CSc 466/566 Computer Security

Assignment 3

Due 23:59, Monday September 16
Worth 16% (ugrads), 16% (grads)

Christian Collberg
Department of Computer Science, University of Arizona

A. Introduction

In this exercise you will learn how to hack code!

B. Crack a Program [100 points]

1. Go to `revenge.cs.arizona.edu` and navigate to the *educational tool*
2. Follow the instructions to set up a virtual machine on the Tools page in the For Students tab.
3. In the virtual machine, log on to `http://revenge.cs.arizona.edu/RevEngE/index.jsp` with the information we provide.
4. Go to the *My Challenges* tab and select *Assignment 3*. Generate and download the challenge. The challenge will be an executable binary compiled for Linux x64.
5. Your task is to

   (a) disable an expired-time check

   that prevent the program from running.
6. Create a `README.txt` file with the following information, exactly in this format:

```
FIRSTNAME:      Bob
LASTNAME:       Jones
EMAILADDRESS:   bob@cia.gov
UNDERGRADUATE,MASTERS,PHD: (U/M/P)
TOOLS:          what tools, if any did you use
TECHNIQUES:     what techniques did you use
TIME:           how long did it take you (in hh format)
DIFFICULTY:     on a scale of 1-10 (1 is the easiest, 10 the hardest)
CHALLENGES:     what, in particular, did you find particularly easy or hard
COMMENTS:       how hard was this, did you enjoy it, what could have been
                done differently, etc.
```

7. Submit the cracked file to `revenge.cs.arizona.edu`.

If you're interested in contributing to Claire's PhD research, ahve a look at the data collection software under the *For Students tab.*

C. 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 may use any technique that you want to work the assignment.
2. You may use any tools (including those that you download from the web, buy, or build yourself) that you want to work the assignment. Previous students report that they have used: IDA 6.1 64bit, gdb, strace, hexedit, ltrace, hxd hex editor, asm, nm, faketime, hexeditor, python, grep, graphviz, VS2010, pen and paper (!), notepad++, Dev-C, GHex, geany, brain (!), bless, codeblocks, WinMerge, freemind. The virtual machine has a subset of these tools built in to use.
3. 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.
4. You may not *provide* help to your classmates.

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