Re\_challenge 3

Goal: print “You are amazing!!”

Steps:

1. Open IDA: analyze graph of assembly
2. Create CFD
3. Analyze the assembly/Run
   1. By the first cmp, it checked if argc == 1
   2. Does a strncmp with 8 as an argument so the word is 8 characters long
      1. It compares the argument with some characters in the code.
   3. During setup, there is a part where letters are assigned to a specific byte
   4. Placing those letters in order as the argument made me reach the goal
4. Run code with “A553Mb1Y” as the argument and it printed my goal

Analysis:

Answer:

1. to 0x080486C9
2. ZF = 0 to 0x080486F7
3. puts(“You are amazing!!”)

Argument is “A553Mb1Y”

> ./re\_challenge3 A553Mb1Y

CFD:

