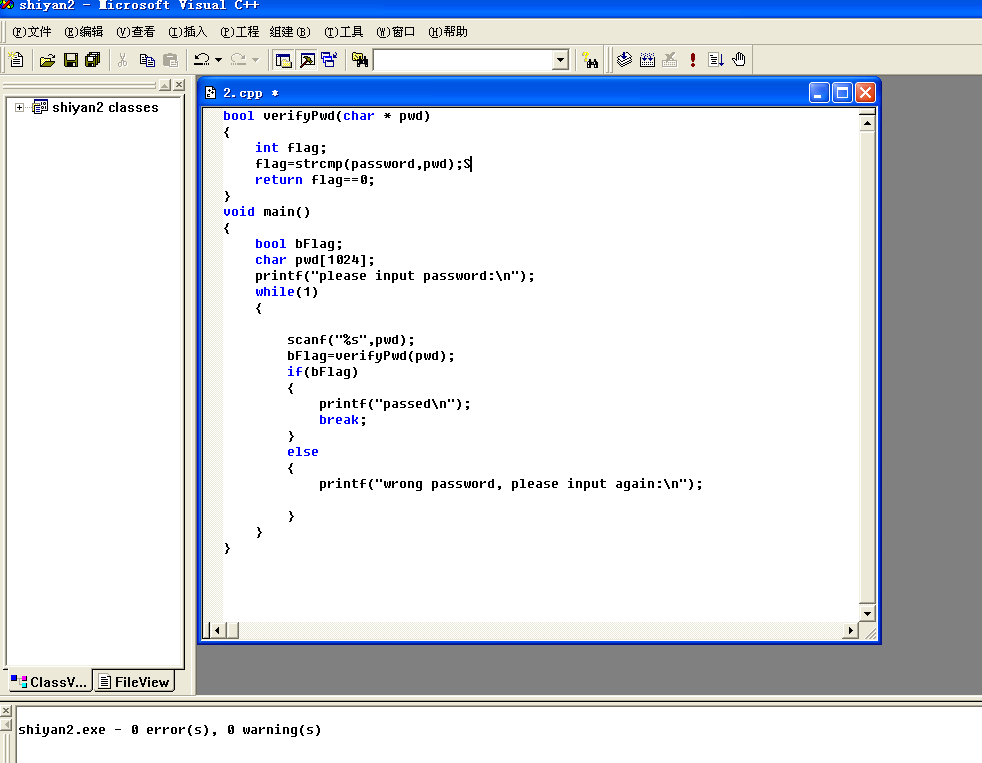
**实验要求：**

1.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。

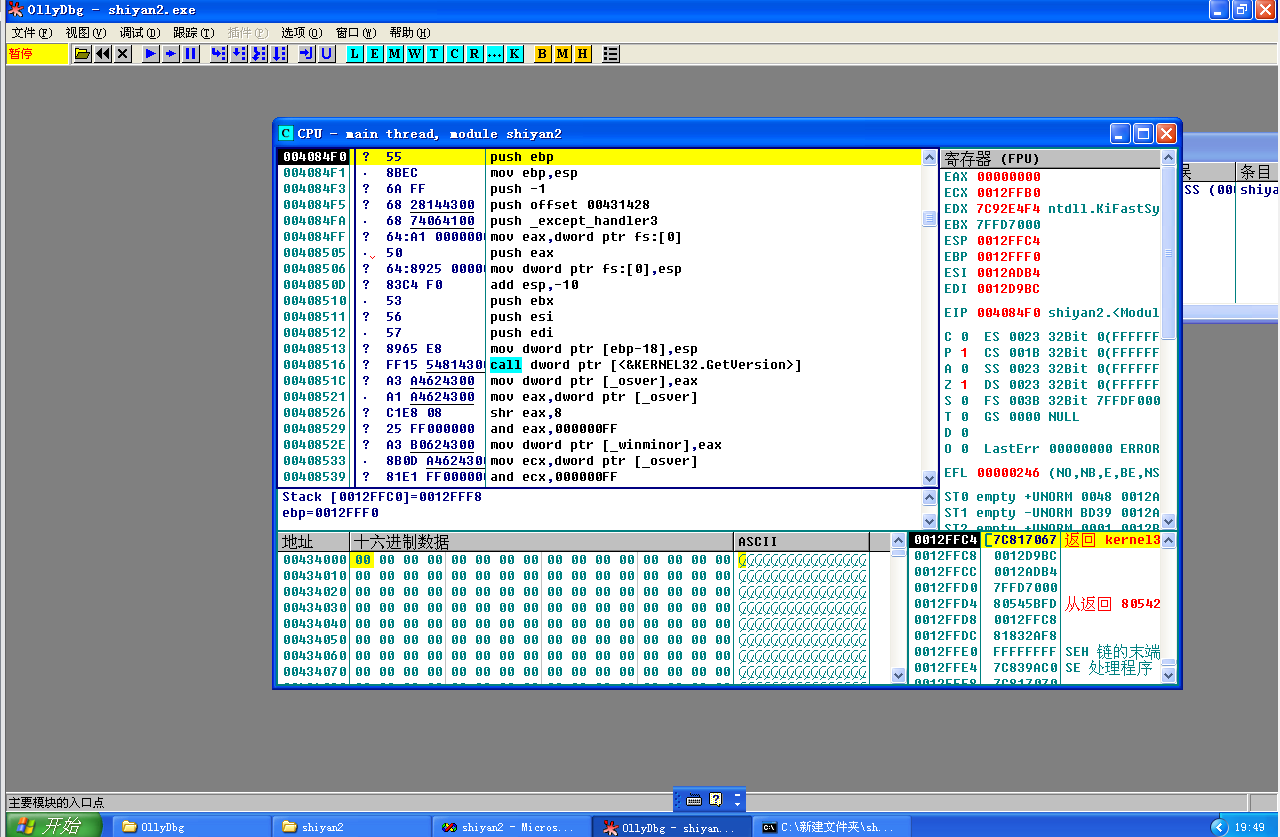
