Module d4: Dynamic analysis for binary sre – Network Traffic Analysis.

# LET’s START ANALYZING NETWORK TRAFFIC!

**Lab Description:** The objective of this lab is to allow you to gain experience analyzing network traffic.

**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 appropriate files. It would also allow instructors to view/step-in to the student environment even when not co-located.

**LAB EXERCISE/STEP 1**

Setup: The instructor should provide a network on which the python server crackme\_610\_server.py is running, and a client on which crackme\_610\_client.py is running. Students should have access to the same network, and be able to observe traffic on that network (e.g., promiscuous mode is allowed on the network, and all traffic is visible by all hosts).

**LAB EXERCISE/STEP 2**

There is a server at <SERVER IP ADDRESS> that responds to 7 commands, and if a command is given correctly the response is "Success part X" where X is the command number.

Your goal is to analyze the network traffic in order to successfully invoke each of the 7 commands yourself. Your instructor will provide you with access to a client and a network on which to monitor traffic and then attempt to invoke the commands. The submission should be a screenshot showing the successful invocation of each command, with a short description of what you needed to do to invoke the command.

# What to submit

Students should present their results to the class.

Instructor notes: Students should **not** be provided access to the crackme\_610\_server.py or crackme\_610\_client.py files. The intent is for students to discern their behavior using only the observed networks interactions between the server and client.