Zrzut ramu zrobiłem na maszynie z Windowsem

PODSTAWOWE INFORMACJE

Na początek warto wyszukać podstawowe informacje na temat obrazu

```
┌──(kali㉿kali)-[~/sledcza/volatility_2.6_lin64_standalone]
└─$ ./volatility_2.6_lin64_standalone -f ../memdump.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
```

Analiza zajmuje długo ponieważ plik waży 9 GB

Niestety volatility w wersji dla pythona 2 nie zadziałała, więc musiałem użyć wersji 3

```
┌──(kali㉿kali)-[~/sledcza/volatility_3/volatility3-1.0.0]
└─$ python vol.py -f ../../memdump.mem windows.info.Info
```

```
Variable        Value

Kernel Base     0×f8055fc00000
DTB     0×1ad000
Symbols file:///home/kali/sledcza/volatility_3/volatility3-1.0.0/volatility3/symbols/windows/ntkrnlmp.pdb/317A67C865B18DBC1E64CBAAB9F971DD-1.json.xz
Is64Bit True
IsPAE   False
primary 0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0×f8056080f388
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors      6
SystemTime      2023-01-24 20:59:33
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Thu Mar 24 20:13:54 2033
```

Widać tutaj podstawowe informacje na temat Kernela i samej maszyny
Kernel Base: 0xf8055fc00000
Directory Table Base: 0x1ad000
Maszyna jest w wersji 64-bitowej
Liczba procesorów (wątków): 6

Zmienne środowiskowe

```
┌──(kali㉿kali)-[~/sledcza/volatility_3/volatility3-1.0.0]
└─$ python vol.py -f ../../memdump.mem windows.envars.Envars
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
PID     Process Block   Variable        Value
```

Zmiennych środowiskowych jest bardzo dużo, ale znajduje się w nich wiele ciekawych informacji

Podstawa systemu plików

```
388     smss.exe        0x15cc1202900   Path    C:\Windows\System32
388     smss.exe        0x15cc1202900   SystemDrive     C:
388     smss.exe        0x15cc1202900   SystemRoot      C:\Windows
```

Liczba procesorów oraz rodzaj systemu windows

```
504     csrss.exe       0x2256e802e10   NUMBER_OF_PROCESSORS    6
504     csrss.exe       0x2256e802e10   OS      Windows_NT
```

Architektura procesora

```
504     csrss.exe       0x2256e802e10   PROCESSOR_ARCHITECTURE  AMD64
504     csrss.exe       0x2256e802e10   PROCESSOR_IDENTIFIER    AMD64 Family 23 Model 96 Stepping 1, AuthenticAMD
```

Nazwa urządzenia

```
3912    svchost.exe     0x21ff4a03340   COMPUTERNAME    DESKTOP-MR396HI
```

MALWARE

```
┌──(kali㉿kali)-[~/sledcza/volatility_3/volatility3-1.0.0]
└─$ python vol.py -f ../../memdump.mem windows.malfind.Malfind
```

Volatility nie znalazło, żadnych wirusów

NETSCAN

```
┌──(kali㉿kali)-[~/sledcza/volatility_3/volatility3-1.0.0]
└─$ python vol.py -f ../../memdump.mem windows.netscan.NetScan
Volatility 3 Framework 1.0.0
```

W netscan nie widzę żadnej podejrzanej aktywności

Widać jedynie procesy systemowe oraz
Spotify
Steam
Microsoft Edge

```
0xc90bd2c282b0  UDPv4   0.0.0.0 1900    *       0               8776    Spotify.exe     2023-01-24 20:53:50.000000
0xc90bd2c2c900  UDPv4   0.0.0.0 51298   *       0               8776    Spotify.exe     2023-01-24 20:53:50.000000
0xc90bd2c2f1a0  UDPv4   0.0.0.0 5353    *       0               4652    msedge.exe      2023-01-24 20:54:06.000000
0xc90bd2c30aa0  UDPv4   0.0.0.0 57621   *       0               8776    Spotify.exe     2023-01-24 20:53:50.000000
0xc90bd2c4a720  UDPv4   0.0.0.0 5353    *       0               8776    Spotify.exe     2023-01-24 20:53:50.000000
0xc90bd2c4a8b0  UDPv4   0.0.0.0 5353    *       0               8776    Spotify.exe     2023-01-24 20:53:50.000000
0xc90bd2c4a8b0  UDPv6   ::      5353    *       0               8776    Spotify.exe     2023-01-24 20:53:50.000000
0xc90bd2c4f540  UDPv4   0.0.0.0 5353    *       0               8776    Spotify.exe     2023-01-24 20:53:50.000000
0xc90bd2c50b20  UDPv4   0.0.0.0 5353    *       0               8776    Spotify.exe     2023-01-24 20:53:50.000000
0xc90bd2c50b20  UDPv6   ::      5353    *       0               8776    Spotify.exe     2023-01-24 20:53:50.000000
```

PSLIST

Patrząc na aktywne procesy znalazłem proces vmtoolsd.exe

```
8684    4844    vmtoolsd.exe    0×c90bd15540c0  6
```

Można po tym wywnioskować, że maszyna, na której został dokonany zrzut to wirtualna maszyna

Jest tu również narzędzie do wykonania zrzutu ram

```
8176    4844    FTK Imager.exe  0×c90bd17a6080  17
```

Tak jak w netscan, tutaj również widać Spotify oraz Steam,
Ale jest też KeePassXC (Menadżer haseł)

```
5296    4844    KeePassXC.exe   0×c90bd20a3080  2
isabled
4952    4844    steam.exe       0×c90bd2195080  28
isabled
9032    856     ShellExperienc  0×c90bd217f300  13
isabled
8776    4844    Spotify.exe     0×c90bd217c080  50
```

Żadnych podejrzanych procesów nie widać