Malware Analysis using Volatility

Cybrary course – **Challenge: Memory Mysteries**

Preparing Kali Linux to perform Malware Analysis.

Volatility and Python3:

1. Download Source Code from link in Kali. Ex. Target Location - /home/kali/Downloads/volatility3-2.4.1.zip
2. Open Terminal and navigate to the directory - /home/kali/Downloads/ and unzip the volatility package.
3. Install python3 using the command - sudo apt install python3

Volatility reference: GitHub

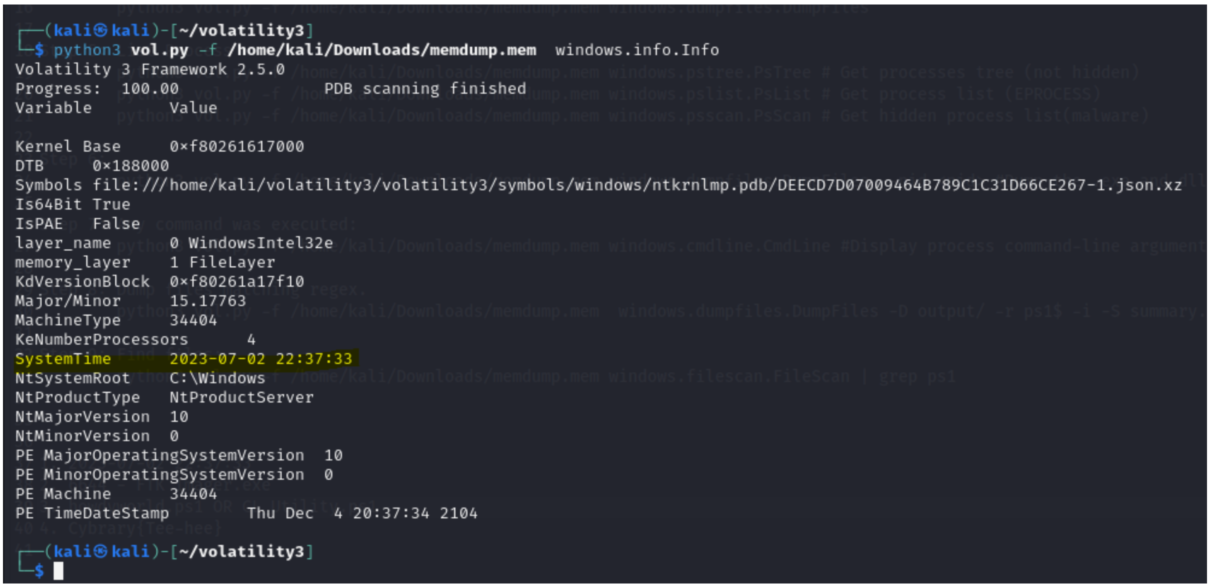
Walkthrough for first challenge: **1.1 Analyzing Memory**

1. What is the date and time (UTC) this memory image was taken? YYYY-MM-DD HH:MM:SS.

Solution: Get OS Information using the syntax - vol.py -f "/path/to/file" windows.info

