

# EJERCICIO SOBRE VOLATILITY



Eric Serrano Marín

CETI Análisis Forense en Ciberseguridad Informática

## ÍNDICE

1. Obtenga el código hash md5 de la imagen de la memoria RAM. ....	3
2. ¿Qué pasaría si se hubiera apagado el servidor? .....	3
3. ¿Qué sistema operativo utilizaba el servidor? De ente todas las posibles, intente deducir cuál es la que más se aproxima a la realidad. ....	4
➤ Demuéstralo con Volatility 2. ....	4
➤ Demuéstralo con Volatility 3. ....	4
4. Obtenga el listado de procesos de la memoria RAM. ....	5
➤ Demuéstralo con Volatility 2. ....	5
➤ Demuéstralo con Volatility 3. ....	6
➤ ¿Cuántos procesos hay? .....	6
5. Indique los comandos ejecutados por consola. ....	7
➤ ¿Cuántos comandos hay? .....	7
➤ Explique uno por uno, qué hace cada comando. Si alguno da error, únicamente debe indicar "Error". ....	8
6. ¿Qué usuarios existían en el sistema operativo (hashdump)? .....	9
➤ ¿Cuál es el código hash de los passwords "encriptados" de los usuarios? 9	
➤ ¿Con qué programa podría intentar, por fuerza bruta, conseguir las claves de los usuarios? .....	10
➤ ¿Qué web online le indica el password del usuario a través del hash de manera automática? .....	10
7. Indique la IP origen del PC. ....	10
➤ Muestre únicamente las líneas que tengan una IP diferente de 0.0.0.0 (tanto en origen como destino). ....	10
➤ ¿Cuál es la IP origen del posible "hacker"? .....	11

8. Detecte el proceso en el cual se haya establecido una conexión del posible “hacker” y descargue la porción de memoria que utiliza este proceso (memdump).....	11
➤ Analice la memoria del proceso con:.....	12
➤ Bulk_extractor 1.6.....	14
➤ Ejercicio sobre Volatility .....	15
9. ¿Qué tipo de comandos ha ejecutado el cibercriminal? .....	16
10. ¿En qué fecha sucedió? .....	16
11. ¿Que sugiere que ha sucedido?.....	16
12. ¿Cómo se han ejecutado los comandos? .....	17
13. ¿Qué actividad maliciosa has visto? .....	17
14. ¿Qué tipo de ataque pudo ser? .....	17
15. Plugin MFTParser en Volatility.....	17

Un estudiante del “Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información” en el IES Martínez Montañés, está inmersa en la investigación de un caso que involucra el análisis de la imagen de la memoria RAM de un servidor del IES que experimentó un comportamiento extraño e inusual.

Un profesor del centro, que se encontraba en el lugar de los hechos, capturó la memoria RAM de la máquina antes de que fuera apagada y se la entregó al estudiante de Análisis Forense Informático.

El profesor del módulo profesional y coordinador de la investigación ha planteado varias preguntas al estudiante del curso de especialización, las cuales ella debe responder en relación con la evidencia recolectada.

Primero de todo, descargue la memoria RAM de la siguiente dirección:

[https://drive.google.com/file/d/1-NLajZK\\_2pBEJ3-](https://drive.google.com/file/d/1-NLajZK_2pBEJ3-V3h64onsHVKSm5O2S/view?usp=sharing)

V3h64onsHVKSm5O2S/view?usp=sharing Muévela a su contenedor Linux para proceder al estudio de evidencias.

Responda a las siguientes preguntas:

### 1. Obtenga el código hash md5 de la imagen de la memoria RAM.

*md5sum memdump.mem*

```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# md5sum memdump.mem
7a4207fcfa3718af5b1c0cc9546ab38a memdump.mem
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~#
```

### 2. ¿Qué pasaría si se hubiera apagado el servidor?

Se pierde la información ya que la RAM es volátil, lo que nos habría dificultado o imposibilitado el análisis de datos para la investigación, como procesos en ejecución y conexiones de red.

