Xingchen Zhao - CS449 Proj3

EXE 1:

Password: RxqMNdYxxekLgWGzoDIm

Initially, I used disas main in the gdb, and I got the disassembly of the main function. And then I saw several functions such as fgets, chomp, printf. After the chomp, I found repz cmps, which compares string. I thought I should inspect the string "0x80b388c", so I used x/s to see what is that. Then, it showed a strange code. I used this code, and I unlocked the program.

EXE 2:

Password: 3.141593

In the beginning, I disas(ed) main and saw "d" function. Then I disas(ed) the d function. There are many functions such as "c", "e" , " fgets" and "printf". And I was really confused with them. Then I tried to disas c and e, and I became more confused. I thought I need to go back to "d" function and pay attention to that. I found this line "0x080485a2 <+93>: je 0x80485b6 <d+113>" , which will jump to d+113 if something is equal. Then I set a break point at this line. I inspected the contents of esi which is above the break point. It showed "3.141593", which is pi. I thought it might be the password. I tried, and I succeeded.

EXE 3:

Password: Any 13 characters(except 9 0 4 c s) plus three(repetition is accepted) of "9 0 4 c s" (16 characters in total) . Eg. 999azazvzazazaza, 444aaaazazxzazaz, azazvzazazaza9cs

Initially, I tried to use disas the main function of exe file, but I failed. I remembered objdump which could let me get a disassembly without the gdb. Then, a lot of code showed up, and I did not know where to start. I scrolled down the disassembly code and found .text. I thought it might be the function that I should traced. I saw there was a bunch of cmp and jump, so I thought it should be the comparison of characters(ASCII: 39: 9 30: 0 34:4 63:c 73:s). I saw there was a for loop which was bounded by 15. I was thinking about if I were the programmer,

what would I checked. It must be a string of 16 characters! Then I tried to type 16 characters which contained “9 0 4 c s”, but I failed again. I traced the disassembly again, and I found that there was a condition that check if the string contains exactly three(repetition is accepted) of “9 0 4 c s”. I tried to use the new password, and it worked! Yeah!