《漏洞利用及渗透测试基础》实验报告

姓名：袁田 学号：2314022 班级：计科三班

**实验名称：**

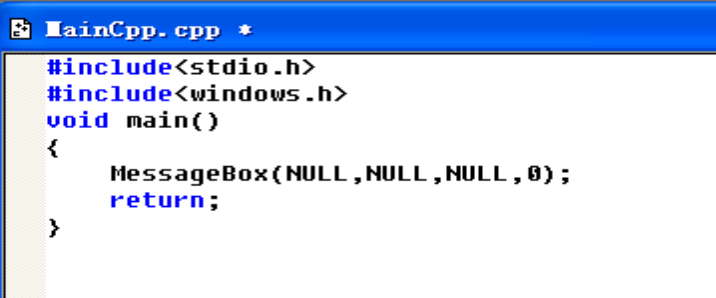
编写及提取shellcode代码

**实验要求：**

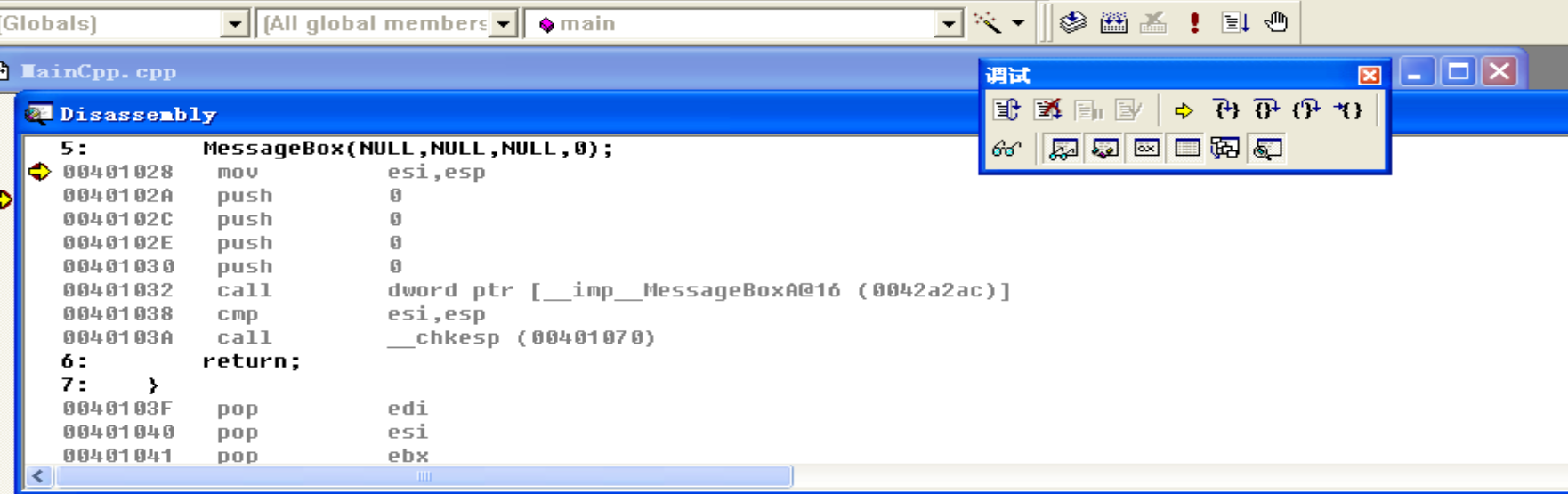
复现第五章实验三，并将产生的编码后的shellcode在示例5-4中进行验证，阐述shellcode编码的原理、shellcode提取的思想。