3. ¿Qué sistema operativo utilizaba el servidor? De ente todas las posibles, intente deducir cuál es la que más se aproxima a la realidad.

➤ Demuéstralo con Volatility 2.

`vol.py -f /root/memdump.mem imageinfo`

```
No es seguro | https://172.22.1.3:8006/?console=lx&xtermjs=1&vmid=12080&vmname=CIBER-LXC-Ubuntu20-EricSerra
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f /root/memdump.mem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO : volatility_debug : Determining profile based on KDBG search
      Suggested Profile(s) : VistaSP1x86, Win2008SP1x86, Win2008SP2x86, VistaSP2x86
      AS Layer1 : IA32PagedMemoryPae (Kernel AS)
      AS Layer2 : FileAddressSpace (/root/memdump.mem)
```

Nos da 4 posibles opciones. La que más sentido tiene es que sea un Windows Sever, ya que el ejercicio dice “investigación de un caso que involucra el análisis de la imagen de la memoria RAM de un **servidor**”.

➤ Demuéstralo con Volatility 3.

`vol3.py -f memdump.mem windows.info`

```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol3.py -f memdump.mem windows.info
Volatility 3 Framework 2.5.2
Progress: 100.00          PDB scanning finished
Variable      Value
Kernel Base   0x8161f000
DTB           0x122000
Symbols file:///opt/volatility3/volatility3/symbols/windows/ntkrpamp.pdb/37D328E3BAE5460F8E662
51D-2.json.xz
Is64Bit       False
IsPAE         True
layer_name    0 WindowsIntelPAE
memory_layer  1 FileLayer
KdDebuggerDataBlock 0x81716c90
NTBuildLab    6001.18000.x86fre.longhorn_rtm.0
CSDVersion    1
KdVersionBlock 0x81716c68
Major/Minor   15.6001
MachineType   332
KeNumberProcessors 3405840385
SystemTime    2015-09-03 10:04:05
NtSystemRoot  C:\Windows
NtProductType NtProductServer
NtMajorVersion 6
NtMinorVersion 0
PE MajorOperatingSystemVersion 6
PE MinorOperatingSystemVersion 0
PE Machine     332
PE TimeDateStamp Sat Jan 19 05:30:58 2008
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~#
```

#### 4. Obtenga el listado de procesos de la memoria RAM.

➤ Demuéstralo con Volatility 2.

`vol.py -f memdump.exe --profile Win2008SP2x86 pstree > pstree.txt`

```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f memdump.mem --profile Win2008SP2x86 pstree >
pstree.txt
```

