Module D2: DYNAMIC ANALYSIS FOR BINARY SRE – BASIC DYNAMIC ANALYSIS TOOLS

# investigating crackme files

**Lab Description:** The objective of this lab is see the effects of your analysis instruments on the sandbox and to minimize the effects of these instruments.

**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.

**LAB EXERCISE/STEP 1**

Setup: Each student should submit C or C++ source code for 3 “crackme” challenges. The source code should include comments indicating which compilers they have confirmed that it compiles on (e.g., gcc, g++, clang, Visual Studio). The instructor should then build executables from this source code and distribute them as 0505\_student\_binaries.zip

The first portion of the code should display instructions for the goal of the particular crackme (e.g., get the “Access Allowed!” message to be displayed).

# Exercise:

1. Each of you submitted source code for several crackme challenges, which I have compiled and distributed in the 0505\_student\_binaries.zip file.
2. Solve at least 8 of the crackme binaries in the 0505\_student\_binaries.zip file. Each of the 8 should be from a different person, and at least 2 must be Linux x86, at least 2 must be Linux x64, and at least 2 should be Windows x86. You should also solve at least 2 using static analysis, and 2 using dynamic analysis.

# What to submit

Instructor Notes: This example includes dynamic analysis of malware.

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

Each student should be able to demonstrate (either in person or in the form of a submitted document) the process by which they were able to achieve the stated goal of their selection of binaries.

**Options:**

* Students that submitted creative or hard to solve crackme challenges can provide a walkthrough of the source code and/or a method by which the challenge could have been solved using dynamic analysis.