Tarea 2.2 - Instalación de Volatility 2 y Volatility 3 sobre un contenedor LXC

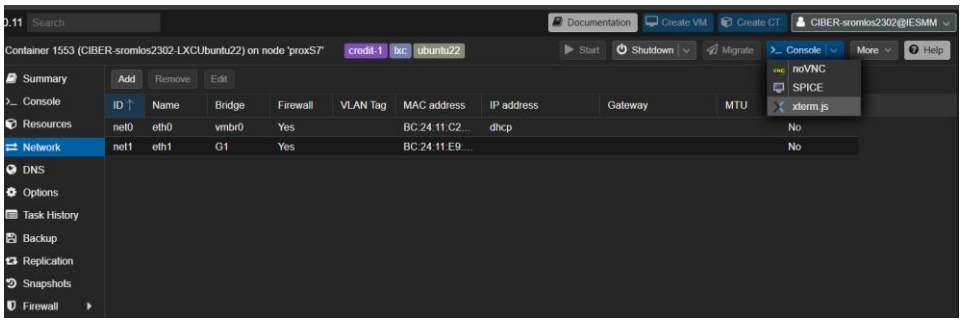
Trabajo realizado por:

Índice

1.- Instalación Volatility 2 y 3

1.1.- Creación del contenedor

Primero, creamos el contenedor y lo abrimos con xterm.js.



1.2.- Instalación Volatility2

Después, instalamos Python2 y pip:

sudo apt update

sudo apt install -y python2 python-pip

Verificamos con el siguiente comando que esté todo bien:

python2 --version

pip2 --version

Instalamos Volatility 2:

sudo pip2 install https://github.com/volatilityfoundation/volatility/archive/refs/heads/master.zip

Para que todos los plugins funcionen (malware, crypto, YARA, etc.):

sudo apt install -y build-essential python2-dev libyara-dev

sudo pip2 install -U "pip==20.3.4" "setuptools==44.1.1" "wheel==0.37.1"

sudo pip2 install pycrypto==2.6.1 distorm3==3.4.4 yara-python==3.10.0 pefile==2019.4.18 pytz==2021.3

Y comprobamos que funciona:

vol.py -h

1.3.- Instalación de Volatility3

Ahora para instalar Volatility 3, primero instalamos Python3 y pip:

sudo apt update

sudo apt install -y python3 python3-venv python3-pip git build-essential libyara-dev

Verificamos que se haya instalado correctamente:

python3 --version

pip3 --version

Clonamos el repositorio oficial:

cd ~

git clone https://github.com/volatilityfoundation/volatility3.git

cd volatility3

Creamos un entorno virtual:

python3 -m venv venv

source venv/bin/activate

Instalamos Volatility3:

python3 -m pip install -U pip setuptools wheel

python3 -m pip install -e

Instalamos algunas dependencias opcionales:

python3 -m pip install pycryptodome impacket capstone pefile yara-python

Y probamos que funcione:

