Module B1: APPROACHES TO SRE

# investigating crackme files

**Lab Description:** The objective of this lab is to use SRE to investigate a collection of crackme files to determine what input is necessary to get the program to report that access is allowed. This will require you to select and execute an approach.

**Lab Environment:** This is intended to be an interactive lab with the instructor providing guidance to extend student demonstrations of very basic SRE 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 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: As with any unknown binary, you should assume that the binaries in this exercise *could* be malicious, and should therefore not execute them outside the lab environment.

**LAB EXERCISE/STEP 2**

For each crackme file in 0320\_crackme\_exec directory, identify and use the appropriate static analysis tools to determine what input is necessary to get the program to report that access is allowed. Your solution should show your analysis in each case, and once you have determined a method, you should be prepare to demonstrate the input and output for a successful execution of the program.

# What to submit

Instructor Notes: Crackme files are widely available on the web and the solutions are closely guarded as publication of a crackme solution (which is widespread), renders the exercise unusable as a homework assignment. However, most collections can be remixed provided the students are required to complete the exercise within the isolated class virtual environment.

For this reason, this is intended to be an in-class exercise with the instructor and students working on the crackme challenges in parallel to ensure that the learning objectives for this module are met (rather than measuring a student’s ability to search the web.)

It is important to learn that there are multiple ways to crack these puzzles and to share these methods for better reverse engineering. Instructors should encourage creativity and diversity in solutions and allow students to walk through unique solutions for the entire class.

**Options –**

Instructors can assign individual crackme files to each student to minimize the time spent on this lab.

Instructors could have students write crackme files and use these for the class exercise.