**Assignment 1**

**Due Monday October 3 at 6:00 pm**

In this assignment, you will be given a program with a buffer-overflow vulnerability; your task is to develop a scheme to exploit the vulnerability and finally gain the root privilege.

You will need to follow the project description located here:

* Go to the link below, then click on “Description”: https://seedsecuritylabs.org/Labs\_16.04/Software/Buffer\_Overflow/

For this assignment, you are only required to complete **Task 1 and Task 2** described in the link above. You will a BUF\_SIZE of 64. This requires you to modify stack.c as such:

#ifndef BUF\_SIZE

#define BUF\_SIZE 64

#endif

You will submit **all of the code** that you used for this project along with a **readme.txt** that describes the files used for each task and how to run them. You will submit a project report that needs to include the information specified in the rubric on Canvas.

**Additional Resources**

* The code and other resources needed for the buffer overflow project: https://seedsecuritylabs.org/Labs\_16.04/Software/Buffer\_Overflow/
* SEEDUbuntu16.04 virtual machine environment, installation steps, and login information for the Ubuntu 16.04 VM: https://seedsecuritylabs.org/lab\_env.html

**Submission**

You need to submit all of the following via canvas:

* The written report in doc or docx format
* A readme.txt file that
* All the files you’ve used for the attack project
* Online students will submit a recording that demonstrates the entire assignment. In-person students will perform a live demo.

**Do not compress these files into a .zip or .tar.gz. Each file must be uploaded separately.**