Certified CyberDefender Cheat Sheet [Memory Forensics]

This cheat sheet is for CCD students who are getting ready for the exam.

System profiling

What to look for?	Plugin	Command line
● Identifying OS version	● imageinfo	● Python vol.py -f <memory_dump> imageinfo
● Analyzing KDBG Signatures	● kdbgscan	● Python vol.py -f <memory_dump> –profile=<profile> kdbgscan

Processes Analysis

What to look for?	**Plugin**	**Command line**
• Processes list	• pslist	• Python vol.py -f <memory_dump> –profile=<profile> -g <kdbg_address> pslist
• Processes' Parent-child relationship	• pstree	• Python vol.py -f <memory_dump> –profile=<profile> -g <kdbg_address> pstree
• Hidden Processes	• psxview	• Python vol.py -f <memory_dump> –profile=<profile> -g <kdbg_address> psxview
• Examining Process Details	• psinfo	• python vol.py -f <memory_dump> –profile=<profile> -g <kdbg_address> psinfo -o <process_physical_address>
• Process privilege	• getsids	• python vol.py -f <memory_dump> –profile=<profile> -g <kdbg_address> getsids -o <process_physical_address>

Checklist:

https://cyberdefenders.org/courses/take/6133c324-7aef-4a75-b1ad-91f92e799ac3/#/memory-forensics/t2-processes-analysis-wrapping-up

Network Connections

What to look for?	Plugin	Command line
● Network connections	● netscan	● Python vol.py -f <memory_dump> –profile=<profile> -g <kdbg_address> netscan

Checklist:
https://cyberdefenders.org/courses/take/6133c324-7aef-4a75-b1ad-91f92e799ac3/#/memory-forensics/t3-network-connections-analysis-wrap-up

Persistence Techniques

What to look for?	Plugin	Command line
● registry keys and values	● printkey	● Python vol.py -f <memory_dump> –profile=<profile> -g <kdbg_address> printkey -K <key_path>
● Looking for all persistence techniques	● winesap	● Python vol.py -f <memory_dump> –profile=<profile> -g <kdbg_address> winesap

Checklist:
https://cyberdefenders.org/courses/take/6133c324-7aef-4a75-b1ad-91f92e799ac3/#/memory-forensics/t4-detecting-persistence-techniques-common-persistence-related-registry-keys

Filesystem

What to look for?	Plugin	Command line
● Parse MFT entries	● mftparser	● Python vol.py -f <memory_dump> –profile=<profile> -g <kdbg_address> mftparser
● Visualize memory filesystem	● rstudio	● N/A