Assignment #3: Buffer Overflow Vulnerability Lab

CSC 574 – Computer and Network Security
Spring 2013 – Prof. Enck
Assignment Value: 100 points

Due date: February 21, 2013

In this assignment, students will learn how buffer overflow exploits work through practical example. To complete this assignment, students should follow the Buffer-Overflow Vulnerability Lab provided as part of the NSF SEED project (`http://www.cis.syr.edu/~wedu/seed/`) and document their experience.

1 Assignment Details

The assignment details are available here:

`http://www.cis.syr.edu/~wedu/seed/Labs/Vulnerability/Buffer_Overflow/`

This page includes a link to a PDF describing the setup and four lab tasks. The end of the document provides an overview of the concepts needed to complete the assignment. Further explanation of exploiting stack-based buffer overflows can be found in the document "Smashing The Stack For Fun and Profit" (linked to from the lab description), as well as many available online resources. While students are required to work independently on this assignment, they are strongly encouraged to search the Web for examples and tips for completing the described tasks (but you are not allowed to post questions to discussion forums).

2 Performing the Tasks

The assignment requires access to a Linux system on which the student has root access. The SEED project provides virtual machine images that can be used for the assignment:

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

Students are not required to use the provided VM image; however, if you encounter difficulties, try using the provided VM image before asking for help. The instructions describe how to perform the lab on both Ubuntu and Fedora, but additional steps may be needed for newer versions of these operating systems.

The experiences and answers to lab questions should be documented in a single PDF file (`lastname-assign3.pdf`). LaTeX is perferred, but for this assignment, the report can be documented in any word processing environment you prefer, as long as the end product is a PDF file.

3 Submission Instructions

You **must** turn in one `.tar.gz` or `.zip` file named `lastname-assign3.tar.gz` or `lastname-assign3.zip`, respectively. No other archive file formats (e.g., RAR) will be accepted. The archive should contain the following:

1. `lastname-assign3.pdf`: This is a PDF that documents your work and experiences.
2. `survey.pdf`: This is a PDF of the lab survey: `http://www.cis.syr.edu/~wedu/seed/Survey_Questionnaires/BufferOverflow_Questionnaire.doc`
3. Any new or modified files used for the assignment. How these files are used should be described in `lastname-assign3.pdf`.

4 Grading Guidelines

Even if you cannot complete a task, describe what you have done, what happens, and what you think might be the problem. Partially credit will be given as appropriate.

5 Note on Academic Dishonesty

As with all assignments in this class, you required to perform the work alone. You are allowed (and encouraged) to research the topic on the Internet and use examples to help construct the solutions to the tasks. However, you are not allowed to copy solutions to this assignment from the Internet.

Failure to abide by these requirements will result in academic sanctions up to dismissal from the class and involvement of Academic Affairs.