

**实验报告**



**题目： Linux环境和GCC工具链**

**班 级： 2023211307**

**学 号： 2023211088**

**姓 名： 罗浩**

**学 院： 计算机学院**

**2024 年 10 月 12 日**

一、实验目的

1. 熟悉linux系统的常用命令；
2. 掌握gcc编译器的使用方法；
3. 掌握gdb的调试工具使用；
4. 掌握objdump反汇编工具使用；
5. 理解反汇编程序（对照源程序与objdump生成的汇编程序）。
6. 实验环境+-

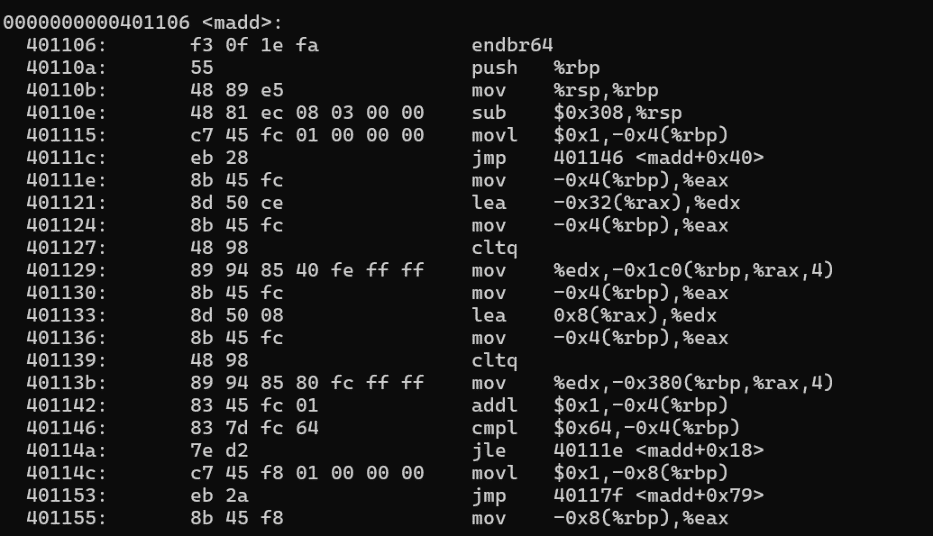
列举所使用的软件工具

1. Windows powershell

三、实验内容

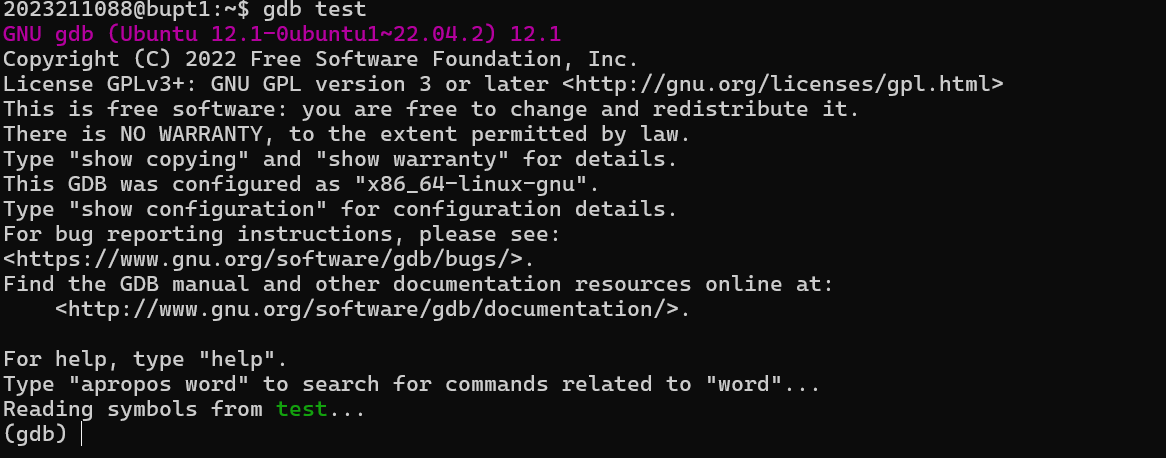
现有两个int型数组a[i]=i-50，b[i]=i+y，其中y取自于学生本人学号2022211x\*y的个位。登录bupt1服务器，在linux环境下使用vi编辑器编写C语言源程序，完成数组a ← a+b的功能，规定数组长度为100，函数名为madd（），数组a，b均定义在函数内，使用gcc编译该程序（使用-g -no-pie -fno-stack-protector选项），

