CS 232 Introduction to C and Unix

HW4 (Due on February 17, 2022, 11:59pm)

This homework will test your ability to use the gdb debugger to step through a C program. It will also test your ability to understand C code as you try to find the passwords that will defuse the "bomb" program. After this homework, you should feel comfortable reading C programs and figuring out what they do. You should also feel comfortable using gdb. Another important aspect of this homework is that it forces you to think methodically and carefully about code in order to fully understand it. Please start this homework assignment early.

Collaboration policy:

Similar to homework 2 and 3, you are to work alone. If you get stuck on part of the homework, you are encouraged to come by office hours. If you cannot make office hours, just send me an email and we can find a time to meet. I'm here to help you, but I do not know how to help if you don't ask me.

Homework description (Defusing a Computer Bomb):

READ THE ENTIRE HOMEWORK DESCRIPTION CAREFULLY BEFORE BEGINNING THE HOMEWORK.

Log into diamond.pfw.edu Linux server and find the executable file “theBomb” under /home/chenz. The “theBomb” can only be run, not read or written except the owner of the file.

Your goal in the homework is to defuse the bomb, which requires that you enter an appropriate password at each of several stages. Each time you enter an incorrect password, the bomb will explode, an email will be sent to you, TA, and the instructor, and then you will lose 3 points (out of 100 total).

Fortunately, Dr. Evil is not the brightest villain in the world, so he forgot to remove the debugging information from the bomb and some of the source code. This information will help you figure out what the passwords are.

Hints:

- The first step is to open the source file theBomb.c (in pdf) and get a sense of what the program will do when you run it. This source file can be found in Brightspace so that you can print it out. You don’t have to understand every step of the code at first, but you

should get some idea of the program flow. In particular, you should know what points in the code could trigger a bomb explosion.

- It is possible to figure out the passwords by just looking at the source code. However, it might be helpful to step through parts of the program in gdb in order to understand the code better. You can run the bomb in gdb using the normal command:

  $ gdb /home/chenz/theBomb

  Note that the bomb can still explode, even when you are running it in gdb. Thus, you should use gdb commands to make sure that the bomb never enters the explosion routine, even if it receives a bad password. (Since part of the assignment is to test your knowledge of gdb, it is up to you to figure out what gdb commands you can use to prevent the bomb from exploding.)
- When you have a guess at one (or more) of the passwords, you can run the bomb in gdb and input those passwords to check if they work. You should use gdb to check the passwords because you can use the gdb commands to provide a safety net in case the password guess is incorrect. That is, use gdb commands to ensure that the bomb will not enter the explosion routine even if your password guess is incorrect. (Note that you will have to set up the safety net before you enter the password guess. Otherwise, it could be too late!)
- Even though it may seem obvious, remember to not let the bomb explode! The bomb can explode any time you run theBomb and enter an incorrect password at any stage. Even if you are running theBomb in gdb, it can still explode. Also, tampering with the bomb executable might cause it to explode (which will lower your grade).
- In addition to the real bomb, there is a practice bomb in the class examples for gdb (in Brightspace under “Slides and Examples” directory). You may experiment with it without risk of losing points for an explosion. We may examine this practice bomb in the class session.
- You should not compile anything for this assignment. You just use the program “theBomb” under “/home/chenz/” at diamond.pfw.edu Linux server that is already compiled for you.
- Remember to use the file name if you are setting breakpoints at specific lines. For example, break theBomb.c:77.

Submission

To successfully complete the assignment, you must place the passwords (in order) in a text file called passwords.txt in the “hw4” directory. There should be one password on each line, with no extra space at the end of the line. You can test your passwords by running the command:

$ /home/chenz/theBomb < /home/Your_User_Name/hw4/passwords.txt

where “Your_User_Name” is the user name that you use to log into diamond.pfw.edu.

Putting incorrect passwords in passwords.txt and running the above command will cause the bomb to explode, so you will want to test your passwords in gdb first to ensure that they work.

After obtaining correct passwords in passwords.txt, upload passwords.txt file to your GitHub repository for CS232 homework under “hw4” subdirectory.

If you have trouble in pushing the code, please let me know.

Grading rubric:

- Defuse stages 1 - 6 – 120pt (each stage is 20 points) (You will earn credit up until the first stage where you do not have a correct password; from there on, you will not receive credit. For example, if you have all the passwords correct except for stage 3, you will only earn 40 points (for stages 1 and 2). **Therefore, make sure you work on the stages in order!**)
- Each time the bomb explodes, you will lose 3 points
- (**Bonus**) Defuse stage 7 – 20pt

Total: 120 points.

I hope that you enjoy this puzzle! Good luck defusing the bomb!

Acknowledgement:

The idea for this homework comes from Professors David O’Hallaron and Randall Bryant’s curriculum for their computer systems course at Carnegie Mellon University. The source code was prepared by Professor Britton Wolfe.