* Make sure buffer size is 64
* Make sure to turn off space randomization **every time you turn on your machine**
* Task 1
  + Just run “malicious” shell code to get into shell
* Task 2
* Use gdb command (it is like an IDE for Linux with built in commands, including adding break points, showing memory location of a function, value of registers, etc.).
* Chapter 4 in the book goes through this lab.
* Place NOPS AFTER return address (the 4 bytes after the location where eip is pointing to).
* IMPORTANT: Char buffer[517] which you will use to over flow includes: the return address, your shell code, and the NOPs).