University of Maryland
CMSC414 — Computer and Network Security
Professor Jonathan Katz

Problem Set 4

Please turn in a hard-copy in class on May 8
This homework is to be done individually

In this homework you will exploit buffer overflow attacks in three password authentication programs. The goal in each case is to get the program to print out an "Authorization successful" message *even though you do not know the password*. The compiled programs and their source code can be found on grace in the following directory:

`/afs/glue.umd.edu/class/spring2008/cmsc/414/0101/public`

I have only tested the programs on the linux cluster; therefore, I recommend that you log into `linux.grace.umd.edu` for this assignment.

For each of the three programs, you should turn in the following:

1. A 1- or 2-paragraph summary of how your attack works/what your attack does.
2. A 1-line command that executes the attack from the command line. E.g., your attack on a program `pwd1` might look like this:

```
perl -e 'print ''abc'' ' | pwd1
```

Each program you attack will reveal words of a phrase; please turn in this phrase as well.

The goal of the assignment is to learn about buffer overflow attacks. Thus, even though there may be other ways to "attack" the programs (e.g., brute-force password guessing; using gdb to figure out the unknown password), these will not be given credit for this homework.

Collaboration. This homework is to be done *without assistance from other students in the class*. Questions about the homework should be directed to the TA and/or the professor. *Start early.*