《漏洞利用及渗透测试基础》实验报告

姓名：沙璇 学号：1911562 班级：信息安全

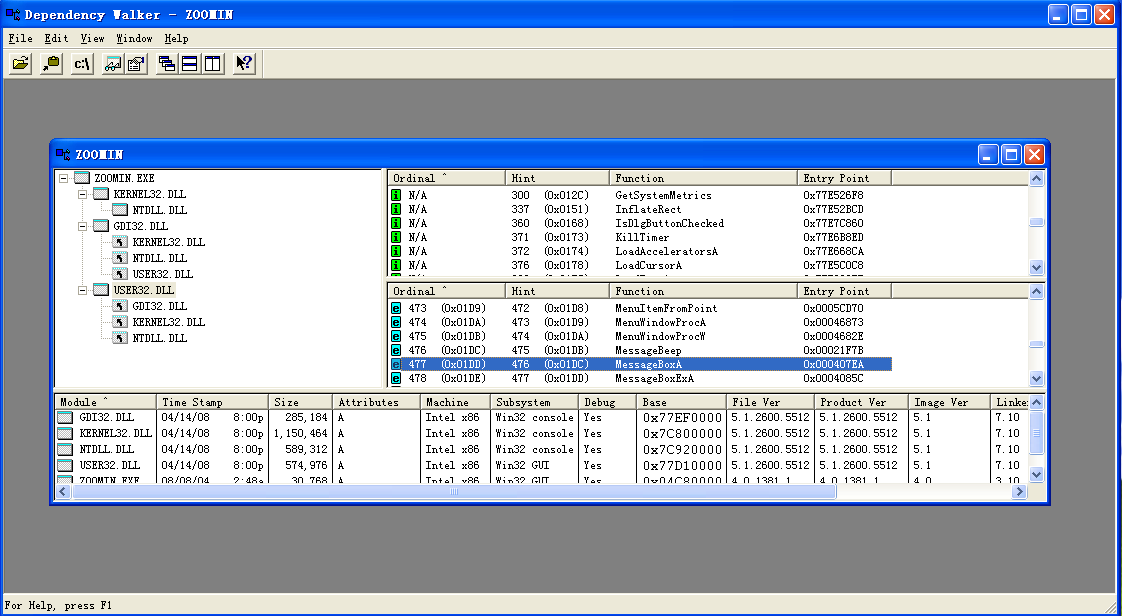
**实验名称：**

Shellcode编写及编码

**实验要求：**

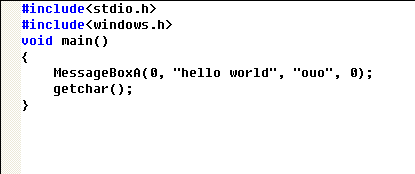
复现第五章实验三，并将产生的编码后的shellcode在示例5-1中进行验证，阐述shellcode编码的原理、shellcode提取的思想。

