INSTALACIÓN DE VOLATILITY EN PARROT

#!/bin/bash

Rutas

IMAGEN_RAM="/home/$USER/memoria.lime"

INFORME="/home/$USER/informe_memoria.txt"

echo "📦 Instalando dependencias y Volatility 3..."

sudo apt update

sudo apt install -y git python3 python3-pip pcregrep

Clonar Volatility 3 si no existe

[! -d volatility3] && git clone https://github.com/volatilityfoundation/volatility3.git

cd volatility3 || { echo "❌ No se pudo entrar en el directorio de Volatility"; exit 1; }

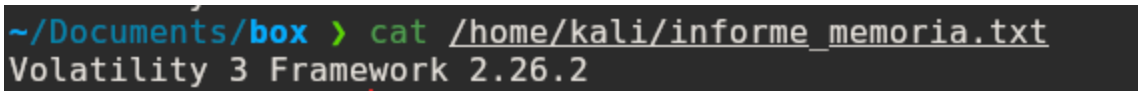
pip3 install -r requirements.txt

echo "🧪 Analizando imagen de memoria: $IMAGEN_RAM"

echo "📝 Informe guardado en: $INFORME"

```
# Iniciar el informe
echo "🔍 Informe de análisis de memoria RAM generado el $(date)" > "$INFORME"
echo "============================================" >> "$INFORME"

# 1. Info del sistema
echo -e "\n📌 Información del sistema (linux.info.LayerStack):" >> "$INFORME"
python3 vol.py -f "$IMAGEN_RAM" linux.info.LayerStack >> "$INFORME" 2>/dev/null
```




```
# 2. Lista de procesos
echo -e "\n🧠 Procesos activos (linux.pslist):" >> "$INFORME"
python3 vol.py -f "$IMAGEN_RAM" linux.pslist >> "$INFORME" 2>/dev/null

# 3. Historial bash
echo -e "\n⌨️  Historial de terminal (linux.bash):" >> "$INFORME"
python3 vol.py -f "$IMAGEN_RAM" linux.bash >> "$INFORME" 2>/dev/null

# 4. Conexiones de red
echo -e "\n🌐 Conexiones de red (linux.netstat):" >> "$INFORME"
python3 vol.py -f "$IMAGEN_RAM" linux.netstat >> "$INFORME" 2>/dev/null

echo -e "\n✅ Análisis finalizado correctamente."
echo "Puedes revisar el informe en: $INFORME"
```

```
Variable        Value
INFO     volatility3.schemas: Dependency for validation unavailable: jsonsc
DEBUG    volatility3.schemas: All validations will report success, even wit

Kernel Base     0x804d7000
DTB     0x39000
Symbols file:///home/kali/vol3-venv/lib/python3.13/site-packages/volatility
Is64Bit False
IsPAE   False
layer_name      0 WindowsIntel
memory_layer    1 FileLayer
KdDebuggerDataBlock     0x8054cde0
NTBuildLab      2600.xpsp_sp3_gdr.090804-1435
CSDVersion      3
KdVersionBlock  0x8054cdb8
Major/Minor     15.2600
MachineType     332
KeNumberProcessors      1
SystemTime      2009-11-18 01:38:30+00:00
NtSystemRoot    C:\WINDOWS
NtProductType   NtProductWinNt
NtMajorVersion  5
NtMinorVersion  1INFO     volatility3.schemas: Dependency for validation un
DEBUG    volatility3.schemas: All validations will report success, even wit

PE MajorOperatingSystemVersion  5
PE MinorOperatingSystemVersion  1
PE Machine      332
PE TimeDateStamp        Tue Aug  4 15:14:34 2009
```

```
INFO     volatility3.framework.automagic: Running automagic: ConstructionMagic
INFO     volatility3.framework.automagic: Running automagic: SymbolCacheMagic
INFO     volatility3.framework.automagic: Running automagic: LayerStacker
DEBUG    volatility3.framework.automagic.windows: Detecting Self-referential pointer for recent windows
DEBUG    volatility3.framework.automagic.windows: Older windows fixed location self-referential pointers
DEBUG    volatility3.framework.automagic.windows: DtbSelfRef32bit test succeeded at 0x39000
DEBUG    volatility3.framework.automagic.windows: DTB was found at: 0x39000
DEBUG    volatility3.framework.automagic.stacker: physical layer maximum address: 534761471
DEBUG    volatility3.framework.automagic.stacker: Stacked layers: ['IntelLayer', 'FileLayer']
INFO     volatility3.framework.automagic: Running automagic: WinSwapLayers
INFO     volatility3.framework.automagic: Running automagic: KernelPDBScanner
DEBUG    volatility3.framework.automagic.pdbscan: Kernel base determination - searching layer module list structure
DEBUG    volatility3.framework.automagic.pdbscan: Setting kernel_virtual_offset to 0x804d7000
INFO     volatility3.framework.symbols.windows.pdbconv: Download PDB file...
DEBUG    volatility3.framework.symbols.windows.pdbconv: Attempting to retrieve http://msdl.microsoft.com/download/symbols/ntoskrnl.pdb/1B2D0DFE2FB942758D615C901BE046922/ntoskrnl.pdb
