guidance

Tags

1.fail a test , type script and make qemu, which log all console output to a file.

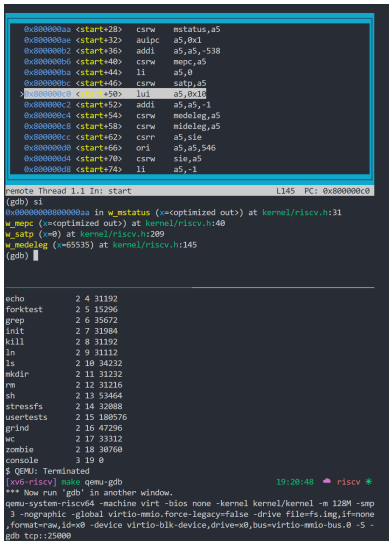
and don’t forget to exit script

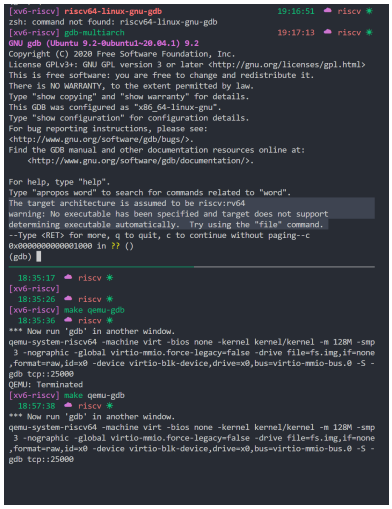
```
                                                    14:28:40
[~] script
Script started, file is typescript
[~] ls
clash  id_rsa  id_rsa.pub  mxy  typescript  xsr  xv6
[~] exit script
Script done, file is typescript
```

```
[~] cat typescript                                                  15:02:50
Script started on 2023-02-16 15:01:59+08:00 [TERM="xterm-256color" TTY="/dev/pts/11" COLUMNS="102" LIN
ES="19"]
[~] ls                                                              15:02:00
clash  id_rsa  id_rsa.pub  mxy  typescript  xsr  xv6
[~] exit script                                                     15:02:10

Script done on 2023-02-16 15:02:20+08:00 [COMMAND_EXIT_CODE="0"]
```

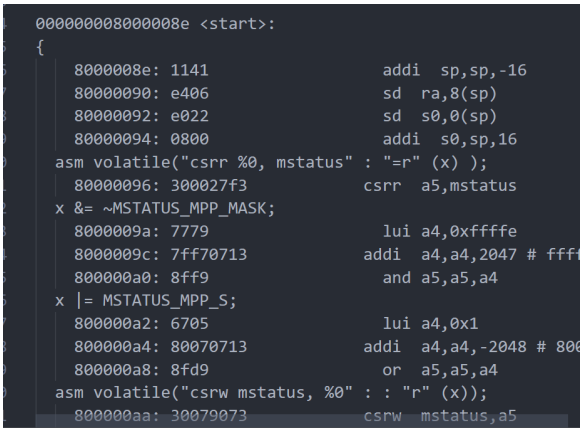
1.5 gdb remote





make qemu-gdb will open qemu-remote-debug on TCP:port .And run gdb(-multiarch in another window" can get the debug info.

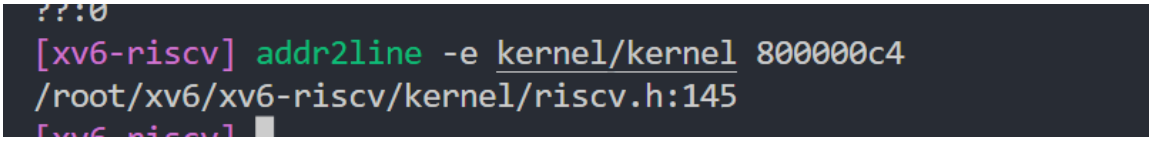
2.see the /kernel/kernel.asm to find out what the assembly he complier generates.



3. When kernel panic: a function will print the value of program counter.

   addr2line - convert addresses into file names and line numbers

   addr2line -e kernel/kernel *pc-value*



(pc-value 是前面的asm地址）

bt: backtrace can get all func_call while running. With it we can get all pc-value and the real func_code.

4. deadlock

   When the kernel appears to hang hit Ctrl-C in the qemu-gdb window and type 'bt' to get a backtrace.

5. qemu’s monitor ,type ctrl-a c.

   usage: info mem :print the page table (type cpu to select the core)