Homework #2

Revision 1 has the new due date, changed from April 21.

Due: April 23, 2021   **Points:** 100

Questions

1. (*10 points*) The *free* statement in the *delete_queue* function in the robust library is not protected by an **if** that checks to see whether queues[cur] is **NULL**. Is this a bug? If not, why don't we need to make the check?

2. (*20 points*) In the example on page 961, why is the tree constructed using a breadth-first search rather than a depth-first search?

3. (*28 points*) Classify the following vulnerabilities using the PA model. Assume that the classification is for the implementation level. Justify your answer.

   (a) The presence of the "wiz" command in the *sendmail* program (see Section 24.2.9).

   (b) The failure to handle the **IFS** shell variable by *loadmodule* (see Section 24.2.9).

   (c) The failure to select an *Administrator* password that was difficult to guess (see Section 24.2.10).

   (d) The failure of the Burroughs system to detect offline changes to files (see Section 24.2.7).

4. (*18 points*) Suppose Alice has *r* and *w* rights over the file *book*. Alice wants to copy *r* rights to *book* to Bob.
   (a) Assuming there is a copy right *c*, write a command to do this.
   (b) Now assume the system supports a copy flag; for example, the right *r* with the copy flag would be written as *rc*. In this case, write a command to do the copy.
   (c) In the previous part, what happens if the copy flag is *not* copied?

5. (*24 points*) In the story "Superiority" by Arthur C. Clarke, one mistake the narrator's military made was relying upon their superior science to defeat an enemy with vastly inferior science. In answering the following questions, show how your answer can be applied to, or says something about, computer security.
   (a) Prof. Norden's claims about the new weaponry were verified by experimentation. Yet the weapons failed to perform as they should have in battle. Why were the weapons so effective in Prof. Norden's experiments, yet such a failure when used in battle?
   (b) The Battle Analyzer was an automated system to analyze the enemy's positions and weapons used during a battle. It worked in one battle—the enemy was badly beaten—but not in the ones following that. What did the Battle Analyzer apparently fail to take into account?
   (c) What was the flaw in Prof. Norden's experiments testing the Exponential Field?