CSC 472/583 Fall 2021 Lab 2

Dr. Si Chen

September 29, 2021

Stack Overflow

The goals of this lab:

- Understanding the concepts of stack overflow
- Exploiting a stack buffer overflow vulnerability

Students should be able to clearly explain: 1) what is stack overflow; 2) why stack overflow is dangerous; 3) how to exploit a stack overflow. With the knowledge about stack overflow, students are expected to launch an attack that exploits a stack buffer overflow vulnerability in a provided toy program.

Our course webpage: https://www.cs.wcupa.edu/schen/ss2021/

Return Hijack Attack (10 points)

The provided C code (lab2.c) contains a stack buffer overflow vulnerability. Please write an exploit Python script using pwntools library to output **"hacked by YOUNAME!!!!"** (replace YOUNAME by your first+last name) on Linux. The high level idea is to overwrite the return address with the address of function hacked(). Once the return instruction is executed, this function will be called and output the string.

You can use our Badger CTF system to complete this project.

Steps:

1. Connect to Badger CTF with your own account.
2. Download the provided C code from our course website to folder "/workdir/". You can type the following command after successfully login Badger CTF to download the source code:

```
wget https://www.cs.wcupa.edu/schen/ss2021/lab/lab2.c
```

3. open the source code with command line text editor (e.g. Vim, nano) and make the following changes:
   - Set the array (char array[]) size **equal to the last two digits of your student ID** (e.g. 0861339 $->$ array size should set to 39).
   - Change the string literal YOUNAME inside "hacked" function to your name (e.g. Si Chen).
4. Compile the C code:

```
gcc lab2.c -o lab2 -m32 -fno-stack-protector -zexecstack -no-pie
```

5. When you run the program and type a very long list of character, you will notice lab2 crashes with memory segfault, this is because the return address has been overwritten by your data.
6. Now you can craft your shellcode by using Python with pwntools library. A script template is available on our website (feel free to use it). Your goal is to overwrite the return address with the address of function **hacked()**. GDB can be used to find these library addresses and test/debug your exploit.
7. Provide a screenshot of you exploiting sort.
8. Have fun.

Deliverables: A screenshot of the exploit script (exploit.py) and a screenshot of the result after executing your script. You also need to answer how to find the **Magic Number** (length of the dummy-character string) which allows your to successfully overwrite the return address.

Submission

- The project due date is on our course website. Late submission will not be accepted;
- The assignment should be submitted to D2L directly.
- Your submission should include: A **detailed project report in PDF format** to describe what you have done, including screenshots and code snippets.
- **No copy or cheating is tolerated**. If your work is based on others', please give clear attribution. Otherwise, you **WILL FAIL** this course.