Lab 4 – IDA Python

SUMMARY:

Test your understanding of IDA Python analysis scripts by writing scripts to solve common problems.

REQUIREMENTS:

The student is required to write three (3) scripts, one to accomplish each of the following:

1. Detect the presence of one of the table entries for a precomputed MD5 Hash Table which has the values (0xd76aa478, 0xe8c7b756, 0x242070db, 0xc1bdceee). Print "MD5 Constants present" if detected.
2. Detect calls to specific functions: Detect whether or not a given file being analyzed makes calls to the following functions (**strcpy**, **sprintf, strncpy, wcsncpy,** and **swprintf**). Print the name of the function, the address that makes the call, and the function called (e.g. sub_100:0x150:strcpy).
3. Building on 2, determine if any exported functions call a function (which may call a function …) that is in the list of functions above. If an exported function calls a function and three calls deep into that function a call to *strcpy* is placed, print the name of the exported function and the function from the list that is called (e.g. sub_700:strcpy)

WHAT TO SUBMIT:

Email me a link to the GitHub repository where your code resides.

COLLABORATION:

This is a group assignment and students make work in groups of up to three (3) students. The knowledge gained in determining each script can be shared, but each student is expected to turn in their own scripts.

GRADING:

Grades are assigned based on meeting the requirements. 100 points total. Requirement 1 is worth 25 points. Requirement 2 is worth 25 points. Requirement 3 is worth 50 points.

DUE:

11:59 P.M. April 3, 2017