CS0449

Project 3

Dane Halle

Project 3 Writeup

dmh148\_1 Executable:

Password: **umKmQQaZHSkbOOloGxqjUEJ**

Writeup: I started with this by running the script provided with mystrings.out and looked through for strings found that were bigger than around 6 characters. In my text editor, it shows a smaller version of the code on the right side and you can see longer lines than the others. The first string I found and tried was:

“QQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQQj”

I am not sure where this would be in the source code but since it didn’t work, I moved on and continued scrolling down. I then got to the Backtrace part and knew it wouldn’t be past that and saw some strings that were familiar. “Sorry! Not correct!” along with success stings. Right above those was a string that was just what I was looking for, a long string of seemingly random characters. I tried it and succeeded. I tested on another day and it still succeeded showing that the password was not dynamically changed.

dmh148\_2 Executable:

Password: **3.141593**

Writeup: I first started with the same approach as the first password. The output file was much shorter, and nothing looked like it could be a password, so I tried other things. I knew it required only one password. I used an objdump to get the executable code, so I have a reference. I looked through the code and found a call to an <fgets@plt> so I set a break point at that line and ran through with “si”. However, there was a lot of code between that line and when it accepts a string, or it skips it because of the commands. I then put a break point to the next line of code, and it accepted a string. I input “abcdefg” and saw it was stored inside of the $ebx register. I followed it through and noticed it got moved to the $eax register. Then I saw the $eax register cleared. Eventually, after checking registers and noticing that a lot of code was dedicated to removing the ‘\n’ on the string, I found the passcode within the $esi register after it was moved from the $ebp+0x8 register. I tested that as it was the first string I found within the program and sure enough it worked. I tested it several more times and it continued to work. This was found on Friday, March 8, 2019. After testing on the next day, I found that this string still worked so there is no dynamic change.

dmh148\_3 Executable:

Password(s):

Writeup: I ran this to see if it was the same as the other two executables, it was not. It required different number of passwords each time I ran it. I knew that using mystrings wouldn’t work but I tried and found an interesting string of “Xe\_3VgfL%” but that did not work. I used an objdump to get the executable code, so I have a reference. Upon initial inspection, I noticed that there wer no real functions but only one large <.text>. I then noticed no <fgets…> calls but quite a lot of <getchar…> calls.