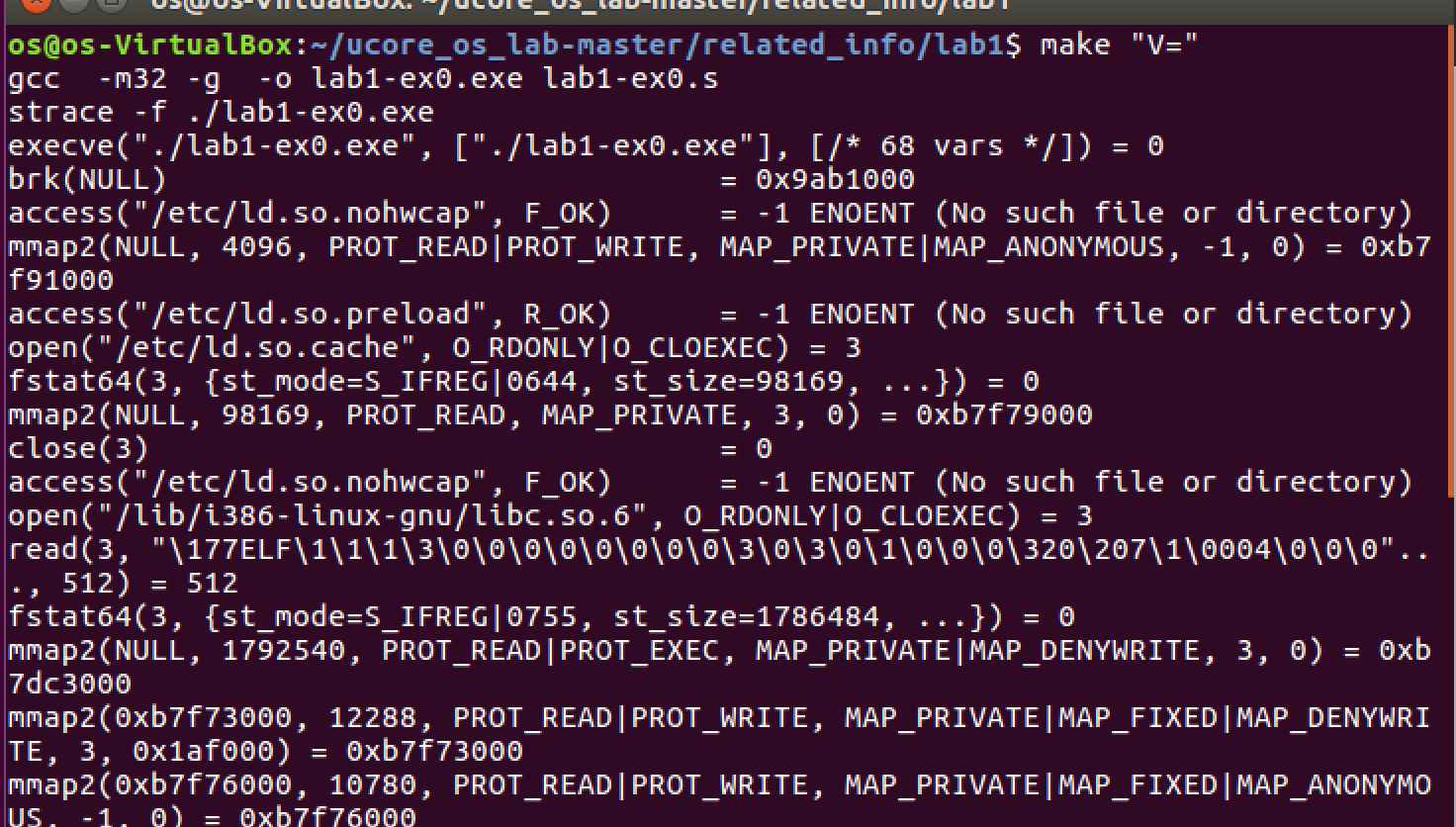
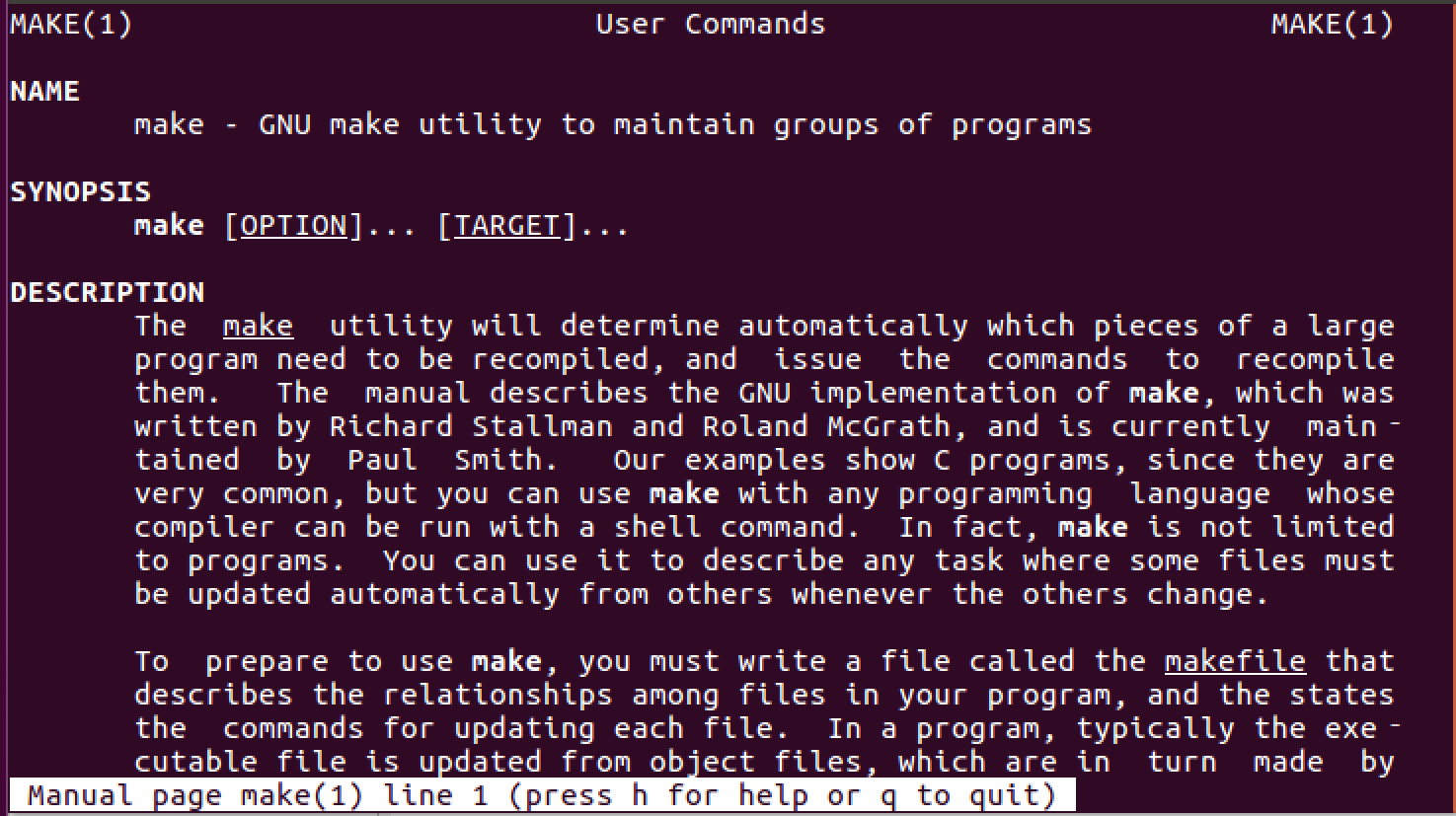
