Memory, Pagefile and Hibernation File

This lesson is going to cover four important topics;

- Memory (Windows and Linux)
- Pagefile (Windows)
- Swapfile (Linux)
- Hibernation File (Windows)

We will explain what these are, and why they're important in regard to digital forensics investigations.

MEMORY

What is Memory?

In computing, memory refers to a device that is used to store information for immediate use in a computer or related computer hardware device. Computer memory operates at a high speed, for example, random-access memory (RAM), as a distinction from storage that provides slow-to-access information but offers higher capacities.

What is Memory Analysis?

Memory forensics (sometimes referred to as memory analysis) refers to the analysis of volatile data in a computer's memory dump. Information security professionals conduct memory forensics to investigate and identify attacks or malicious behaviors that do not leave easily detectable tracks on hard drive data.

What is in a Memory Dump?

A memory dump (also known as a core dump or system dump) is a snapshot capture of computer memory data from a specific instant. A memory dump can contain valuable forensics data about the state of the system before an incident such as a crash or security compromise, such as running processes, network connections, and malware that doesn't take the form of files, but instead resides purely in memory.

Why is Memory Forensics Important?

Memory forensics can provide unique insights into runtime system activity, including open network connections and recently executed commands or processes. In many cases, critical data pertaining to attacks or threats will exist solely in system memory – examples include network connections, account credentials, chat messages, encryption keys, running processes, injected code fragments, and internet history which is non-cacheable. Any program – malicious or otherwise – must be loaded in memory in order to execute, making memory forensics critical for identifying otherwise obfuscated attacks.

As attack methods become increasingly sophisticated, memory forensics tools and skills are in high demand for security professionals today. Security solutions such as antivirus programs and endpoint detection and response (EDR) agents may be unable to detect malware written directly into a computer's physical memory or RAM. Security teams should look to memory forensics tools and specialists to protect invaluable business intelligence and data from stealthy attacks such as fileless, in-memory malware or RAM scrapers.

PAGEFILE

What is Pagefile.sys?

The Pagefile.sys is used within Windows operating systems to store data from the RAM when it becomes full. The Pagefile.sys is a contiguous file, so it can be read more quickly, that is located on the root of the hard drive and, normally, the more infrequently used memory pages are stored to it. Whilst RAM is used by the system to store active data as, due to the speed of the operation of it, the system functions more quickly than if that data were stored and read from the hard drive. However, through normal use, RAM is filled by the system and then Windows is able to identify which data to move from it to the Pagefile.sys where it can remain until required again.

It can also be used as a backup of data in the event of a system crash. By default, the Windows operating system configures the size of the Pagefile.sys, however, it can also be altered by the user. Normally the Pagefile.sys can be a significant proportion of data present on the hard drive, however, removing it can greatly reduce the operating speed of the computer.

Deleting Pagefile.sys

The Pagefile.sys is hidden from the normal Windows user by default as, like many other files on the hard drive, it is a system file that Windows identifies as important in the normal operation of the system. If the file is deleted fully then the system will not function correctly and is likely to become unstable, however, the system can be configured to store the pagefile.sys onto another secondary hard drive.

SWAPFILE

The Swap file in Linux

Similarly to within Windows, Linux uses swap space to store RAM when it is full or when the data is not in current use. Within Linux however, traditionally it is a swap partition rather than a swap file and is therefore separate from the other files as it is contained on its own partition. However, it is possible to create a swap file within Linux and to manage the size of that file if required, whereas it is not as easy and sometimes impossible to adjust the size of a swap partition. This can be done via the command `sudo fallocate -l [file size] /swapfile` once the swap file has been temporarily disabled.

Swap space Related Commands in Linux

In order to check the amount of swap space available to the system, the `free -h` command can be used which will provide the breakdown of total, used and free swap space on the system. The `swapon -show` command can then be used to identify whether the swap space is a file or a partition. It is also possible to adjust how often the swap space is used within Linux, the default being 60, however, it can be increased from between 0 (for servers) to 100 (for desktop) which makes the system use the swap space more frequently.

HIBERNATION FILE

What is a Hibernation File?

Starting with Windows 2000, Microsoft introduced the hibernation feature that allows the operating system to store the current state of operation when you turn off the computer, or the system goes into sleep mode. During hibernation everything from memory is copied to the disk in a file called hiberfil.sys, when the computer is restored, the system moves to the saved state. Hibernation files are a good source of information for digital forensic practitioners, as they store data in RAM file without having to run special tools.

Previous Topic | Mark Complete | Next Topic

Back to Lesson