George Meisinger
gem56

Program 1

password: oILjjTxJzOZCyMQMTnLLtFOT

I ran the program, guessed a couple of times, found no clues, so I ran mystrings on it. After a quick scan I found the part with "Congratulations!" and saw a string that honestly just *looked* like a password. I tried it and it worked.

Program 2

password: 99.109.111.93 44620 22, upon further review, I see that this is my ssh session info.

I started with mystrings, didn't find anything. I toiled in gdb until I figured out how to disassemble main, where I found a call to strncmp() after the fgets(). I set a breakpoint at that address, and looked at the registers involved. They appeared to line up with the arguments for strncmp, one of them was an int and the other two were memory addresses I assumed would hold strings. Sure enough one of them held my guess, so I tried the other one and it worked.

Program 3

password: of 8 characters entered, 6 must be in ([,],{,})

This program took 1 char at a time, and seemed to manipulate it somehow. I assume the password is not static, and I believe it has something to do with the ASCII values of the characters I type. I found what I believe was main(), and found that it kept track of my last character entered as well as a counter.

FOUND IT:

After finally finding the correct section at the end of the program, I found a section that compares the chars I entered with specific ascii values (91, 93, 123, 125). It keeps track of how many of these I entered, and if that number is EXACTLY 6, it unlocks.