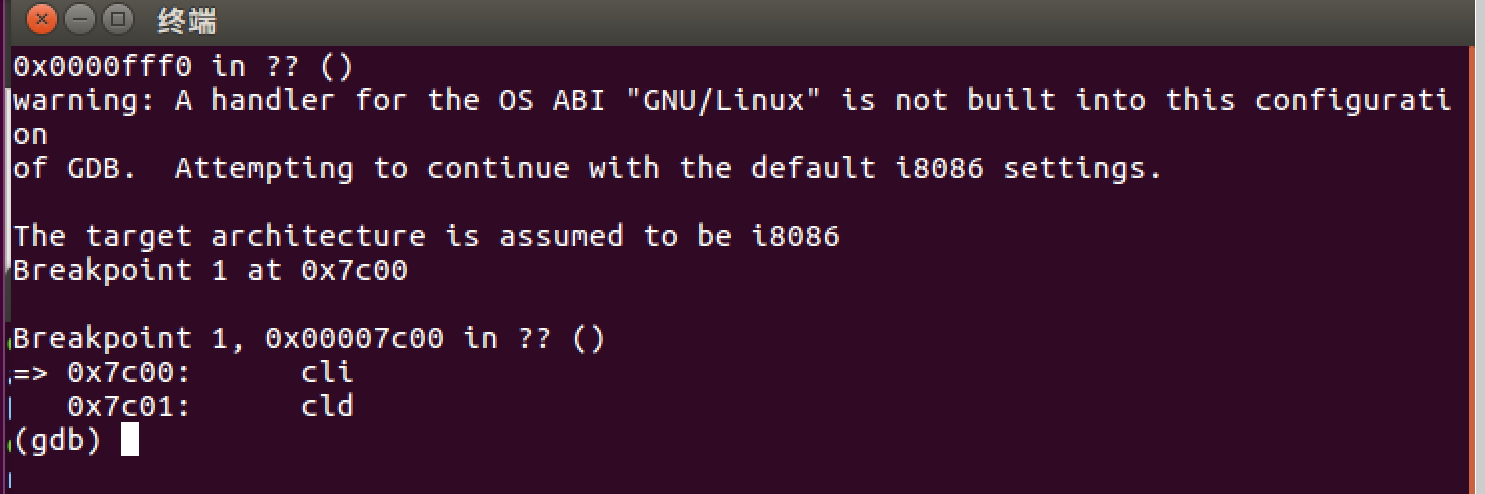
练习1.1