vol -h

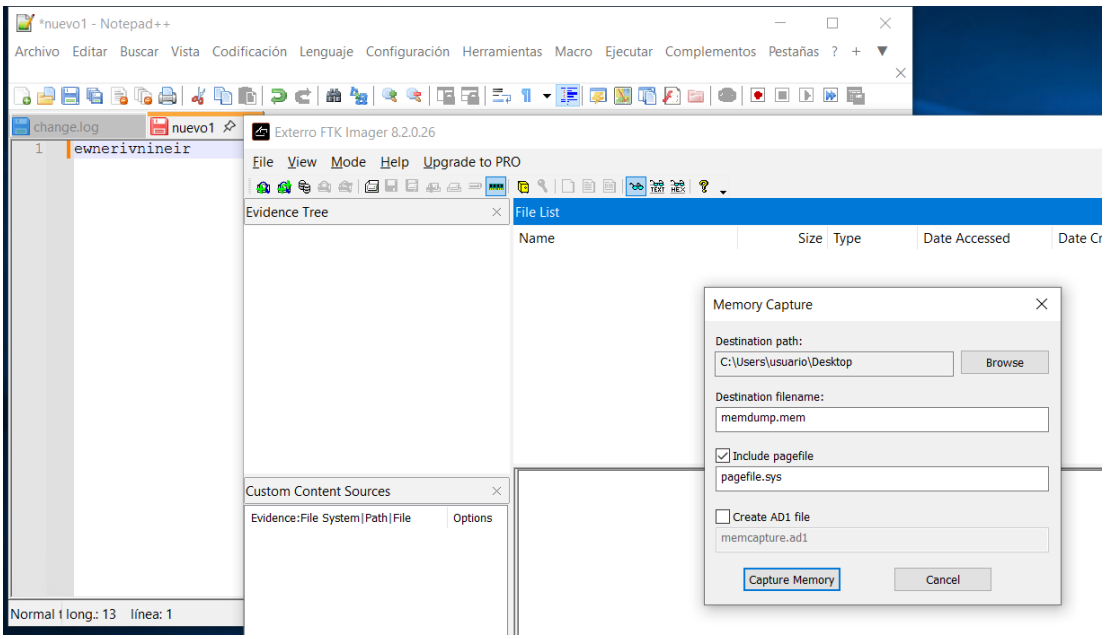
Para acceder desde cualquier carpeta:

sudo ln -sf ~/volatility3/venv/bin/vol /usr/local/bin/vol3

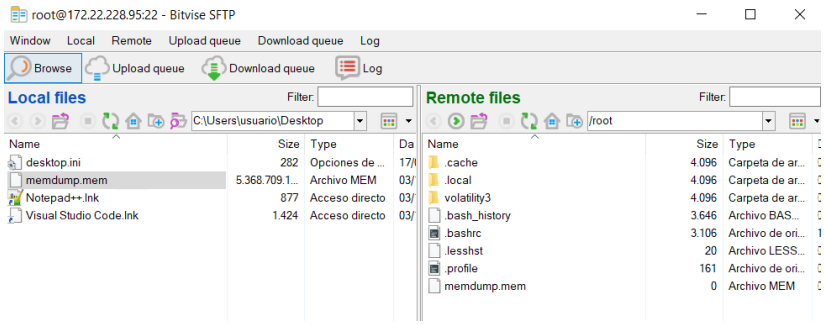
2.- Uso de Volatility 2 y 3

Instalo NotePad++ y CodeBlocks.

Ahora dejándolos abiertos, hago una copia de la ram.

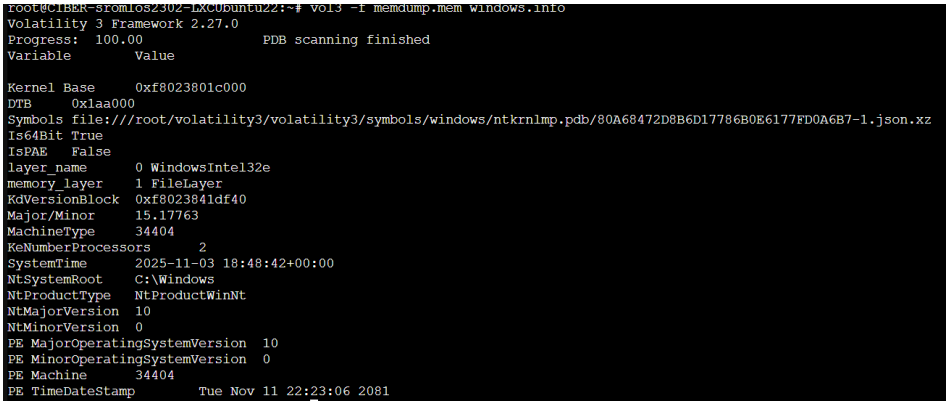


Ahora mediante Bitvise me paso el archivo.