**实验过程：**

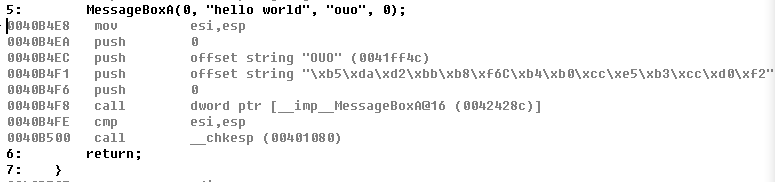
1.基于工具来获得函数入口地址。

2.使用内联汇编语言编写函数

编写hello world函数如下：



其对应的汇编代码为：



获取字符串（hello world）地址：

（1）MsgBox标题：ouo --> \x6F\x75\x6F

（2）MsgBox内容：helloworld--> \x68\x65\x6c\x6c\x6f\x20\x77\x6F\x72\x6c\x64

四个字符一组进行压栈（空缺的地方用空格\x20）：

（1）MsgBox标题：ouo --> push 0x206F756F

（2）MsgBox内容：hello world -->push 0x20646c72

push 0x6f77206f

push 0x6c6c6568

因为esp指针始终指向栈顶位置，在字符串压栈后，栈顶位置压入的是字符串，所以用esp指针可以指向所需的字符串

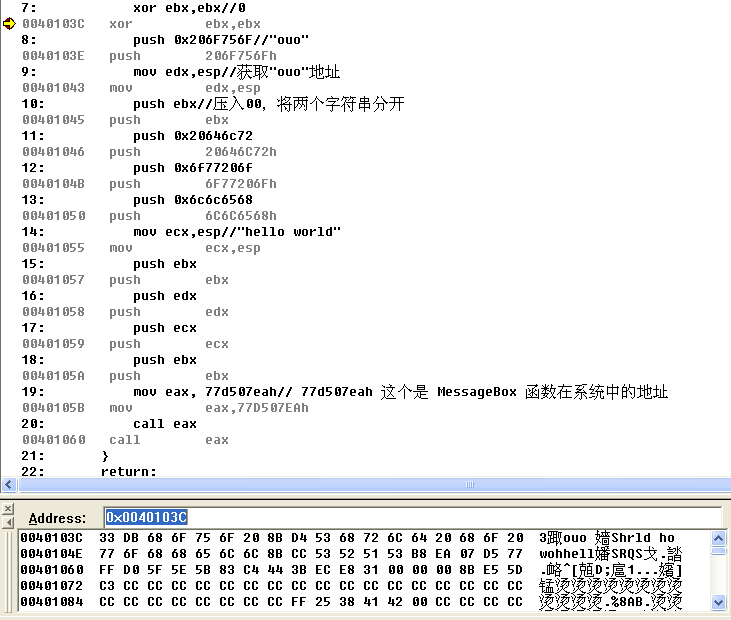
修改后得到的汇编代码如下：



执行后弹出窗口：

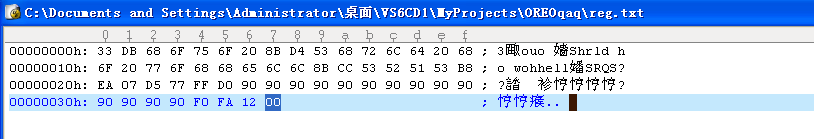
说明汇编代码正确

3. 汇编代码-->机器码:

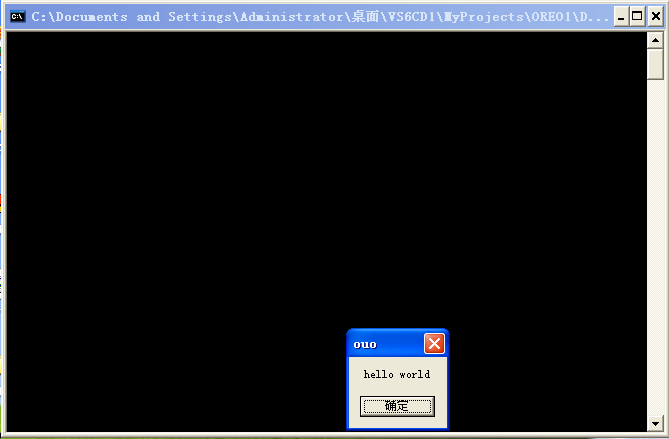


即33 DB 68 6F 75 6F 20 8B D4 53 68 72 6C 64 20 68 6F 20 77 6F 68 68 65 6C 6C 8B CC 53 52 51 53 B8 EA 07 D5 77 FF D0 （Buffer地址：0012faf0）

4.编辑reg.txt



5.执行exe后弹出窗口



**心得体会：**

1.shellcode编码原理：Shellcode实际是一段代码（也可以是填充数据），是用来发送到服务器利用特定漏洞的代码，一般可以获取权限。另外，Shellcode一般是作为数据发送给受攻击服务的。 Shellcode是溢出程序和蠕虫病毒的核心。

2.shellcode提取思想：采用高级语言编写程序🡪获取汇编指令🡪获取机器码。