**Student Name:** **Student ID:**

# Objectives

* Use soft hooking with Python debugger.
* Use hard hooking with Immunity debugger.
* Demonstrate Python to IDA Pro API.

# Important Information

* For *every* lab and home assignment, store all your work in your personal repository in a subdirectory named **mXX**, where XX is the module number. Carefully name the program as described in each problem.
* Your programs are extracted from your repository by a Python script. If there are any errors in the program name, then your instructor will never see your program, and you will receive a mark of zero.
* Push your work to the server often, and ensure that you push the final version of a program by the deadline specified, because the script extracting them can be run at any time after the deadline.

# Instructions

1. Read chapter 6 in the *Gray Hat Python* textbook. The following links are also useful:
   * <https://www.sans.org/reading-room/whitepapers/malicious/basic-reverse-engineering-immunity-debugger-36982>
   * <https://sgros-students.blogspot.ca/2014/05/immunity-debugger-basics-part-1.html>
2. Complete Problem 2.

**Note:** Problem numbering continues from the module’s lab.

## Problem 2

1. Study section 6.2 of the *Grey Hat Python* textbook in detail.
2. Implement the code **hippie\_easy.py** and observe its behaviour.
3. Answer the following questions and submit your answers in a file named **m08lab02.txt**.

* What is the difference between STDCALLFastLogHook() and FastLogHook()?
* What does the imm.getKnowledge() function return (e.g., is it an integer, a string, a dictionary)?
* What is the second parameter of the imm.disasmBackward()function?