1. 使用objdump工具生成汇编程序，找到madd函数的汇编程序，给出截图；

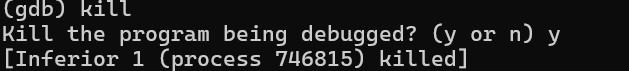


1. 用gdb进行调试，练习下列gdb命令，给出截图；

Gdb：



Kill：

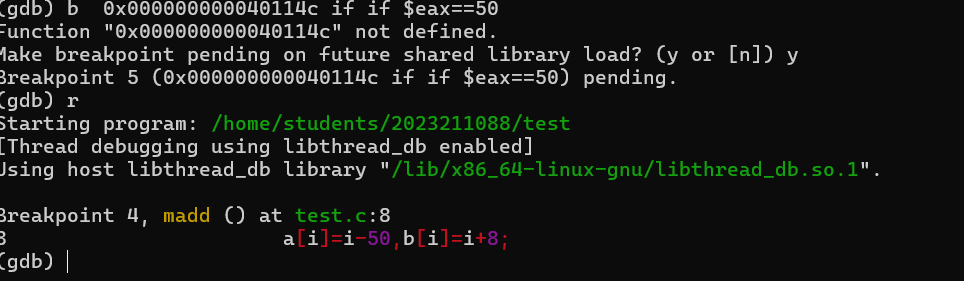


Quit：

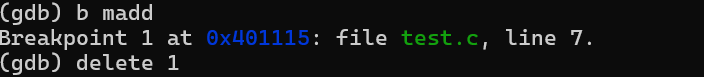


break（break \*0x地址 if $rax==401234）：





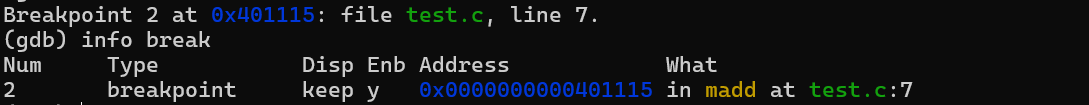
Delete：



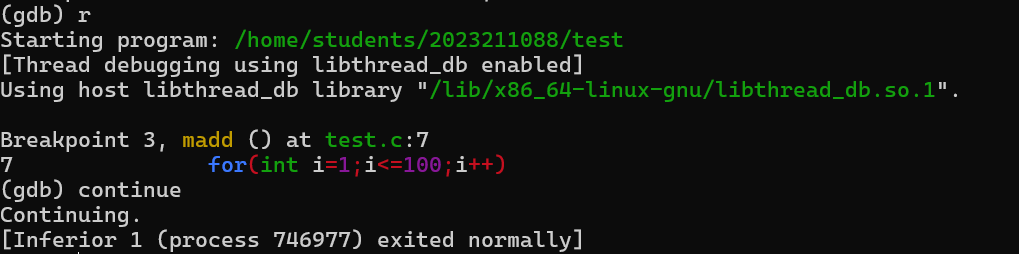
Clear:



