CS390R: Project 1

February 15, 2023

Please submit all screenshots in one pdf file with each clearly labeled (The corresponding question) for grading. Code should be handed in as separate py files with the specified names. The writeup for challenge three should be its own pdf file. All other files will be ignored.

1. The first challenge is a simple ”crackme” program where you are asked to give an input and have it pass two checks. Passing both checks will award you 30 points, 15 for only one. Submit a python script called Lastname_Firstname_p1c1.py that prints the completion message for the checks you pass when run against the challenge. (30 pts).

2. This challenge is from our friend who decided to learn to write their own library functions. This binary is stripped so there are no symbols! You will have to find out what function is main on your own using the ”entry” function which Ghidra should still be able to identify by the ELF header. After that you will have to give the program the correct input (Hint command line arguments AND user input), to print the congratulations message. (Hint: remember that the main of C functions take argv and argc as variables)

   You will receive 10 pts for finding the main function. Please provide a screenshot of main in the ”Decompile” window and ”Listing” windows as proof. The other 20 pts will be awarded for your solve script called Lastname_Firstname_p1c2.py based on how many inputs you get correct.

3. This challenge is another ”crackme”. It is harder than the previous two, but fortunately, the developer left some debug print statements that can be enabled! Your goal is to enable the debug messages, and find out how to print the win message. Submit a python script called Lastname_Firstname_p1c3.py.

   Having your script enable and show the debug messages will give you 10 pts. Finishing the challenge will give you 20 more for a total of 30.

4. Last we want you to make a writeup of challenge 3. This should be a professional document that you could for instance provide to a company if you were hired to do a security audit of their products. In general, it should be technical, explaining what the program is doing, your understanding and process through the reversing, and your process of writing the exploit script. A technical reader should be able to reproduce all the steps based on your reasoning and come out understanding the code just as much as you do. The writeup will be graded based on your technical explanation, and professional presentation, so make sure to include screenshots of whatever you feel needs to accompany your explaination to make it understandable. Submit this in a pdf called Lastname_Firstname_p1w.pdf (10 pts)