Lab 3: Buffer-Overflow Vulnerability Lab (Set-UID Version)

This lab assignment aims to let you gain first-hand experience on buffer-overflow vulnerability.

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

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.

In this lab, the values for L1 and L2 in the Makefile are set to 120; do not modify these values.

Moreover, 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 (These can be a screenshot):

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

Work only on the required tasks as follows:

- Environment Setup – 5pts
- Task 1 (Getting Familiar with Shellcode) – 10pts
- Task 2 (Understanding the Vulnerable Program) – 5pts
- Task 3 (Launching Attack on 32-bit program (Level 1)) – 70pts
  - Investigation – 30 pts
  - Launching Attacks – 40 pts
- Task 5 (Defeating dash's Countermeasure) – 30pts
- Task 6 (Defeating Address Randomization) – 10pts
- Task 7 (Experimenting with Other Countermeasures) – 20pts
  - Turn on the StackGuard Protection – 10pts
  - Turn on the Non-executable Stack Protection – 10pts

Total: 150pts

Bonus: Task 4 (Launching Attack without Knowing Buffer Size (Level 2)) – 20pts