Module d3: Dynamic analysis for binary sre – Debuggers.

# LET’s START ANALYZING BINARIES!

**Lab Description:** The objective of this lab is to allow you to choose appropriate static analysis tools and techniques to safely examine a binary file to achieve a specified objective.

**Lab Environment:** This is intended to be an interactive lab with the instructor providing guidance to extend student demonstrations of very basic static analysis skills. The exercise should be run in a protected environment as it may deal with malware. It can be run in the SRE class virtual environment, which would contain the crackme files and tools for static analysis. It would also allow instructors to view/step-in to the student environment even when not co-located.

**LAB EXERCISE/STEP 1**

The instructor needs to clearly express the following warning:

WARNING: This lab may expose you to malware. Malware needs to be handled carefully. Malware may trigger Anti-Virus or other similar security tools. DO NOT EXECUTE THESE BINARIES ON ANY SYSTEM. The safest approach is to examine this within the environment you have been provided.

**LAB EXERCISE/STEP 2**

1. Complete the two crackme challenges (i.e., get the "Access granted!" message to be displayed) in 0440\_crackme directory using the debugger. Provide screenshots to demonstrate how you accomplished this. You may not alter the source code for these files (i.e., your solution must work on the code as compiled) but the source has been provided for your reference. You are encouraged to try these challenges without looking at the code (at least at first).
2. Complete the two crackme challenges (i.e., get the "Access granted!" message to be displayed) in 0440\_crackme directory without using a debugger (i.e., using one of the other methods discussed in class). Provide screenshots to demonstrate how you accomplished this. You may not alter the source code for these files (i.e., your solution must work on the code as compiled) but the source has been provided for your reference. You are encouraged to try these challenges without looking at the code (at least at first).
3. Complete your choice of at least 5 of the challenges (numbered 06-15) in the 0320\_crackme\_exec directory using any dynamic method we have covered. Provide screenshots to demonstrate how you accomplished this. You may not modify the binaries.

**LAB EXERCISE/STEP 3 (OPTIONAL)**

Demonstrate solutions to more than 5 of the challenges (numbered 06-15) in the 0320\_crackme\_exec directory.

# What to submit

Students should present their results to the class.

Instructor Notes:

Results will be greatly varied as student select difference file and approach the RE process and documenting the RE process differently. Prompts you might use during presentations include:

Why did you choose that tool?

Would (alternative tool) have performed better/worse/differently?

Would results have been different if you had use different options with the command?

Using just the file and your documentation, could another analyst fully understand the results and be confident that you did not make an error?

Using your provided analysis, could another analyst repeat your process and obtain the same results?

**Options –**

Instructors can assign determine if the optional assignment is required/optional/requested, etc.