
ATTACK
DEFENSE
by PentesterAcademy

Name	Volatility: Basic II (Windows)
URL	https://attackdefense.com/challengedetails?cid=1118
Type	Forensics: Memory Forensics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

A memory dump of a Windows machine is provided in the home directory of the root user. You have to use Volatility to analyze the memory dump and answer the following questions:

Q1. What is the virtual address of SYSTEM registry hive?

Answer: 0xffffc0018b243000

Command: vol.py -f memory_dump.mem --profile=Win10x64_10240_17770 hivelist

```
root@attackdefense:~#
root@attackdefense:~# vol.py -f memory_dump.mem --profile=Win10x64_10240_17770 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual            Physical           Name
------------------ ------------------ ----
0xffffc0018b229000 0x0000000000021000 [no name]
0xffffc0018b243000 0x000000000002f000 \REGISTRY\MACHINE\SYSTEM
0xffffc0018b256000 0x0000000000fa2000 \REGISTRY\MACHINE\HARDWARE
0xffffc0018be88000 0x000000001f0fd000 \Device\HarddiskVolume1\Boot\BCD
0xffffc0018be7f000 0x000000001f026000 \SystemRoot\System32\Config\SOFTWARE
0xffffc0018c715000 0x0000000030f86000 \SystemRoot\System32\Config\DEFAULT
0xffffc0018ddde000 0x00000000128cd000 \SystemRoot\System32\Config\SECURITY
0xffffc0018c814000 0x000000001ff47000 \SystemRoot\System32\Config\SAM
0xffffc0018ca16000 0x000000001fa68000 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xffffc0018cb8a000 0x000000000d0b9000 \SystemRoot\System32\Config\BBI
0xffffc0018caef000 0x0000000003352f000 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xffffc0018d509000 0x0000000060eb5000 \REGISTRY\A\{00b6ab5b-3a9d-8f8c-2ef6-48485d855974}
0xffffc0018e334000 0x0000000057171000 \??\C:\Users\Nishant\ntuser.dat
```

Q2. What is the SID of the process 'AppXSvc'?

Answer: S-1-5-80-1949724575-2387902436-65106593-1201171665-3967308604

Command: vol.py -f memory_dump.mem --profile=Win10x64_10240_17770 getservicesids

```
root@attackdefense:~# vol.py -f memory_dump.mem --profile=Win10x64_10240_17770 getservicesids
Volatility Foundation Volatility Framework 2.6.1
servicesids = {
    'S-1-5-80-4151353957-356578678-4163131872-800126167-2037860865': '.NET CLR Networking 4.0.0.0',
    'S-1-5-80-3459415445-2224257447-3423677131-2829651752-4257665947': '3ware',
    'S-1-5-80-2670625634-2386107419-4204951937-4094372046-2600379021': 'acpiex',
    'S-1-5-80-3267050047-1503497915-401953950-2662906978-1179039408': 'acpipagr',
    'S-1-5-80-772678238-4220935223-620583658-4118486195-1180343772': 'acpitime',
    'S-1-5-80-1832646050-3387416444-908081792-3295314013-3228576234': 'AdobeARMservice',
    'S-1-5-80-3261807240-4279319092-2126406095-947934052-2578847935': 'ADOVMPPackage',
    'S-1-5-80-2046354688-3987051615-3879164971-215375460-2633017214': 'ADP80XX',
    'S-1-5-80-3882103802-2937937445-2149894622-934926057-1088273958': 'ahcache',
    'S-1-5-80-3532809085-2652327567-2620918877-1058261733-582902671': 'AJRouter',
    'S-1-5-80-2020831507-1298702824-3288167190-116113825-4190209': 'AppReadiness',
    'S-1-5-80-1949724575-2387902436-65106593-1201171665-3967308604': 'AppXSvc',
    'S-1-5-80-3455535628-48649026-488456003-1228671886-4032453889': 'aswVmm',
```

Q3. What is the name of the privilege assigned to OpenVPN which allows it to load/unload drivers?

