Lab 4: Return-to-libc Attack Lab

This lab assignment aims to let you gain first-hand experience with an interesting attack on buffer overflow vulnerability; this attack can bypass an existing protection scheme currently implemented in Linux operating systems. Please refer to the following link at SEEDLabs:

- The lab description is provided on Brightspace.
- Some code is also provided on Brightspace Labsetup.zip

In this lab, the value for BUF_SIZE is set to **N = 80; do not modify this value**

Please review the "Grading rubric" below and work only on the required tasks.

If you have any questions, please let the instructor know.

Deliverables:

Upload a Word document containing each Task's terminal outputs (Use screenshots):

Please include all source code, shell commands, and running results in the lab report. That is, please describe what you have done and what you have observed, including screenshots and code snippets. Do not forget to include your observations when required.

Note: Include your code (or a screenshot of it) when (1) first calling the program and (2) when modifying the code

Work only on the required tasks as follows:

- Environment Setup – 20pts
- Task 1 – 20pts
- Task 2 – 20pts
- Task 3 – 40pts (= 30pts + 5pts + 5pts)

Total: 100pts

Bonus: Task 4 – 15 pts