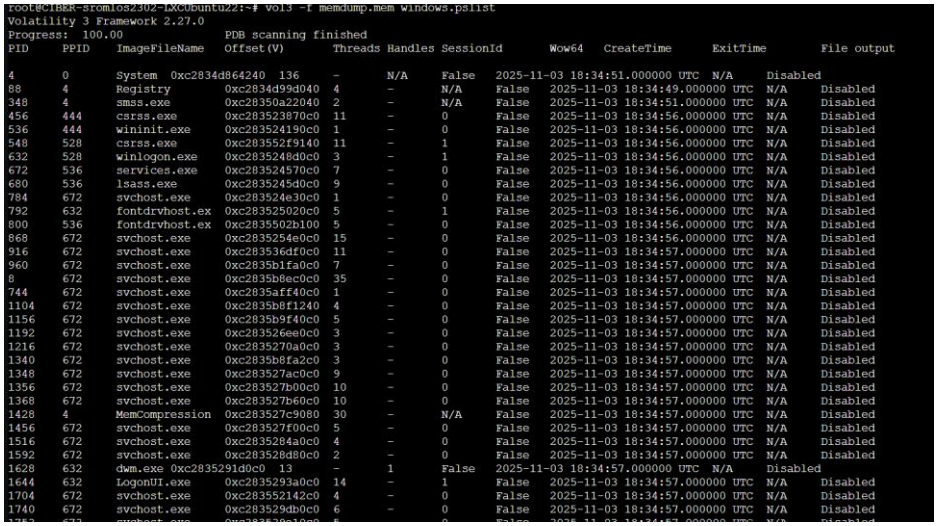
Y empezamos a usar Volatility 3. Primero con información del sistema operativo:

vol3 -f memdump.mem windows.info



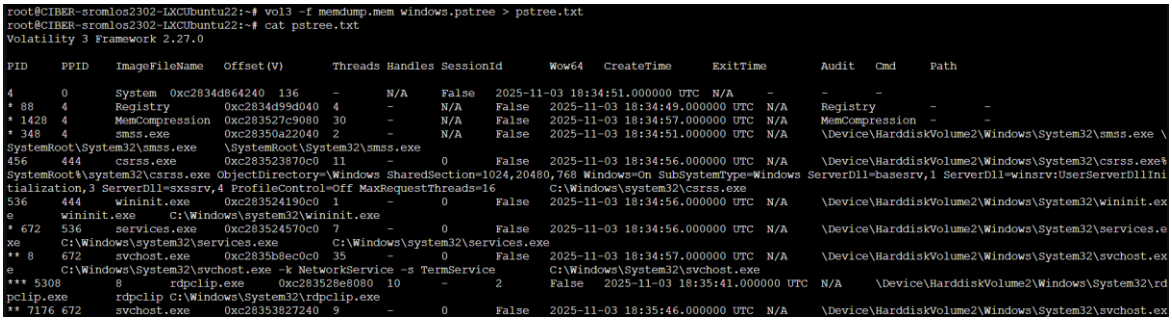
Para ver el listado de procesos:

vol3 -f memdump.mem windows.pslist



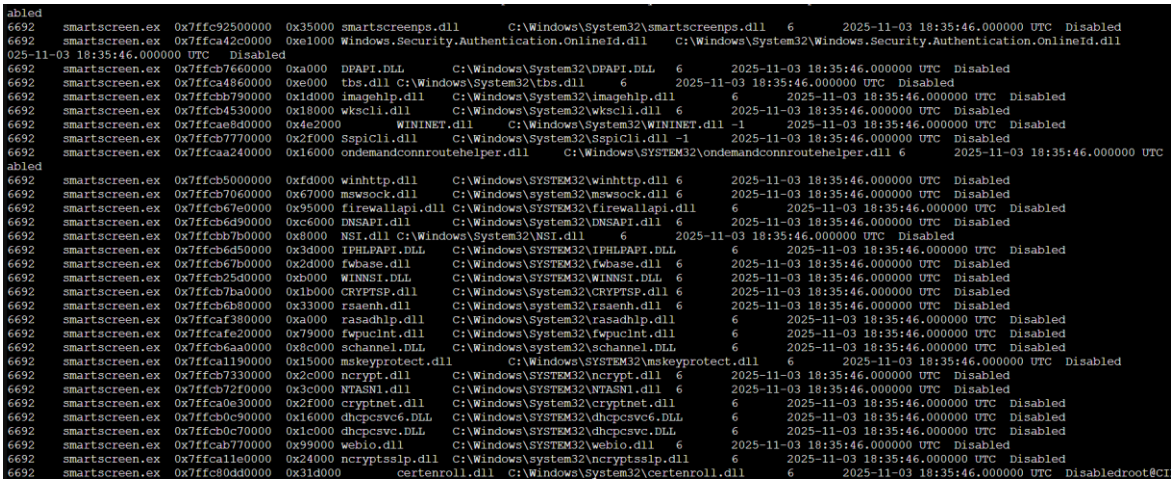
Para ver el listado de procesos en forma de árbol:

