Lab 14: Memory Analysis

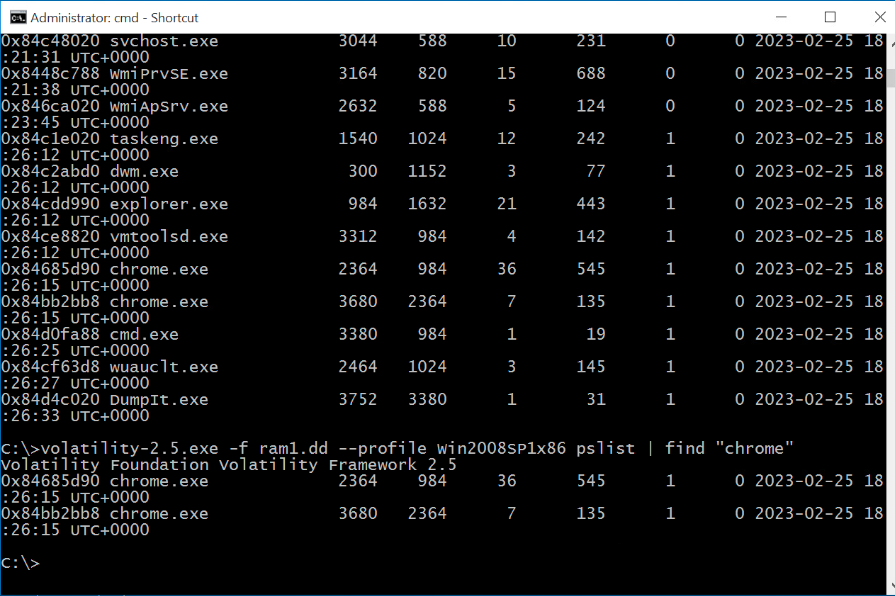
Lab 14 report Name: Kevin Ubilla

This Lab is required for Unit 6. It is worth 15 points. The Challenge Flags are worth 2.5 Extra Credit points.

1. **Use Dumpit to Extract Running Physical Memory, Step 26.**  Please take a few moments to search “volatility framework” to see what this tool is and is used for and summarize what you find in several sentences, below (yes, I realize it means compressing a lot into a small space).

**→**The volatility framework mainly serves as an incident response and analysis tool. It is open-source, written in python, and supports Windows, Mac, and Linux. We use this program during investigations to link artifacts across all file sharing services on a computer, as well as running processes, commands, screenshots, and saved data so that we can gain a better understanding of the incident. I think it is cool how we can uncover footprints like this.**←**

1. **Use Dumpit to Extract Running Physical Memory, Step 29.**  Please capture a portion of the list you generated when you used Volatility to find “chrome” and paste it below.

**→** **←**

1. **Attacking a System Using Armitage, Step 12.** Please do a quick search to find what service(s) port 445 is directly involved in, and, in particular, speculate about what SMB is and how it might be used to attack a machine and summarize it (maybe 4 sentences is a better limit this time) below.

**→** The SMB protocol allows computers to communicate for file, print, or device sharing. It is basically a network file sharing protocol. Port 445 is the access point that allows a computer to connect over the internet. In order to keep it safe we must use MAC address filtering, implement VLANs, install VPN and enable firewall protection. **←**

1. **Attacking a System Using Armitage, Step 21.** Please capture the picture that Armitage displays showing that the Windows system is compromised and display it below.

**Graphical user interface, text

Description automatically generated→ ←**

1. **Attacking a System Using Armitage, Discussion.** Please name what features Armitage offers in addition to those we used in this lab. (Remember, three sentences or less.)

**→** Armitage helps us visualize targets on a GUI, recommend exploits, and shows when a system has been compromised. In addition to what we did in the lab, it can also show post-exploitation features that we have gained access to. **←**

**If you encountered any issues, either positive or negative, with this Lab, please let me know by commenting here. (This IS an experiment, after all.) I am tuning this according to what you say.**

**→ ←**