Homework 5

Due Date: March 16, 1998 at 11:59PM **Points**: 100
Late Date: March 18, 1998 at 11:59PM (20% penalty)

1. A race condition requires a window of vulnerability in the code and certain environmental conditions to exist during that window. Typically, this window is very small because the relevant lines of code follow one another:

   ```
   if (access("/tmp/xyz", R_OK) == 0)
         fd = open("/tmp/xyz", RD_ONLY);
   ```

   Replacing the file "/tmp/xyz" during this window can be quite difficult because the window in which the replacement will have an effect is very brief. Describe how to increase the probability of hitting this window and successfully making the replacement.

2. The following is a fragment of code used to initialize a random password generator. Critique it. Is it good, or does it allow attackers to guess passwords easily?

   ```
   srandom(time()^getpid());
   ```

3. In class, we alluded to the year 2038 being a problem for most UNIX systems because of the way time is represented. What specific aspect of the representation makes that year a problem? When during the year does the problem occur? (Give a specific date and time.)

4. Any user-supplied passwords should be erased from a program's memory as quickly as possible. Why? Describe a scenario in which failing to erase a password may lead to the compromise of that password without an attacker reading the process memory.