Department of computer science and technology

Introduction to Computer System Class Exercise LaTeX

第七八章作业

2019年6月13日

南京大学

姓名: 张逸凯

学号: 171840708

指导老师: 汪亮, 苏丰

邮箱: zykhelloha@gmail.com

联系电话: 18051988316

目录

1 课后习题

1.1 第7章

4 .

(1) 第一行虚拟地址 0x80482e0, laddr也是, 页大小是4KB的, 从地址结尾看出不符合起始地址, 所以在之前就已经被装入主存了. 所以上面7条都不会缺页.

(2) 第一条指令: 数据访问缺页, 可恢复, 暂停P转到kernel执行页故障处理程序, 将地址0x80497d0所在页面调入内存, 结束了再到movl执行.

第二行指令缺页. 过程同上不再赘述.

第六行注意到 0x804a000已经在主存中, 所以不会缺页.

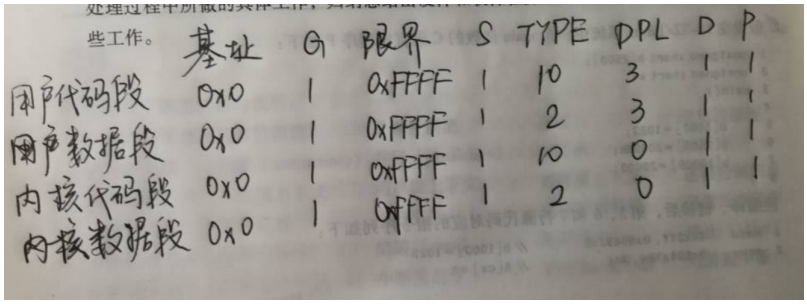
第七行很奇怪, 0x804de20这是一个很远的地址, 偏离了数组的很多. 可能偏离到栈两头之间的空洞区了, 这就段错误了. 先是缺页, 在缺页处理时段错误(SIGSEGV), 然后显示并中断用户进程.

(3) 整除0, 不可恢复的故障. k没有初始化, 在.bss节中被初始化为 0.

5 .

(1) 在int 80 之前都是用户态, 第二小问为陷入了内核态.

(2) 是, 通过系统门描述符来激活异常处理程序. 中断类型号0x80.



(3)

第5行指令的执行过程如下:

0x80嘛, 然后从IDTR取128个表项, P = 1, DPL = 3, TYPE = 1111B. 段选择符 0x60. 然后根据IDT中段选择符, 从GDTR指向的GDT取出相应的段描述符, 得到异常处理程序的DPL之

类的信息, 然后检测特权级有没有越权, 因为第五行CPL = 3, DPL = 0, 所以陷入内核态, 来使用内核栈.

用户栈到内核栈的切换又可以细分为读TR, 将TSS段保存的东西装入SS, ESP等. 在第五行后面的指令的逻辑地址写到CS和EIP, 将IDT中段选择符写到CS, 然后IDT偏移地址装入EIP, 这指向系统调用处理程序的第一条指令.

1.2 第8章

3 .

(1) stdout 输出 ”Hello world”.

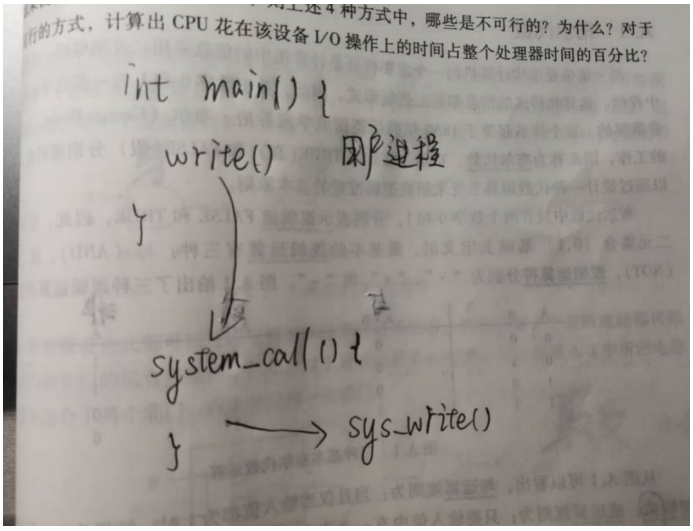
(2) int $0x80

(3) 16行调用了 sys_write(), 20行调用了sys_exit().

4 .

(1) main进了3个参数, R[esp] + 8存放了 0xe, R[esp] + 4存放了0x80aa848. R[esp]存放了0x1.

(2)



(3) 本题用封装好的, 给write()传不同参数即可, 更方便更可靠.

8 .

最快 50行 × 80字 × 6 = 24 000 个字符一分钟.

最长间隔1 / 400s = 0.0025 s 处理中断, 但是中断响应时间很短 $1000 \times 1 / 1500 \times 1000 = 0.000\,002$ s. 所以可以用中断方式.

2 总结

最后一次作业了, 有点舍不得, *ics* 马上结课咯, 致敬曾经犯过的错误, 为了更好的明天!
Edited by LaTeX, 感谢助教哥耐心检查, 辛苦啦~

参考文献