<参考答案见视频源码下载>

1、练习如下操作：

1) 创建空项目

2) 添加一个CPP文件，并在文件中填写入口函数和头文件

3) F7编译 然后去文件夹查看是否成功生成.exe文件

4) F5运行

2、指出下面的函数名哪些是错误的：

int、5new、while、do、L+3、\_5、c++、A-5、A.B.C、#123、char

错误的是int,5new,while,do, L+3, c++, A-5, A.B.C, #123, char

3、在函数调用处下断点，抄写函数的汇编框架。

#include<stdio.h>

int plus(int x,int y)

{

return 0;

}

void main()

{

plus(1,2); //下断点 F11跟进去 抄写plus函数的反汇编框架 要求理解每一行

return;

}

Push 2 传入参数

Push 1 传入参数

Call 401005 函数调用

Add esp,8 外平栈

Jmp 401020 中转

函数

Push ebp 保存ebp

Mov ebp,esp 提升ebp

Sub esp,40h 提升esp

Push ebx 保存ebx

Push esi 保存esi

Push edi 保存edi

Lea edi,[ebp-40h] 初始edi的值,把ebp-40h地址给edi

Mov ecx,10h 循环寄存器ecx,循环10h

Mov eax,0CCCCCCCCh 填充eax,为0CCCCCCCCh

Rep stos dword ptr [edi] 循环将 **eax** 中的数据传送到目的地址edi中

Xor eax,eax 是异或运算，两数相反为1；两数相同为0。由于这两个数相同，异或后等于清0由于它比mov eax,0效率高，所以一般用它！,return 0所以这么做

Pop edi 取回edi

Pop esi 取回esi

Pop ebx 取回ebx

Mov esp,ebp 恢复esp

Pop ebp 取回ebp

Ret 函数返回