CSc 466/566 Computer Security

Assignment 5

Due 23:59, Wednesday Oct 9, 2019
Worth 16% (ugrads), 16% (grads)

Christian Collberg
Department of Computer Science, University of Arizona

A. Introduction

In this assignment we'll study buffer overflow attacks.

B. Preparation

1. Install VirtualBox on your machine:

   `https://www.virtualbox.org/wiki/Downloads`

2. Go to

   `http://www.cis.syr.edu/~wedu/seed/lab_env.html`

   and download

   `SEEDUbuntu-16.04-32bit.zip`

   This file contains an image of the virtual machine on which you should work. The homework will be graded only on this virtual machine.

3. Read these manuals, and follow the instructions to start up your VM:

   - `http://www.cis.syr.edu/~wedu/seed/Documentation/Ubuntu16_04_VM/Ubuntu16_04_VM_Manual.pdf`
   - `http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Documents/SEEDVM_VirtualBoxManual.pdf`

4. Log on to the system, using the following credentials:

   ```
   Username : seed
   Password: dees
   ```

   Certain steps in the homework will require you to have root access. In such cases, use the following credentials:

   ```
   Username: root
   Password: seedubuntu
   ```

C. Buffer Overflow Attacks

1. Go to

   `http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Software/Buffer_Overflow/`

2. Copy the files `stack.c`, `call_shellcode.c`, `exploit.c` into your VM.

3. Prepare, by

   (a) reading the **Description**, in particular Section 3, **Guidelines**:

   `http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Software/Buffer_Overflow/Buffer_Overflow.pdf`

   (b) and by watching the videos:

   `http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Software/Buffer_Overflow`

4. Follow the instructions in **Description** and solve the following tasks:

Task	Marks
1	25
2	25
3	25
4	25

5. Write a lab report that explains what you did. Include the modifed files `stack.c` and `exploit.c`. Provide screen shots that illustrate your findings and show that your code works (i.e., for task 1, that you get a root shell).

6. Your lab-report should consist of **one pdf file**, called `labreport.pdf`.

7. Submit `labreport.pdf` to d2l.

D. Academic Integrity

This is an individual take-home assignment and it is obviously possible for you to get help solving it. This, however, **IS NOT ALLOWED**. You are bound by the University's rules of academic conduct as well as these rules:

1. You are not allowed to discuss the assignment with any human. This includes
   - Posting questions and getting help from online forums;
   - Getting help from classmates;
   - Getting help from anyone outside class.
2. You may not *provide* help to your classmates.

If you have any questions about the assignment you should see the instructor or the TA.