CIS/ECE 387 Fall 2018 Lab3

Due: **10/10/2018**

ACTIVITY: PRACTICING VOLATILITY

DOWNLOAD THE MEMORY IMAGE

You can download the memory image file, zeus.vmem, on canvas under the Files->Labs->Lab3 folder.

Zeus is a malware designed to steal credentials.

GOAL

The open-source toolkit, Volatility framework, is one of the best memory forensic analysis tools to extract valuable information from a memory dump or a .vmem file. In this activity, you will practice volatility's basic plugins for extracting valuable information from a memory image.

INSTRUCTIONS

1. Launch **SIFT Workstation 3**.
2. Run `vol.py -h` to see volatility's options and plugins.
3. Practice these basic plugins to understand how you can use the result for your investigation. For example, `vol.py -f zeus.vmem imageinfo`

imageinfo	Shows basic system information such as type of OS
pslist	Lists the processes of a system
psscan	Finds processes that previously terminated (inactive) and processes that have been hidden or unlinked by a rootkit

pstree	Displays the process listing in tree form
connections	Shows the TCP connections that were active at the time of the memory acquisition
connscan	Extracts TCP connections that were active at the time of the memory acquisition and previous connections that have since been terminated.
hivelist	Locates the virtual addresses of registry hives in memory and the full paths to the corresponding hive on disk
hivescan	Displays the physical addresses of registry hives in memory
printkey	Displays the subkeys, values, data, and data types contained within a specified registry key

If you are interested in learning other plugins that are not covered in the lecture, you can refer to the Volatility Command Reference.

Report

Your report should include the activity log (the main steps you take or the commands you run) with some screenshots and/or outputs and a brief reflection on what you learned (one or two paragraphs).

Please submit your lab report to Canvas under the “lab3” assignment folder. Each group just submits one report.