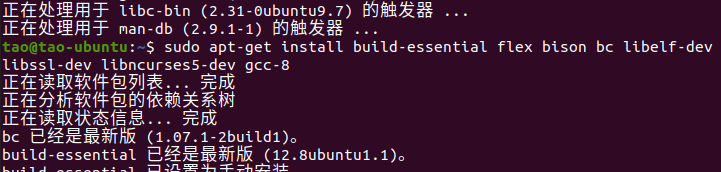
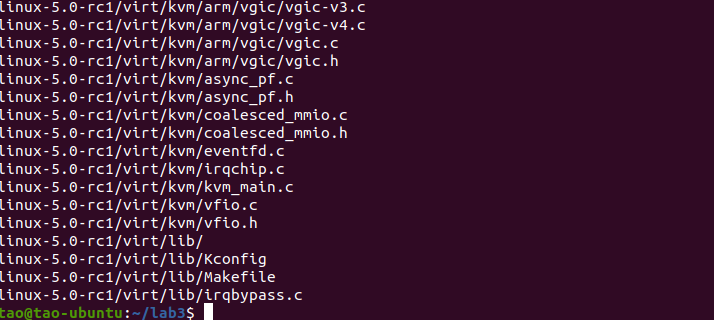
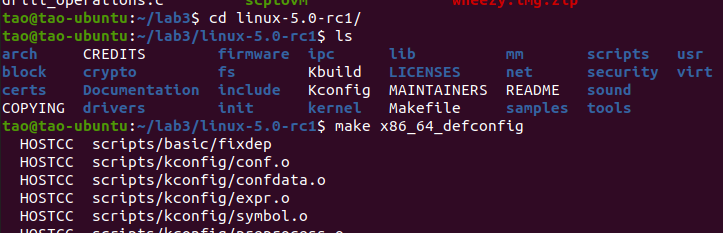
安装QEMU

