**同济大学计算机系**

**操作系统实验报告**

****

**学 号 2152809**

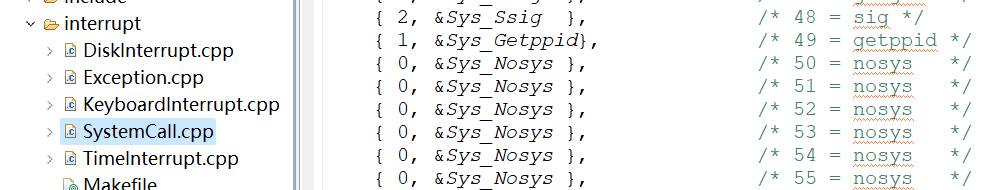
**姓 名 曾崇然**

**专 业 计算机科学与技术**

**授课老师 方钰老师**

**一. 添加新的系统调用接口**

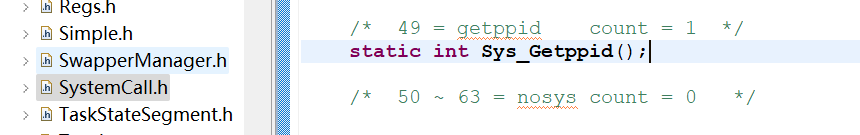
**（1）修改系统调用处理子程序入口表**



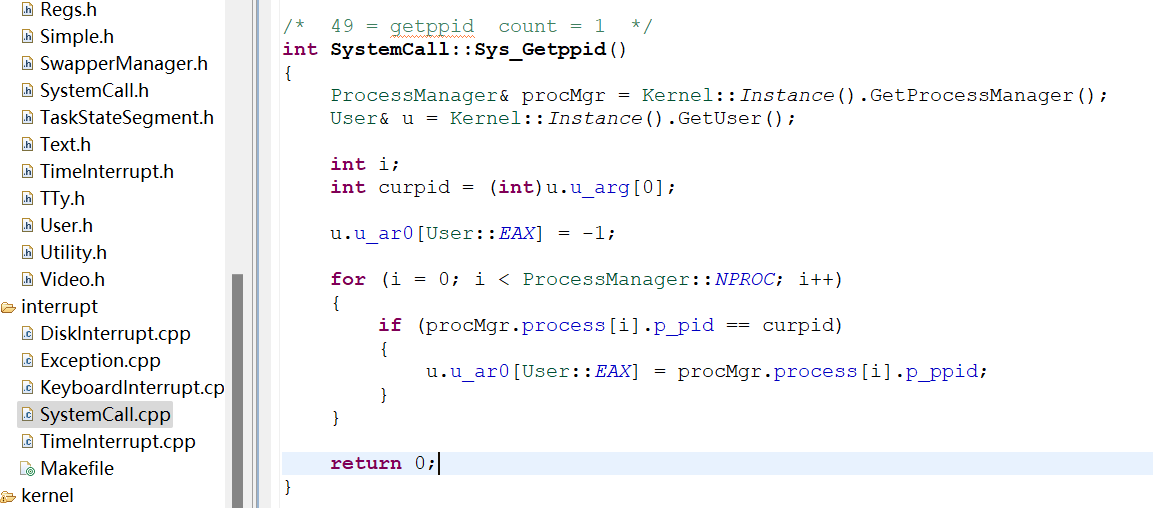
{0, &Sys\_Nosys}项表示该入口未被使用，将其替换为所要添加的{1, &Sys\_Getppid}，1表示参数，&Sys\_Getppid表示系统调用处理子程序的入口地址。此处为所要新增的系统调用添加了入口。

