《漏洞利用及渗透测试基础》实验报告

姓名：姜志凯 学号：2011937 班级：信安班

**实验名称：**

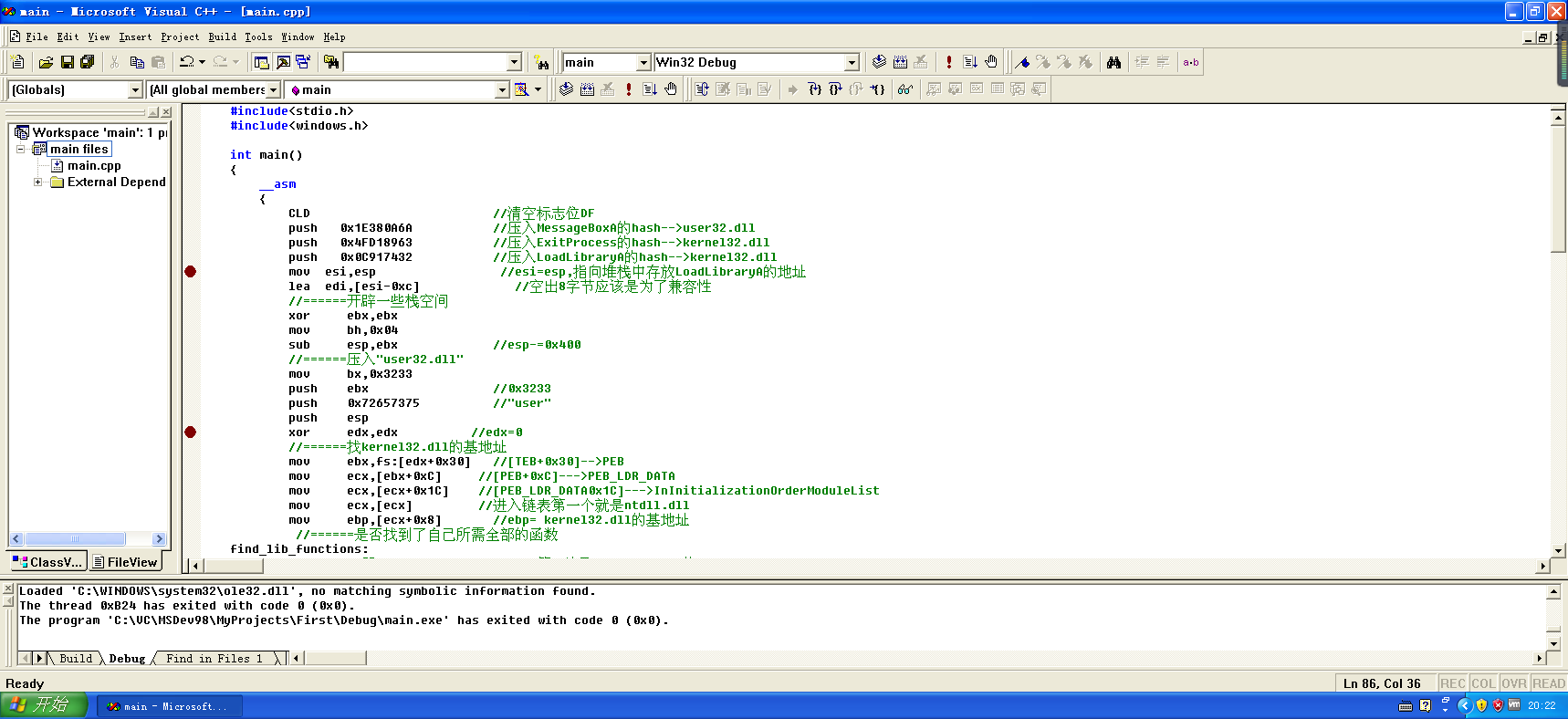
API函数自搜索实验

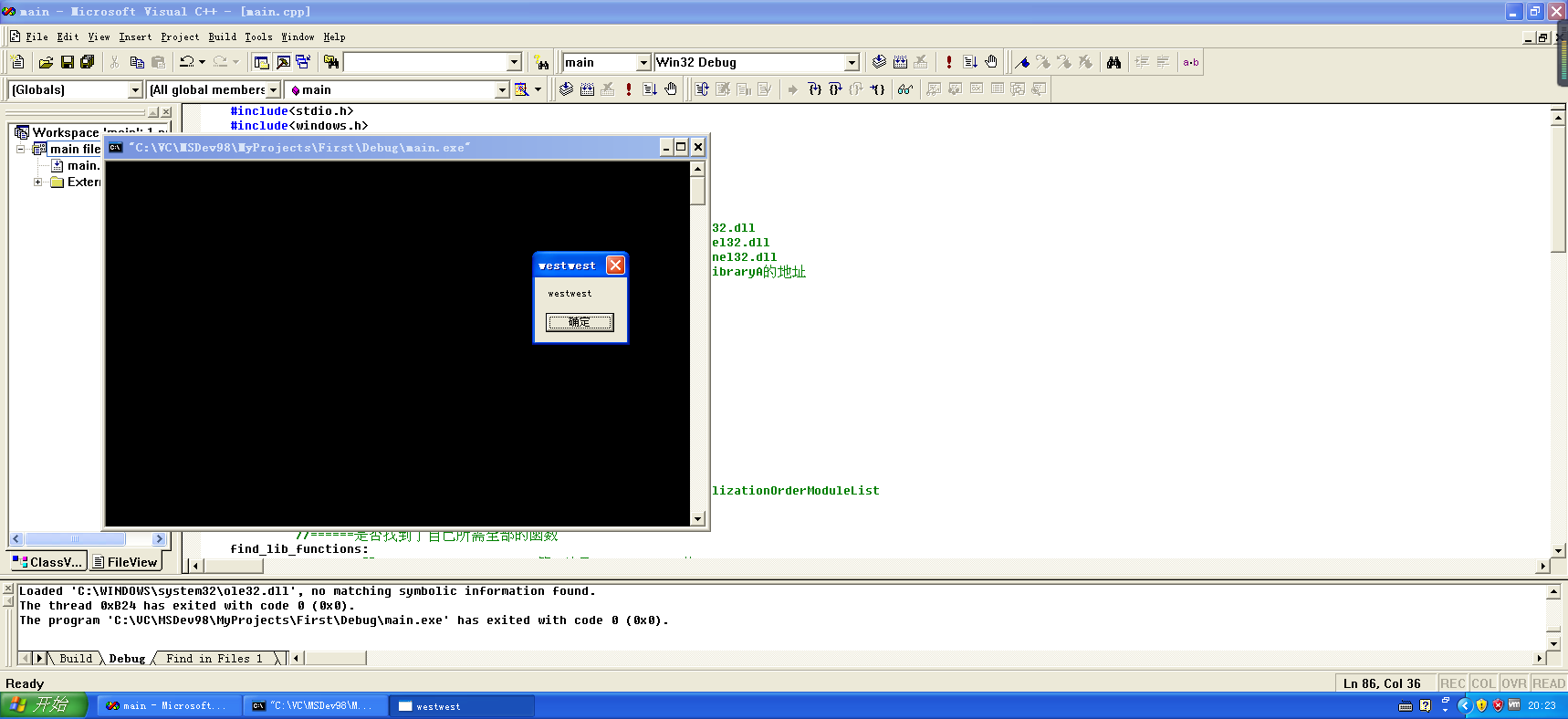
**实验要求：**

复现第五章实验七，基于示例5-11，完成API函数自搜索的实验，将生成的exe程序复制到windows 10操作系统里里验证是否成功。

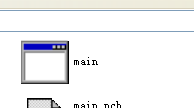
**实验过程：**

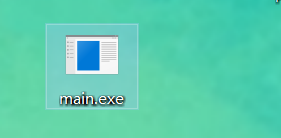
1. **打开虚拟机，打开VC++，新建程序，输入代码，并打好断点便于分析，执行，并生成exe文件**

