SEGURIDAD EN SISTEMAS OPERATIVOS

4º Grado en Informática – Complementos de Ing. del Software

Curso 2018-19

Práctica [3]. Auditoría informática e Informática forense

Sesión [1]. Análisis forense en Linux (ii)

Autor[1]: Matilde Cabrera González

Ejercicio 1.

Crear un volcado de memoria en formato *.lime* de la máquina que estéis utilizando.

```
mati@mati-VirtualBox:~$ git clone https://github.com/504ensicsLabs/LiME.git
Clonando en 'LiME'...
remote: Enumerating objects: 22, done.
remote: Counting objects: 100% (22/22), done.
remote: Compressing objects: 100% (15/15), done.
remote: Total 264 (delta 10), reused 15 (delta 7), pack-reused 242
Recibiendo objetos: 100% (264/264), 1.59 MiB | 1.50 MiB/s, listo.
Resolviendo deltas: 100% (129/129), listo.
mati@mati-VirtualBox:~$
```

```
mati@mati-VirtualBox:~$ uname -r
4.15.0-42-generic
mati@mati-VirtualBox:~$
```

```
mati@mati-VirtualBox:~$ sudo apt install make build-essential linux-headers-4.15.0-42
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
build-essential ya está en su versión más reciente (12.4ubuntu1).
fijado build-essential como instalado manualmente.
make ya está en su versión más reciente (4.1-9.1ubuntu1).
fijado make como instalado manualmente.
linux-headers-4.15.0-42 ya está en su versión más reciente (4.15.0-42.45).
fijado linux-headers-4.15.0-42 como instalado manualmente.
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  linux-headers-4.15.0-34 linux-headers-4.15.0-34-generic linux-image-4.15.0-34-generic
  linux-modules-4.15.0-34-generic linux-modules-extra-4.15.0-34-generic
Utilice «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
mati@mati-VirtualBox:~$
```

[1] Como autor declaro que los contenidos del presente documento son originales y elaborados por mi. De no cumplir con este compromiso, soy consciente de que, de acuerdo con la "Normativa de evaluación y de calificaciones de los estudiantes de la Universidad de Granada" esto "conllevará la calificación numérica de cero … independientemente del resto de calificaciones que el estudiante hubiera obtenido ..."

```
mati@mati-VirtualBox:~$ cd LiME/src
mati@mati-VirtualBox:~/LiME/src$ make
make -C /lib/modules/4.15.0-42-generic/build M="/home/mati/LiME/src" modules
make[1]: se entra en el directorio '/usr/src/linux-headers-4.15.0-42-generic'
Makefile:975: "Cannot use CONFIG_STACK_VALIDATION=y, please install libelf-dev, libelf-devel or
elfutils-libelf-devel"
  CC [M]  /home/mati/LiME/src/tcp.o
  CC [M]  /home/mati/LiME/src/disk.o
  CC [M]  /home/mati/LiME/src/main.o
  CC [M]  /home/mati/LiME/src/hash.o
  LD [M]  /home/mati/LiME/src/lime.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/mati/LiME/src/lime.mod.o
  LD [M]  /home/mati/LiME/src/lime.ko
make[1]: se sale del directorio '/usr/src/linux-headers-4.15.0-42-generic'
strip --strip-unneeded lime.ko
mv lime.ko lime-4.15.0-42-generic.ko
mati@mati-VirtualBox:~/LiME/src$
```

Tenemos preparada la herramienta para hacer un volcado de memoria RAM.
Ahora realizamos el volcado

```
mati@mati-VirtualBox:~/LiME/src$ sudo insmod lime-4.15.0-42-generic.ko path=/hom
e/mati/LiME/volcado.dd format=raw
mati@mati-VirtualBox:~/LiME/src$ cd ..
mati@mati-VirtualBox:~/LiME$ ls
doc  LICENSE  README.md  src  volcado.dd
```

```
mati@mati-VirtualBox:~/LiME$ du volcado.dd
2954800 volcado.dd
mati@mati-VirtualBox:~/LiME$ ls -l
total 2954832
drwxr-xr-x 2 mati mati       4096 dic 16 23:02 doc
-rw-r--r-- 1 mati mati      18027 dic 16 23:02 LICENSE
-rw-r--r-- 1 mati mati       3650 dic 16 23:02 README.md
drwxr-xr-x 3 mati mati       4096 dic 17 07:34 src
-r--r--r-- 1 root root 3025620992 dic 17 07:50 volcado.dd
mati@mati-VirtualBox:~/LiME$
```

Ejercicio 2.