pstree.txt: Bloc de notas

Archivo Edición Formato Ver Ayuda

Name	Pid	PPid	Thds	Hnds	Time
-----					
0x8392c9f8:wininit.exe	532	472	3	102	2015-08-23 20:27:28 UTC+0000
.. 0x8393bd90:services.exe	608	532	7	238	2015-08-23 20:29:06 UTC+0000
.. 0x83a0eb88:svchost.exe	1024	608	37	913	2015-08-23 10:29:53 UTC+0000
... 0x8427c730:wuauclt.exe	2516	1024	2	140	2015-09-02 09:01:13 UTC+0000
... 0x83dca020:taskeng.exe	1984	1024	5	135	2015-08-23 10:30:08 UTC+0000
... 0x83b2b020:taskeng.exe	1444	1024	10	245	2015-08-23 10:30:34 UTC+0000
.. 0x8324cb70:TrustedInstall	3848	608	5	110	2015-09-03 10:03:06 UTC+0000
.. 0x83a1e020:SLsvc.exe	1040	608	4	75	2015-08-23 10:29:53 UTC+0000
.. 0x83a365d0:svchost.exe	1176	608	22	257	2015-08-23 10:29:56 UTC+0000
... 0x83e2f168:dwm.exe	1688	1176	3	77	2015-08-23 10:30:34 UTC+0000
.. 0x839d4020:svchost.exe	792	608	8	305	2015-08-23 20:29:45 UTC+0000
.. 0x839ded90:VBoxService.exe	836	608	8	115	2015-08-23 20:29:46 UTC+0000
.. 0x83ae6c28:svchost.exe	1568	608	3	73	2015-08-23 10:30:05 UTC+0000
.. 0x83a3e020:svchost.exe	1204	608	18	518	2015-08-23 10:29:56 UTC+0000
.. 0x83a18020:svchost.exe	1012	608	6	147	2015-08-23 10:29:53 UTC+0000
.. 0x83f8e5d0:msdtc.exe	2620	608	11	165	2015-08-23 10:32:10 UTC+0000
.. 0x83acad90:spoolsv.exe	1476	608	17	282	2015-08-23 10:30:04 UTC+0000
.. 0x838ed8c8:svchost.exe	1352	608	18	271	2015-08-23 10:29:58 UTC+0000
.. 0x83a35630:svchost.exe	1108	608	23	450	2015-08-23 10:29:54 UTC+0000
.. 0x83a06020:svchost.exe	984	608	15	306	2015-08-23 10:29:52 UTC+0000
.. 0x83af2d90:svchost.exe	1680	608	5	44	2015-08-23 10:30:05 UTC+0000
.. 0x83adfd90:svchost.exe	1512	608	9	117	2015-08-23 10:30:04 UTC+0000
.. 0x83f84d90:svchost.exe	2424	608	9	227	2015-08-23 10:31:51 UTC+0000
.. 0x83ae4af0:svchost.exe	1556	608	5	123	2015-08-23 10:30:05 UTC+0000
.. 0x839f0020:svchost.exe	892	608	7	262	2015-08-23 10:29:52 UTC+0000
.. 0x83942020:lsass.exe	620	532	19	628	2015-08-23 20:29:18 UTC+0000
.. 0x83945d90:lsm.exe	628	532	10	166	2015-08-23 20:29:19 UTC+0000
0x83912208:csrss.exe	484	472	11	400	2015-08-23 20:27:22 UTC+0000
0x83e368e0:explorer.exe	816	676	22	756	2015-08-23 10:30:34 UTC+0000
.. 0x83e652a0:VBoxTray.exe	1816	816	8	114	2015-08-23 10:30:38 UTC+0000
.. 0x83f68300:FTK Imager.exe	2120	816	13	382	2015-09-03 10:03:37 UTC+0000
.. 0x83faa020:xampp-control.e	2768	816	2	119	2015-08-23 10:32:17 UTC+0000
.. 0x83e4d7c0:httpd.exe	2796	2768	1	92	2015-08-23 10:32:21 UTC+0000
... 0x83fd77a8:httpd.exe	2880	2796	155	483	2015-08-23 10:32:26 UTC+0000
.. 0x83fd5200:FileZillaServer	2856	2768	5	35	2015-08-23 10:32:25 UTC+0000
.. 0x83f9ec70:mysqlld.exe	2804	2768	23	570	2015-08-23 10:32:23 UTC+0000
.. 0x83e7b7f8:cmd.exe	612	816	1	72	2015-08-23 10:30:44 UTC+0000
.. 0x84259100:cmd.exe	1972	816	1	19	2015-09-02 09:28:30 UTC+0000
0x82f57910:System	4	0	105	504	2015-08-23 20:27:20 UTC+0000
.. 0x838382d0:smss.exe	420	4	4	28	2015-08-23 20:27:20 UTC+0000
0x8392d530:csrss.exe	524	516	9	536	2015-08-23 20:27:28 UTC+0000
0x8387ed90:winlogon.exe	560	516	4	125	2015-08-23 20:27:28 UTC+0000

