COSC 647
Application Software Security
Assignment Sheet #1

1. Write any C program. Compile it using gcc.
   
   (a) What is the effect of the option `-Wall`?
   (b) What is the effect of the option `-pedantic`?
   (c) What is the difference in the size of the code compiled with and without `-g`?
   (d) What is the difference in the size of the code compiled with `-O1` , `-O2`, and `-O3`?

2. Open the previous C program in the debugger gdb. Set a breakpoint at the first line. Run the
   program to that point.
   
   • What is the current ESP?
   • What is the current EBP?
   • What is the current EIP?
   • Use the `x` command to show the assembly language code for the next few commands to be
     executed.

3. Repeat the previous question, but use the graphical debugger. Show the relevant screen shots.

4. Use objdump to find the address of the following sections in your program:
   
   • `text`
   • `bss`
   • `data`

5. Write the “Hello World” program described in class. Compile it and link it.
   
   (a) Include the source, object, and executable code.
   (b) Debug the program. What memory addresses contain the program’s environment strings?
   (c) Debug the program. What memory address contains the program’s arguments?
   (d) Debug the program, and stop it immediately before the syscall for write.
     
     • What is the current ESP?
     • What is the current EBP?
     • What is the current EIP?
   (e) Debug the program. Where is the message string located?
   (f) How many bytes are needed for the `.start` function?