**实验过程：**

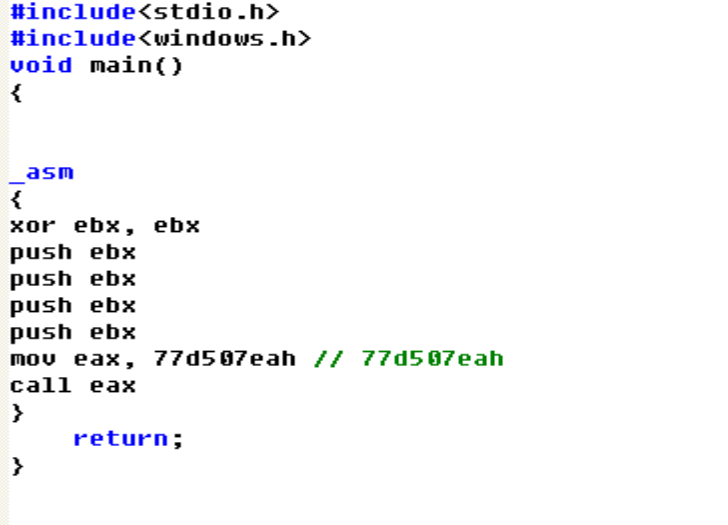
1.在VC6中编写cpp文件，并书写我们要执行的shellcode



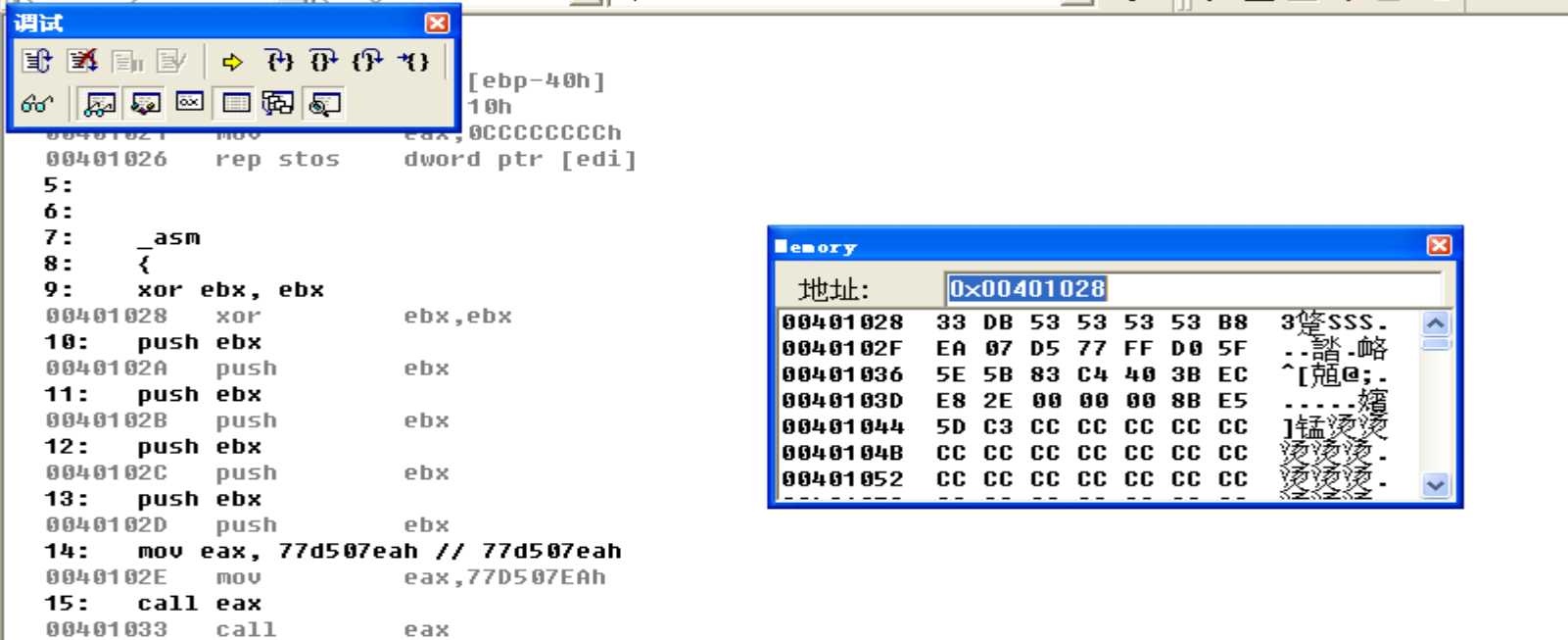
2.通过调试和反汇编，获取MessageBox对应的汇编代码



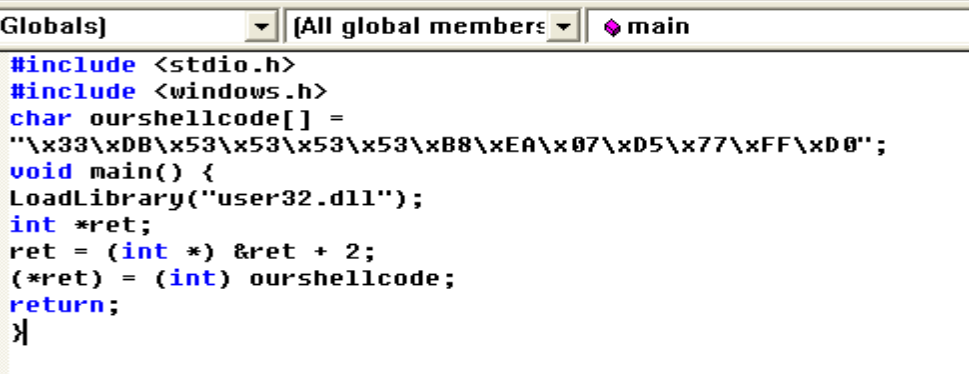
3.通过在VC6中编写汇编代码(利用\_asm语句)

