
ATTACK
DEFENSE
by PentesterAcademy

Name	Volatility: Basics II
URL	https://attackdefense.com/challengedetails?cid=1100
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.

Q1. A process named 'malware' was running on the system. This binary was executed from which shell? Provide full path.

Answer: /bin/bash

Command: vol.py -f memory_dump.img linux_pstree

```
..lightdm            1079
.sshd                816
..sshd               1184
...sshd              1277            1000
....bash             1279            1000
.....sudo            1295
......su             1296
.......bash          1297
........insmod       1350
....bash             1311            1000
.....sudo            1327
......su             1328
.......bash          1329
........malware      1342
.........[malware]   1347
.........[malware]   1348
.........[malware]   1349
```

Q2. Which DNS Server was running on the system?

Answer: dnsmasq

Command: vol.py -f memory_dump.img linux_pstree

```
.dbus-daemon          640                 106
.cups-browsed         667
.NetworkManager       668
..dhclient            833
..dnsmasq             847                 65534
.snapd                681
.polkitd              781
.lightdm              796
```

Q3. What is the MAC address of the machine with IP address 192.168.8.206?

Answer: 34:e6:ad:56:e1:04

Command: vol.py -f memory_dump.img linux_arp

```
root@attackdefense:~# vol.py -f memory_dump.img linux_arp
Volatility Foundation Volatility Framework 2.6.1
[224.0.0.251                            ] at 01:00:5e:00:00:fb    on enp0s3
[192.168.8.255                          ] at ff:ff:ff:ff:ff:ff    on enp0s3
[255.255.255.255                        ] at ff:ff:ff:ff:ff:ff    on enp0s3
[0.0.0.0                                ] at 00:00:00:00:00:00    on lo
[192.168.8.206                          ] at 34:e6:ad:56:e1:04    on enp0s3
[192.168.8.1                            ] at e4:95:6e:44:3b:b1    on enp0s3
[224.0.0.22                             ] at 01:00:5e:00:00:16    on enp0s3
[ff02::1                                ] at 33:33:00:00:00:01    on enp0s3
[ff02::fb                               ] at 33:33:00:00:00:fb    on enp0s3
[::1                                    ] at 00:00:00:00:00:00    on lo
[ff02::1:fffe:d687                      ] at 33:33:ff:fe:d6:87    on enp0s3
[ff02::2                                ] at 33:33:00:00:00:02    on enp0s3
[ff02::16                               ] at 33:33:00:00:00:16    on enp0s3
root@attackdefense:~#
```

Q4. When was the memory dump taken? Provide date in DDMMYYYY.

Answer: 22062019

Command: vol.py -f memory_dump.img linux_bash

```
root@attackdefense:~# vol.py -f memory_dump.img linux_bash
Volatility Foundation Volatility Framework 2.6.1
Pid      Name                 Command Time                   Command
-------- -------------------- ------------------------------ -------
    1279 bash                 2019-06-22 18:52:34 UTC+0000   sudo su
    1297 bash                 2019-06-22 18:52:37 UTC+0000   cd ~
    1297 bash                 2019-06-22 18:52:39 UTC+0000   ls -l
    1297 bash                 2019-06-22 18:52:48 UTC+0000   lsmod | grep lime
    1297 bash                 2019-06-22 18:53:00 UTC+0000   cd LiME/
    1297 bash                 2019-06-22 18:53:04 UTC+0000   cd src/
    1297 bash                 2019-06-22 18:55:22 UTC+0000   insmod lime-4.15.0-45-generic.ko "path=tcp:4444 format=lime"
    1311 bash                 2019-06-22 18:54:32 UTC+0000   sudo su
    1329 bash                 2019-06-22 18:54:35 UTC+0000   cd ~
    1329 bash                 2019-06-22 18:54:37 UTC+0000   ls -l
    1329 bash                 2019-06-22 18:54:49 UTC+0000   cp /home/osboxes/malware .
    1329 bash                 2019-06-22 18:54:53 UTC+0000   chmod +x malware
    1329 bash                 2019-06-22 18:54:55 UTC+0000   ./malware
    1354 bash                 2019-06-22 18:55:39 UTC+0000   sudo su
    1373 bash                 2019-06-22 18:55:44 UTC+0000   cd /root/
    1373 bash                 2019-06-22 18:56:10 UTC+0000   nc localhost 4444 > memory_dump.img
root@attackdefense:~#
```

Q5. An SSH session was established with another machine. What is the IP address of the other machine?

Answer: 192.168.8.206

Command: vol.py -f memory_dump.img linux_netstat

```
TCP      192.168.8.123   :    22 192.168.8.206   : 1100 ESTABLISHED                 sshd/1277
UNIX 20742                sshd/1277
UNIX 20949                sshd/1277
UNIX 21011                sudo/1295
UNIX 21014                sudo/1295
UNIX 21031                  su/1296
UNIX 21132                sudo/1327
UNIX 21135                sudo/1327
UNIX 21152                  su/1328
```

Q6. Recover the binary for the 'malware' process from the memory dump.

Solution:

Checking process list

Command: vol.py -f memory_dump.img linux_pslist

```
0xffff8b8715ee2d80 malware             1347            1342            0               0       ------------------ 0
0xffff8b8718de4440 malware             1348            1342            0               0       ------------------ 0
0xffff8b8715eec440 malware             1349            1342            0               0       ------------------ 0
0xffff8b8715eedb00 insmod              1350            1297            0               0       0x0000000018f5e000 0
0xffff8b871e24db00 malware             1351            1342            0               0       ------------------ 0
0xffff8b8713ed16c0 malware             1353            1342            0               0       ------------------ 0
0xffff8b8713efc440 bash                1354            1277            1000            1000    0x0000000018f58000 0
0xffff8b871efb8000 sudo                1370            1354            0               1000    0x0000000018f82000 0
0xffff8b871d78ad80 malware             1371            1342            0               0       ------------------ 0
0xffff8b871d78c440 su                  1372            1370            0               0       0x0000000018f6e000 0
0xffff8b871d78db00 bash                1373            1372            0               0       0x0000000018fda000 0
0xffff8b8715c616c0 malware             1383            1342            0               0       ------------------ 0
0xffff8b8715c65b00 malware             1384            1342            0               0       ------------------ 0
```

Dumping binary using ppid

Command: vol.py -f memory_dump.img linux_procdump -p 1342 --dump-dir .

```
root@attackdefense:~# vol.py -f memory_dump.img linux_procdump -p 1342 --dump-dir .
Volatility Foundation Volatility Framework 2.6.1
Offset             Name                 Pid             Address            Output File
------------------ -------------------- --------------- ------------------ -----------
0xffff8b871d1dc440 malware              1342            0x0000000000400000 ./malware.1342.0x400000
root@attackdefense:~#
```

References:

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