26. Write a program that contains a buffer overflow that can be meaningfully exploited without modifying the execution of the program. [It should be like the gamble.c example in class.]

   Include:
   
   - The source code for the program,
   - The executable for the program,
   - An explanation of the buffer overflow condition, and
   - A demonstration of how the buffer overflow results in a program compromise.

   The overflow condition should not be immediately obvious to someone reading the source code.

27. Write a program that contains an integer overflow that can be meaningfully exploited in some way.

   Include:
   
   - The source code for the program,
   - The executable for the program,
   - An explanation of the buffer overflow condition, and
   - A demonstration of how to exploit the program.

   The overflow condition should not be immediately obvious to someone reading the source code.

28. Write a program that demonstrates the use of format strings for output functions. It should be a suitable example for an introductory programming course.

29. Write a program that has a format string flaw. Exploit the flaw to return the value of an unrelated variable.

30. Using the previous program, exploit the flaw and modify the value of the unrelated variable. Show how to control the result.

31. Read the documentation from the GNU project about function attributes. Write a program that implements an attribute [other than destructor,fastcall or stdcall].

   The documentation for the latest version of gcc can be found at, for example, http://gcc.gnu.org/onlinedocs/gcc/Function-Attributes.html.

   The current version of gcc is 4.1.1; however this is not installed on the lab machines. The lab has 3.3.5, and the documentation specific to that version is available at http://gcc.gnu.org/onlinedocs/gcc-3.3.5/gcc/Function-Attributes.html.

32. Write a program that has a format string flaw. Make the program SUID root, and exploit it to obtain a root shell. Overwrite the .dtors section to start the execution of the shellcode.

33. Exploit the previous program to obtain a root shell, but this time overwrite an entry in the .plt table.