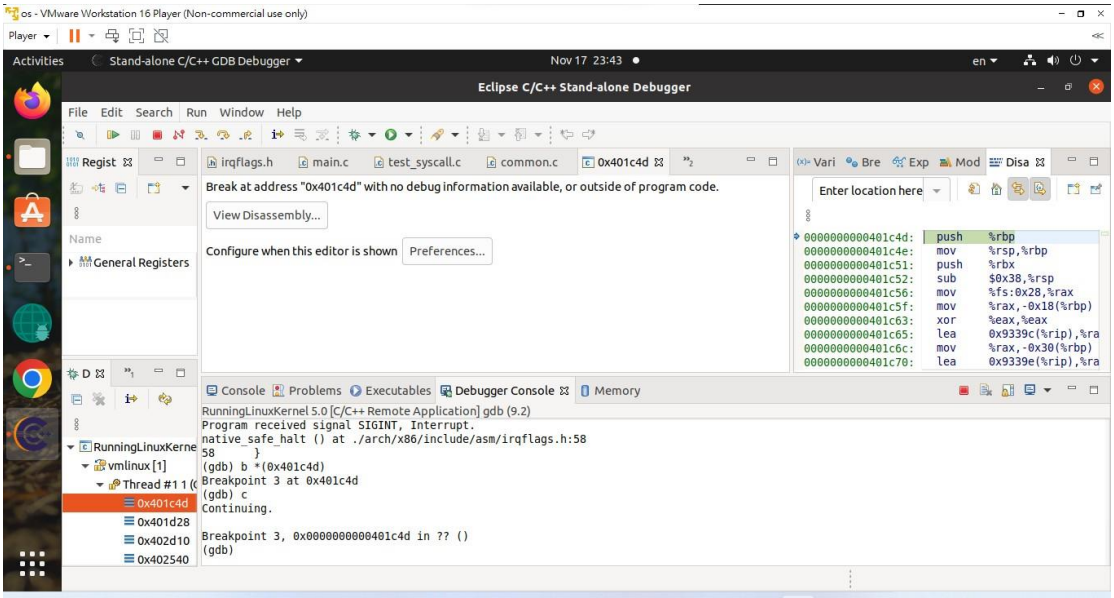
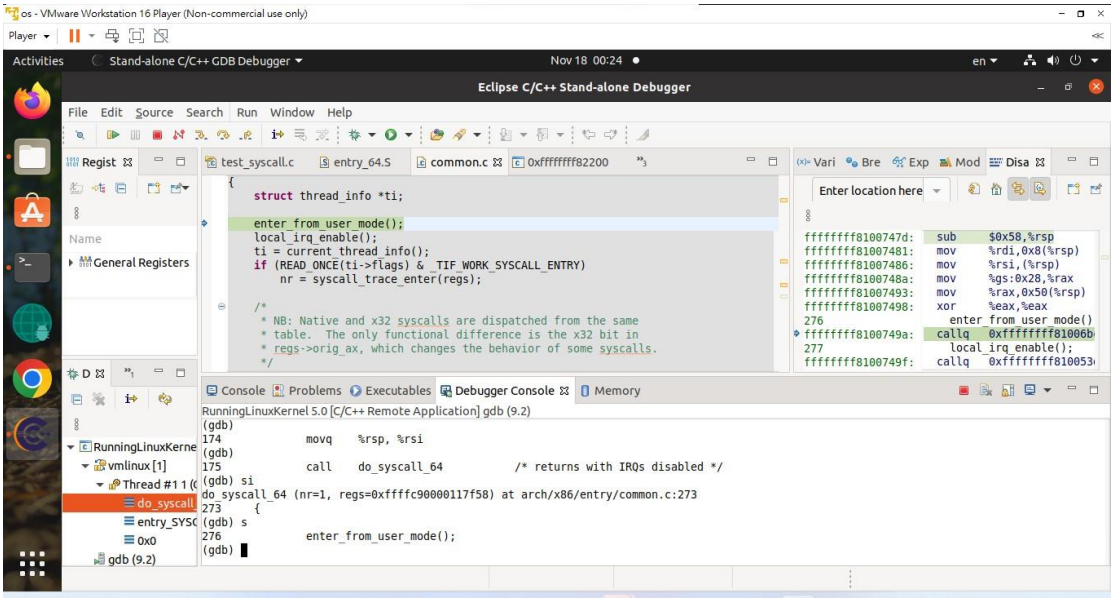
HW8 從使用者模式追蹤到核心模式

系級：資工三　學號：409410114　姓名：周 x 君

1. 設定中斷點在 test_syscall 發出 system call 之前，請在這個地方截圖



2. 使用單步追蹤（si），直到 Linux kernel，請在進入 Linuxkernel 時截圖



3. 請說明 Linux kernel 如何用 RAX 暫存器判斷要呼叫哪個 Linux 內部的函數
   Linux System Call Table

   system call 所經過的流程:
   1. 在使用者程式中呼叫 system call
   2. 藉由一個軟體中斷 trap (svc #0) 進入 kernel mode，此時系統會將 mode bit 由 user mode 改成 kernel mode (1 -> 0)
   3. 查詢 system call table 來找尋對應的 trap service routine
   4. 當執行完 trap service routine 後發出中斷通知 OS 已經完成

   function call->Interrupt->透過查詢 interrupt vector table 得知採用哪種 interrupt service routine(ISR)->從該 ISR 得知要查詢 system call table->查詢到做哪個 system call service routine 後完成該 system call service routine->呼叫中斷切回 user space

4. 請大致說明作業系統如何處理 write。
   追蹤到 ksys_write 即作業系統開始處理 write
   先拿到 file position 再呼叫 vfs_write 把檔案讀出來，而 vfs_write 實現的方式和其後的函數有關
   讀出來的檔案有實作 read、write 等，是作業系統實現物件導向的方式

參考資料: https://hackmd.io/@combo-tw/Linux-%E8%AE%80%E6%9B%B8%E6%9C%83/%2F%40a29654068%2FHyD4Lu_Dr