COSC 647

Homework 2 – Due Oct 21, 2015

1. Write your shellcode to, instead of spawning a shell, do the “ls -a” command. Test your shellcode to show it works.

2. Write a program that contains a stack-based (or stack smashing) buffer overflow. Explain in detail why the program has a stack based buffer overflow flaw. Demonstrate the flaw by causing the program to crash with a segmentation fault. Include the state of the stack before the crash, and determine exactly why the program crashed?

3. Employ your shellcode in question #1 to problem #2. Demonstrate that the exploited program will run the command “ls -a”. Display your results. (Hint: The lab will help)

4. Give an example of a program that contains an integer overflow error, and explain the problem. Correct the flaw by implementing appropriate range checking. Do not change the types (int, unsigned int, etc) of any of the variables.