Homework 3

Due Date: February 17, 2006 Points: 100

1. (*10 points*) Text, problem 2.1.
2. (*15 points*) Text, problem 2.5.
3. (*5 points*) Text, problem 4.1.
4. (*20 points*) Text, problem 4.5.
5. (*50 points*) The goal of this program is to have you use a static source code analyzer to find potential security problems. To do this problem, you need to download the file *lsu.tar*, copy it onto a system at the CSIF, and unpack it. Once on the CSIF, type

   ```
   tar xvf lsu.tar
   ```

   and you will find a directory named *lsu* containing the program *lsu*. It consists of several source files. The ones of interest to us end in ".c". First, we'll run a souce code analyzer over the program to find possible errors. Then, we will examine several.

   a. Run the program

      ```
      /usr/local/FortifySoftware/SCAS-TE/sourceanalyzer gcc *.c
      ```

      from within the *lsu* directory. Save the output in a file; it's long, and you'll need to refer to it later. The program *sourceanalyzer* is a tool written by Fortify Software. It analyzes programs for possible vulnerabilities, and when it finds one, it describes it and gives a trace of the routines involved in an attack exploiting the vulnerability.

   b. Look at the output. You are to choose one flaw from each of the following categories:
      - Buffer overflow (pick one marked "high". Note: do not pick the one at *util.c*(36)!)
      - Process control
      - Integer overflow
      - Race condition: TOCTOU

      For each one you selected, describe in detail the flow of data that would allow an attacker to exploit the flaw. For example, for integer overflow, you should say something like this:
      1. Attacker passes 2^{31}–1 arguments to program (via main function in file main.c line 25)
      2. Program appends 3 more arguments (see main.c line 36)
      3. Counter for loop in which the arguments are appended overflows (see main.c lines 34-38)

      Of course, this is a made-up example, not one drawn from *lsu*. But it gives you the level of detail we want. Please copy the messages from the run of *sourceanalyzer* describing the vulnerability and the trace of functions and files below it. Then write your description beneath. You can pick any instance of the type of flaw except for the ones noted for buffer overflow, above.

   c. Now go back to the buffer overflow at *util.c*(36). It's the first buffer overflow marked "high" in the output, assuming you used the command given above. Analyze this report. Is it an exploitable buffer overflow flaw? If so, please explain exactly where the overflow occurs, and why. If not, please explain why it is not exploitable (or not a vulnerability).

Extra Credit

1. (*20 points*) Text, problem 3.1.
2. (*25 points*) Text, problem 3.3.