DEBUG    volatility3.framework.layers.resources: Caching file at: /home/kali/.cache/volatility3/data_75b3d2a8a9a5ae10e7adf0616eed60e4adb0549ea5ee6fb1b081f20409aec29ef20536f984f584e0fded7a8a07
57c55eee4ffa10b34503ee4f37b10fba9b530b.cache
DEBUG    volatility3.framework.layers.resources: Trying to use already cached file at: /home/kali/.cache/volatility3/data_75b3d2a8a9a5ae10e7adf0616eed60e4adb0549ea5ee6fb1b081f20409aec29ef2053
6f984f584e0fded7a8a0757c55eee4ffa10b34503ee4f37b10fba9b530b.cache
```

```
~/Documents/box/vol/volatility3 develop ?1 ❯ python3 vol.py -f  /run/media/kali/2fb599ef-7a78-4
ea2-891f-17571de0f2df/Remember.raw windows.malware.suspicious_threads.SuspiciousThreads >> info
rme.txt 2>/dev/null
```

```
~/Documents/box/vol/volatility3 develop ?1 ❯ python3 vol.py -f /run/media/kali/2fb599ef-7a78-4e
a2-891f-17571de0f2df/Remember.raw isfinfo.IsfInfo
Volatility 3 Framework 2.27.0
Progress:  100.00               PDB scanning finished
URI     Valid   Number of base_types    Number of types Number of symbols       Number of enums
Identifying information

file:///home/kali/Documents/box/vol/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/25F4F1
A66D0C4385902C9414E61870A2-1.json.xz    True (cached)   14      899     19016   118     b'ntkrn
lmp.pdb|25F4F1A66D0C4385902C9414E61870A2|1'
```

```
~/Doc/b/vol/volatility3 develop ?1 ❯ python3 vol.py -f /run/media/kali/2fb599ef-7a78-4ea2-891f-17571de0f2df/Remember.raw windows.verinfo.VerInfo | grep .exe
N/AgressN/A100.00xf80002a18000  ntoskrnl.exe    6       1       7601    26111
236     smss.exe        0x47990000      smss.exe        -       -       -       -
236     smss.exe        0x76d70000      -       -       -       -       -
308     csrss.exe       0x497b0000      csrss.exe       -       -       -       -
308     csrss.exe       0x76d70000      ntdll.dll       -       -       -       -
308     csrss.exe       0x7fefc750000   CSRSRV.dll      -       -       -       -
308     csrss.exe       0x7fefc730000   basesrv.DLL     -       -       -       -
308     csrss.exe       0x7fefc6f0000   winsrv.DLL      -       -       -       -
308     csrss.exe       0x76c70000      USER32.dll      -       -       -       -
308     csrss.exe       0x7fefed30000   GDI32.dll       -       -       -       -
308     csrss.exe       0x76b50000      kernel32.dll    -       -       -       -
308     csrss.exe       0x7fefcc10000   KERNELBASE.dll  -       -       -       -
308     csrss.exe       0x7fefcc80000   LPK.dll -       -       -       -
308     csrss.exe       0x7fefeb00000   USP10.dll       -       -       -       -
308     csrss.exe       0x7fefea60000   msvcrt.dll      -       -       -       -
308     csrss.exe       0x7fefc6e0000   sxssrv.DLL      -       -       -       -
308     csrss.exe       0x7fefc5e0000   sxs.dll 6       1       7601    26019
308     csrss.exe       0x7fefd960000   RPCRT4.dll      -       -       -       -
308     csrss.exe       0x7fefc5d0000   CRYPTBASE.dll   -       -       -       -
308     csrss.exe       0x7fefec50000   ADVAPI32.dll    6       1       7601    26111
```

```
~/Documents/box/vol/volatility3 develop ?1 ❯ python3 vol.py -f /run/media/kali/2fb599ef-7a78-4ea2-891f-17571de0f2df/Remember.raw windows.scheduled_tasks.ScheduledTasks
Volatility 3 Framework 2.27.0
/home/kali/Documents/box/vol/volatility3/volatility3/framework/deprecation.py:28: FutureWarning: This API (volatility3.plugins.windows.registry.scheduled_tasks.ScheduledTasks.run) will be
oved in the first release after 2025-09-25. This plugin has been renamed, please call volatility3.plugins.windows.registry.scheduled_tasks.ScheduledTasks rather than volatility3.plugins.wi
ws.scheduled_tasks.ScheduledTasks.
  warnings.warn(

Task Name       Principal ID    Display Name    Enabled Creation Time   Last Run Time   Last Successful Run Time        Trigger Type    Trigger Description     Action Type     Action  Acti
Arguments       Action Context  Working Directory       Key Name