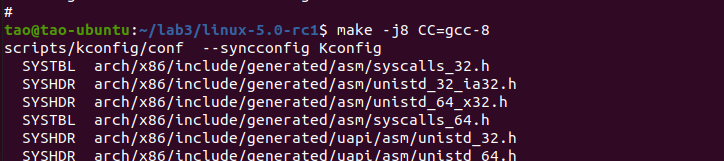


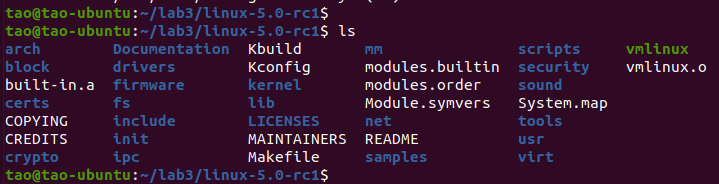


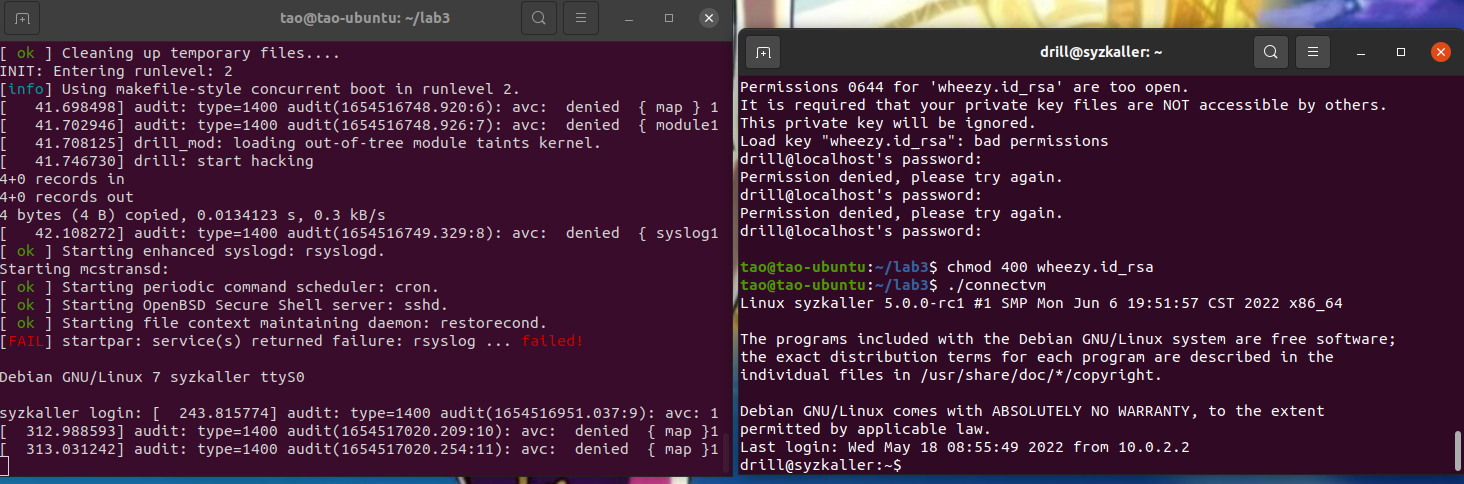