### ➤ Demuéstralo con Volatility 3.

`vol3.py -f memdump.mem windows.pstree > pstreeVol3.py`

```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol3.py -f memdump.mem windows.pstree >
pstreeVol3.txt
```

pstreeVol3.txt: Bloc de notas

Archivo Edición Formato Ver Ayuda

Volatility 3 Framework 2.5.2

PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime
4	0	System	0x82f57910	105	504	N/A	False	2015-08-23 20:27:20.000000	N/A
* 420	4	smss.exe	0x838382d0	4	28	N/A	False	2015-08-23 20:27:20.000000	N/A
484	472	csrss.exe	0x83912208	11	400	0	False	2015-08-23 20:27:22.000000	N/A
524	516	csrss.exe	0x8392d530	9	536	1	False	2015-08-23 20:27:28.000000	N/A
532	472	wininit.exe	0x8392c9f8	3	102	0	False	2015-08-23 20:27:28.000000	N/A
* 608	532	services.exe	0x8393bd90	7	238	0	False	2015-08-23 20:29:06.000000	N/A
** 1024	608	svchost.exe	0x83a0eb88	37	913	0	False	2015-08-23 10:29:53.000000	N/A
*** 1984	1024	taskeng.exe	0x83dca020	5	135	0	False	2015-08-23 10:30:08.000000	N/A
*** 2516	1024	wuauclt.exe	0x8427c730	2	140	1	False	2015-09-02 09:01:13.000000	N/A
*** 1444	1024	taskeng.exe	0x83b2b020	10	245	1	False	2015-08-23 10:30:34.000000	N/A
** 3848	608	TrustedInstaller.exe	0x8324cb70	5	110	0	False	2015-09-03 10:03:06.000000	N/A
** 1040	608	SLsvc.exe	0x83a1e020	4	75	0	False	2015-08-23 10:29:53.000000	N/A
** 1680	608	svchost.exe	0x83af2d90	5	44	0	False	2015-08-23 10:30:05.000000	N/A
** 1556	608	svchost.exe	0x83ae4af0	5	123	0	False	2015-08-23 10:30:05.000000	N/A
** 792	608	svchost.exe	0x839d4020	8	305	0	False	2015-08-23 20:29:45.000000	N/A
** 1176	608	svchost.exe	0x83a365d0	22	257	0	False	2015-08-23 10:29:56.000000	N/A
*** 1688	1176	dwm.exe	0x83e2f168	3	77	1	False	2015-08-23 10:30:34.000000	N/A
** 1568	608	svchost.exe	0x83ae6c28	3	73	0	False	2015-08-23 10:30:05.000000	N/A
** 1204	608	svchost.exe	0x83a3e020	18	518	0	False	2015-08-23 10:29:56.000000	N/A
** 2620	608	msdtc.exe	0x83f8e5d0	11	165	0	False	2015-08-23 10:32:10.000000	N/A
** 836	608	VBoxService.exe	0x839ded90	8	115	0	False	2015-08-23 20:29:46.000000	N/A
** 1476	608	spoolsv.exe	0x83acad90	17	282	0	False	2015-08-23 10:30:04.000000	N/A
** 1352	608	svchost.exe	0x838ed8c8	18	271	0	False	2015-08-23 10:29:58.000000	N/A
** 1108	608	svchost.exe	0x83a35630	23	450	0	False	2015-08-23 10:29:54.000000	N/A
** 984	608	svchost.exe	0x83a06020	15	306	0	False	2015-08-23 10:29:52.000000	N/A
** 1512	608	svchost.exe	0x83adfd90	9	117	0	False	2015-08-23 10:30:04.000000	N/A
** 1012	608	svchost.exe	0x83a18020	6	147	0	False	2015-08-23 10:29:53.000000	N/A
** 2424	608	svchost.exe	0x83f84d90	9	227	0	False	2015-08-23 10:31:51.000000	N/A
** 892	608	svchost.exe	0x839f0020	7	262	0	False	2015-08-23 10:29:52.000000	N/A
* 628	532	lsass.exe	0x83945d90	10	166	0	False	2015-08-23 20:29:19.000000	N/A
* 620	532	lsass.exe	0x83942020	19	628	0	False	2015-08-23 20:29:18.000000	N/A
560	516	winlogon.exe	0x8387ed90	4	125	1	False	2015-08-23 20:27:28.000000	N/A
816	676	explorer.exe	0x83e368e0	22	756	1	False	2015-08-23 10:30:34.000000	N/A
* 612	816	cmd.exe	0x83e7b7f8	1	72	1	False	2015-08-23 10:30:44.000000	N/A
* 2120	816	FTK Imager.exe	0x83f68300	13	382	1	False	2015-09-03 10:03:37.000000	N/A
* 2768	816	xampp-control.e	0x83faa020	2	119	1	False	2015-08-23 10:32:17.000000	N/A
** 2856	2768	FileZillaServer	0x83fd5200	5	35	1	False	2015-08-23 10:32:25.000000	N/A
** 2796	2768	httpd.exe	0x83e4d7c0	1	92	1	False	2015-08-23 10:32:21.000000	N/A
*** 2880	2796	httpd.exe	0x83fd77a8	155	483	1	False	2015-08-23 10:32:26.000000	N/A
** 2804	2768	mysqld.exe	0x83f9ec70	23	570	1	False	2015-08-23 10:32:23.000000	N/A
* 1972	816	cmd.exe	0x84259100	1	19	1	False	2015-09-02 09:28:30.000000	N/A
* 1816	816	VBoxTray.exe	0x83e652a0	8	114	1	False	2015-08-23 10:30:38.000000	N/A

