《漏洞利用及渗透测试基础》实验报告

姓名： 学号： 班级：

**实验名称：**

IDE反汇编实验

**实验要求：**

根据第二章示例2-1，在XP环境下进行VC6反汇编调试，熟悉函数调用、栈帧切换、CALL和RET指令等汇编语言实现，将call语句执行过程中的EIP变化、ESP、EBP变化等状态进行记录，解释变化的主要原因。

**实验过程：**

1. 进入VC反汇编

~~~~~~~

2. 观察add函数调用前后语句

~~~~~~~

3. add函数内部栈帧切换等关键汇编代码

（此处根据实际操作过程，留下具体操作步骤、附加一些自己的理解，即可）

**心得体会：**

通过实验，掌握了RET指令的用法；

RET指令实际就是执行了Pop EIP

此外，通过本实验，掌握了多个汇编语言的用法