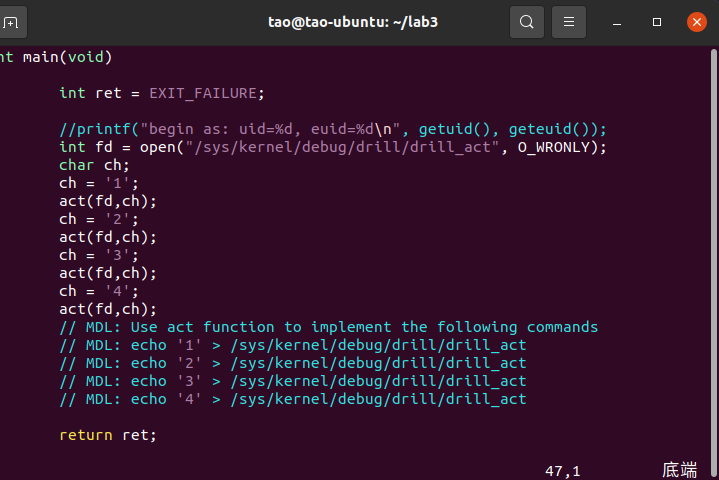


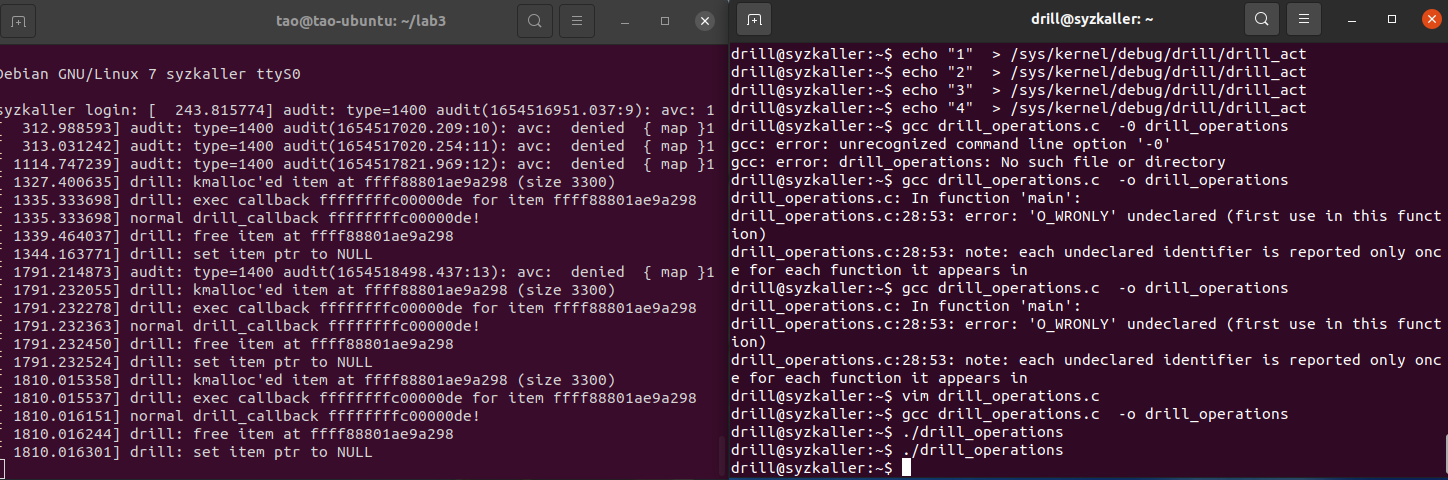


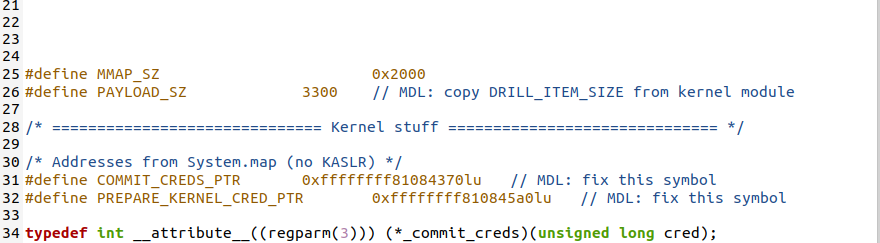


