在每种系统中找出任意想要的动态链接库和函数的地址，C代码如下：



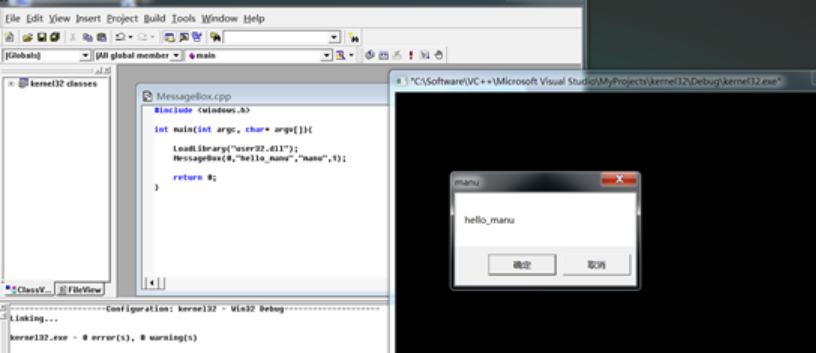
1. 注意：在不同版本的windows平台下对应的msvcrt.dll链接库地址不同，因此system函数地址也不同。

2. 系统中没有LoadLibray这个函数的，只有LoadLibraryA和LoadLibraryW这两个函数，在ASCII参数时系统会用LoadLibraryA，在Unicode参数时会用LoadLibraryW。LoadLibrary函数属于kernel32.dll，因此可找到系统中kernel32.dll链接库的地址。

windows系统弹出对话框的C代码如下：



对应的效果如下：



实验具体需要完成：

1. 实现功能：完成弹窗效果；

2. 实现方式：将以上源码组合，反汇编后，形成shellcode，而后基于c语言实现对shellcode的调用，形成弹窗；

3. 至少在windows两个以上不同的版本中完成shellcode的执行效果，从而证明shellcode的通用性。