**（2）添加系统调用处理子程序的声明和定义**

在SystemCall.h中添加声明：

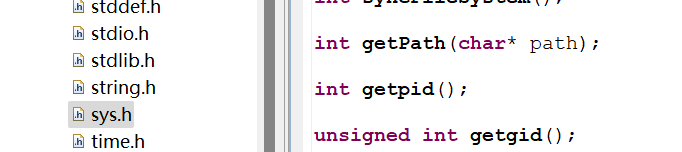


在SystemCall.cpp中添加定义：

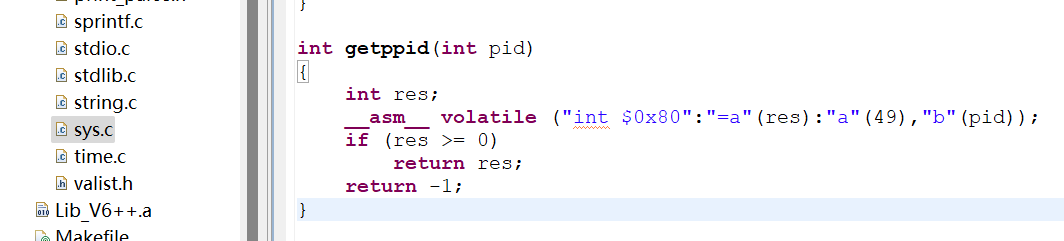


**二. 为新的系统调用添加新的库函数**

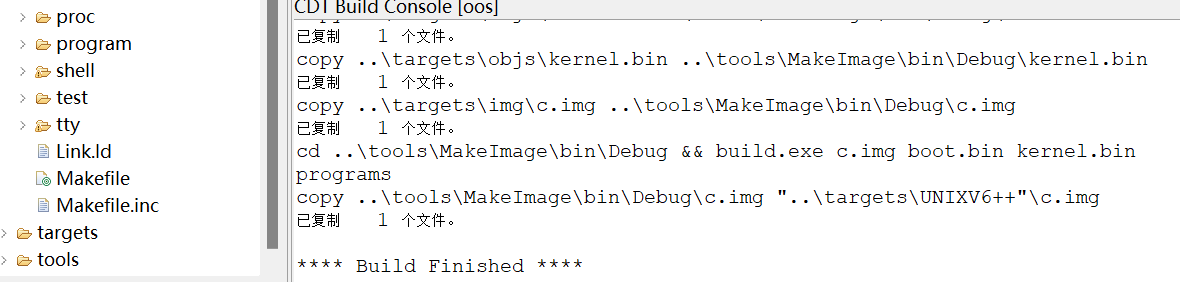
**（1）添加库函数的声明**



**（2）添加库函数的定义**



**（3）进行编译**

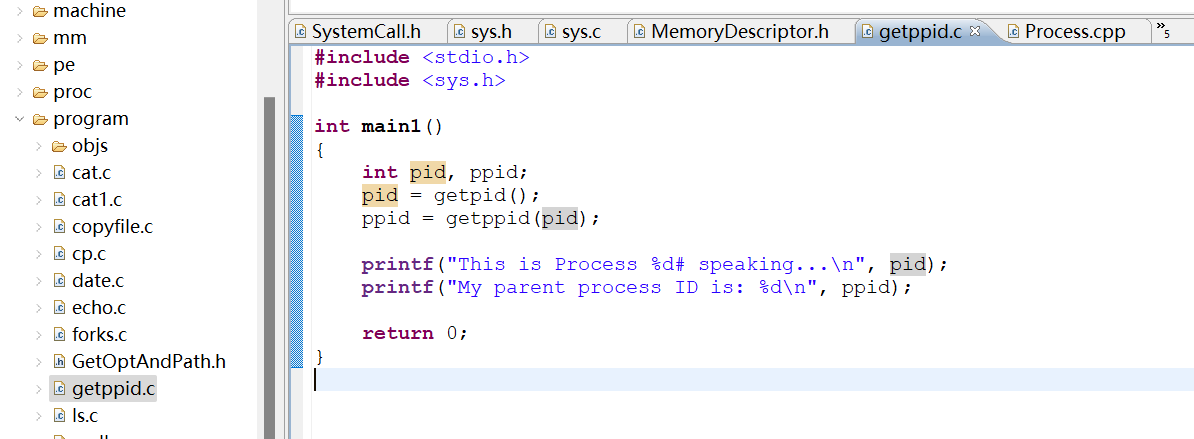


编译成功，系统调用处理子程序和对应的库函数添加成功

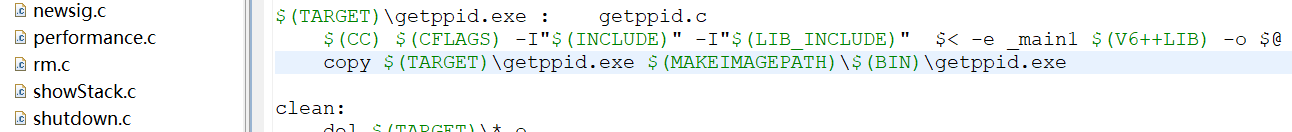
**三. 添加测试程序进行测试**

**（1）添加代码并编译生成程序**

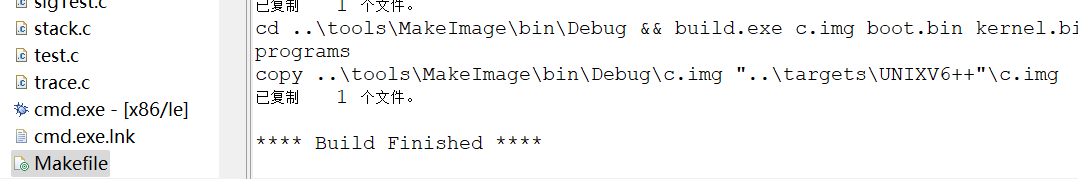
添加代码：



修改配置文件：

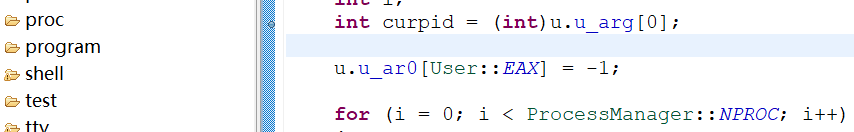


编译生成：

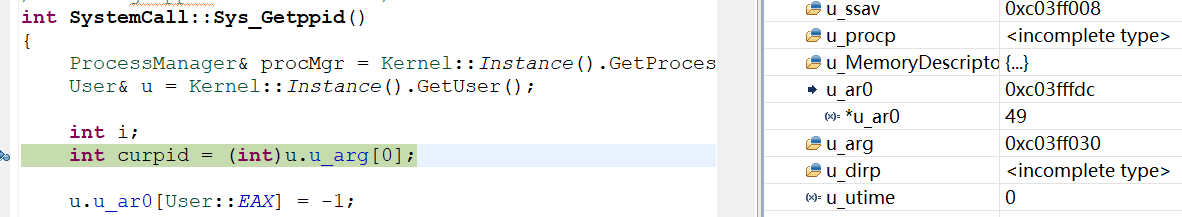


**（2）运行和调试**

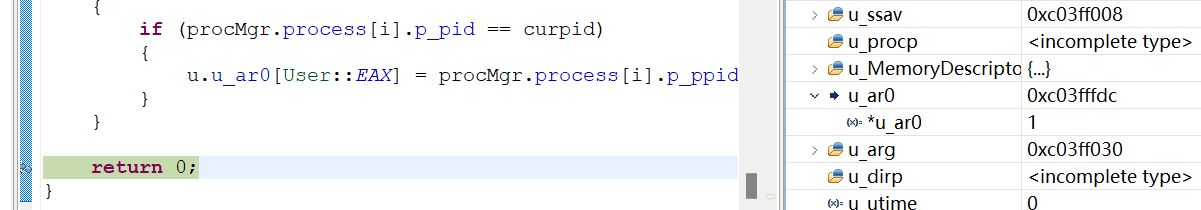