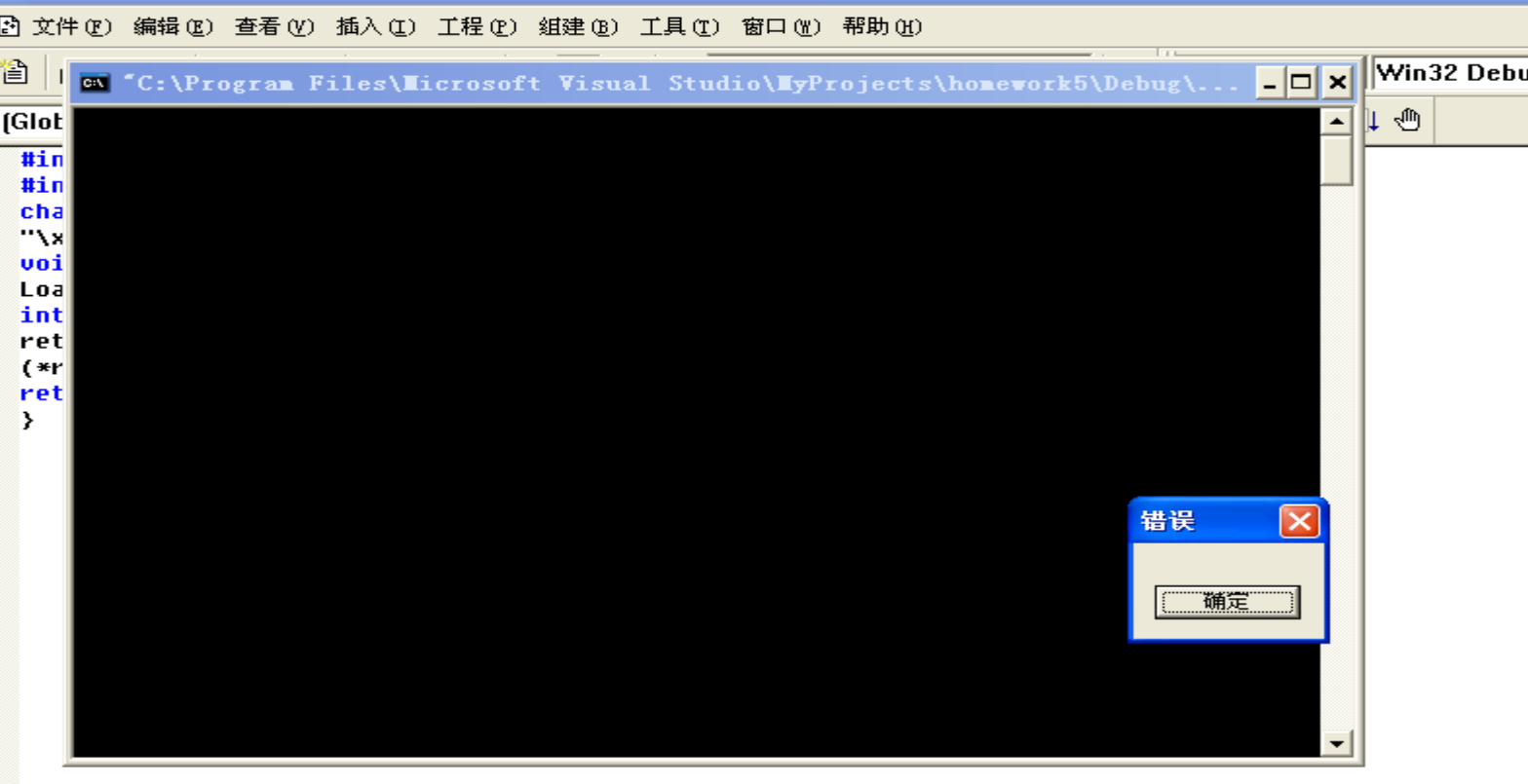


4.对修改后的代码进行调试进入反汇编，便可以获得对应的机器码



5.利用获取的机器码进行漏洞的利用





**心得体会：**

通过本次实验，我知道了Shellcode编码的主要目的是隐藏原始恶意代码的特征，使其能够绕过安全检测（如杀毒软件、IDS/IPS）或适应特定的漏洞利用环境（如避免坏字符）；并了解了该如何进行shellcode的编写，另外对于汇编语言的掌握有了提升。