Homework 5

Due: Friday, March 14, 1997 at 11:59PM

Analytical

These are worth 40 points each.

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 *system*(3) library function spawns a subshell to execute the command given in *system*'s argument string. How would you sanitize the environmental variables to make the subproces immune to exploits involving those variables? Specifically, which variables would you delete from the environment, and which would you allow through (note any restrictions on the value of these that you would enforce).

3. A (possibly apocraphyl) version of the setuid-to-*root* program*su*(1) would attempt to open the password file to validate a password. If the password file could not be opened, it assumed a catastrophic system failure occurred and immediately granted *root* access to the user. Do you think this was a good idea? Specifically, describe how an attacker could acquire *root* access when the password file was present and accessible to *root*.
   Hint: The number of file descriptors available to a program was 19.

4. 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());
   ```

5. What is the danger in the following code fragment? How would you fix it?

   ```
   int main(int argc, char *argv[])
   {
         char filename[MAXPATHLEN];
         if (argc==1)
               (void) sprintf(filename, "/tmp/xxx%d", getpid());
         else
               (void) sprintf(filename, "/tmp/%s", argv[1]);
         if ((fd = open(filename, O_RDWR|O_EXCL|O_CREAT, 0644) )< 0){
               perror(filename);
               exit(1);
         }
         …
   ```

Programming

There is no program on this assignment. Please use the time for your projects, which are due on March 14!