Project 2: Passwords

Joseph Reidell

JMR240@pitt.edu

**1 jmr240\_1**

**1.1 Explanation:**

At first, I tried to base it off the recitation lab. I put a break point at main and then used “disas” to display the assembler code from the main function. When looking at the code I found a specific line that said “repz cmpsb %es:(%edi),%ds:(%esi)”. I found this to be very interesting and put a breakpoint at that line. I figured this was comparing two strings in these registers. I typed in “something” at first. I started off with looking at register “$eax”. That displayed just an empty string. I then tried looking at the registers that was displayed in the line. I first checked “$edi” and it displayed what I typed in. I then checked the other register which was “$esi”. That register displayed this exact string. I disabled the breakpoint and typed that in. It unlocked the program with that string.

**1.2 Password**

The password that worked with this program was the string “ YFCPAIjEbndKtyMyGCkOkORoUrojZB ”

**2 jmr240\_2**

**2.1 Explanation:**

With this password, I honestly did not think I would get it as quick as I did. I put a break point at main and used “disas” to display the assembler code from the main function. At first, I found a call to “strcmp@pitt”. I thought about checking that first but, I saw it was testing the register “$eax” after that. I wanted to check that first so I put a breakpoint at the line 0x08048586. I figured it was possible the password would be in “$eax”. That displayed it was out of bounds so nothing was in that register. I then thought, the first password was in “$esi”. I decided to check “$edi” however because it is possible to be in a different register. It was also out of bounds at the line as well. I finally checked “$esi” and that register displayed my username: jmr240.

I figured I would try it out and it unlocked the program. I was not too sure how my username was the possible password. I went through again and went back to put a breakpoint at “strcmp@pitt”. I typed in “joe” this time and I checked other registers. I discovered “joe” was in the register “$ebx”. The register “$esi” still held “jmr240”. What I think is happening, is that “strcmp@pitt” is checking a pitt username list and comparing the string you enter in to a specific username needed for that program.

* 1. **Password**

The only password I could find that worked with this program was “jmr240”.

**3 jmr240\_3**

**3.1 Explanation**

This program was probably the hardest one to figure one. This program does not have a main function which really screws everything up. It is difficult to figure where the program actually begins. I decided to give the regular command “strings jmr240\_3” to see if I could figure out the methods. I found that there was a getchar method that was called. Anytime you run the program, it can take in 8 single characters till it says whether you are wrong or right. While checking getchar, I did not have much luck in finding any character that would help find the password. At this point, I ran into a dead end. I was not sure where else to look. I feel like it’s right under my nose but I can’t seem to find it.

**3.2 Password**

Didn’t figure out the password.