CMPSCI 177 – Computer Security
Fall 2013
Homework #6 – Buffer Overflow

Due: 27 NOV 12 2:00pm

This assignment helps you develop a detailed understanding of the call stack organization on IA32 Intel Pentium processors. It is divided into two parts as explained below.

Part 1

In this part, your task is to write a program exploit.c that will exploit the program check_auth.c. The code for check_auth.c can be found at:

https://gist.github.com/cs177/26b988d7ca6c5bdb36f0

This program accepts a password from the command line and either denies access or grants access. Your goal is to supply an input that causes a buffer overflow and diverts the control flow to the statement that prints "Access Granted!" Try to avoid causing any segmentation faults.

Part 2

In this part, your task is to write a program exploit.c that will exploit the program, vulnerable.c. It can be found here: https://gist.github.com/cs177/9b9b6763a751af5d2242

Unlike part1, to exploit this program you will have to execute code on the stack, which is the actual challenge involved in buffer overflow exploits. Your exploit should open a new shell (/bin/sh).

Test Environment

You should carry out the buffer overflow assignment on 192.35.222.54. Your login and password have been provided via email. If you did not receive it, please email your TA at kyle [a t] cs.ucsb.edu.

Assignment Turnin and Instructions

To submit, create two directories, part1 and part2. In each directory, place all source files, a makefile to compile everything, and a README explaining in detail how you exploited the buffer overflow.

Lastly, create an archive of the directories part1 and part2 called solution.tgz in your home directory. We will use this archive for grading, not the directories.

We will be shutting down the server and collecting all solutions at the deadline, so make sure you get it created on time.