Instalar `volatility` para analizar la imagen de la RAM obtenida en el Ejercicio 1 con tres *plugins* para ver la información de suministran.

```
mati@mati-Lenovo-50-70:~$ sudo apt install python python-crypto
[sudo] contraseña para mati:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
python ya está en su versión más reciente (2.7.15~rc1-1).
fijado python como instalado manualmente.
python-crypto ya está en su versión más reciente (2.6.1-8ubuntu2).
fijado python-crypto como instalado manualmente.
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
  linux-headers-4.15.0-36 linux-headers-4.15.0-36-generic
  linux-image-4.15.0-36-generic linux-modules-4.15.0-36-generic
  linux-modules-extra-4.15.0-36-generic
Utilice «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 39 no actualizados.
mati@mati-Lenovo-50-70:~$
```

Visito la página, elijo una versión e inspecciono, copio el enlace al mismo (https://storage.googleapis.com/google-code-archive-downloads/v2/code.google.com/volatility/volatility-2.3.1.tar.gz)

```
mati@mati-VirtualBox:~$ curl -L https://storage.googleapis.com/google-code-archive-do
wnloads/v2/code.google.com/volatility/volatility-2.3.1.tar.gz -o volatility-2.3.1.tar
.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 1722k  100 1722k    0     0  1504k      0  0:00:01  0:00:01 --:--:-- 1504k
mati@mati-VirtualBox:~$ tar -xvf volatility-2.3.1.tar.gz
volatility-2.3.1/
volatility-2.3.1/README.txt
volatility-2.3.1/Makefile
volatility-2.3.1/setup.py
volatility-2.3.1/setup.cfg
volatility-2.3.1/MANIFEST.in
volatility-2.3.1/volatility/
volatility-2.3.1/volatility/exceptions.py
volatility-2.3.1/volatility/commands.py
volatility-2.3.1/volatility/protos.py
volatility-2.3.1/volatility/plugins/
volatility-2.3.1/volatility/plugins/volshell.py
volatility-2.3.1/volatility/plugins/registry/
volatility-2.3.1/volatility/plugins/registry/hivelist.py
volatility-2.3.1/volatility/plugins/registry/lsadump.py
volatility-2.3.1/volatility/plugins/registry/__init__.py
volatility-2.3.1/volatility/plugins/registry/hivescan.py
volatility-2.3.1/volatility/plugins/registry/printkey.py
volatility-2.3.1/volatility/plugins/registry/shimcache.py
volatility-2.3.1/volatility/plugins/registry/shellbags.py
```

```
mati@mati-VirtualBox:~$ sudo mv volatility-2.3.1 /opt/
mati@mati-VirtualBox:~$ cd /opt/volatility-2.3.1/
mati@mati-VirtualBox:/opt/volatility-2.3.1$ make
python setup.py build
running build
running build_py
creating build
creating build/lib.linux-x86_64-2.7
creating build/lib.linux-x86_64-2.7/volatility
copying volatility/constants.py -> build/lib.linux-x86_64-2.7/volatility
copying volatility/__init__.py -> build/lib.linux-x86_64-2.7/volatility
copying volatility/dwarf.py -> build/lib.linux-x86_64-2.7/volatility
copying volatility/cache.py -> build/lib.linux-x86_64-2.7/volatility
copying volatility/registry.py -> build/lib.linux-x86_64-2.7/volatility
copying volatility/utils.py -> build/lib.linux-x86_64-2.7/volatility
copying volatility/timefmt.py -> build/lib.linux-x86_64-2.7/volatility
copying volatility/protos.py -> build/lib.linux-x86_64-2.7/volatility
copying volatility/conf.py -> build/lib.linux-x86_64-2.7/volatility
copying volatility/exceptions.py -> build/lib.linux-x86_64-2.7/volatility
copying volatility/fmtspec.py -> build/lib.linux-x86_64-2.7/volatility
copying volatility/obj.py -> build/lib.linux-x86_64-2.7/volatility
copying volatility/scan.py -> build/lib.linux-x86_64-2.7/volatility
copying volatility/debug.py -> build/lib.linux-x86_64-2.7/volatility
copying volatility/addrspace.py -> build/lib.linux-x86_64-2.7/volatility
copying volatility/commands.py -> build/lib.linux-x86_64-2.7/volatility
creating build/lib.linux-x86_64-2.7/volatility/win32
copying volatility/win32/xpress.py -> build/lib.linux-x86_64-2.7/volatility/win32
copying volatility/win32/__init__.py -> build/lib.linux-x86_64-2.7/volatility/win32
```

```
mati@mati-VirtualBox:/opt/volatility-2.3.1$ sudo make install
python setup.py install
running install
running build
running build_py
running build_scripts
running install_lib
creating /usr/local/lib/python2.7/dist-packages/volatility
copying build/lib.linux-x86_64-2.7/volatility/constants.py -> /usr/local/lib/python2.
7/dist-packages/volatility
copying build/lib.linux-x86_64-2.7/volatility/__init__.py -> /usr/local/lib/python2.7
/dist-packages/volatility
copying build/lib.linux-x86_64-2.7/volatility/dwarf.py -> /usr/local/lib/python2.7/di
st-packages/volatility
```