### ➤ ¿Cuántos procesos hay?

`wc -l pstree.txt`

El commando nos dice 44, pero en el txt vemos que hay dos líneas que corresponden al título y a la parte alta de la tabla. Así que hay 42.

```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# wc -l pstree.txt
44 pstree.txt
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~#
```

## 5. Indique los comandos ejecutados por consola.

*vol.py -f memdump.mem --profile Win2008SP2x86 cmdscan*

```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f memdump.mem --profile Win2008SP2x86 cmdscan
```

```
cmdscanvol2.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
*****
CommandProcess: csrss.exe Pid: 524
CommandHistory: 0x5a24708 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 17 LastAdded: 16 LastDisplayed: 16
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x2d8
Cmd #0 @ 0xe907c8: ipconfig
Cmd #1 @ 0xe91af8: cls
Cmd #2 @ 0xe91db0: ipconfig
Cmd #3 @ 0x5a34bd0: net user user1 user1 /add
Cmd #4 @ 0x5a34eb8: net user user1 root@psut /add
Cmd #5 @ 0x5a34c10: net user user1 Root@psut /add
Cmd #6 @ 0x5a24800: cls
Cmd #7 @ 0x5a34c58: net /?
Cmd #8 @ 0x5a34d88: net localgroup /?
Cmd #9 @ 0x5a34f48: net localgroup "Remote Desktop Users" user1 /add
Cmd #10 @ 0x5a34c70: net /?
Cmd #11 @ 0xe911b0: netsh /?
Cmd #12 @ 0xe907e8: netsh firewall /?
Cmd #13 @ 0xe91218: netsh firewall set service type = remotedesktop /?
Cmd #14 @ 0xe91288: netsh firewall set service type = remotedesktop enable
Cmd #15 @ 0xe91300: netsh firewall set service type=remotedesktop mode=enable
Cmd #16 @ 0xe91380: netsh firewall set service type=remotedesktop mode=enable scope=subnet
*****
CommandProcess: csrss.exe Pid: 524
CommandHistory: 0x5a30950 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 2 LastAdded: 1 LastDisplayed: 1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x7ec
Cmd #0 @ 0xe91970: netsh firewall set service type=remotedesktop mode=enable scope=subnet
Cmd #1 @ 0x5a17b58: netsh firewall set service type=remotedesktop mode=enable scope=subnet
Cmd #38 @ 0x5a30bc8:
Cmd #39 @ 0x5a24890: et.exe
Cmd #48 @ 0x5a24890: et.exe
Cmd #49 @ 0xe91af8: cls
*****
CommandProcess: csrss.exe Pid: 524
CommandHistory: 0x5a30ad0 Application: httpd.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x3bc
```

### ➤ ¿Cuántos comandos hay?

El CommandCount dice que hay 19 en total, 17 en la parte de arriba y 2 en la parte de abajo.