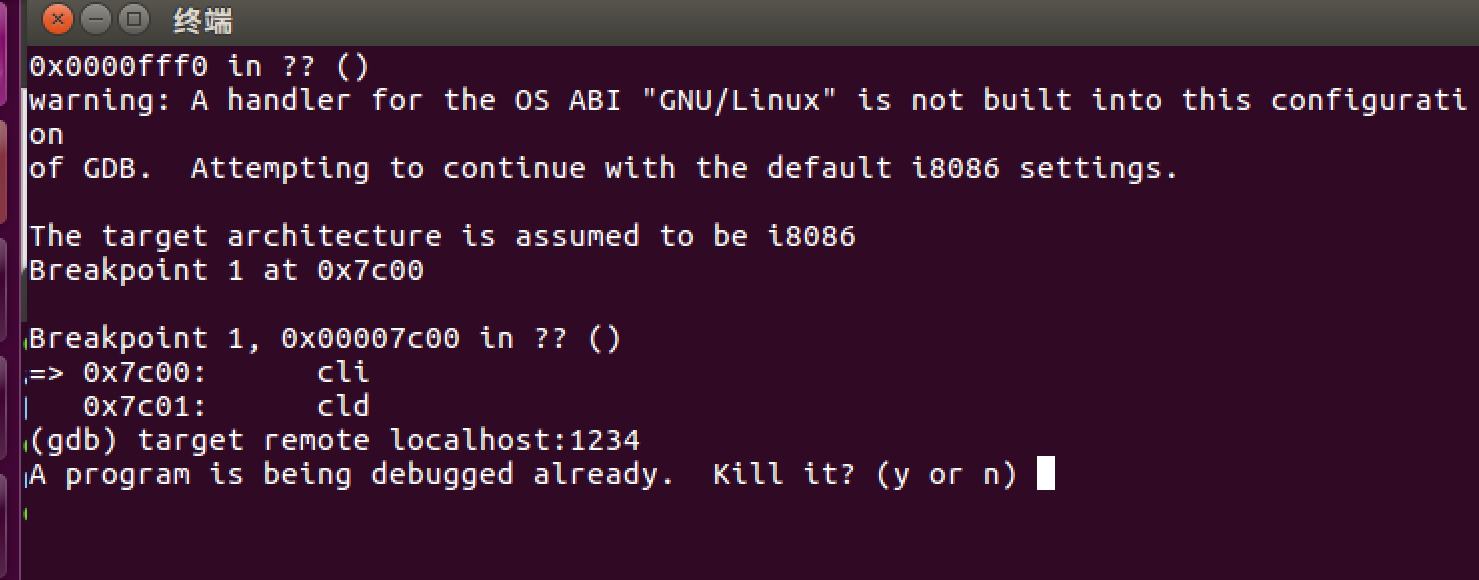


练习2

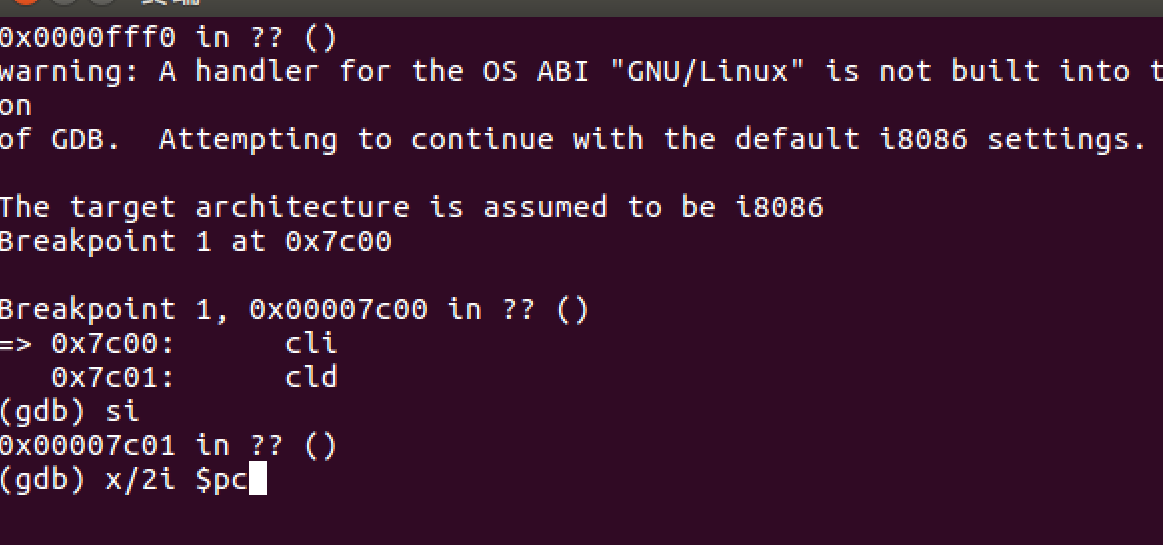
输入make lab1-mon



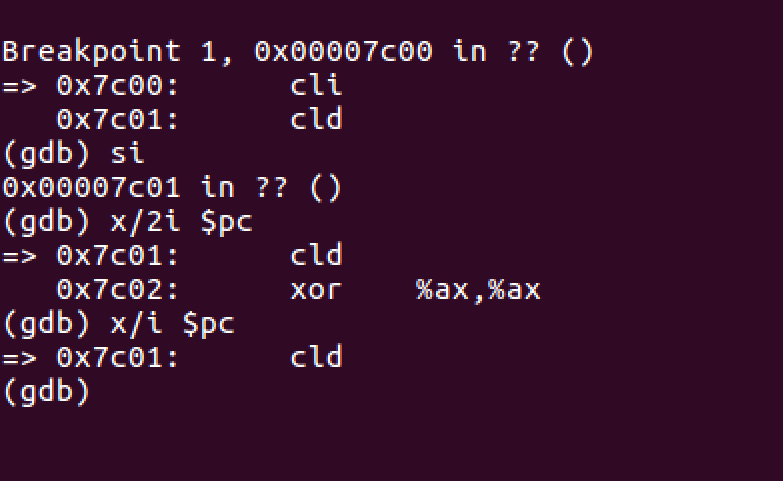
