Assignment 3: Triage Data Collection

Triage is a vital aspect of the incident response process, as it allows the IR team to gather any volatile information that may hint at how the attack occurred, what the attack is accomplishing, and how to prevent the attack from happening again. The corporate world cannot operate in an efficient state if compromised infrastructure is out of commission for a long period of time. Due to this, the IR team must take careful measures to get business operations up and running again, while safeguarding the company from further detriment. For this assignment, I decided to use a fresh install of Windows 10 running on a virtual machine in VirtualBox. Because this installation is brand new, there should not be any indicators of compromise present, but it may provide some useful information to establish a baseline detailing how a normal, uncompromised machine should behave. While the triage tools I used are intended for professional incident response, they could also be used for malicious information gathering if the machine is not properly secured. To perform the triage, I used the BriMor Triage scripts available at https://www.brimorlabs.com/tools/. This webpage has zipped folders available for a multitude of Incident Response purposes, but for now the only one we need is the Live Response Collection tool. This tool is useful because it provides scripts that can be run on Windows, Linux, or MacOS, which covers any operating system that may be present on an enterprise network. Upon downloading and extracting the tools, BriMor makes it incredibly easy to get the information needed by including an EXE file that allows you to choose which scripts in the tool to run. There are 3 scripts available, Triage, Memory Dump, and Complete. Each of these also have a secure option, which will compress the results and password protect them. The Triage script is a basic level script that gathers volatile data to be erased when the machine shuts down. Memory Dump does everything the Triage script does, but also adds the memory register collection process for getting RAM information. Finally, the Complete script will do everything the previous scripts do, but also creates a full copy of the Disk image. For my collection, I ran the Memory Dump script to gather information from RAM and other volatile data. I did not need to gather a full disk image, but I now know that this option is available should I need it. In the UserInfo folder, I was able to find information about the users stored on the computer. Since I was the only user, only one username showed. The scripts also gathered a large volume of network information, stored in the NetworkInfo folder. These include nbtstat, gateway ARP lookup, NetBIOS, and TCPView commands. Under the CopiedFiles folder, any file present on the machine and its metadata are collected, which can be useful in determining the origin of a malware infection. This also makes a copy of the registry to find information that may have changed in those entries. Perhaps the most comprehensive script is the BasicInfo script, which gathers a long list of information that can be found throughout the machine, such as running processes, directories, system info, hidden directories, slack space, internet history, Installed software, etc.

During this triage process, I did not run into any issues thanks to the simplicity provided by the BriMor Tools. These tools only require the compressed file to be decompressed, and then the EXE can be run. Others may run into issues that have to do with running these scripts. It's possible that a user may download the wrong scripts resulting in the incorrect information being gathered. This may cause the investigator to lose important data from not validating the correct information was gathered and turning off the machine