Lab 05 – Args/Globals/Patching

This lab will walk you through analyzing a binary for global variables, function arguments/returns, and patching an executable.

Scenario

Welcome to Jurassic Park!
Watch this with sound, be inspired/amused: https://www.youtube.com/watch?v=-w-58hQ9dLk

The dinosaurs are running throughout the park, security systems are down, power is out, and Dennis Nerdy has stolen the Dinosaur Embryos. The only way to save the day is to access the **Jurassic Park System Security Interface**. Unlike John Arnold, you're 1337 and can probably actually get in. You've got access to the binary (**lab05.exe**) and can RE it.

Figure 1: Dennis Nerdy

Figure 2: John Arnold

Helpful Hints

This binary was compiled without helpful debug symbols. Your job becomes a little bit harder because you need to track down "main". Here is one approach you may take.

Ghidra

1. To find the main function, search for a string or something that you know exists.
    a. Find XREFs to the string or object you found.
    b. Look at the call tree and figure out what the first caller was, that will likely be main.

2. Alternative: Locate the entry function. Usually, one of the last calls or jumps it makes will lead you to main.

Instructions

For this lab, you will be working with the **lab05.exe** binary. Analyze the binary using the tools that we have discussed in Windows (Ghidra, WinDBG, etc.).

1. Dennis wrote the program using some anti-pattern global variables. Track the two global down and determine whether or not they are initialized. That may come in handy later, maybe not.

2. In the program, there is one function that is responsible for creating the PIN. Look at the function and figure out the algorithm. Do not rely solely upon the decompiler; it's a good start, but I want you to look at the assembly to get the exact algorithm.

3. Inside of the function that validates the users pin, a number of arguments get passed. As you know, these arguments are at a higher address than EBP. Find the argument that carries the generated pin number.

   Hint: After this step, you should know what PIN works with your name.

4. We don't have time to figure out everyone's PIN! Patch the binary so that it will always accept the pin entered. This patch needs to be permanent.