Memory analysis

### 

What Volatility plugin will dump a process to an executable file sample?

procdump

What Volatility plugin will extract command history by scanning for \_COMMAND\_HISTORY?

cmdscan

What Volatility plugin will show driver objects?

driverscan

What command do you run to find which memory profile to use with a memory image?

imageinfo

What switch/argument will list all plugins for Volatility?

The process running under PID 544 seems malicious. What is the md5hash of the executable?

What remote IP and port did the system connect to?

Flag format: *ip:port*

**.\volatility\_2.6\_win64\_standalone.exe -f .\0zapftis.vmem --profile=WinXPSP2x86 connscan**

Windows\_Memory\_Analysis\_Basics\_4

10

What profile do you use in conjunction with this memory image?

Use the following file (memory image) to answer the rest of the Memory Analysis challenges.

0zapftis.vmem

**.\volatility\_2.6\_win64\_standalone.exe -f ".\0zapftis.vmem" imageinfo**

Windows\_Malware\_1

10

What command did the attacker type to check the status of the malware?

**.\volatility\_2.6\_win64\_standalone.exe -f ".\0zapftis.vmem" consoles**

sc query malware

Windows\_Malware\_2

10

What are the last 7 digits of the memory offset for the driver used by the malware?

**.\volatility\_2.6\_win64\_standalone.exe -f ".\0zapftis.vmem" driverscan**

1a498b8