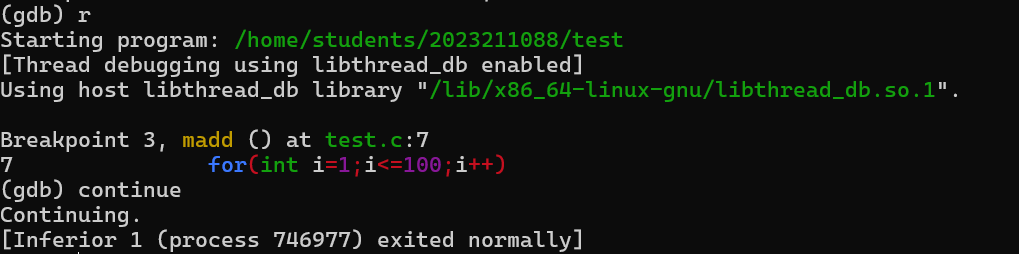
info break：



Run：



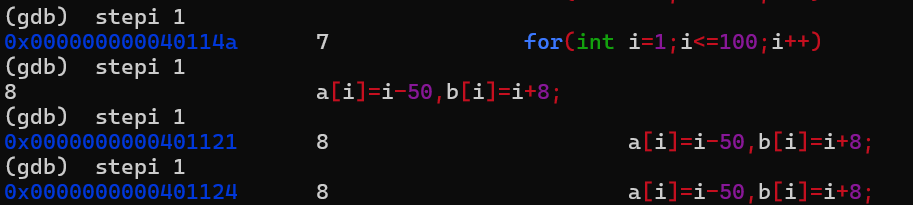
Continue：



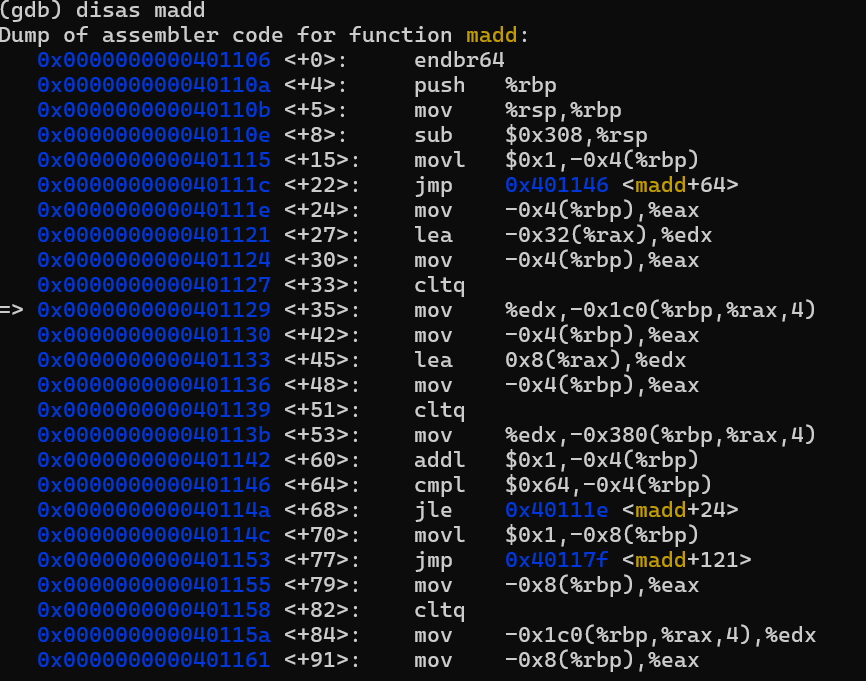
Nexti：



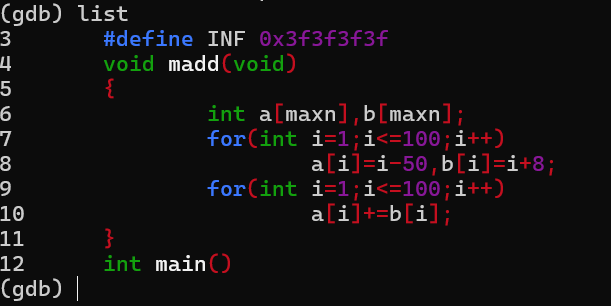
Stepi：



Disassemble：



