Andrew “Connor” Riley

CSCE 451-500

02 MAR 2020

CSCE 451 - Homework 3 Documentation

Diagram Item	Description
Obtain Binary File	Determine the binary file that you would like to observe and reverse engineer.
Dynamic / Static	Determine whether you would like to analyze the binary using either a dynamic or static approach.
Run file Observe behavior	If one decides to use the dynamic approach, they will load the binary on a virtual machine (to prevent unintended consequences) and run the binary and determine the behavior. One may repeat this step, changing inputs, until the desired outcome is achieved or ready to switch to static analysis.
Open file in GDB	Open the executable file in GDB and run the file.
Disassemble Main	Disassemble the main function to see any called functions or other important pieces to better determine the structure of the binary.
Find established control flow and desired outcome	Add breakpoints in the binary in order to check stack values and determine the control structure of the file in order to more easily access the desired outcome.
Open file in IDA	As the item suggests in the title, open the binary in IDA so that we can better see the structure of the binary.
Observe any creation/passing of variables, jmp commands, and calling of libraries	Using IDA we will, for sake of clarity, rename any variables that are created and passed so that we may better understand what is going on in the program. We will observe the functions and libraries called and see of any conditional statements or loops using the control flow diagram generated by IDA. The purpose of using IDA is solely for ease of understanding using a user-friendly GUI.