vol3 -f memdump.mem windows.pstree > pstree.txt



Ahora, para ver las librerías del sistema que se están utilizando:

vol3 -f memdump.mem windows.dlllist > dlllist.txt



Vemos la dirección IP que tenía el equipo:

vol3 -f memdump.mem windows.netstat

Para ver las conexiones de red realizadas (puertos y servicios):

vol3 -f memdump.mem windows.netscan

```
root@CIBER-sromlos2302-LXCUbuntu22:~# vol3 -f memdump.mem windows.netscan
Volatility 3 Framework 2.27.0
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xc2834d871590  TCPv4   127.0.0.1       22352   0.0.0.0 0       LISTENING       400     CmWebAdmin.exe  2025-11-03 18:43:05.000000 UTC
0xc2834d8716e0  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       672     services.exe    2025-11-03 18:34:58.000000 UTC
0xc2834d8716e0  TCPv6   ::      49669   ::      0       LISTENING       672     services.exe    2025-11-03 18:34:58.000000 UTC
0xc2834d871c20  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       672     services.exe    2025-11-03 18:34:58.000000 UTC
0xc2834da934f0  UDPv4   0.0.0.0 0       *       0               2084    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da934f0  UDPv6   ::      0       *       0               2084    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da93660  UDPv4   0.0.0.0 0       *       0               2084    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da93660  UDPv6   ::      0       *       0               2084    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da947a0  UDPv4   0.0.0.0 0       *       0               4       System  2025-11-03 18:35:09.000000 UTC
0xc2834da94910  UDPv4   0.0.0.0 0       *       0               2084    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da95bc0  UDPv4   0.0.0.0 0       *       0               4       System  2025-11-03 18:35:09.000000 UTC
0xc2834da962f0  UDPv4   0.0.0.0 0       *       0               4064    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da962f0  UDPv6   ::      0       *       0               4064    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da96e70  UDPv4   0.0.0.0 0       *       0               2084    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da972c0  UDPv4   0.0.0.0 0       *       0               2084    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da972c0  UDPv6   ::      0       *       0               2084    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da97880  UDPv4   0.0.0.0 0       *       0               4064    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da97880  UDPv6   ::      0       *       0               4064    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da979f0  UDPv4   0.0.0.0 0       *       0               4064    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da97cd0  UDPv4   0.0.0.0 0       *       0               4064    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da98850  UDPv4   0.0.0.0 0       *       0               4500    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da989c0  UDPv4   0.0.0.0 0       *       0               4500    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da989c0  UDPv6   ::      0       *       0               4500    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da98b30  UDPv4   0.0.0.0 0       *       0               4500    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da98b30  UDPv6   ::      0       *       0               4500    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da98ca0  UDPv4   0.0.0.0 0       *       0               4500    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da99820  UDPv4   0.0.0.0 0       *       0               4064    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da99820  UDPv6   ::      0       *       0               4064    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da99b00  UDPv4   0.0.0.0 0       *       0               4064    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da99c70  UDPv4   0.0.0.0 0       *       0               4500    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da9aad0  UDPv4   0.0.0.0 0       *       0               4064    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da9aad0  UDPv6   ::      0       *       0               4064    svchost.exe     2025-11-03 18:35:09.000000 UTC
0xc2834da9b370  UDPv4   0.0.0.0 0       *       0               4064    svchost.exe     2025-11-03 18:35:09.000000 UTC
```