Answer: SeLoadDriverPrivilege

Command: vol.py -f memory_dump.mem --profile=Win10x64_10240_17770 privs -p 1064

```
root@attackdefense:~# vol.py -f memory_dump.mem --profile=Win10x64_10240_17770  privs -p 1064
Volatility Foundation Volatility Framework 2.6.1
Pid      Process          Value  Privilege                                Attributes               Description
-------- ---------------- ------ ---------------------------------------- ------------------------ -----------
    1064 openvpn-gui.ex        2 SeCreateTokenPrivilege                                            Create a token object
    1064 openvpn-gui.ex        3 SeAssignPrimaryTokenPrivilege                                     Replace a process-level token
    1064 openvpn-gui.ex        4 SeLockMemoryPrivilege                                             Lock pages in memory
    1064 openvpn-gui.ex        5 SeIncreaseQuotaPrivilege                                          Increase quotas
    1064 openvpn-gui.ex        6 SeMachineAccountPrivilege                                         Add workstations to the domain
    1064 openvpn-gui.ex        7 SeTcbPrivilege                                                    Act as part of the operating system
    1064 openvpn-gui.ex        8 SeSecurityPrivilege                                               Manage auditing and security log
    1064 openvpn-gui.ex        9 SeTakeOwnershipPrivilege                                          Take ownership of files/objects
    1064 openvpn-gui.ex       10 SeLoadDriverPrivilege                                             Load and unload device drivers
    1064 openvpn-gui.ex       11 SeSystemProfilePrivilege                                          Profile system performance
```

Q4. Recover the binary for OneDrive process.

Solution:

Get the PID of the process from the process list

Command: vol.py -f memory_dump.mem --profile=Win10x64_10240_17770 pslist | grep OneDrive

```
root@attackdefense:~# vol.py -f memory_dump.mem --profile=Win10x64_10240_17770 pslist | grep OneDrive
Volatility Foundation Volatility Framework 2.6.1
0xffffe00194eb7080 OneDrive.exe          1260    708     13        0      1      1 2019-06-26 17:53:30 UTC+0000

root@attackdefense:~#
```

Extract the binary from the process using PID

Command: vol.py -f memory_dump.mem --profile=Win10x64_10240_17770 procdump -p 1260 --dump-dir .

```
root@attackdefense:~# vol.py -f memory_dump.mem --profile=Win10x64_10240_17770 procdump -p 1260 --dump-dir .
Volatility Foundation Volatility Framework 2.6.1
Process(V)         ImageBase          Name                 Result
------------------ ------------------ -------------------- ------
0xffffe00194eb7080 0x00000000009e0000 OneDrive.exe         OK: executable.1260.exe
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~#
root@attackdefense:~# file executable.1260.exe
executable.1260.exe: PE32 executable (GUI) Intel 80386, for MS Windows
root@attackdefense:~#
```

Q5. Which command can be used to view the loaded kernel modules?

Command: vol.py -f memory_dump.mem --profile=Win10x64_10240_17770 modules

```
root@attackdefense:~# vol.py -f memory_dump.mem --profile=Win10x64_10240_17770 modules
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                 Base                             Size File
------------------ -------------------- ------------------ ------------------ ----
0xffffe001914548c0 ntoskrnl.exe         0xfffff8030908f000           0x852000 \SystemRoot\system32\ntoskrnl.exe
0xffffe00191454740 hal.dll              0xfffff8030901e000            0x71000 \SystemRoot\system32\hal.dll
0xffffe001914545d0 kdcom.dll            0xfffff80307ff7000             0xb000 \SystemRoot\system32\kd.dll
0xffffe00191454450 mcupdate.dll         0xfffff80091d70000            0x8d000 \SystemRoot\system32\mcupdate_GenuineIntel.dll
0xffffe001914542e0 werkernel.sys        0xfffff80091400000            0x10000 \SystemRoot\System32\drivers\werkernel.sys
0xffffe00191454170 CLFS.SYS             0xfffff80091410000            0x64000 \SystemRoot\System32\drivers\CLFS.SYS
0xffffe00191453010 tm.sys               0xfffff80091480000            0x23000 \SystemRoot\System32\drivers\tm.sys
0xffffe00191453ea0 PSHED.dll            0xfffff800914b0000            0x17000 \SystemRoot\system32\PSHED.dll
0xffffe00191453d40 BOOTVID.dll          0xfffff800914d0000             0xb000 \SystemRoot\system32\BOOTVID.dll
0xffffe00191453bd0 cmimcext.sys         0xfffff800914e0000             0xe000 \SystemRoot\System32\drivers\cmimcext.sys
0xffffe00191453a60 ntosext.sys          0xfffff800914f0000             0xc000 \SystemRoot\System32\drivers\ntosext.sys
0xffffe001914538e0 CI.dll               0xfffff80091500000            0x99000 \SystemRoot\system32\CI.dll
```

References:

1. Volatility (https://github.com/volatilityfoundation/volatility)