Getting by Passwords Without Knowing Them

MARE Spring 2018 - Luis Garcia's Cameo Class

April 16, 2018

Motivation: Your friend gives you a demo of his new chess game that he claims is better and more entertaining than GTA V. The game is in the form of an executable (you can presume it was implemented in `C++`). However, it's password protected and he completely forgot to give you the password before he left on vacation forever. How can we play the game ASAP?

Goal: In this assignment, you will modify the binary of the chess game to bypass the password protection of this game. You want to permanently remove this password check so that you can play it WITHOUT having to (1) figure out the password and (2) enter the password every time you play. There are several ways this assignment can be implemented.

Materials:

- Source code of game (`C++`)

Requirements:

- You must compile the source code as is. You may NOT modify the source code in any way. The code was given to you so that you can compile the binary to be platform independent.
- You must analyze the code in IDA Pro and identify the points that need to be modified.
- You should generate the byte code using a sample assembly program as was done in the in-class assignment to figure out the appropriate patch for the binary.
- Write a report (minimum of 1 page long, but can be as long as you want) that discusses your analyses of the binary in IDA Pro, the sample assembly instructions, a description of how you compiled the code, as well as any relevant analyses or figures that will clarify any decisions you made for your attack.
- Once finished, you can send me a thank you e-mail for providing you access to the greatest chess game you will have ever encountered.