输入：target remote localhost：1234进入gdb命令



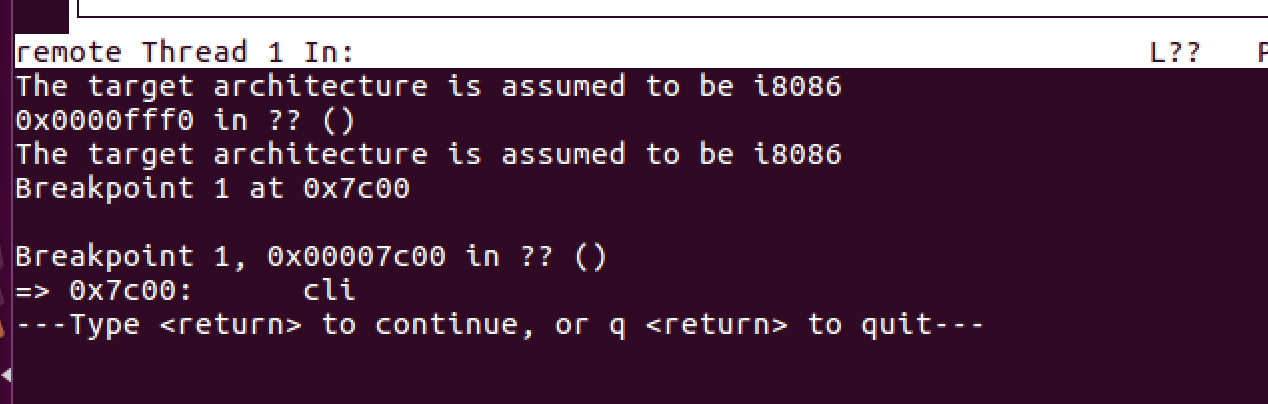
输入si，单步追踪BIOS



输入x/2i $pc或x/i $pc:

