CSE351 – Section 4
Lab 2 and related things

October 17\textsuperscript{th}, 2013
Useful Info

- Use `gdb`, `objdump`, etc. to defuse the bombs
- The main files involved:
  - `bomb`, the executable bomb
  - `bomb.c`, defines the entry point of the program and calls functions whose source code is not available to you
  - `defuser.txt`, contains passphrases for each stage, separated by newlines; add each passphrase here as you discover it
- Start early!
  - Like lab 1, this can often take more time than expected
  - We have lots of office hours to help you, but this works better earlier than later
Lab 2 Notes

Notes

- Each student has a different bomb; no two have the same answers
- Put the passphrases you've already discovered into defuser.txt so that you don't have to type them in every time
- gdb has built-in help for all its functions, and also has extensive online documentation
- Unix commands `man` and `apropos` (searches `man` pages) are your friend!
The bomb uses `sscanf`, which parses a string into values

As an example:

```c
int a, b;
sscanf("123, 456", "%d, %d", &a, &b);
```

The first argument is parsed according to the format string (the second argument)

Upon success, the values of `a` and `b` will be set to 123 and 456, respectively

Refer to `man 3 sscanf` for more information
Calling Conventions

Parameters
- x86 typically passes all parameters on the stack
- x64 passes first six arguments through registers
  - %rdi, %rsi, %rdx, %rcx, %r8, %r9
  - The rest go on the stack, like x86
- Pros and cons?

Return Values
- Typically stored in %rax
Caller- and Callee-Saving

Register Conventions

- Registers can either be “caller-saved” or “callee-saved”
- Caller-saved: If the contents of the register need to be preserved, the caller should save them on the stack prior to invoking a function
- Callee-saved: If a function wants to use the register, it must save the value and restore it to the register before returning
- Why use one type of register versus another?

x86 vs x64

- In x86, callee-saved registers are `%edx`, `%esi`, `%edi`, `%ebp`; all others are caller-saved
- In x64, callee-saved registers are `%rbx`, `%rbp`, `%r12-%r15`; all others are caller-saved