CS 213, Spring 2000
Lab Assignment L2: Defusing a Binary Bomb
Assigned: Feb. 10, Due: Wednesday, Feb. 23, 11:59PM

Patrick Chiu (`ppc@andrew.cmu.edu`) is the lead person and bomb squad chief for this lab.

1. Introduction

The nefarious *Dr. Evil* has planted several "binary bombs" on the fish cluster. A binary bomb is a program that consists of a sequence of phases. Each phase expects you to type a particular string on *stdin*. If you type the correct string, then the phase is *defused* and the bomb proceeds to the next phase. Otherwise, the bomb *explodes* by printing `"BOOM!"` and then terminating. The bomb is defused when every phase has been defused.

There are too many bombs for us to deal with, so we are giving each group a bomb to defuse. Your mission, which you have no choice but to accept, is to defuse your bomb before the due date. Good luck, and welcome to the bomb squad!

Step 1: Get Your Bomb

Each group of students will attempt to defuse their own personalized bomb. Each bomb is an Intel Red Hat Linux 5.2 binary executable file that has been compiled from a C program. Each bomb consists of 6 phases.

To obtain your group's bomb, send mail to Patrick Chiu (ppc@andrew.cmu.edu) with the string *"Lab 2 bomb request"* in the subject header, and the names and Andrew ID's of the group members in the message body. Patrick will then send you the location of your bomb and your group's number.

Step 2: Defuse Your Bomb

Once you have received your bomb from Patrick, copy it to your personal directory. Your job is to defuse the bomb.

You can use many tools to help you with this; please look at the **hints** section for some tips and ideas. The best way is to use your favorite debugger to step through the disassembled binary.

Each time your bomb explodes it notifies the staff, and you lose 1/4 point (up to a max of 10 points) in the final score for the lab. So there are consequences to exploding the bomb. You must be careful!

Each phase is worth 10 points, for a total of 60 points. (Remember that each lab is worth about 8% of your final grade.)

The phases get progressively harder to defuse, but the expertise you gain as you move from phase to phase should offset this difficulty. However, the last phase will challenge even the best students, so please don't wait until the last minute to start.

To avoid accidently detonating the bomb, you will need to learn how to single step through the assembly code and how to set breakpoints. You will also need to learn how to inspect both the registers and the memory states. One of the nice side-effects of doing the lab is that you will get very good at using a debugger. This is a crucial skill that will pay big dividends the rest of your career.

Logistics

As usual, you may work in a group of up to 2 people.

Any clarifications and revisions to the assignment will be posted on the class bboard and Web page.

You should do the assignment on the class machines (the fish cluster). In fact, there is a rumor that Dr. Evil really is evil, and the bomb will always blow up if run elsewhere. There are several other tamper proofing devices built into the bomb as well.

Hand In

There is no explicit hand-in. The bomb will notify your TA automatically after you have successfully defused it. You can keep track of how you (and the other groups) are doing by looking at:

http://www.cs.cmu.edu/afs/cs/academic/class/15213-s00/www/bombstat.html

This web page will be updated every 5 minutes or so to show the progress of each group.

Hints *(Please read this!)*

There are many ways of defusing your bomb. You can examine it in great detail without ever running the program, and figure out exactly what it does. This is a useful technique, but it not always easy to do. You can also run it under a debugger, watch what it does step by step, and use this information to defuse it. This is probably the fastest way of defusing it.

We do make one request, *please do not use brute force!* You could write a program that will try every possible key to find the right one. But this is no good for several reasons:

- You lose 1/4 point (up to a max of 10 points) every time you guess incorrectly and the bomb explodes.
- Every time you guess wrong, a message is sent to the staff. You could very quickly saturate the network with these messages, and cause the system administrators to revoke your computer access.
- We haven't told you how long the strings are, nor have we told you what characters are in them. Even if you made the (wrong) assumptions that they all are less than 80 characters long and only contain letters, then you will have 26^{80} guesses for each phase. This will take a very long time to run, and you will not get the answer before the assignment is due.

There are many tools which are designed to help you figure out both how programs work, and what is wrong when they don't work. Here is a list of some of the tools you may find useful in analyzing your bomb, and hints on how to use them.

- **objdump -t**

  This will print out the bomb's symbol table. The symbol table includes the names of all functions and global variables in the bomb, the names of all the functions the bomb calls, and their addresses. You may learn something by looking at the function names!

- **objdump -d**

  Use this to disassemble all of the code in the bomb. You can also just look at individual functions. Reading the assembler code can tell you how the bomb works.

- **strings**

  This utility will display the printable strings in your bomb.

- **gdb**

  The GNU debugger, this is a command line debugger tool available on virtually every platform. You can trace through a program line by line, examine memory and registers, look at both the source code and assembly code (we are not giving you the source code for most of your bomb), set breakpoints, set memory watch points, and write scripts. For documentation, type "help" at the gdb command prompt, or type "man gdb", or "info gdb" at a Unix prompt. If you prefer using a GUI to a command line, try using the tool `ddd`. Some people also like to run `gdb` under `gdb-mode` in `emacs`.

- **ddd**

  This software is the result of a research project in debugger interfaces from the Technical University of Braunschweig, Germany (http://www.gnu.org/software/ddd). It is a graphical interface which takes the pain out of using the `gdb` command line. It still has bugs, but it is the best free tool around. For the parts of your bomb that have no source code available, use the "Display Machine Code" option.

Looking for a particular tool? How about documentation? Don't forget, the commands `apropos` and `man` are your friends. In particular, `man ascii` might come in useful. Also, the web may also be a treasure trove of information. If you get stumped, feel free to ask your TA for help.