Raj Patel

Dr. Misurda

Intro to Systems Software

October 23, 2016

Project 2 Passwords

1. Password: EhbdmPXjmPuqTnDapazuVtW

At first I used the debugger console gdb to try to figure out the password. I took a look at the disassembled code and found that there was a cmp function used at line 0x08048314. I set a breakpoint at both main and this line, and started inspecting the registers being used. After getting either random numbers or blank registers, I examined $ebx, and it contained the phrase “hbdmPXjmPuqTnDapazuVtW”. I tried this phrase and it failed. After an exhaustive search of the registers, I looked back at the project prompt. It suggests to use the mystrings program. So I copied the files over to my directory, and ran mystrings for the first file. It seemed to contain just about every phrase and character known to C. I searched for the phrase I found, and lo and behold, I discovered that the full phrase was found right next to the phrase “Congratulations!”: “EhbdmPXjmPuqTnDapazuVtW”. I tried this password, and it worked.

1. Password: SO

I ran this second file through the debugger, and when I opened up the disassembled code, I found function calls named “time”, “localtime” and “strftime”. I figured time just meant time, but I looked up the function localtime to learn that it stores today’s current date and day. I also learned that “strftime” formats the time values to specify date, time, day, etc. So I looked back at the debugger and found two instances of “strftime” function call. I inspected the register used just before the call, $ebx, for each instance. It gave me Sunday and October. I tried both individually, I used both together, with and without spaces. I then tried the first 2 letters, and finally it worked.

1. Password: :0\*7t[u (

I tried using the debugger, but when I tried to set a breakpoint at main, the debugger console couldn’t find a main method. Because I couldn’t run the file, I tried using my mystrings program to find a hint. It turns out I found the password the same way I found the first password, looking to where the file contained “Congratulations!”.