CS 5153/6053 Network Security, Spring 2023
Project 2: Buffer Overflow Attack

Instructor: Dr. Boyang Wang

Due Date: 2/27/2023 (Monday), 11:59pm.
Format: Please submit a zip file of your code in Canvas.
Total Points: 12 points

Note: This is an individual project. The instructor would like to thank Dr. Wenliang Du from Syracuse University for making the project materials of SEED Labs public and free for students to use.

1 Project Description

In this project, you will need to implement Buffer Overflow Attack by using the project materials offered by SEED Labs 1.0 (based on Ubuntu 16.04) [4]. The description of the buffer overflow attack project offered by SEED Labs can be found at [1]. A copy of the description can also be found in Canvas.

There are several tasks described in the description. **You only need to complete Task 2 Exploiting the Vulnerability** by following the example we discussed in class. You do not need to write the code from scratch. Most of the code (in `stack.c, exploit.c, exploit.py`) are already given and can be found at [1]. You will need to download the code and complete the parts that are still missing. The buffer size `BUF_SIZE` in `stack.c` is **100 (for CS5153) and 130 (for CS6053)**. You can use either `exploit.c` or `exploit.py` to generate the `badfile`. More details can be found in the project description.

To complete the project, you will need to first install a Virtual Machine with Linux (Ubuntu 16.04-32bit). You can find the instruction regarding how to install it and download a copy of the Linux at this webpage [2]. You can also find information regarding the setting for your Virtual Machine at this webpage [3]. You will need the virtual machine in other projects as well so please spend time to get familiar with the setting and make sure you setup the VM properly.

2 Basic Requirements

Program Directory: Please name your project folder in the form of `buffer_m123456`, where `buffer` is the name of this project and `m123456` is your UCID. The recommended directories of your program should be organized as follows:

```
./buffer_m123456/src
./buffer_m123456/report.pdf
```

Folder `src` should include all the source files that you have completed. In `report.pdf` file, you should describe

- How do you perform the attack in your VM;
- How do you find the value of ebp;
- How do you decide the content of badfile;
- Whether your attack is successful.

In addition, you need to include screenshots to show each of those steps in your report.

References

1. Buffer-overflow vulnerability lab, `https://seedsecuritylabs.org/Labs_16.04/Software/Buffer_Overflow/`
2. Lab enviroment setup, `https://seedsecuritylabs.org/lab_env.html`
3. Lab enviroment setup manual, `https://seedsecuritylabs.org/Labs_16.04/Documents/SEEDVM_VirtualBoxManual.pdf`
4. Seed labs (hands-on labs for security education), `https://seedsecuritylabs.org/`