

## Programming Project 1: Buffer Overflow and Return-to-Libc

Out: 08/28/19 Due: 09/18/19 10:59am

### Instructions

1. Strictly adhere to the University of Maryland Code of Academic Integrity.
2. Submit the source code as a .zip file containing the .c code, as well as a writeup explaining what you did as a pdf document at Canvas. Include your full name in the writeup. Name the .zip file as x-project1.zip and the writeup as x-project1.pdf, where x is your first and last name. For example, if your name is “Jane Doe,” you should be handing in two files named “JaneDoe-project1.zip” and “JaneDoe-project1.pdf.”

*Labs are sourced from SEED labs <https://seedsecuritylabs.org/>*

## 1 Overview

In this lab, students will be given a program with a buffer-overflow vulnerability; their task is to develop a scheme to exploit the vulnerability and finally gain the root privilege. There are two parts to the lab. In the first part of the lab, the non-executable stack countermeasure is turned off, making the attack easier, since a simple injection of the shellcode works. In the second part of the lab, the non-executable stack countermeasure is turned on, making the attack harder. In this case, code injection is not possible and instead the students will execute a “Return-to-Libc” attack. In addition to the above, students will be guided to walk through several additional protection schemes that have been implemented in the operating system to counter against the buffer-overflow attacks. Students need to evaluate whether the schemes work or not and explain why.

## 2 Lab Tasks

### 2.1 Setting Up the Virtual Machines

Most of our labs are taken from the SEED website: [https://seedsecuritylabs.org/Labs\\_16.04/](https://seedsecuritylabs.org/Labs_16.04/). Before you can start doing the labs, you must install Virtual Box and must load the pre-built Ubuntu virtual machine (SEEDUbuntu16.04.zip). In order to do this, see instructions here: [https://seedsecuritylabs.org/lab\\_env.html](https://seedsecuritylabs.org/lab_env.html). Please make sure to carefully read the documentation here [https://seedsecuritylabs.org/Labs\\_16.04/Documents/SEEDVM\\_VirtualBoxManual.pdf](https://seedsecuritylabs.org/Labs_16.04/Documents/SEEDVM_VirtualBoxManual.pdf) which explains how to configure and run the machine.

## 2.2 Part I

Follow the instructions for the SEED Buffer Overflow lab, which can be found here: [https://seedsecuritylabs.org/Labs\\_16.04/Software/Buffer\\_Overflow/](https://seedsecuritylabs.org/Labs_16.04/Software/Buffer_Overflow/).

## 2.3 Part II

Follow the instructions for the SEED Return-to-Libc lab, which can be found here: [https://seedsecuritylabs.org/Labs\\_16.04/Software/Return\\_to\\_Libc/](https://seedsecuritylabs.org/Labs_16.04/Software/Return_to_Libc/).

## 3 Submission

Students need to submit the source code as a .zip file containing the .c code, as well as a writeup explaining what you did as a pdf document at Canvas. Some questions in the labs are open-ended and there is not necessarily a right or wrong answer. Be sure to include screenshots and document your step-by-step process to receive full credit. Include your full name in the writeup. Name the .zip file as x-project1.zip and the writeup as x-project1.pdf, where x is your first and last name. For example, if your name is “Jane Doe,” you should be handing in two files named “JaneDoe-project1.zip” and “JaneDoe-project1.pdf.”