2.对生成的DEBUG程序进行破解，复现课本上提供的两种破解方法

**实验过程：**

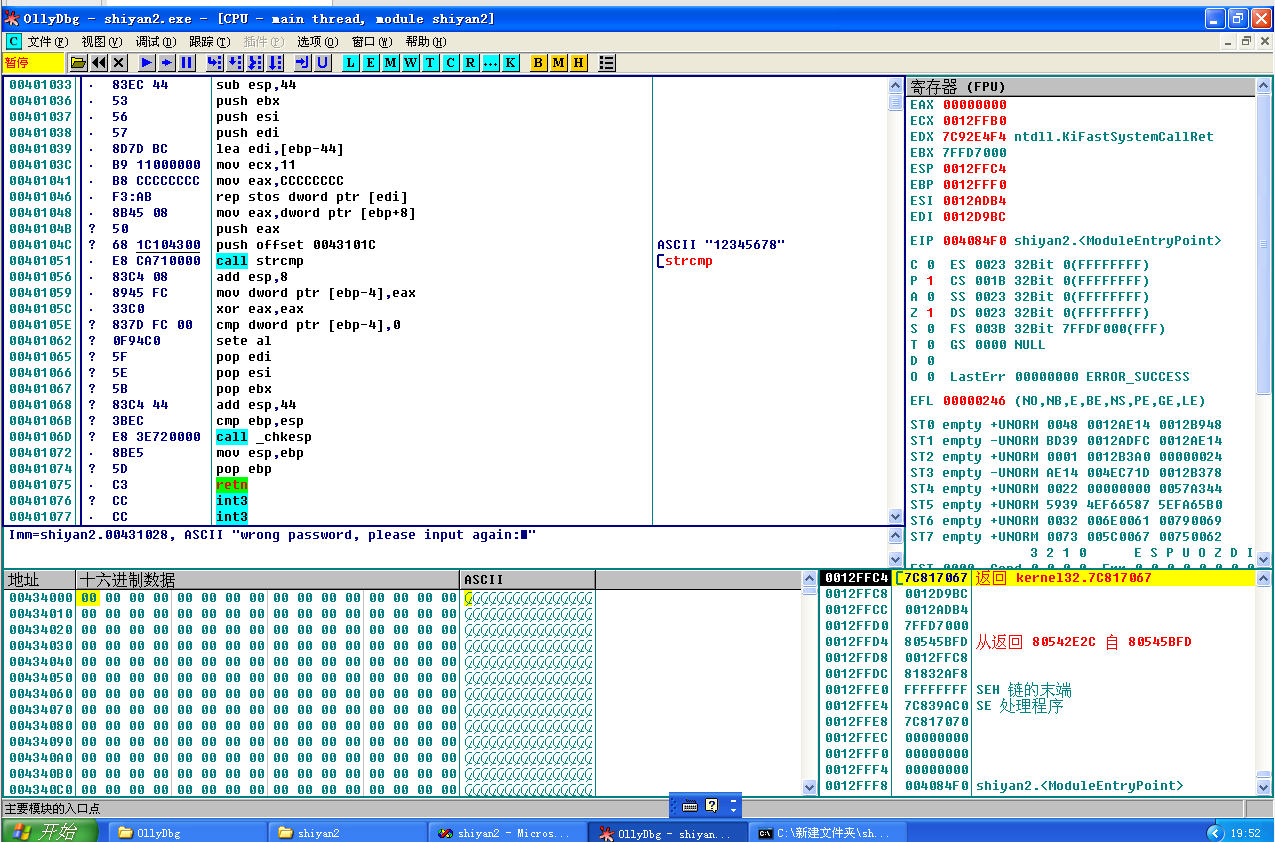
1.程序编写



2.使用OLLYDBG对程序进行调试



3.verifyPWD函数对应flag==0的汇编代码及代码解释