└─$ python3 vol.py -f /home/kali/Downloads/memdump.mem windows.info.Info

2023-07-02 22:37:33



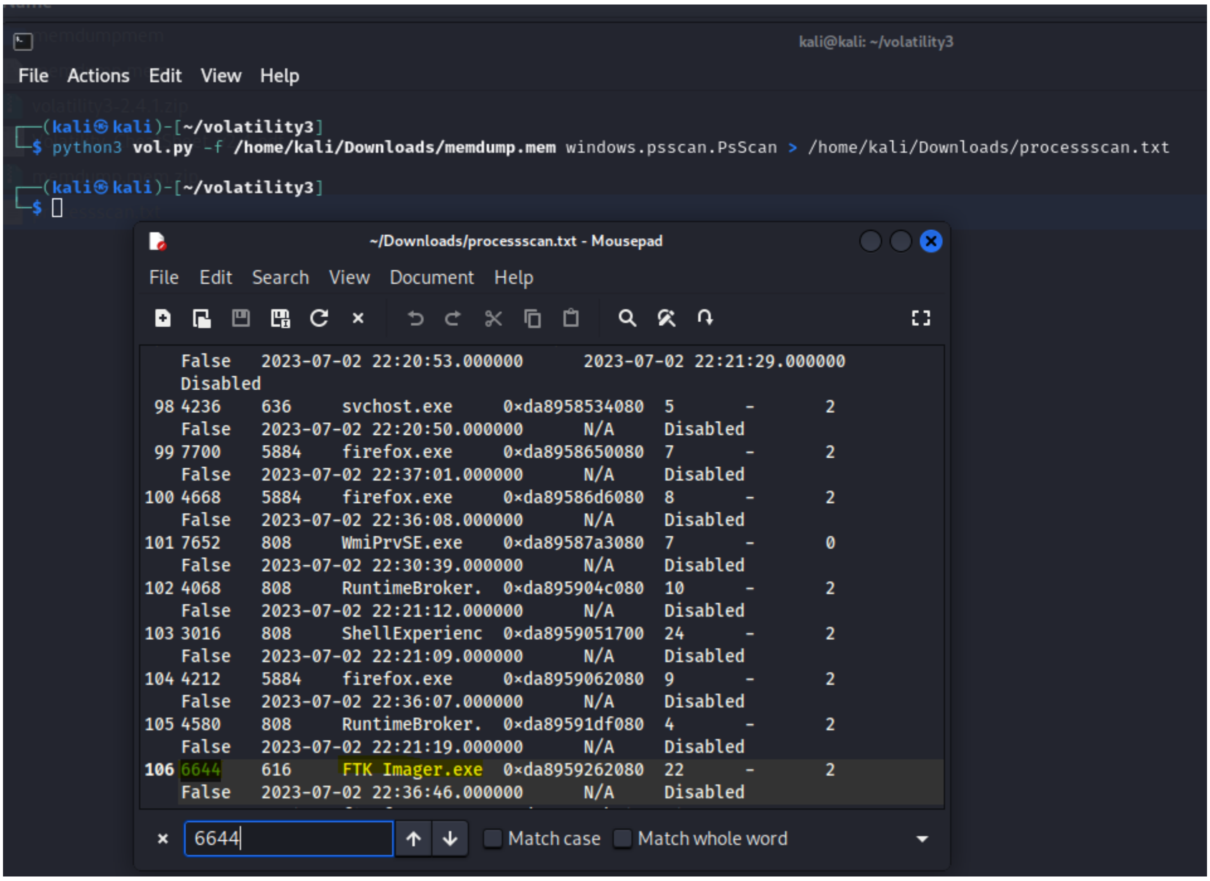
```
┌──(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/kali/Downloads/memdump.mem  windows.info.Info
Volatility 3 Framework 2.5.0
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0×f80261617000
DTB     0×188000
Symbols file:///home/kali/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/DEECD7D07009464B789C1C31D66CE267-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0×f80261a17f10
Major/Minor     15.17763
MachineType     34404
KeNumberProcessors      4
SystemTime      2023-07-02 22:37:33
NtSystemRoot    C:\Windows
NtProductType   NtProductServer
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Thu Dec  4 20:37:34 2104

┌──(kali㉿kali)-[~/volatility3]
└─$ █
```

2. What is name of the executable with the process ID 6644?

Solution: Look for all Processes in the memory dump and identify the process name against the PID using the syntax – vol.py -f "/path/to/file" windows.psscan.psscan.

└─$ python3 vol.py -f /home/kali/Downloads/memdump.mem windows.psscan.PsScan > /home/kali/Downloads/processscan.txt

FTK Imager.exe



kali@kali: ~/volatility3
File Actions Edit View Help
~/Downloads/processscan.txt - Mousepad
File Edit Search View Document Help
6644
Match case
Match whole word

```
┌──(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/kali/Downloads/memdump.mem windows.psscan.PsScan > /home/kali/Downloads/processscan.txt

┌──(kali㉿kali)-[~/volatility3]
└─$ 
```

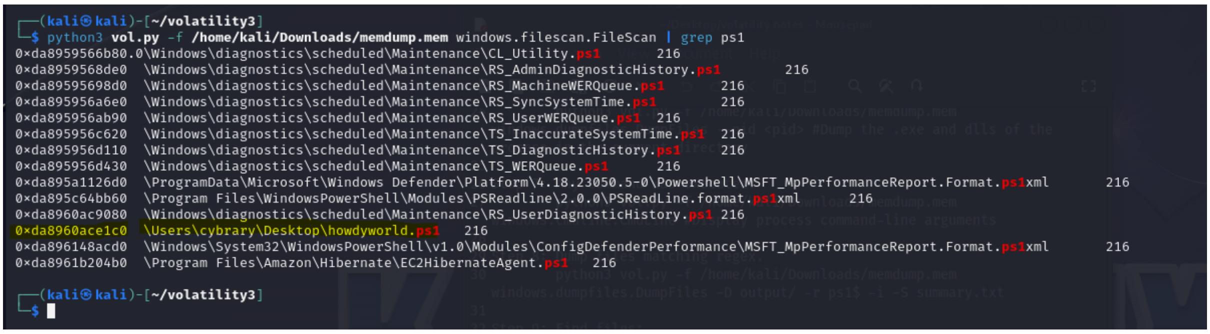
```
    False   2023-07-02 22:20:53.000000      2023-07-02 22:21:29.000000
    Disabled
98 4236     636     svchost.exe     0xda8958534080  5       -       2
    False   2023-07-02 22:20:50.000000      N/A     Disabled
99 7700     5884    firefox.exe     0xda8958650080  7       -       2
    False   2023-07-02 22:37:01.000000      N/A     Disabled
100 4668    5884    firefox.exe     0xda89586d6080  8       -       2
    False   2023-07-02 22:36:08.000000      N/A     Disabled
101 7652    808     WmiPrvSE.exe    0xda89587a3080  7       -       0
    False   2023-07-02 22:30:39.000000      N/A     Disabled
102 4068    808     RuntimeBroker.  0xda895904c080  10      -       2
    False   2023-07-02 22:21:12.000000      N/A     Disabled
103 3016    808     ShellExperienc  0xda8959051700  24      -       2
    False   2023-07-02 22:21:09.000000      N/A     Disabled
104 4212    5884    firefox.exe     0xda8959062080  9       -       2
    False   2023-07-02 22:36:07.000000      N/A     Disabled
105 4580    808     RuntimeBroker.  0xda89591df080  4       -       2
    False   2023-07-02 22:21:19.000000      N/A     Disabled
106 6644    616     FTK Imager.exe  0xda8959262080  22      -       2
    False   2023-07-02 22:36:46.000000      N/A     Disabled
```