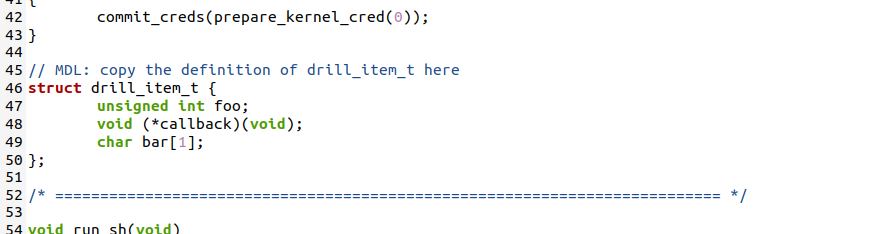




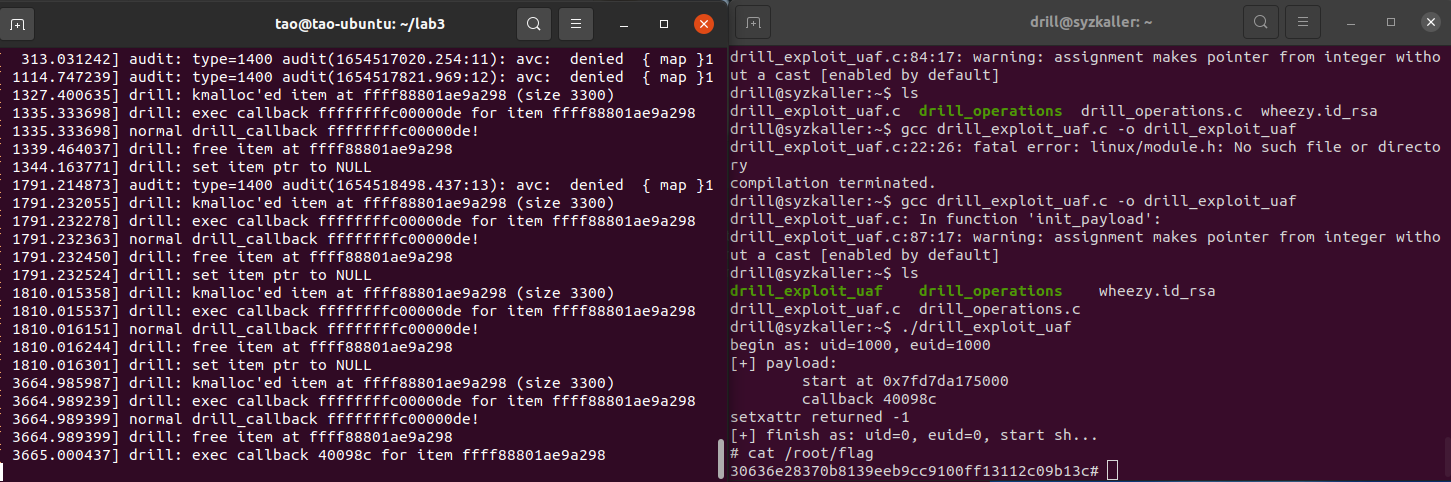


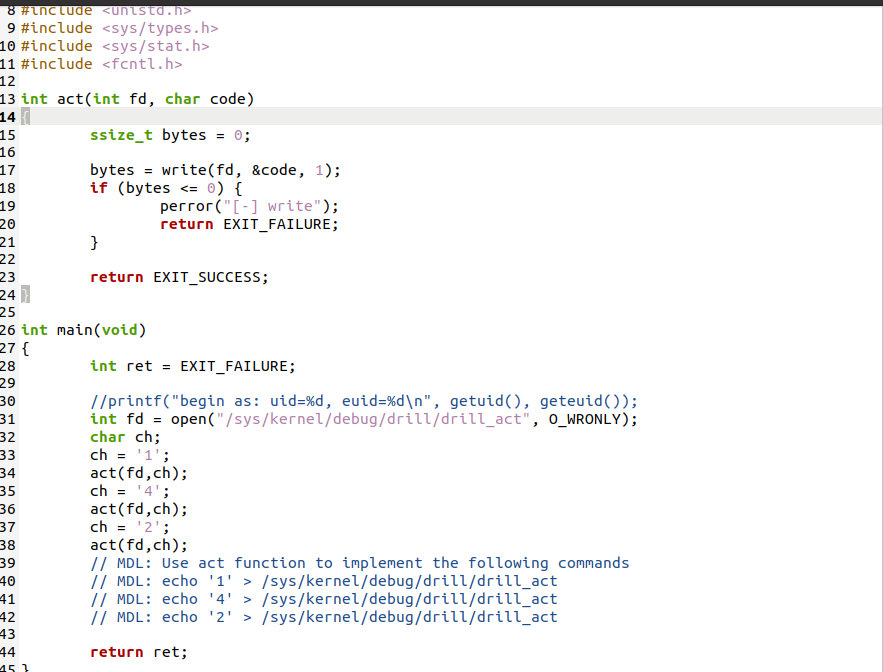