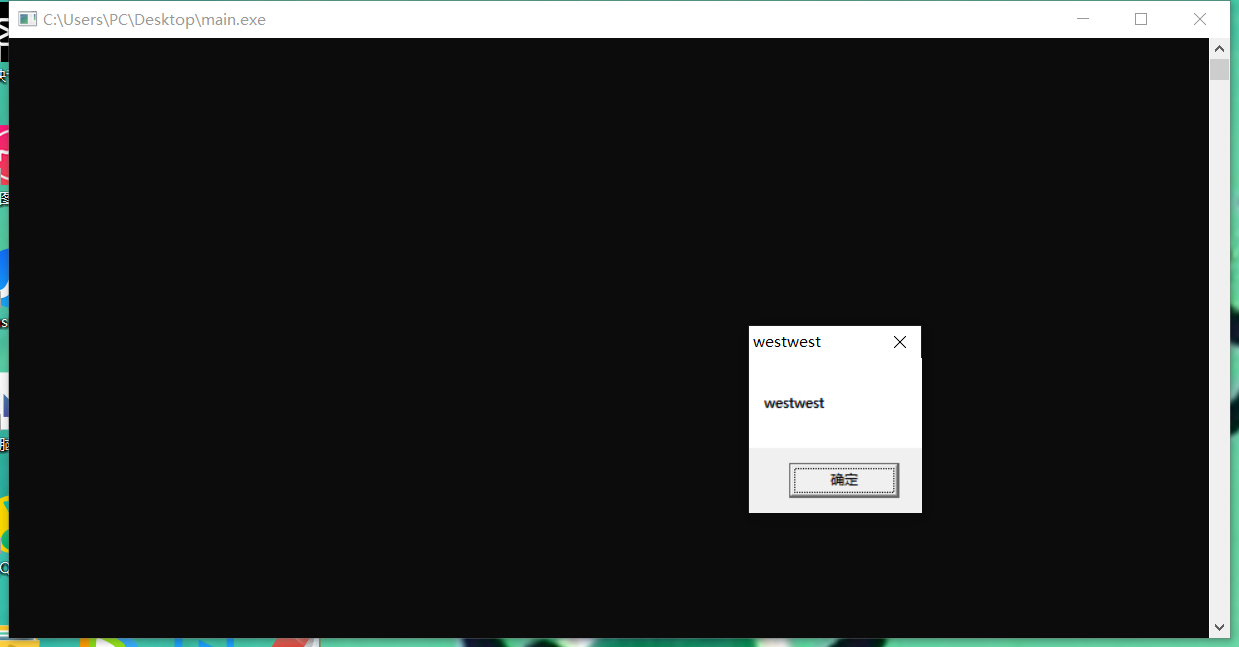




1. 将exe文件复制到win10，运行







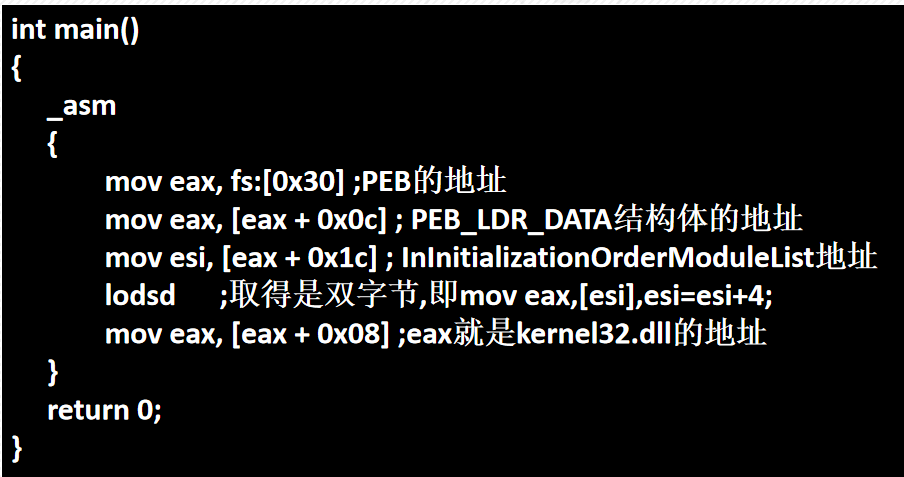
成功！

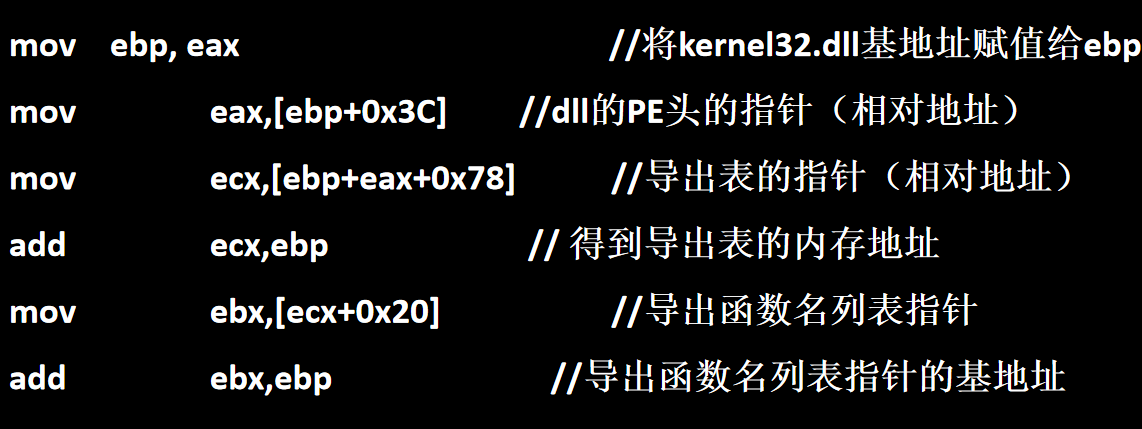
**心得体会：**

通过实验，大体了解了API函数自搜索的过程：

1. 首先，明确API函数自搜索的意义：很多的shellcode攻击时需要使用API函数，而大多数shellcode都是采用硬编址的方式调用API函数，即直接将函数地址写入shellcode。但若系统版本变化等情况出现时，API函数地址就可能发生变化，这是直接调地址就会失败。所以shellcode自身就必须具备动态的自动搜索所需API函数地址的能力，即API函数自搜索技术。
2. 编写逻辑：要得到MessageBoxA函数的地址，先要装载user32.dll，所以要先定位装载函数LoadLibrary。

①定位kernel32.dll，然后解析它的导出表，得到LoadLibrary函数。

定位kernel32.dll

解析导出表

导出表偏移0x1c处的指针指向存储导出函数偏移地址（RVA）的列表；导出表偏移0x20处的指针指向存储导出函数函数名的列表。可以通过遍历两个函数相关列表，算出所需函数的入口地址。按照这个方法，就可以获得kernel32.dll中的任意函数。

②根据user32.dll字符串地址，调用LoadLibrary函数，装载user32.dll。

③再定位user32.dll的导出表，循环比较，得到MessageBoxA的地址。

④然后就可以编写shellcode调用搜索到的API函数了。

⑤本实验还定位了程序结束函数ExitProcess，比较完整。

此外，通过本实验，掌握了多个汇编语言的用法