OS lab6 Report

name: 刘乐奇

sid: 12011327

Ubuntu用户名: lynchrocket

1. 代码中通过何种方式从S mode 进入U mode?

在 /kern/process/proc.c 中的 init_main() 函数新建了一个进程来执行函数 user_main() 。init_main 作为管理者，调用 do_wait() 等待子进程的结束。等待的过程中通过 schedule() 调度 user_main 执行。user_main() 函数中的 `KERNEL_EXECVE(hello);` 是一个宏，加载了存储在这个位置的程序 hello 并在 user_main 这个进程里开始执行。这时 user_main 就从内核进程变成了用户进程。

2. 代码中用户进程调用系统调用的过程是怎样的?

用户程序在用户态运行(U mode), 系统调用在内核态执行(S mode)。这里有一个CPU的特权级切换的过程, 要用到 ecall 指令从U mode进入S mode。
在本次lab的代码中，要靠/user/libs/syscall.c的 `syscall(int num, ...)` 进行系统调用，其中的内联汇编进行 ecall 环境调用。这将产生一个trap, 进入S mode进行异常处理。

3. 代码中用户进程执行结束后发生了什么，模式是否切换?

在do_execve()函数的最后调用了do_exit()函数，该函数会将进程退出。

- 首先执行 lcr3(boot_cr3)，切换到内核的页表上，这样用户进程就只能在内核的虚拟地址空间上执行。然后开始回收内存资源，进而把对应的页表项内容清空，并把页表项和页目录表清空，释放页目录表所占用的内存。最后调用 mm_destroy 释放 vma 与 mm 的内存，把 mm 置为NULL，表示与当前进程相关的用户虚拟内存空间和对应的内存管理成员变量所占的内核虚拟内存空间已经回收完毕。
- 设置进程的状态为 PROC_ZOMBIE 表示该进程变成僵尸进程，等待父进程来回收资源，回收内核栈和进程控制块。当前进程的退出码为 error_code 表示该进程已经不能被调度。
- 如果当前进程的父进程处于等待子进程的状态，则唤醒父进程让父进程回收资源

- 如果该进程还有子进程，那么就指向第一个孩子，把后面的孩子全部置为空，然后把孩子过继给内核线程 initproc ，把子进程插入到 initproc 的孩子链表中，如果某个子进程的状态是僵尸的状态，并且 initproc 的状态时等待孩子的状态，则唤醒 initproc 来回收子进程的资源。
- 然后开启中断，执行 schedule 函数，选择新的进程执行

4. 进程如何变成僵尸进程?

当用户进程执行结束后，do_exit()函数会将进程退出，其中会将进程的状态设置为 PROC_ZOMBIE ，表示该进程变成僵尸进程。