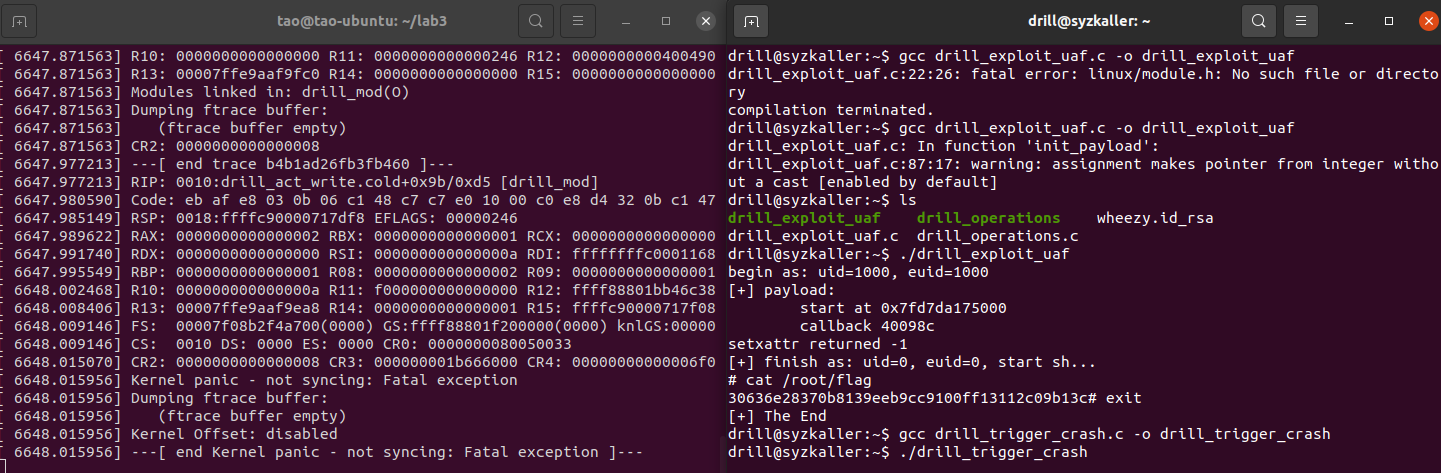


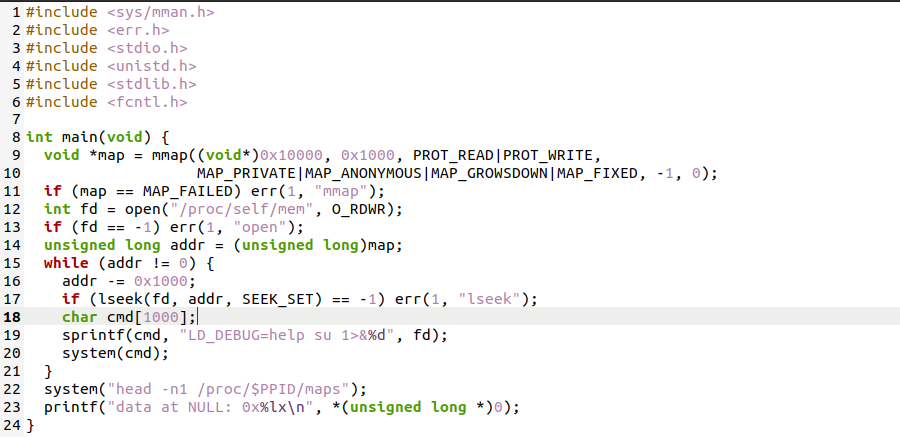


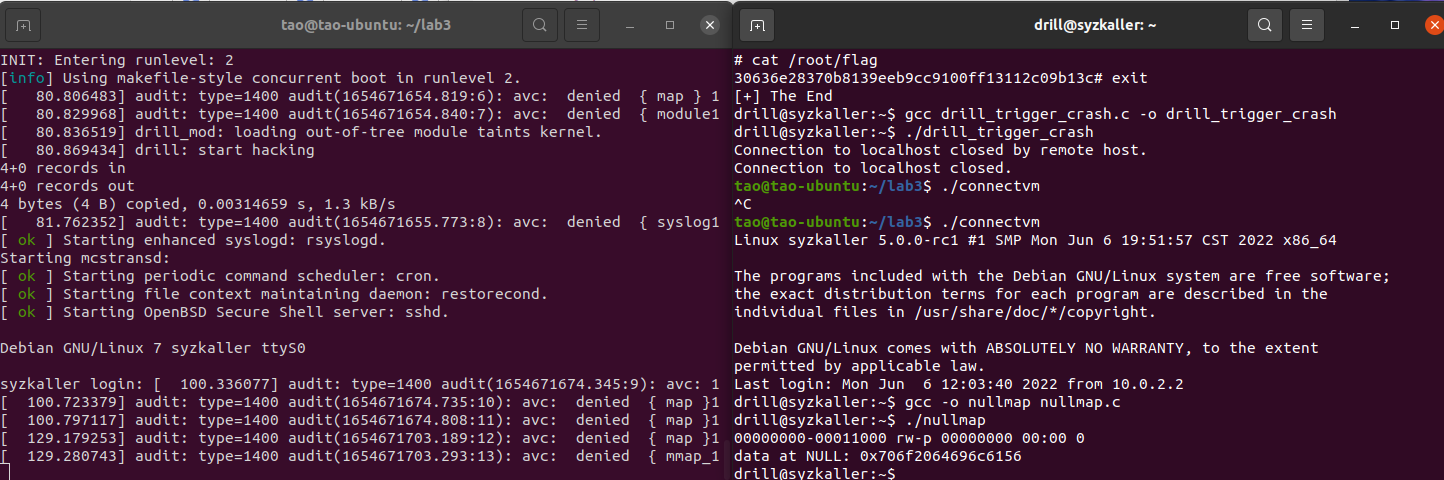