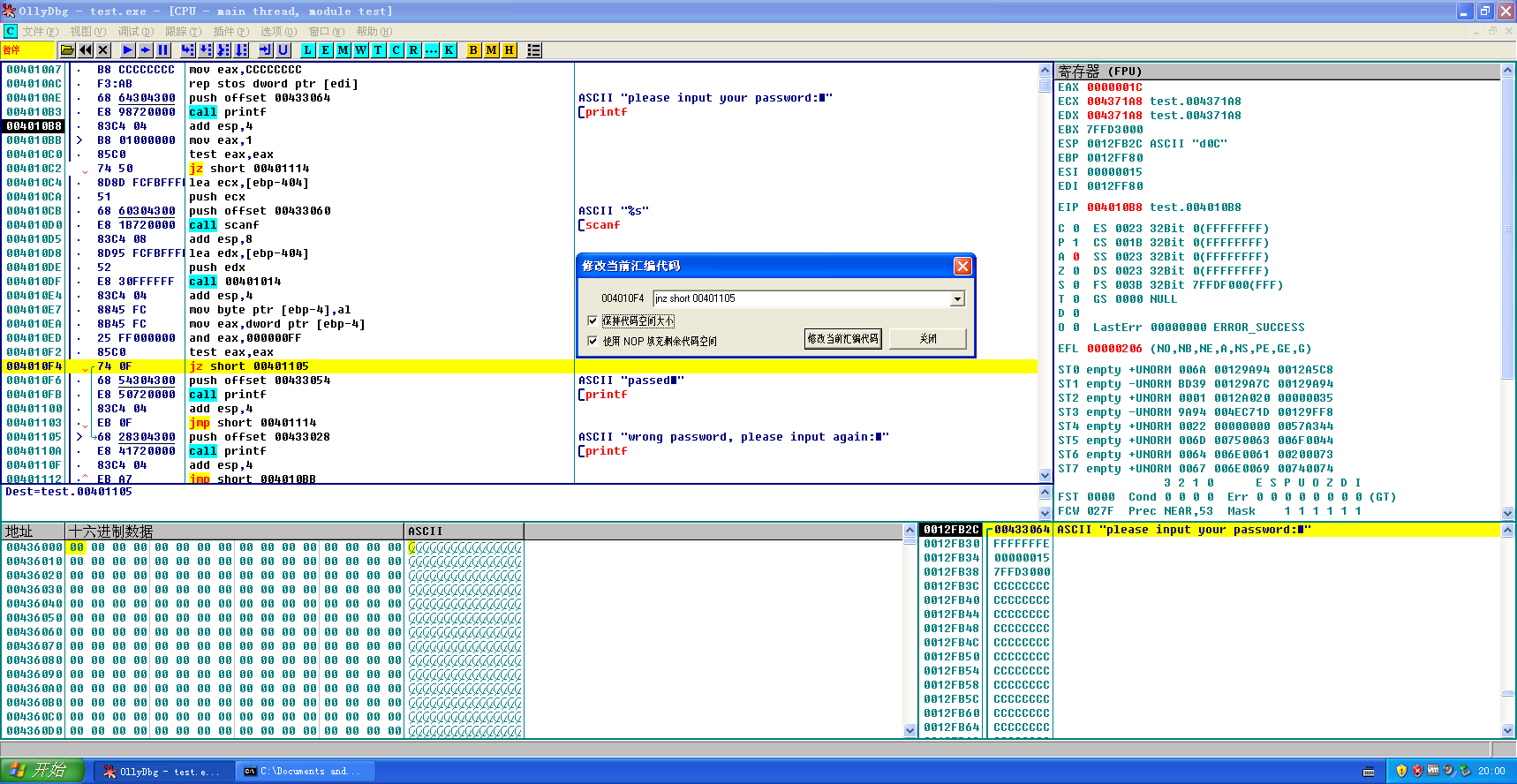


函数对应flag==0处的汇编代码首先通过“mov dword ptr [ebp–4],eax”指令将字符串比较结果存入本地变量flag中。然后“xor eax,eax”将eax寄存器清零。之后的“cmp dword ptr [ebp-4],0”将flag和0进行比较。“sete al”指令当比较结果为相等时将al置为1。

