CSC 471/583 Spring 2021 Lab 1

Dr. Si Chen

DLL Injection and OllyDbg

The goals of this lab:

- Understanding the concepts of DLL Injection.
- Know how to use OllyDbg to modify binary files.

Objectives and Targets

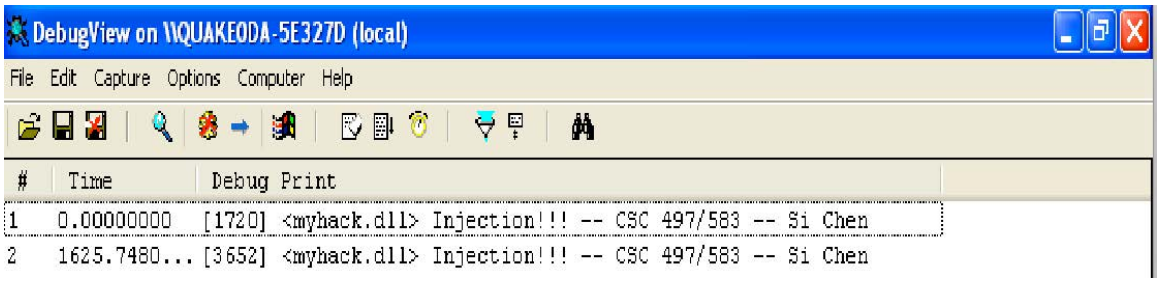

Figure 1: Debug View Screenshot

Change the debug information in DebugView window from *Injection!!! – CSC 497/583 – Si Chen* to *Hello World! – XXX* (Replace "XXX" with your name :)

Experiment Setup

1. Download and install VirtualBox software on your computer.

   https://www.virtualbox.org/wiki/Downloads

2. Download XP VirtualBox image from our class website and imported it.

   https://www.cs.wcupa.edu/schen/malware2021/download/xpxp.ova

3. Boot up windows XP inside VirtualBox.

4. Inside windows XP, download or copy the *hack_dll.zip* to a folder.

https://www.cs.wcupa.edu/schen/malware2021/download/hack_dll.zip

5. Unzip *hack_dll.zip*.
6. Use Ollydbg to open myhack.dll.
7. Following our lecture video to modify the debug string.
8. Following our lecture video to launch DLL Injection attack with the modified DLL file.

More...

Please check the lecture video (Class2 Lab 1: Getting Started with Ollydbg and DLL Injection)

Submission

- The lab due date is available on our course website. Late submission will not be accepted;
- The assignment should be submitted to D2L directly.
- Your submission should include: A **detailed project report in PDF format** to describe what you have done, including screenshots of the final result
- **No copy or cheating is tolerated**. If your work is based on others', please give clear attribution. Otherwise, you **WILL FAIL** this course.