/home/kali/Documents/box/vol/volatility3/volatility3/framework/deprecation.py:105: FutureWarning: This plugin (volatility3.plugins.windows.scheduled_tasks.ScheduledTasks) has been renamed
 will be removed in the first release after 2025-09-25. Please ensure all method calls to this plugin are replaced with calls to volatility3.plugins.windows.registry.scheduled_tasks.Schedu
Tasks
  warnings.warn(

SynchronizeTime -       -       True    -       2009-07-14 05:08:50.000000 UTC  -       Time    -       -       -       -       -       {044A6734-E90E-4F8F-B357-B2DC8AB3B5EC}
IpAddressConflict1      -       -       True    -       2009-07-14 05:08:50.000000 UTC  -       Event   Event trigger: Subscription: <QueryList><Query Id="0" Path="System"><Select Path="Sy
m">*[System[Provider[@Name='Tcpip'] and EventID=4198]]</Select></Query></QueryList>, Queries: []       -       -       -       -       -       {088482FA-65B8-4E17-9ABF-1DCD48E8D373}
IpAddressConflict2      -       -       True    -       2009-07-14 05:08:50.000000 UTC  -       Event   Event trigger: Subscription: <QueryList><Query Id="0" Path="System"><Select Path="Sy
m">*[System[Provider[@Name='Tcpip'] and EventID=4199]]</Select></Query></QueryList>, Queries: []       -       -       -       -       -       {09F06BFE-A3C8-40E3-846A-6E6F4000C238}
Interactive     -       -       -       -       2009-07-14 05:08:50.000000 UTC  -       -       -       -       -       -       -       {1F7B7221-AE8F-44F3-BA82-F7D260F51964}
-       -       -       True    -       2009-07-14 05:08:50.000000 UTC  -       Logon   Logon trigger   -       -       -       -       -       {2470470F-2634-478E-B181-571E98A789BB}
-       -       -       -       -       -       -       -       -       -       -       -       -       {28011108-68DF-4C73-B91B-57427D501BBA}
ResolutionHost  -       -       -       -       -       -       -       -       -       -       -       -       {9435F817-FED2-454E-88CD-7F78FDA62C48}
SR      -       -       True    -       2009-07-14 05:08:50.000000 UTC  -       Time    -       -       -       -       -       {994C86AD-A929-4B2C-88A0-4E25A107A029}
SR      -       -       True    -       2009-07-14 05:08:50.000000 UTC  -       Boot    Boot trigger    -       -       -       -       -       {994C86AD-A929-4B2C-88A0-4E25A107A029}
-       -       -       True    -       2009-07-14 05:08:53.000000 UTC  -       Session Unknown -       -       -       -       -       {9979CB83-103A-4105-9E5D-C74B0AF6D198}
-       -       -       True    -       2009-07-14 05:08:53.000000 UTC  -       Session Unknown -       -       -       -       -       {9979CB83-103A-4105-9E5D-C74B0AF6D198}
-       -       -       True    -       2010-11-21 03:55:41.000000 UTC  -       Time    -       -       -       -       -       {A1D60D55-A6B8-401B-BC05-2938E02DF2F2}WARNING  volat
ty3.plugins.windows.registry.scheduled_tasks: Invalid trigger magic 0x0

-       -       -       -       -       -       2009-07-14 05:08:50.000000 UTC  -       -       -       -       -       -       -       {A35BB7A6-5F0C-4C9F-8450-2B3BED532D51}
-       -       -       -       -       -       -       -       -       -       -       -       -       {A48CABBF-24C8-4B87-B00F-9261807C3B43}
QueueReporting  -       -       True    -       2009-07-14 05:08:50.000000 UTC  -       Logon   Logon trigger   -       -       -       -       -       {D0250F3F-6480-484F-B719-42F659AC64D
-       -       -       True    -       2009-07-14 05:08:50.000000 UTC  -       Boot    Boot trigger    -       -       -       -       -       {D7B6E81D-3CF4-432C-84D2-24213F4316E6}
-       -       -       True    -       2009-07-14 05:08:56.000000 UTC  -       Logon   Logon trigger   -       -       -       -       -       {DA41DE71-8431-42FB-9DB0-EB64A961DEAD}
SvcRestartTask  -       -       True    -       2009-07-14 05:08:56.000000 UTC  -       Time    -       -       -       -       -       {DD9F510C-95F4-499A-90C8-BAC5BC372FF4}
-       -       -       True    -       2009-07-14 05:08:56.000000 UTC  -       Event   Event trigger: Subscription: <QueryList><Query Id="0" Path="System"><Select Path="System">*/System/P