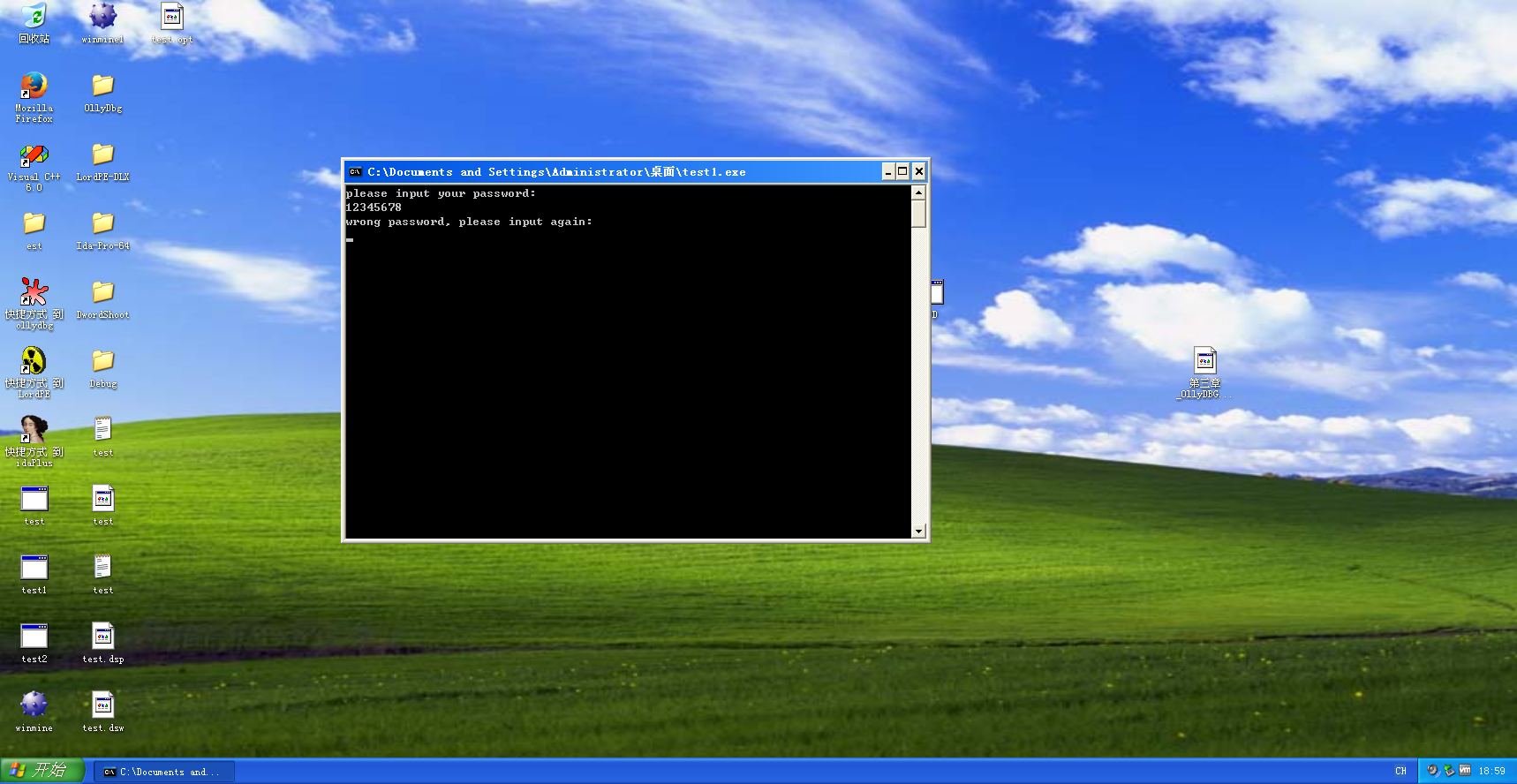
4. 按破解方法1破解程序

首先观察程序运行结果，当用户输入密码错误时程序会输出“wrong password”提示，在OllyDBG中查询此字符串，定位提示信息所在的位置，对该处代码分析。

