
ATTACK
DEFENSE
by PentesterAcademy

Name	Malware I
URL	https://attackdefense.com/challengedetails?cid=1106
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.

An unauthorized SSH connection was established with a production server and a suspicious program was executed on it. The memory dump of that server is given to you. You have to use Volatility to analyze the memory dump and answer the following questions:

Q1. What is the name of the suspicious program?

Answer: runtime

Command: vol.py -f memory_dump.img linux_pstree

```
....gdbus              15042           1000
.sshd                  834
..sshd                 2182
...sshd                2283            1000
....sftp-server        2284            1000
....bash               7682            1000
.....sudo              11724
......su               11756
.......bash            11757
........runtime        14084
.........[sh]          14085
.........[unity-active-pl] 14968           -1
```

Q2. What is the name of the directory in which the suspicious program file is kept?

Answer: Downloads

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
-------- -------------------- ------------------------------ -------
   11757 bash                 2019-06-25 14:21:17 UTC+0000   ./Downloads/runtime
   14159 bash                 2019-06-25 14:21:28 UTC+0000   sudo su
   14159 bash                 2019-06-25 14:21:28 UTC+0000   sudo su
   14259 bash                 2019-06-25 14:21:33 UTC+0000   exit
   14259 bash                 2019-06-25 14:21:33 UTC+0000   exit
   14259 bash                 2019-06-25 14:21:33 UTC+0000   ./runtime
```

Q3. What is the IP address of the machine from which the SSH connection was initiated?

Answer: 192.168.8.206

Command: vol.py -f memory_dump.img linux_netstat

```
UNIX 24333      update-notifier/2058
TCP      192.168.8.123   :   22 192.168.8.206   :51370 ESTABLISHED                sshd/2182
UNIX 27312                sshd/2182
UNIX 27465                sshd/2182
TCP      192.168.8.123   :   22 192.168.8.206   :51370 ESTABLISHED                sshd/2283
UNIX 27312                sshd/2283
```

Q4. Which language was used to write the suspicious program?

Answer: python

Command:

Check the pid for the suspicious process

Command: vol.py -f memory_dump.img linux_pslist

```
0xffff9636d9734440 kworker/0:1          9262            2               0               0       ------------------ 0
0xffff9636d3adad80 sudo                 11724           7682            0               1000    0x000000001e6fc000 0
0xffff9636cf9e96c0 su                   11756           11724           0               0       0x0000000014188000 0
0xffff9636cf76ad80 bash                 11757           11756           0               0       0x0000000019696000 0
0xffff9636de50ad80 runtime              14084           11757           0               0       0x000000000fb1e000 0
0xffff9636cf69ad80 sh                   14085           14084           0               0       ------------------ 0
0xffff9636d9730000 bash                 14159           2283            1000            1000    0x00000000190cc000 0
0xffff9636cf768000 sudo                 14232           14159           0               1000    0x00000000133c6000 0
0xffff9636db645b00 su                   14256           14232           0               0       0x0000000019394000 0
0xffff9636d030c440 bash                 14259           14256           0               0       0x000000000fb18000 0
```

Dump the program file

Command: vol.py -f memory_dump.img linux_procdump -p 14084 --dump-dir .

```
root@attackdefense:~# vol.py -f memory_dump.img linux_procdump -p 14084 --dump-dir .
Volatility Foundation Volatility Framework 2.6.1
Offset             Name                 Pid             Address            Output File
------------------ -------------------- --------------- ------------------ -----------
0xffff9636de50ad80 runtime              14084           0x0000000000400000 ./runtime.14084.0x400000
root@attackdefense:~#
```

Store all strings in one file and check those

Commands:
strings runtime.14084.0x400000 > strings_runtime
Cat strings_runtime | grep python

```
root@attackdefense:~# strings runtime.14084.0x400000 > strings_runtime
root@attackdefense:~#
root@attackdefense:~# cat strings_runtime | grep python
<prefix>/pythonX.X
python
Try `python -h' for more information.
Non-ASCII character '\x%.2x' in file %.200s on line %i, but no encoding
-0263/ for details
python: Can't reopen .pyc file
lib/python2.7
python2.7
/usr/bin/python2.7
root@attackdefense:~#
```

Python is being used by the program.

Q5. Which virtualization environment was used to run this server?

Answer: virtualbox

Command: vol.py -f memory_dump.img linux_dmesg

```
[1620965463049.1620] CPU: 0 PID: 14862 Comm: insmod Tainted: G        WC OE    4.15.0-45-generic #48~16.04.1-Ubuntu
[1620965464788.1620] Hardware name: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
[1620965468890.1620] RIP: 0010:inet_accept+0x154/0x170
[1620965470714.1620] RSP: 0018:ffffa19fc044fb78 EFLAGS: 00010286
[1620965473570.1620] RAX: 0000000000000001 RBX: ffff9636c125b000 RCX: 0000000000000000
[1620965475695.1620] RDX: 000000000000018a RSI: 00000000fffffe01 RDI: ffffffff99639190
```

References:

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