# PCS Lab 1: Buffer Overflow Instructions

## Instructions

Read and follow the SEED lab instructions below, and answer the questions in the next page.

SEED Lab Instruction on Buffer Overflow:
http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Software/Buffer_Overflow/Buffer_Overflow.pdf

Background info and code templates:
http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Software/Buffer_Overflow/

About the VM: http://www.cis.syr.edu/~wedu/seed/lab_env.html
User ID: seed
Password: dees

**NOTE**: Running program under GDB may make stack frames a few bytes off track compared to normal execution. For the final submission, always make sure your exploit works when running './stack' without GDB.

## Submission

**Due: Feb 27, 11:00 PM (EST)**

Late submissions are accepted with 50% grading penalty within 24 hours of the due. Submissions that are late for more than 24 hours will NOT be accepted.

Please submit your solution in PDF or image on https://www.gradescope.com/courses/38640, using Entry Code: **95KJWX**. And kindly choose the right page for your answer to every question.

# Questions

Question 1: Please provide the names and NetIDs of your collaborator (up to 2). If you finished the lab alone, write None.

**Collaboration Policy**

1. **You can optionally form study groups consisting of up to 3 person per group (including yourself).**
2. **Everybody should write individually by themselves, and submit the lab reports separately. DO NOT copy each other's lab reports, or show your lab reports to anyone other than the course staff, or read other students' lab reports.**

Question 2: Please describe your observations "Task 1: Running Shellcode", including necessary screenshots.

Question 3: Please describe your observations "Task 2: Exploiting the Vulnerability", including necessary screenshots.

Question 4: Please paste the memory address of the variable "buffer" in your VM.

Question 5: Please paste your exploit.c or exploit.py for "Task 2: Exploiting the Vulnerability".

Question 6: Please paste the output of "hexdump badfile" for "Task 2: Exploiting the Vulnerability".

Question 7: Please describe your observations of "Task 3: Defeating dash's Countermeasure", including necessary screenshots. You should also explain why the changes in Task 3 defeat dash's Countermeasure.

Question 8: Please describe and explain your observations of "Task 4: Defeating Address Randomization", including necessary screenshots.

Question 9: Please describe and explain your observations of "Task 5: Turn on the StackGuard Protection", including necessary screenshots.

Question 10: Please describe and explain your observations of "Task 6: Turn on the Non-executable Stack Protection".

Question 11: Please fix the problem so that bof is able to copy arbitrarily long inputs without causing memory corruption. (hint: malloc)