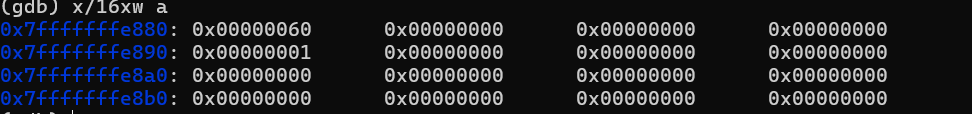
List：



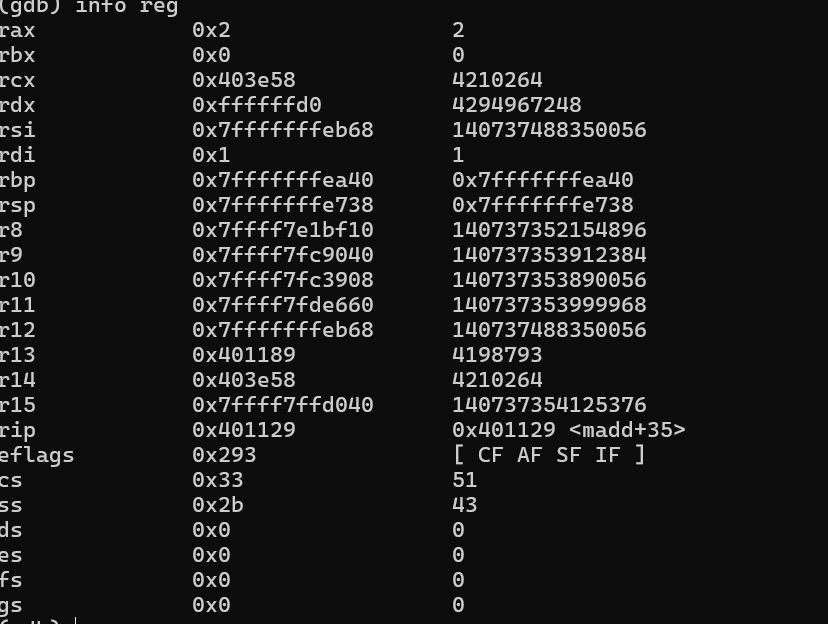
Print：



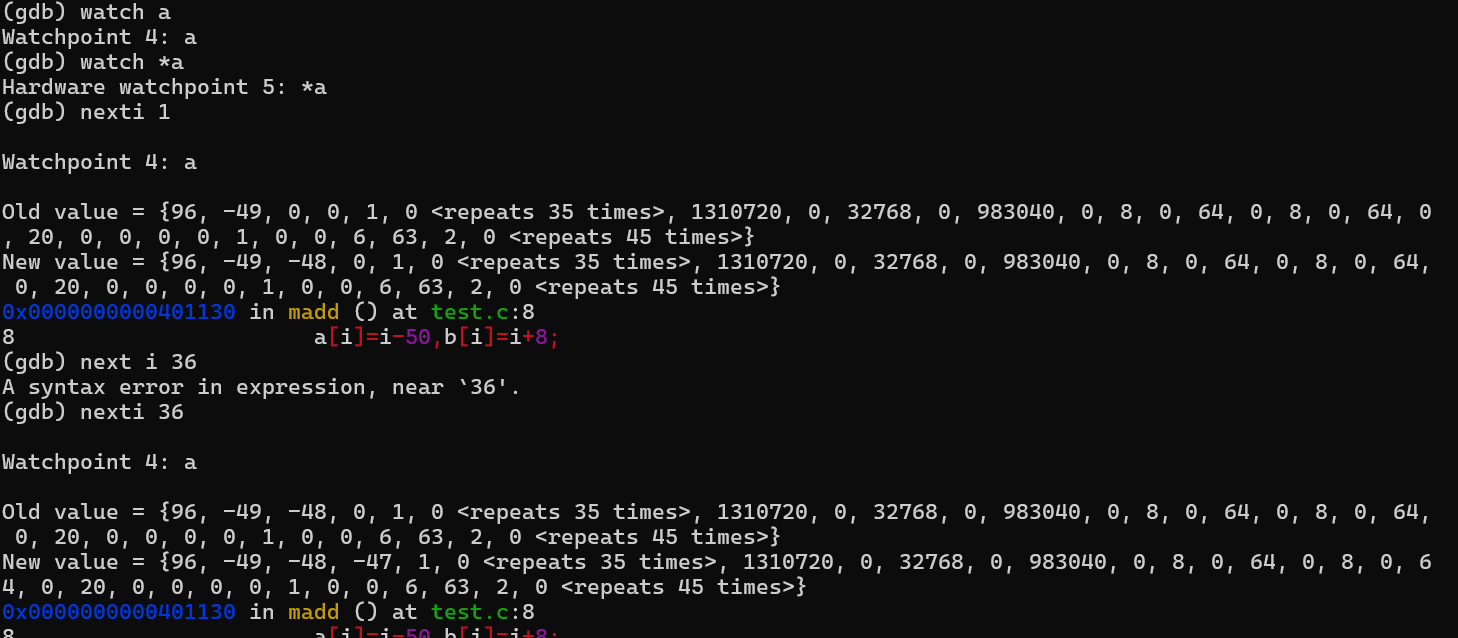
X：



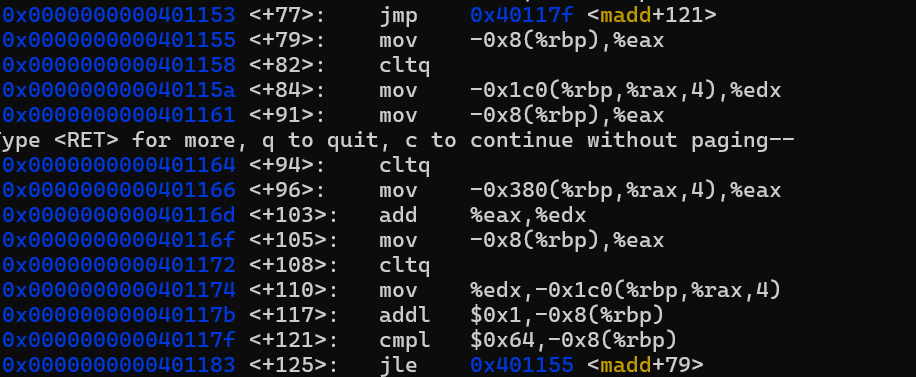
info reg：



Watch



1. 找到a[i]+b[i]对应的汇编指令，指出a[i]和b[i]位于哪个寄存器中，给出截图；