Para extraer una librería del sistema y subirla a VirusTotal, primero extraemos las librerias:

vol3 -f memdump.mem windows.dlllist

```
3392    conhost.exe     0x7ffcb78e0000  0x5d000 powrprof.dll    C:\Windows\System32\powrprof.dll        6       2025-11-03 18:47:44.000000 UTC  Disabled
3392    conhost.exe     0x7ffcb9d50000  0x52000 shlwapi.dll     C:\Windows\System32\shlwapi.dll 6       2025-11-03 18:47:44.000000 UTC  Disabled
3392    conhost.exe     0x7ffcb7890000  0x11000 kernel.appcore.dll      C:\Windows\System32\kernel.appcore.dll  6       2025-11-03 18:47:44.000000 UTC  Disabled
3392    conhost.exe     0x7ffcb7ba0000  0x1b000 cryptsp.dll     C:\Windows\System32\cryptsp.dll 6       2025-11-03 18:47:44.000000 UTC  Disabled
7712    SearchFilterHo  0x7ff67e1c0000  0x3f000 SearchFilterHost.exe    C:\Windows\system32\SearchFilterHost.exe        -1      2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcbb8c0000  0x1ee000        ntdll.dll       C:\Windows\SYSTEM32\ntdll.dll   -1      2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb8bb0000  0xb3000 KERNEL32.DLL    C:\Windows\System32\KERNEL32.DLL        -1      2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb80f0000  0x29d000        KERNELBASE.dll  C:\Windows\System32\KERNELBASE.dll      -1      2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb9780000  0x9e000 msvcrt.dll      C:\Windows\System32\msvcrt.dll  6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb8ae0000  0xc4000 OLEAUT32.dll    C:\Windows\System32\OLEAUT32.dll        6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb7b00000  0xa0000 msvcp_win.dll   C:\Windows\System32\msvcp_win.dll       6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb7a00000  0xfa000 ucrtbase.dll    C:\Windows\System32\ucrtbase.dll        6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb8e80000  0x32a000        combase.dll     C:\Windows\System32\combase.dll 6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb9a10000  0x118000        RPCRT4.dll      C:\Windows\System32\RPCRT4.dll  6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb7970000  0x82000 bcryptPrimitives.dll    C:\Windows\System32\bcryptPrimitives.dll        6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb9820000  0xa8000 advapi32.dll    C:\Windows\System32\advapi32.dll        6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb9ca0000  0xa2000 sechost.dll     C:\Windows\System32\sechost.dll 6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb7940000  0x26000 bcrypt.dll      C:\Windows\System32\bcrypt.dll  6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffca3d60000  0x334000        TQUERY.DLL      C:\Windows\system32\TQUERY.DLL  6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb70d0000  0x15000 cryptdll.dll    C:\Windows\system32\cryptdll.dll        6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb9410000  0x2e000 imm32.dll       C:\Windows\System32\imm32.dll   6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb8ce0000  0x197000        USER32.dll      C:\Windows\System32\USER32.dll  6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb7f70000  0x20000 win32u.dll      C:\Windows\System32\win32u.dll  6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb9570000  0x29000 GDI32.dll       C:\Windows\System32\GDI32.dll   6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb7dc0000  0x1a8000        gdi32full.dll   C:\Windows\System32\gdi32full.dll       6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb7890000  0x11000 kernel.appcore.dll      C:\Windows\System32\kernel.appcore.dll  6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffcb9360000  0xa8000 clbcatq.dll     C:\Windows\System32\clbcatq.dll 6       2025-11-03 18:47:47.000000 UTC  Disabled
7712    SearchFilterHo  0x7ffc7edb0000  0x28000 mssprxy.dll     C:\Windows\system32\mssprxy.dll 6       2025-11-03 18:47:47.000000 UTC  Disabled
```