3. What is the name of the .PS1 script the user ran?

Solution: Search for any filename with the string .ps1 from the file scan using the syntax - vol.py -f "/path/to/file" windows.filescan.FileScan

└─$ python3 vol.py -f /home/kali/Downloads/memdump.mem windows.filescan.FileScan | grep ps1

howdyworld.ps1



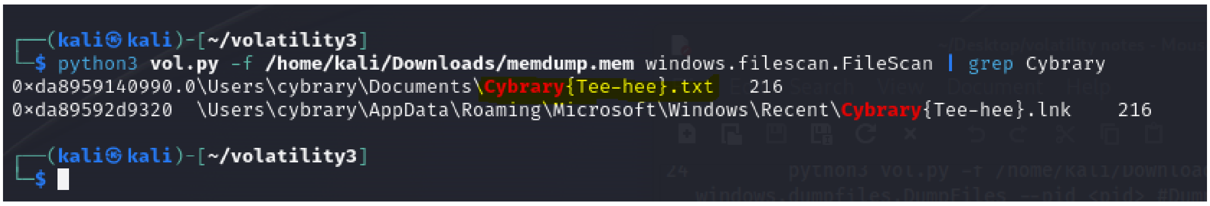
```
┌──(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/kali/Downloads/memdump.mem windows.filescan.FileScan | grep ps1
0xda8959566b80.0\Windows\diagnostics\scheduled\Maintenance\CL_Utility.ps1        216
0xda8959568de0  \Windows\diagnostics\scheduled\Maintenance\RS_AdminDiagnosticHistory.ps1        216
0xda89595698d0  \Windows\diagnostics\scheduled\Maintenance\RS_MachineWERQueue.ps1       216
0xda895956a6e0  \Windows\diagnostics\scheduled\Maintenance\RS_SyncSystemTime.ps1        216
0xda895956ab90  \Windows\diagnostics\scheduled\Maintenance\RS_UserWERQueue.ps1  216
0xda895956c620  \Windows\diagnostics\scheduled\Maintenance\TS_InaccurateSystemTime.ps1  216
0xda895956d110  \Windows\diagnostics\scheduled\Maintenance\TS_DiagnosticHistory.ps1     216
0xda895956d430  \Windows\diagnostics\scheduled\Maintenance\TS_WERQueue.ps1      216
0xda895a1126d0  \ProgramData\Microsoft\Windows Defender\Platform\4.18.23050.5-0\Powershell\MSFT_MpPerformanceReport.Format.ps1xml       216
0xda895c64bb60  \Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadLine.format.ps1xml      216
0xda8960ac9080  \Windows\diagnostics\scheduled\Maintenance\RS_UserDiagnosticHistory.ps1 216
0xda8960ace1c0  \Users\cybrary\Desktop\howdyworld.ps1   216
0xda896148acd0  \Windows\System32\WindowsPowerShell\v1.0\Modules\ConfigDefenderPerformance\MSFT_MpPerformanceReport.Format.ps1xml       216
0xda8961b204b0  \Program Files\Amazon\Hibernate\EC2HibernateAgent.ps1   216

┌──(kali㉿kali)-[~/volatility3]
└─$ 
```

4. What is the hidden flag found in memory? Starts with Cybrary{*}

Solution: Check for filename with the string Cybrary using the file scan plugin using the same syntax above.

└─$ python3 vol.py -f /home/kali/Downloads/memdump.mem windows.filescan.FileScan | grep Cybrary

Cybrary{Tee-hee}



```
┌──(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f /home/kali/Downloads/memdump.mem windows.filescan.FileScan | grep Cybrary
0×da8959140990.0\Users\cybrary\Documents\Cybrary{Tee-hee}.txt   216
0×da89592d9320  \Users\cybrary\AppData\Roaming\Microsoft\Windows\Recent\Cybrary{Tee-hee}.lnk    216

┌──(kali㉿kali)-[~/volatility3]
└─$ 
```