Comprobamos la primera y no va, la segunda si

```
mati@mati-VirtualBox:/opt/volatility-2.3.1$ vol.py imageinfo -f /home/mati/LiME/volca
do.dd
Volatility Foundation Volatility Framework 2.3.1
Determining profile based on KDBG search...
```

Pluying no responden, la maquina se termina bloqueando:

```
mati@mati-VirtualBox:/opt/volatility-2.3.1$ python vol.py imageinfo -f /home/mati/LiME/vo
lcado.dd --profile=VistaSP0x64
Volatility Foundation Volatility Framework 2.3.1
Determining profile based on KDBG search...
```

He estado mirado la información, me pilla los profiles de Windows

```
mati@mati-VirtualBox:/opt/volatility-2.3.1$ python vol.py --info
Volatility Foundation Volatility Framework 2.3.1


Profiles
--------
VistaSP0x64     - A Profile for Windows Vista SP0 x64
VistaSP0x86     - A Profile for Windows Vista SP0 x86
VistaSP1x64     - A Profile for Windows Vista SP1 x64
VistaSP1x86     - A Profile for Windows Vista SP1 x86
VistaSP2x64     - A Profile for Windows Vista SP2 x64
VistaSP2x86     - A Profile for Windows Vista SP2 x86
Win2003SP0x86   - A Profile for Windows 2003 SP0 x86
Win2003SP1x64   - A Profile for Windows 2003 SP1 x64
Win2003SP1x86   - A Profile for Windows 2003 SP1 x86
Win2003SP2x64   - A Profile for Windows 2003 SP2 x64
Win2003SP2x86   - A Profile for Windows 2003 SP2 x86
Win2008R2SP0x64 - A Profile for Windows 2008 R2 SP0 x64
Win2008R2SP1x64 - A Profile for Windows 2008 R2 SP1 x64
Win2008SP1x64   - A Profile for Windows 2008 SP1 x64
Win2008SP1x86   - A Profile for Windows 2008 SP1 x86
Win2008SP2x64   - A Profile for Windows 2008 SP2 x64
Win2008SP2x86   - A Profile for Windows 2008 SP2 x86
Win7SP0x64      - A Profile for Windows 7 SP0 x64
Win7SP0x86      - A Profile for Windows 7 SP0 x86
Win7SP1x64      - A Profile for Windows 7 SP1 x64
Win7SP1x86      - A Profile for Windows 7 SP1 x86
WinXPSP1x64     - A Profile for Windows XP SP1 x64
WinXPSP2x64     - A Profile for Windows XP SP2 x64
WinXPSP2x86     - A Profile for Windows XP SP2 x86
WinXPSP3x86     - A Profile for Windows XP SP3 x86
```

Sigo haciendo pruebas, pero no dan resultado…

```
mati@mati-VirtualBox:/opt/volatility-2.3.1$ python vol.py imageinfo -f /home/mati/LiME/vo
lcado.dd --profile=winXPSP2x64
Volatility Foundation Volatility Framework 2.3.1
ERROR   : volatility.addrspace: Invalid profile winXPSP2x64 selected
mati@mati-VirtualBox:/opt/volatility-2.3.1$ python vol.py imageinfo -f /home/mati/LiME/vo
lcado.dd --profile=win7SP1x64
Volatility Foundation Volatility Framework 2.3.1
ERROR   : volatility.addrspace: Invalid profile win7SP1x64 selected
mati@mati-VirtualBox:/opt/volatility-2.3.1$ python vol.py imageinfo -f /home/mati/LiME/vo
lcado.dd --profile=win2008SP2x64
Volatility Foundation Volatility Framework 2.3.1
ERROR   : volatility.addrspace: Invalid profile win2008SP2x64 selected
mati@mati-VirtualBox:/opt/volatility-2.3.1$ python vol.py imageinfo -f /home/mati/LiME/vo
lcado.dd --profile=win2003SP1x64
Volatility Foundation Volatility Framework 2.3.1
ERROR   : volatility.addrspace: Invalid profile win2003SP1x64 selected
mati@mati-VirtualBox:/opt/volatility-2.3.1$ python vol.py imageinfo -f /home/mati/LiME/vo
lcado.dd --profile=VistasSP2x64
Volatility Foundation Volatility Framework 2.3.1
ERROR   : volatility.addrspace: Invalid profile VistasSP2x64 selected
mati@mati-VirtualBox:/opt/volatility-2.3.1$
```