实验二：Linux内核模块编程

1. 实验要求
2. 设计一个模块，要求列出系统中所有内核线程的程序名、PID、进程状态、进程优先级、父进程的PID；
3. 设计一个带参数的模块，其参数为某个进程的PID号，模块的功能是列出该进程的家族信息，包括父进程、兄弟进程和子进程的程序名、PID号及进程状态；
4. 根据自身情况，进一步阅读分析程序中用到的相关内核函数的源码实现。
5. 函数设计

本实验由两个任务组成，任务1要求列出系统中所有的内核线程的相关信息，任务2要求累出某个进程的家族信息。

对于任务1，程序利用Linux内核提供的宏for\_each\_process()，从init\_task进程开始，遍历所有进程；同时，由于内核线程的mm字段为NULL，因此可根据进程的task\_struct中的mm字段是否为NULL来判断进程是否为内核线程。从而，输出内核线程的相关信息。具体流程如下图：



对于任务2，程序主要利用Linux进程间的家族关系输出进程的家族信息。对于一个进程，其task\_struct中的parent字段指向其父进程；其task\_struct中的children字段指向其子进程链表的头部；父进程相同的所有进程称为兄弟进程，由task\_struct中的sibling字段链接成父进程的children链表。同时利用宏list\_for\_each()和list\_entry()，获取节点的起始地址，以引用节点中的其他域。

输出进程的父进程的相关信息，只需通过其task\_struct的parent字段获取指向其父进程的task\_struct的指针即可。

输出进程的子进程的相关信息，需通过其task\_struct的children字段获取指向其子进程链表头部的指针，遍历该链表即可。

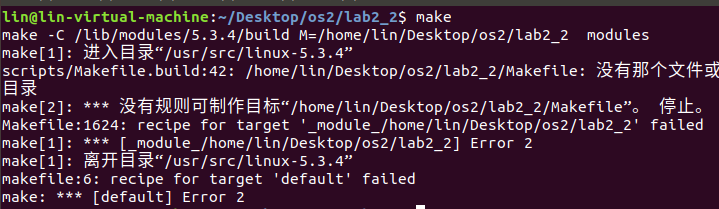
输出进程的兄弟进程的相关信息，需通过其父进程的task\_struct的children字段获取指向其兄弟进程链表头部的指针，遍历该链表即可。

具体流程如下图：



1. 在实验中遇到的问题

1.在执行make命令时，报错如下图：



解决方案：

这个问题是因为将Makefile的文件名写成了makefile

1. 实验结果讨论
2. 任务一实验结果

加载模块后，使用dmesg命令输出日志文件，得到内核线程的部分相关信息如下图：



使用ps -ef命令查看系统的所有进程，CMD一栏名称加方括号的为内核线程，经比对，实验结果正确。

1. 任务二实验结果

用命令insmod m2.ko pid=2加载模块后，使用命令dmesg输出日志文件，得到pid为2的进程的部分家族信息如下图所示：

