**CS5250 Advanced Operating Systems**

**Pop Quiz 7**

**(Due: 10 Mar 2022, 11.59pm)**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Student Number: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Please do a code walkthrough of the Linux 5.16.1 kernel and explain how, starting with **context\_switch()** in **kernel/sched/core.c:4921**, how context switching is achieved. In particular, staying on the 64 bit x86 architecture, trace the control flow and:

1. Identify the macros and procedures encountered, and try to explain what they do;
2. Identify the stacks involved and where the stack switches occur;
3. At key points where the control flow changes, what is on the top of the current stack? (“Key” is up to you to define but it should be used to clearly explain the flow that you have identified.)
4. Show how control will return back to the current task being switched out eventually.

Also, answer the following questions:

1. Why are RBP, RBX, R12-R15 pushed and then popped in **\_\_switch\_to\_asm** (found in **arch/x86/entry/entry\_64.S:225**)?
2. What is the effect of the do-while loop in the **switch\_to** macro?

Submit your answer in a PDF into the corresponding Luminus submission folder.