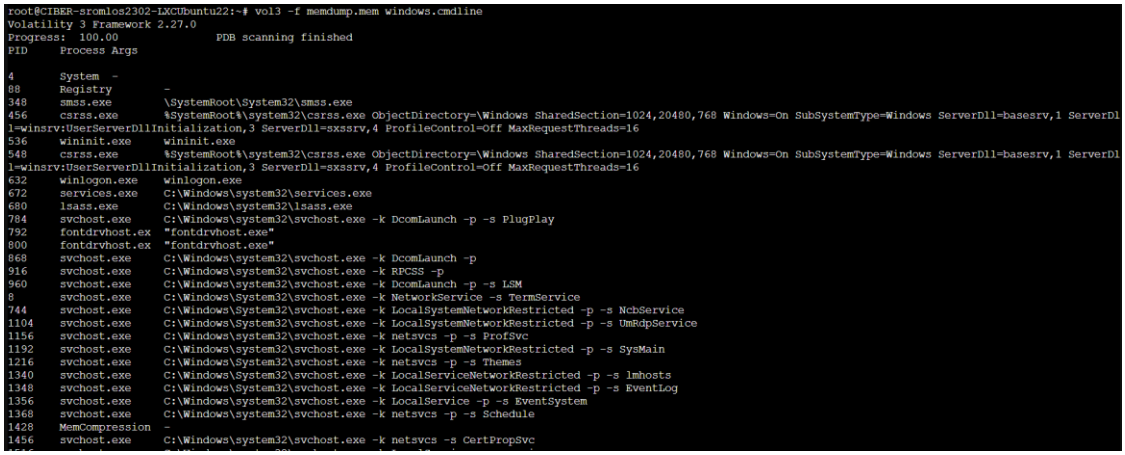
Una vez identificada una libreria, escribimos lo siguiente:

mkdir -p extracted

vol3 -f memdump.mem -o extracted/ windows.dumpfiles --name IQUERY.DLL

Para ver un listado de comandos ejecutados:

vol3 -f memdump.mem windows.cmdline



Tres pluggins adicionales:

vol3 -f memdump.mem windows.sockets

vol3 -f memdump.mem windows.malfind

vol3 -f memdump.mem windows.clipboard

windows.sockets muestra todos los sockets (conexiones de red activas) abiertos por los procesos en el momento del volcado de memoria. Es especialmente útil para descubrir comunicaciones activas o sospechosas que podrían indicar conexión con servidores de comando y control (C2), túneles o exfiltración de datos.

windows.malfind busca inyecciones de código malicioso en la memoria de los procesos. Detecta regiones de memoria con permisos de lectura, escritura y ejecución simultáneos (RWX), típicos de malware que se oculta o ejecuta directamente en memoria.

windows.clipboard extrae el contenido del portapapeles (clipboard) que estaba almacenado en la memoria en el momento del volcado. Puede contener texto, comandos, contraseñas, URLs, o información sensible copiada por el usuario o un atacante.

3.- Comparativa entre Volatility 2 y 3

Volatility 2 se basa en Python 2.7, lo que limita su compatibilidad con sistemas actuales, aunque sigue siendo ampliamente usada por su amplio catálogo de plugins, su salida en texto estructurado y su madurez. Permite trabajar fácilmente con perfiles de sistemas (por ejemplo, Win7SP1x64) y ofrece una representación más visual, como en pstree, donde el árbol de procesos es claro y jerárquico. Sin embargo, su dependencia de perfiles predefinidos hace que analizar sistemas nuevos o sin perfil oficial sea más complicado.

Por otro lado, Volatility 3 representa una reescritura completa en Python 3, enfocada en modularidad, rendimiento y extensibilidad. Ya no depende de perfiles específicos, sino que detecta automáticamente la estructura de memoria del sistema, lo que la hace más flexible y moderna. Además, introduce una arquitectura de plugins más limpia, mejor soporte multiplataforma y una base de código más mantenible.
No obstante, algunos plugins de Volatility 2 aún no están disponibles en la versión 3, y la salida es menos visual por defecto, requiriendo redirecciones a archivos o tratamiento adicional para informes legibles.