ider[@Name='Service Control Manager'] and */System/EventID='7040' and */EventData/Data[@Name='param4']='BFE'</Select></Query></QueryList>, Queries: []  -       -       -       -       -
E22A8667-F75B-4BA9-BA46-067ED4429DE8}
-       -       -       -       -       -       2009-07-14 05:08:56.000000 UTC  -       -       -       -       -       -       {E3163C33-301D-4730-A266-5518C5ED3967}
RacTask -       -       True    -       2009-07-14 05:08:56.000000 UTC  -       Event   Event trigger: Subscription: <QueryList><Query Id="0" Path="Application"><Select Path="Application">
```

```
~/Documents/box/vol/volatility3 develop ?2 ❯ python3 vol.py -f /run/media/kali/2fb599ef-7a78-4e
* 236ess4  100.0smss.exe        0xfa800852a040  2       30      N/A     False   2024-09-25 00:0
tem32\smss.exe  \SystemRoot\System32\smss.exe
308     300     csrss.exe       0xfa8008ecc930  9       423     0       False   2024-09-25 00:0
stem32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType
ServerDllInitialization,2 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16    C:\Wind
356     300     wininit.exe     0xfa8006d5c860  3       80      0       False   2024-09-25 00:0
:\Windows\system32\wininit.exe
* 448   356     services.exe    0xfa80083e5b00  13      210     0       False   2024-09-25 00:0
em32\services.exe       C:\Windows\system32\services.exe
** 640  448     svchost.exe     0xfa8009165b00  8       268     0       False   2024-09-25 00:0
em32\svchost.exe -k RPCSS       C:\Windows\system32\svchost.exe
** 1184 448     taskhost.exe    0xfa800841c430  12      232     1       False   2024-09-25 00:0
:\Windows\system32\taskhost.exe
** 1796 448     SearchIndexer.  0xfa80084e6280  17      684     0       False   2024-09-25 00:0
ows\system32\SearchIndexer.exe /Embedding       C:\Windows\system32\SearchIndexer.exe
*** 1128        1796    SearchProtocol  0xfa80083747e0  8       315     0       False   2024-09
"C:\Windows\system32\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe1_ Global\UsGthrCtr
 MSIE 6.0; Windows NT; MS Search 4.0 Robot)" "C:\ProgramData\Microsoft\Search\Data\Temp\usgthrs
*** 1544        1796    SearchProtocol  0xfa8006f375f0  7       273     1       False   2024-09
"C:\Windows\system32\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe_S-1-5-21-943106337
2827894967-10002 1 -2147483646 "Software\Microsoft\Windows Search" "Mozilla/4.0 (compatible; MS
"DownLevelDaemon"  "1"  C:\Windows\system32\SearchProtocolHost.exe
*** 2796        1796    SearchFilterHo  0xfa8006eb1060  5       88      0       False   2024-09
C:\Windows\system32\SearchFilterHost.exe" 0 512 516 524 65536 520       C:\Windows\system32\Sea
** 712  448     svchost.exe     0xfa8009498060  22      462     0       False   2024-09-25 00:0
em32\svchost.exe -k LocalServiceNetworkRestricted       C:\Windows\System32\svchost.exe
*** 944 712     audiodg.exe     0xfa8008e0d480  4       111     0       False   2024-09-25 00:0
em32\AUDIODG.EXE 0x2c4  C:\Windows\system32\AUDIODG.EXE
** 2696 448     mscorsvw.exe    0xfa8008d1e060  8       110     0       False   2024-09-25 00:0
corsvw.exe      C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe    C:\Windows\Micr
*** 1692        2696    mscorsvw.exe    0xfa80087abb00  8       134     0       False   2024-09
30319\mscorsvw.exe      C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe -StartupEv
ows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
** 988  448     svchost.exe     0xfa80084be760  6       139     0       False   2024-09-25 00:0
em32\svchost.exe -k GPSvcGroup  C:\Windows\system32\svchost.exe
** 844  448     svchost.exe     0xfa800938b4a0  36      952     0       False   2024-09-25 00:0
em32\svchost.exe -k netsvcs     C:\Windows\system32\svchost.exe
** 1052 448     spoolsv.exe     0xfa8017bfe3a0  14      279     0       False   2024-09-25 00:0
em32\spoolsv.exe        C:\Windows\System32\spoolsv.exe
** 1100 448     svchost.exe     0xfa8008291290  20      328     0       False   2024-09-25 00:0
```