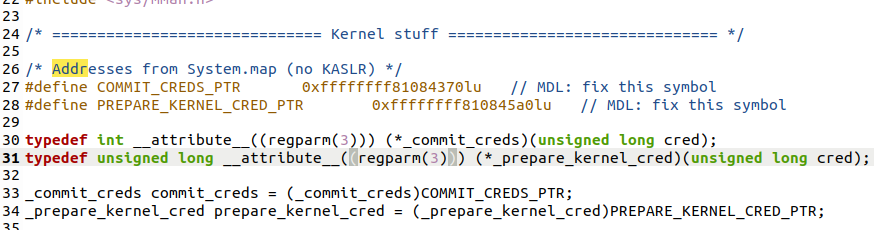






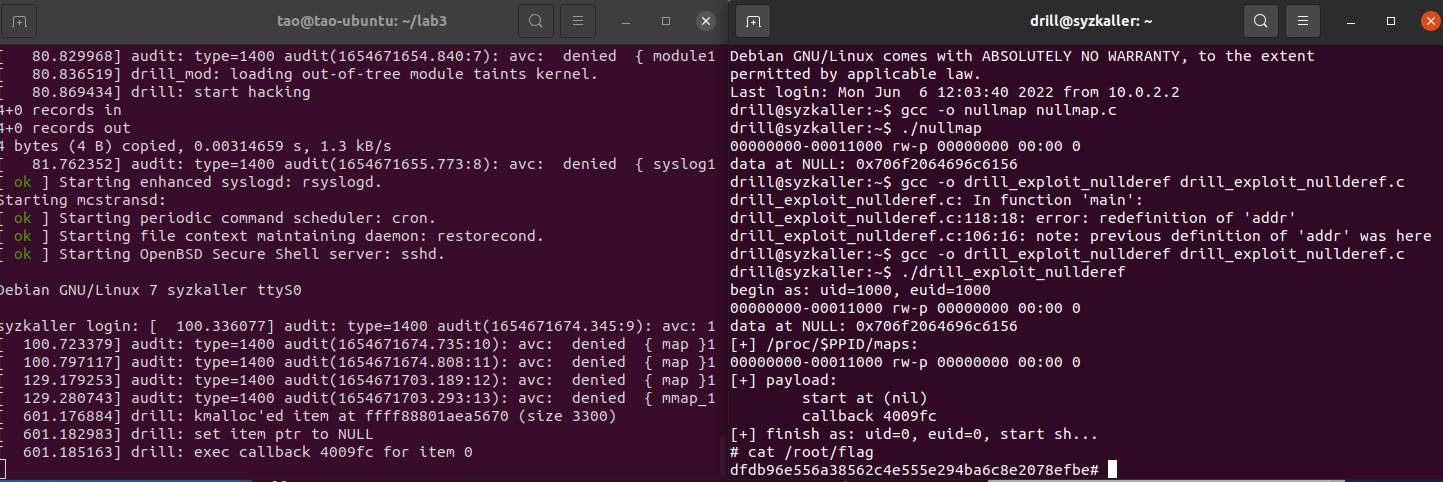












第二次分配的时候，数据任由自己安排，然后给第一次指针的callback函数换成root it，完成提权。