ComSec_HW3

Ruizhi Pu

October 29, 2019

1 Q1

As we can see from the assembly code in the olleydbg, when we want to output the result of successful invade into the exe, we need to change the condition of the comparison from the input with serial, change the condition to whatever the input would be. Firstly we need to find the position of the successful return starts with the "Great work" which is the 00401362D in the stack, after that, we can go back the location of the call function of this address and change the comparison assembly code above the command, which means change JE TO JNE, change the jump while equal function to the jump while not equal, so every input we have would be able to crack the code. And it is a 1bit change in assembly code.

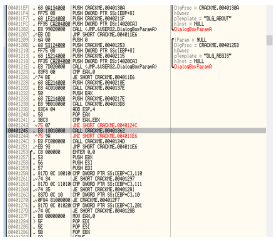

Figure 1: The content of the exe file in olleydbg

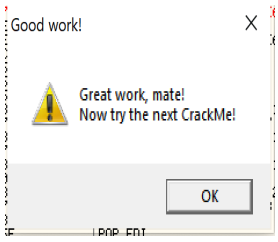

Figure 2: The result of changing 1 bit assembly code in exe file in olleydbg

2 Q2

After using olleydbg to analysis the code, I found that it is a application which use the input string to do the math calculation to invert the string to a int, and with the analysis of IDA, we can find the procedure of the assembly code, and it is :
Firstly, sum up the input string and XOR WITH 5678H,
Secondly, XOR with the 1234h.

The rewrite of the code consists of two parts:
The first part requires a input, and in the terminal it should be implemented like :
python3 q1_part2.py input
the input is the string which we would like to get its serial number.
The second part is the demo for my case id : rxp. And the result of the serial number.

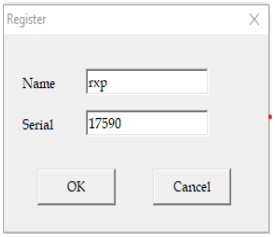

Figure 3: The content of input and serial number

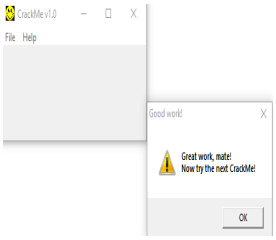

Figure 4: The result