Memory Forensics “Lab”

**Tools Needed:**

Volatility

VMware

**Goal: Teach new individuals and users the basics of using Volatility and executing forensics skills on a memory dump.**

Download the zip file “FinalProject.zip” and use file “memdump.vmem”.

1. Once you acquired the proper memory dump, what plugin is needed to identify the Operating System and see where the memory dump was taken from. This plugin allows you to basically get a summarization of the file at hand**. Answer: imageinfo**
2. Once you pick your profile from the memory dump, what plugin should be executed when trying to find Pid and PPid of the system? **Answer: psscan**
3. What plugin is needed in order to show all of the hives to get information regarding the system? This plugin prints a list of registry hives and acknowledges of the virtual addresses. **Answer: hivelist**
4. What plugin is needed in order to print the values of the registry hives that were found? **Answer: Printkey**
5. What plugin can you use if you want to find out the possible commands the attacker wrote to the cmd.exe? **Answer: consoles**
6. How can you find the IP addresses of the hacker’s internet server? Answer: **netscan because it shows any network connection corresponding to a specific PID.**
7. How can you find the encrypted passwords of all the users? **Answer: hashdump**
8. How do you show the command line history? **Answer: cmdline**