COE 0449 Project 2

Ava Chong – alc260\_3

Procedure

I attempted at using strings -a and putting a breakpoint at main in gdb but all was unsuccessful. There is no main, so we must use “objdump -d” to disassemble the file. The label “\_\_lib\_start\_main@plt” seemed promising so I followed the function call within the text. I was able to identify the prologue start at 0x08048424. After reading through the code, I was able to identify patterns within certain registers and translate that into pseudo code that I would understand.

There are two main variable that are initialized to 0 using movl at the beginning of the function.

* -0x10(%ebp)
  + I will call this “count”
* -0xc(%ebp)
  + I will call this “i”

After this, a series of compares occur with %eax.

8048470: 83 f8 39 cmp $0x39,%eax //compares to 9

8048473: 74 1b je 8048490 <puts@plt+0x13c> //count++

8048475: 83 f8 39 cmp $0x39,%eax //compares to 9

8048478: 7f 0c jg 8048486 <puts@plt+0x132> //jump if greater than

804847a: 83 f8 30 cmp $0x30,%eax //compares to 0

804847d: 74 11 je 8048490 <puts@plt+0x13c> //count++

804847f: 83 f8 34 cmp $0x34,%eax //compares to 4

8048482: 74 0c je 8048490 <puts@plt+0x13c> //count++

8048484: eb 0f jmp 8048495 <puts@plt+0x141> //i++

8048486: 83 f8 63 cmp $0x63,%eax //compares to c

8048489: 74 05 je 8048490 <puts@plt+0x13c> //count++

804848b: 83 f8 73 cmp $0x73,%eax //compares to s

804848e: 75 05 jne 8048495 <puts@plt+0x141> //i++ if NOT equal

//count ++ if equal

8048490: 83 45 f0 01 addl $0x1,-0x10(%ebp) //count++

8048494: 90 nop

8048495: 83 45 f4 01 addl $0x1,-0xc(%ebp) //i+1

8048499: 83 7d f4 10 cmpl $0x10,-0xc(%ebp) //i==16

804849d: 7e c3 jle 8048462 <puts@plt+0x10e>

804849f: 83 7d f0 04 cmpl $0x4,-0x10(%ebp) //count==4

From this information we know that i has to equal 16 and count has to equal 4 to unlock the passphrase.

The criteria for a character to count towards to the count variable are as followed:

* Equals 9
* Equals 0
* Equals 4
* Equals c
* Equals s

The program loops through all the characters and is unlocked when all fulfillments are made. All other characters go towards the increment of i and not count.

Solution

In total, we need a string input of 16 characters with four of them being any combination of 9, 0, 4, c, or s.