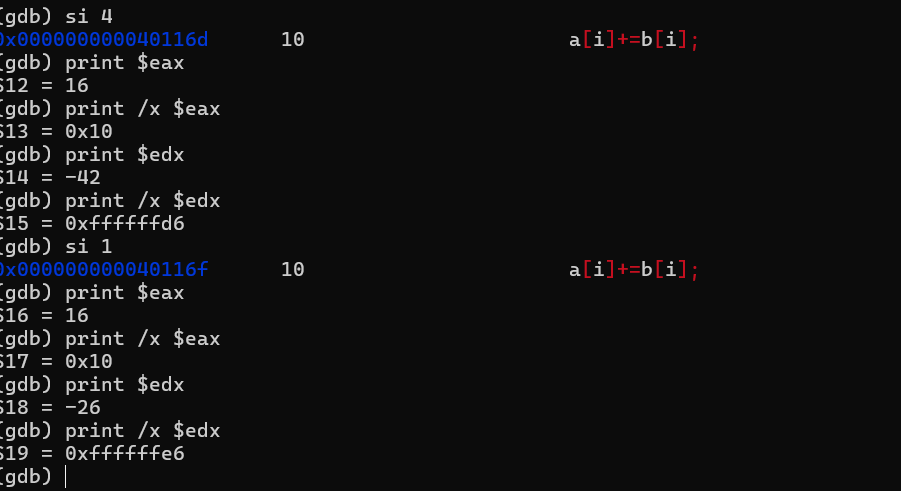


其中a[i]在%edx中，b[i]在%eax中

a[i]+b[i]截图:

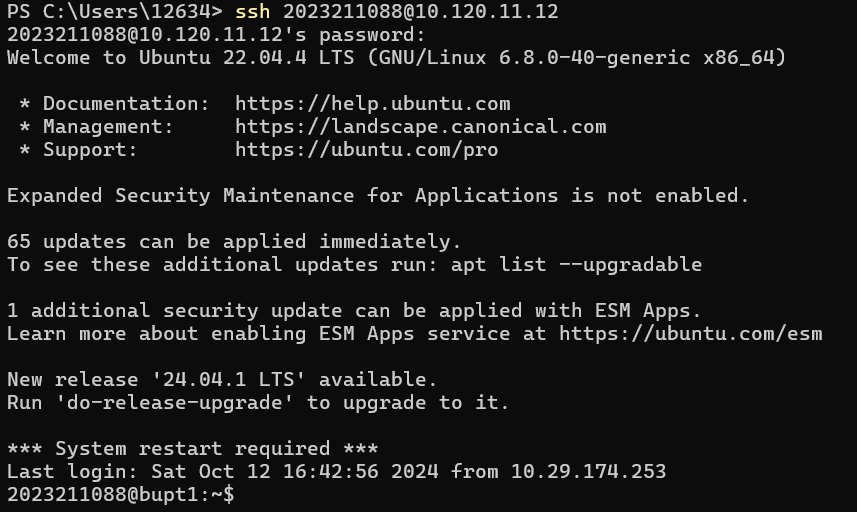
1. 使用单步执行命令及gdb相关命令，显示a[xy]+b[xy]对应的汇编指令执行前后操作数寄存器十进制和十六进制的值，其中x，y取自于学生本人学号2022211x\*y的百位和个位。

