Lab 5: Social and Reverse Engineering

Report by: Ryan Blair 9:30am section

Task I. Security Questions

In this task, your job is to pick a celebrity or historical figure and see if you can find the answers to the following common security questions:

Please submit the name of your target subject plus answers to as many of the security questions as you can to PolyLearn by the reported deadline.

A: Bill Gates

1. What was the make and model of your first car? - Porsche 911
2. What was the name of your elementary / primary school? - View Ridge Elementary
3. In what city or town does your nearest sibling live? - Seattle (Libby)
4. What time of the day were you born? (hh:mm) - 22:00
5. What is your pet's name? - Oreo
6. In what year was your father born? - 1925
7. What is your favorite color? - Blue, Yellow, Red
8. What was your favorite place to visit as a child? - Australia

Task II. Ransomware Attack!

Response questions

- How far did you get?

  I got up to attack 2. Due to the lack of both time and priority of other projects that needed to be done during the last week, I did not have enough time to finish it (not that the extension of time was not enough, I ran out of time)

- What was easy/challenging about the lab?

  The walkthrough really helped with the first attack. Trying to review assembly after forcefully removing it from my brain after sophomore year was the most challenging thing about this lab.

- Where did you get frustrated, and why?

  I was frustrated because I was never able to tell if I got the right answer. All the "decrypted" images were still unable to be opened by my virtual Linux system.

- What things did you try that worked/didn't work?
  For the first attack, I analyzed the XOR command because the value was hard-coded into the assembly. The second attack I was trying to analyze how the program came up with the string key. I thought it was similar to how we used cbc encryption towards the beginning of the quarter, but never ended up verifying it. I tried following the registers and writing down exactly what values were being inputted. After a couple of frustrating hours, I moved on to other tasks as they demanded more of my attention.

- What resources did you find useful or unhelpful?
  Online websites of assembly code were somewhat helpful in determining what commands were being run and how the information was flowing. I think the real problem I had was the fact that I had not dealt with assembly for so long, that the hints you gave for the attack were not really helpful (or at least obvious).

- The experiences you had with the lab you think would be helpful for me to know so that the lab can be improved.
  Again, the decrypted images I got were not showing positive results when I got the right answer for the first attack, so that was frustrating. I would also recommend having a resource that would describe relevant assembly commands, and maybe a refresher on possible attacks.