添加断点



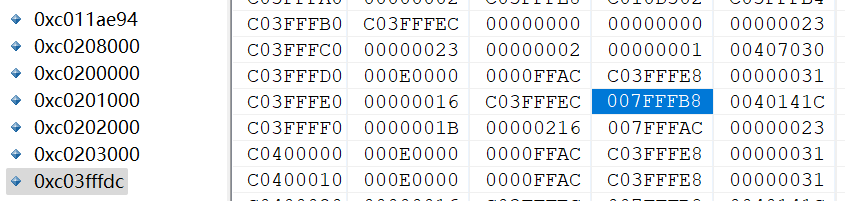
执行到断点处，通过u\_ar0可知系统调用号49通过压栈操作由EAX带入核心栈



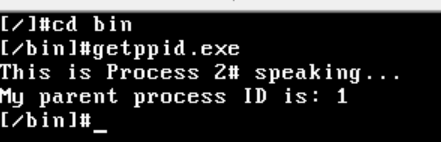
执行到Sys\_Getppid最后一步，u\_ar0指向的地址的内容变为1



查看核心栈（停止在int curpid = (int)u.u\_arg[0]时）：

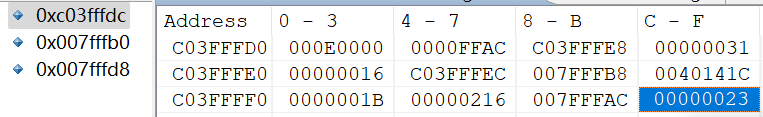


运行结果：



**四. 确定黄色标注的地址**

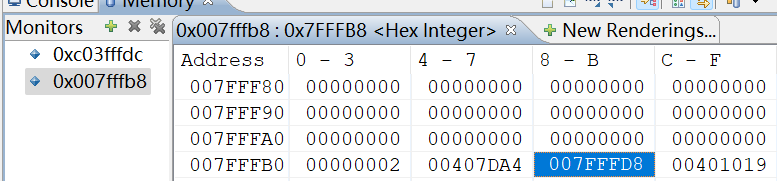
**（1）获取核心栈内容**



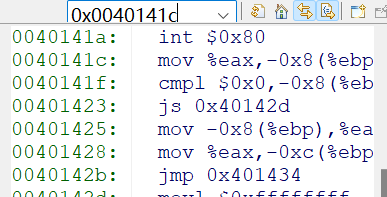
|  |  |  |
| --- | --- | --- |
| 0xC03FFFDC | EAX | 0x00000031 |
| 0xC03FFFE0 | 入口局变 | 0x00000016 |
| 0xC03FFFE4 | 入口局变 | 0xC03FFFEC |
| 0xC03FFFE8 | OLD EBP | 0x007FFFB8 |
| 0xC03FFFEC | EIP | 0x0040141C |
| 0xC03FFFF0 | CS | 0x0000001B |
| 0xC03FFFF4 | EFLAGS | 0x00000216 |
| 0xC03FFFF8 | ESP | 0x007FFFAC |
| 0xC03FFFFC | SS | 0x00000023 |

**（2）观察用户栈**

根据ebp找到用户栈



**（3）找到对应指令**



**（4）确定黄色块的内容**

|  |  |  |  |
| --- | --- | --- | --- |
| 0xC03FFFD8 | EBP | 0xC03FFFE8 | 指向当前栈帧基地址 |
| 0xC03FFFDC | EAX | 0x00000031 |  |
| 0xC03FFFE0 | 入口局变 | 0x00000016 |  |
| 0xC03FFFE4 | 入口局变 | 0xC03FFFEC |  |
| 0xC03FFFE8 | OLD EBP | 0x007FFFB8 | 调用程序的基址 |
| 0xC03FFFEC | EIP | 0x0040141C | 指向返回后下一条指令 |
| 0xC03FFFF0 | CS | 0x0000001B |  |
| 0xC03FFFF4 | EFLAGS | 0x00000216 |  |
| 0xC03FFFF8 | ESP | 0x007FFFAC | 调用程序用户栈栈顶指针 |
| 0xC03FFFFC | SS | 0x00000023 |  |