Project #1 Grading Rubric

Task 1 (40 points)

1. A C program containing a stack buffer overflow vulnerability

   15 points

2. Drawing a figure to illustrate the stack frame layout when your stack buffer overflow occurs, including: 1) the order of parameters (if applicable), return address, saved registers (if applicable), and local variable(s); 2) their sizes in bytes; 3) size of the overflowing buffer to reach return address and overflowing direction. The figure should be searchable in pdf, instead of other formats like png.

   20 points

   1) correct order: 7 points
   2) sizes: 6 points
   3) overflowing: 7 points

Briefly explaining how to exploit your stack buffer overflow

   5 points

Task 2 (60 points)

1. If your *script* or *data.txt* can successfully open the shell by exploiting the stack buffer overflow, you will get full points.

2. If not,

1) correct addresses of *system()* and *"sh"*

   each accounts for 15 points

2) correct locations of addresses of *system()* and *"sh"* in your generated overflowing buffer

   each accounts for 15 points