学号2023211088，a[8]+b[8]单步执行前后的截图如下：



1. 实验步骤及实验分析
2. 远程登录

使用ssh [2023211088@10.120.11.12](mailto:2023211088@10.120.11.12)并提交密码



实验一：

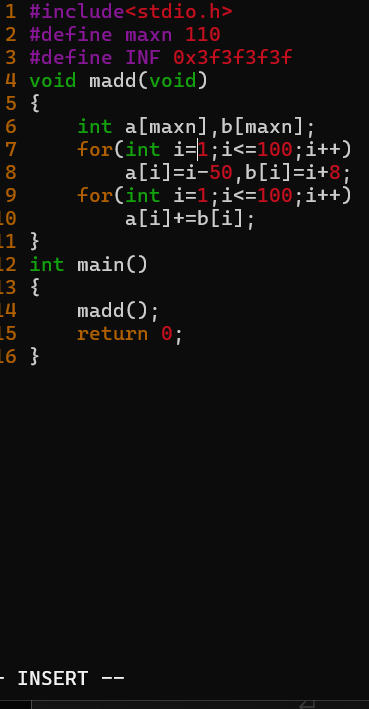
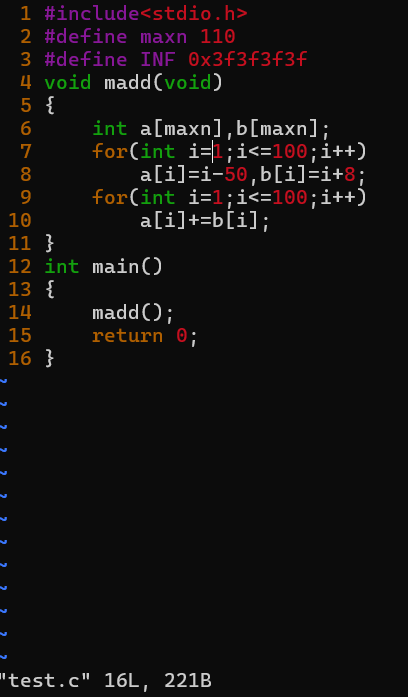
1. 创建.c文件并着手编辑

使用命令touch test.c创建.c文件

并唤起vi:vi test.c

第一次编写一个新文件，此时处于vi编辑器的插入状态

如果再次编辑已有文件，则会先进入命令模式



按下esc触发底行模式，此时可决定是否保存或退出。

开始书写.c文件

1. 使用gcc编译test.c文件

命令：gcc -g -no-pie -fno-stack-protector -o test test.c

-o 后面依次是目标文件与依赖文件

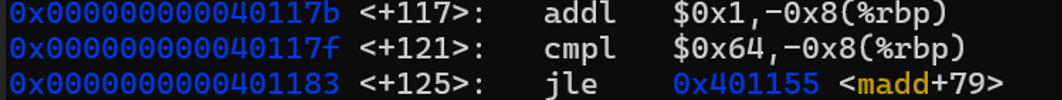
1. 使用objdump -d test得到反汇编机器代码完成第一个实验

实验二：

1. 命令：gdb test 进行c语言调试状态,依次输入相关命令完成实验2；

实验三：

1. 进入gdb调试状态
2. 在函数处设置断点 b madd
3. 使用命令r运行程序，程序会停留在一个断点处
4. 使用disas命令查找源代码操作对应的汇编代码，可先定位循环条件如（依次是i++,与循环条件判断）：



之后在该循环体中寻找，发现-50的赋值操作对应汇编行的：

****

**由此可找到a[i],同理可找到b[i];**

**完成实验三。**

实验四：

1. 设置断点定位a[xy]+b[xy]对应的位置：b 0x40114c if(i==xy);
2. 根据定位找到：



即为a[i]=b[i]+a[i];

1. 使用si或者ni跳转到add %eax %edx处
2. 使用print命令打印a[i],b[i]对应的寄存器值
3. 并使用si/ni 1跳转至下一行机器代码，此时相当于已完成add %eax %edx操作，重新重复打印操作。完成实验四。

五、总结体会

1.心得

忘记调试或文件操作相关命令的情况很常见，需要始终多查多用，才能牢固记忆。

Gdb拥有强大的调试功能，与现有的编译器软件基本功能相近。

2.所遇问题

* + 难以直接通过s或n命令使逐步跳转到所求汇编代码位置

分析：汇编代码执行命令多而冗杂，如果仅凭计算或逐步跳转会耗费许多时间，所以应当设置条件断点，或直接将断点设置在对接近某段汇编代码的位置。

解决方案：使用b+汇编行所在的最近的函数接口地址（如for函数）+if(reg==x)或其它条件，输入r时会跳转至最近的函数接口上。

建议，尽量通过查手册多去了解每个命令的各种不同作用，不断简化达成某个目的的成本。