CISC 367 – Spring 2016

Homework Assignment – Buffer Overflow Attack

1. Given C program `test.c`, produce an input string, via the help of `gdb`, that will trigger function `bar()` to be invoked and message "Why am I here???" printed.

   Use Unix command `script` to capture the execution trace of running `test.c` with your produced string as the command-line argument (in terms of a Python expression).

   Work out your solution on `mlb.acad.ece.udel.edu` only. In addition to submitting a Python expression, you should also describe how you come to this Python expression. You may use "script" to capture the `gdb` session you use to derive the answer.

2. Given C program `jumpover.c`, use `gdb` to figure out the (integer) values needed in lines 7 and 8, respectively, so that the program prints out 0, instead of 3. (Use `/usr/bin/gcc` to complie the program.)