“test eax, eax”指令对寄存器eax的值进行测试。若寄存器eax的值为0，“jz short 004001105”指令将会跳转至提示输入密码错误的分支处。因此，我们只需将“jz”修改为“jnz”即可在输入密码错误时使程序跳转至提示输入密码正确的分支

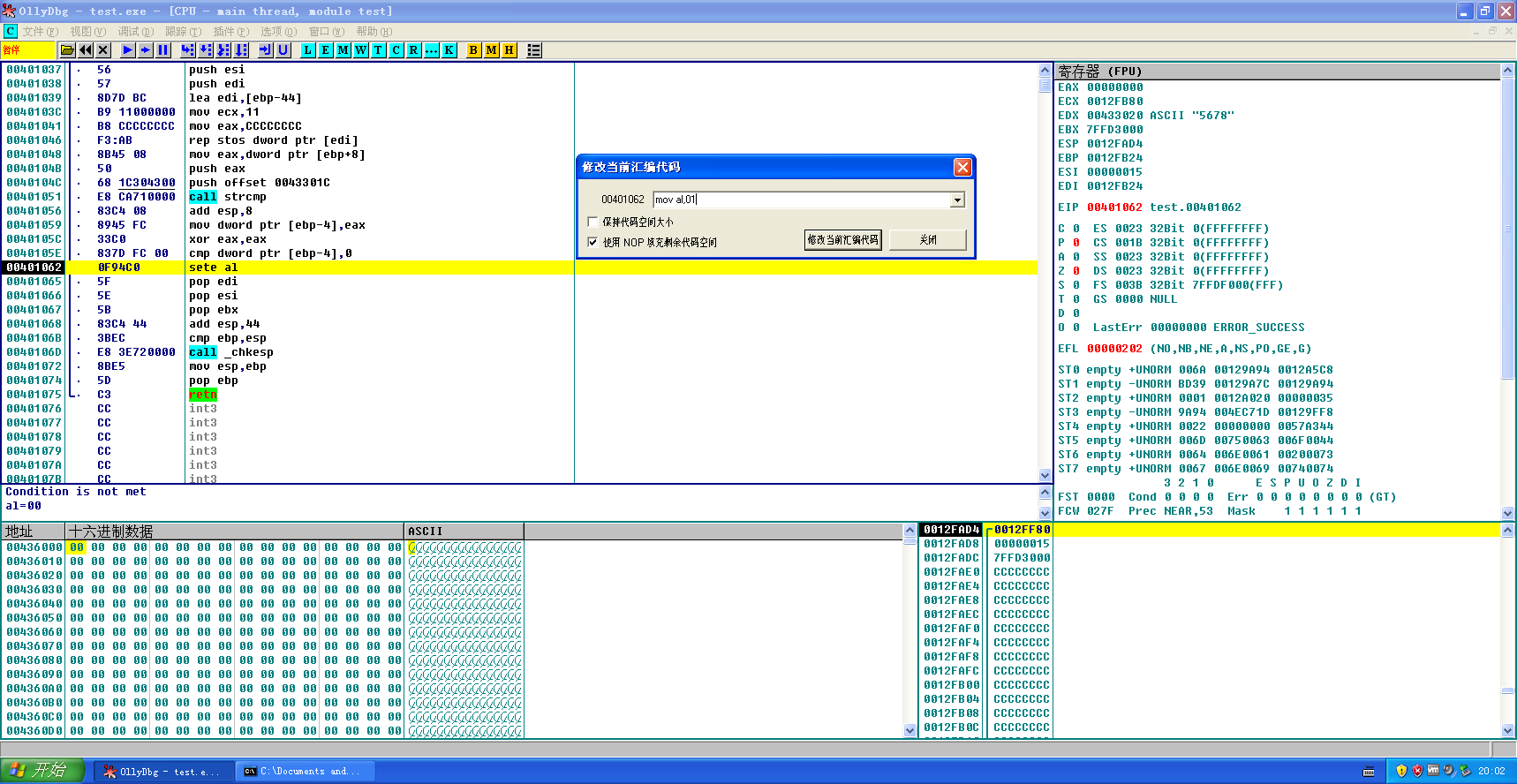


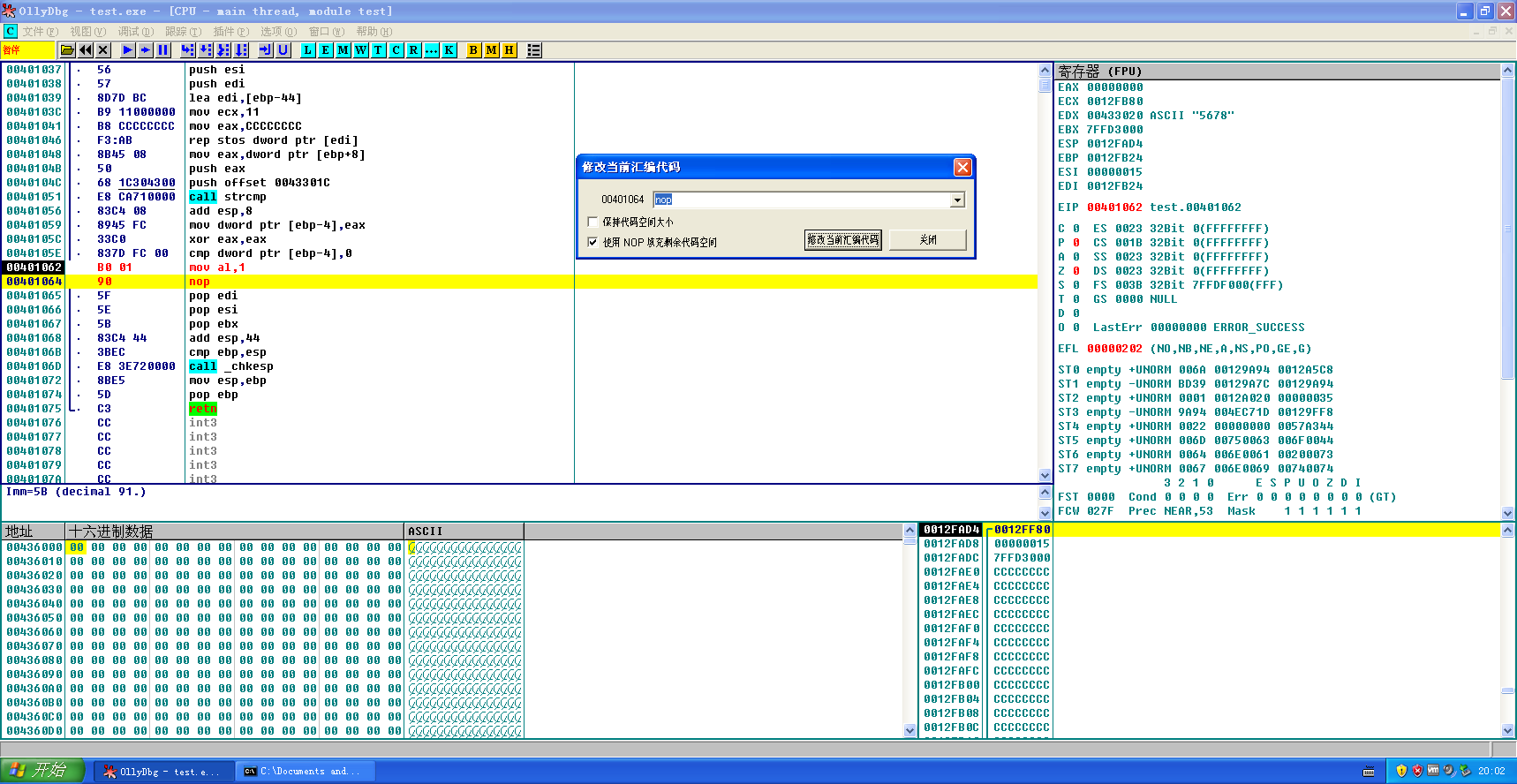
这种修改方法会使用户密码输入正确时提示密码错误。



5.按破解方法2破解程序

分析verifyPWD函数，不难发现，只需要将函数设置返回值的“sete al”指令修改为“mov al, 01”“nop”指令即可达到无论密码输入正确与否，函数均会返回表示密码正确的值1。经检验可知程序破解成功。





**心得体会：**

通过实验，学习了使用OLLYDBG调试工具对程序进行动态的调试和修改。通过实现两种不同的程序破解方法，意识到保护自己代码不被破解的困难和重要性。