Lab 8

Turn in a hard copy of your answers, due in class on Tuesday the 23rd of October.

Read this write-up and then answer the following questions:

http://isec.pl/vulnerabilities/isec-0022-pagefault.txt

1) The Linux kernel provides memory lazily, as a process needs it. This is also called...

*on d*_____

2) What "core components of the Linux VM subsystem" is called when there is a page fault?

3) True or False?: If I put some data on the top of the stack (where the stack is growing backwards) it might cause a page fault.

4) True or False?: This page fault means that the process has to be killed with a SIGSEGV.

5) In the Linux kernel down_read() obtains a semaphore lock for reading, and up_read() releases a lock obtained for reading. More than one thread of execution can hold the read lock and execute concurrently. Conversely, down_write and up_write are used for obtaining and releasing write locks, which are exclusive meaning that the lock ensures that if a writer obtains it then no other thread of execution can have the lock, and therefore must wait. This race condition occurs because the first line of code does a down_read() instead of a down_write().

What is being written to, and by what part of the code, that makes this a race condition?

6) The writeup shows PAGE1 and PAGE2 being added to the page table for the process after the race condition. One of these can now be used to subvert the security of the system. Which one? Why?