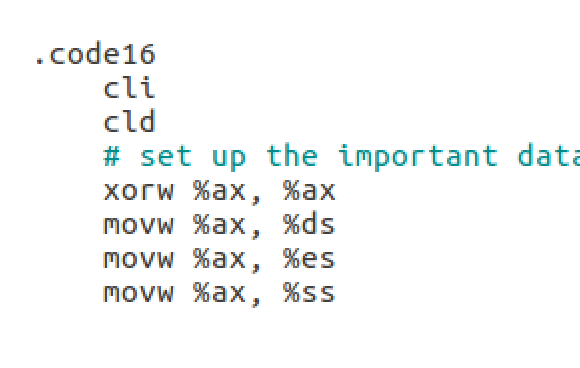


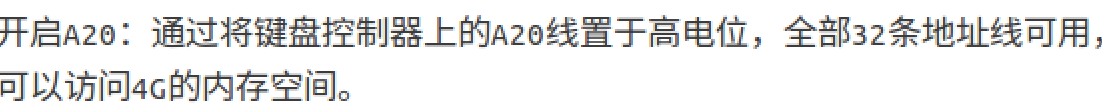
测试断点是否正常

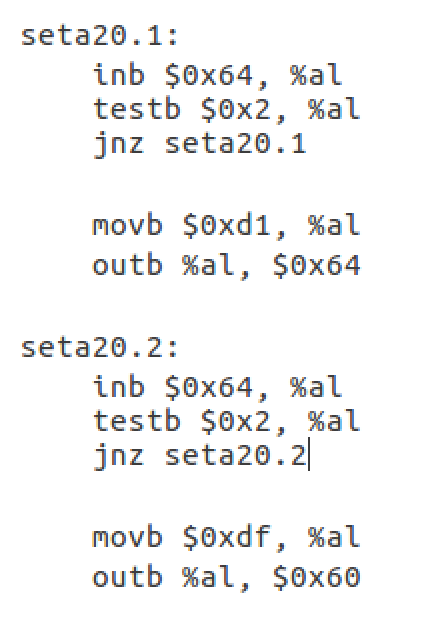


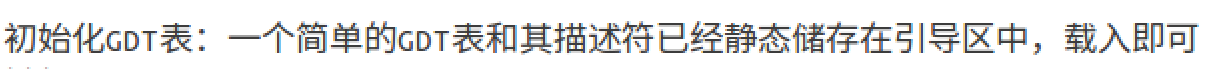
3、分析bootloader进入保护模式的过程

A:



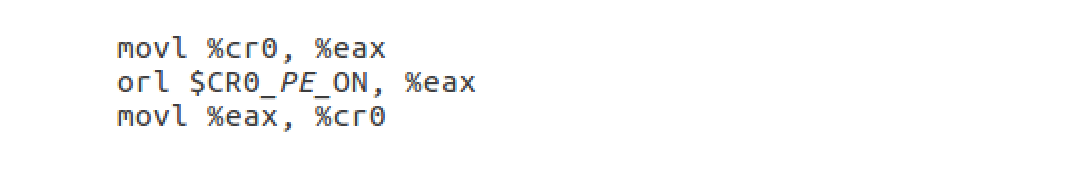
B



C

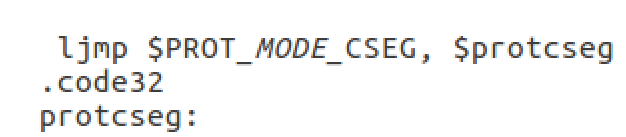


D



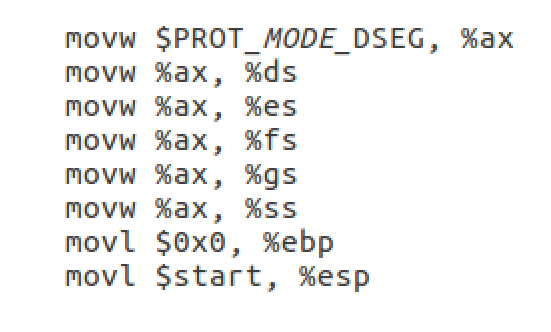
E

通过常跳设置cs基地址



F

设置段寄存器，建立堆栈



G转到保护模式完成，进入boot

Call bootmate