CS4379/CS5375
Dr. Jaime C. Acosta
Software Reverse Engineering

Homework Assignment – Static Binary Analysis

Due Date: Before 6:00pm on September 15, 2022
Late assignments will be accepted no later than 11:59pm on September 17, 2022 with a 2 letter grade deduction.

This assignment will be done in groups of either 2 or 3. You will use the environment that you setup in the "Homework Prep" assignment.

In class we talked about x86 and how IDA Pro can be used to analyze binary files statically and at runtime. In this assignment you will become familiar with IDA pro and will use it to statically identify areas of interest within a binary file (a dynamically linked library or DLL) that lacks high-level source code.

When answering each question, be very explicit in describing your steps and include screenshots.

The file that you will analyze for this assignment can be downloaded from the course web page: http://cs5375.cs.utep.edu/ The password for the password protected zip files is: *infected*

You will need to install 7zip in order to decompress the password-protected file for analysis. https://www.7-zip.org/download.html

IMPORTANT: Please ensure that you use IDA Pro v5 to complete the assignment: http://cs5375.cs.utep.edu/software/ida5.exe

Other versions of IDA may result in different solutions.

In your Windows VM, download (from the course webpage) and extract the cooldown10.dll with 7zip and using the password: *infected*

Use IDA Pro v5 (free) and analyze the cooldown10.dll file to answer the following questions.

1. What external functions (also know as subroutines) are located at address 0x1002 5776 and

0x1006 CA82?

2. What function is ***called*** at 0x1006 B918? List the parameters what they mean as well as what the function does in this context. You may consult the online Microsoft Documentation (https://docs.microsoft.com) and others, but remember to cite your sources.

3. What program (***and version***) was used to generate this file? (hint: look at and around addresses 0x1006 BCE0 to 0x1006 BDC7).

4. Navigate to subroutine at address **0x1005 BC70**. Describe the three conditions that are validated to avoid a call to the ***abort*** function.

5. How many places in the code directly ***call*** the following functions:

    a. _wsplitpath_s

    b. memset

    c. cpMomentForBox

6. A Domain Name System Server is a machine on a network that resolves names to IP addresses (e.g., a request of google.com will may reveal the address 74.125.227.197). Focusing on the call to gethostbyname located at 0x1002 702B, which name is being resolved? Explain how you know this.

7. Explain, at a high-level, what is happening from address 0x1002 708F up to and including address 0x1002 70A7.

8. How many local variables and arguments has IDA Pro recognized for the function at 0x1002 6720? List the number of bytes allocated for each local variable and each argument **in decimal**. Show/describe how you arrived at your answers.

9. In a few sentences, describe what the instruction at 0x1002 6FDC does (including where input is read and output is stored). (You will need to consult additional sources, e.g., the Internet, for the full answer).

10. Use the online Microsoft Documentation (https://docs.microsoft.com) page for **WSASocketA** and the named symbolic constants functionality in IDA Pro, change the representation of the arguments for the call at 0x1002 7011 to instead show the correct symbolic constant. If no symbolic constant name exists, add a comment instead that indicates ***what*** the values mean.

11. Analyze the function at 0x1002 6FC0 and then write a few sentences describing the high-level behavior. (Hint: focus on the function calls)

Extra Credit: At 0x1002 75E4, there is a call to Sleep (an API function that takes one parameter containing the number of milliseconds to sleep). Looking backward through the code, how long will the program sleep if this code executes?

Deliverables: Email a zip file with the subject **Assignment-StaticBinaryAnalysis** to fall22cs5375@gmail.com The zip file must contain the following:

- A write-up with steps detailing your thoughts and actions (including screenshots) during your completion of each question. Create a Word document and embed plenty of text/screenshots as if you are writing a tutorial. Your logical flow will heavily influence your grade.

- Your IDA database file (.idb extension). This is the file saved by IDA Pro. ***Ensure that you include*** comments, renamed functions, groupings, etc. to show that used these features during your reversing of the binary.

IMPORTANT NOTE: **Do not** include the original DLL file in your zip file as it may be flagged and cause email delays/rejections.