Module E1: obfuscation and anti-sre.

# Anti-sre techniques

**Lab Description:** The objective of this lab is to allow you to investigate anti-SRE techniques.

**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. Write a program that uses at least two of the anti-SRE techniques presented in this module (or other technique that you can find).
2. Demonstrate the effects of the techniques you selected, then demonstrate how you could circumvent the anti-SRE techniques to successfully reverse engineer the binary.

# What to submit

Students should present their results to the class.

Instructor Notes:

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

* Why did you choose that technique?