Computer Science 330
Operating Systems
Siena College
Spring 2012

Lab 9: Security

Due: 4:00 PM, Monday, April 30, 2012

In this last lab, you will spend some time looking at a common security problem based on the problem of the *buffer overflow*.

You may work alone or with a partner on this lab.

Readings

Start by reading these pages, which are quite long and detailed, but also interesting and informative. You will find there is some overlap in content.

- Smashing The Stack For Fun And Profit
- FreeBSD Developer's Handbook Section on Buffer Overflow
- Wikipedia Article on Buffer Overflow

Trying Things Out

We will use `winterstorm.teresco.org` to try this out. In the shared area, you will find a directory called `bufferoverflow` containing several files, including some from the documents you just read, compiled for use on this FreeBSD system.

The only one we will try is in `bufferoverflow.c`, which has been compiled up to an executable called `bufferoverflow`.

Here, we read characters into a buffer that's local to main then call a function that copies it into a smaller buffer. If the input we type is longer than 80 characters, it doesn't fit.

The script `trysizes` is provided to allow you to run this program with various interesting numbers of spaces on the input. We can also watch what's happening here by compiling with `-g` (which the executables in the shared area have been) and running in `gdb`.

Question 1: Explain what is happening here. You will see that some inputs lead to a correct execution, while others cause a data corruption but successful execution to completion, and others cause the program crash.

Look also at `vulnerable.c`, which contains a similar error and `exploit.c` which attempts to exploit this vulnerability. In versions of FreeBSD prior to 7.0 (which I no longer have available to me, unfortunately), this could be used to demonstrate an exploited buffer overflow, resulting in a regular user gaining root access if the vulnerable executable was installed as setuid root.

Submission and Evaluation

This lab will be graded out of 10 points (based on your answer to the one question above).

By 4:00 PM, Monday, April 30, 2012, submit your answer to the lab questions by email to *jteresco@siena.edu*.