- **Explique uno por uno, qué hace cada comando. Si alguno da error, únicamente debe indicar “Error”.**

COMANDO	¿QUÉ HACE?	¿ERROR?
ipconfig	Enseña ajustes de configuración principales en la red TCP/IP	No.
cls	Limpia la ventana de comandos	No
net user user1 user1 /add	Agrega un nuevo usuario llamado user1 con contraseña user1 al sistema.	No
Net user user1 root@psut /add	Agrega un nuevo usuario llamado user1 con contraseña root@psut.	No, aunque ya existe user1, el comando reemplazaría la contraseña de user1 a root@psut.
Net /?	Para obtener información de ayuda sobre el comando net.	No
net localgroup /?	Obtener ayuda específica sobre el comando net localgroup.	No
net localgroup "Remote Desktop Users" user1 /add	Agrega user1 al grupo local "Remote Desktop Users"	No
netsh /?	Ayuda para el comando netsh	No
netsh firewall /?	Solicita ayuda del comando netsh con el parámetro firewall.	No, pero porque el Windows Server es el 2008, a partir de Windows 2012 ya no funcionaría el comando, sería "netsh advfirewall".
netsh firewall set service type = remotedesktop /?	Está buscando ayuda para ver que parámetros puede poner después de remotedesktop.	No
netsh firewall set service type = remotedesktop enable	Habilita el servicio de Escritorio Remoto en el firewall.	No
netsh firewall set service type=remotedesktop mode=enable scope=subnet	Habilita el servicio de Escritorio Remoto y configura el firewall para permitir conexiones desde la subred.	No
Et.exe	Ejecuta el archive Et.exe	Depende de si existe el programa o no, y de si está poniendo la ruta correcta o en el directorio correcto.

## 6. ¿Qué usuarios existían en el sistema operativo (hashdump)?

Hivelist para enumerar y mostrar los archivos del Registro de Windows:

```
vol.py -f memdump.mem --profile Win2008SP2x86 hivelist
```

Ahora que sabemos el código de SAM (Security Accounts Manager) usamos hashdump.

```
vol.py -f memdump.mem --profile Win2008SP2x86 hashdump -y 0x87b7d008
```

```
FileAddressSpace: Must be first Address Space
ArmAddressSpace: No valid DTB found

root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f memdump.mem --profile Win2008SP2x86 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual    Physical    Name
-----
0x87b4ba20 0x3c0c0a20 \Device\HarddiskVolume1\Windows\System32\config\COMPONENTS
0x87b55a20 0x3c192a20 \Device\HarddiskVolume1\Windows\System32\config\SOFTWARE
0x87b7d008 0x3a6a2008 \Device\HarddiskVolume1\Windows\System32\config\SAM
0x87b7d6a8 0x3a6a26a8 \Device\HarddiskVolume1\Windows\System32\config\DEFAULT
0x8ab7aa20 0x3c285a20 \Device\HarddiskVolume1\Boot\BCD
0x8f4c8a20 0x25828a20 \Device\HarddiskVolume1\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x8f565a20 0x251eba20 \Device\HarddiskVolume1\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x90eca20 0x1c1d5a20 \Device\HarddiskVolume1\Users\Administrator\AppData\Local\Microsoft\Windows\U
srClass.dat
0x90f09a20 0x1ab8ea20 \Device\HarddiskVolume1\Users\Administrator\NTUSER.DAT
0x86210008 0x00ac8008 [no name]
0x86216008 0x00a94008 \REGISTRY\MACHINE\SYSTEM
0x86216008 0x00a76008 \REGISTRY\MACHINE\HARDWARE
0x87b77a20 0x3c1f5a20 \Device\HarddiskVolume1\Windows\System32\config\SECURITY
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f memdump.mem --profile Win2008SP2x86 hashdump
-y 0x87b7d008
vol.py: command not found
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f memdump.mem --profile Win2008SP2x86 hashdump
-y 0x87b7d008
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:63d6a39b8467b94ae92ab1931d4079dd:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
user1:1005:aad3b435b51404eeaad3b435b51404ee:817875ce4794a9262159186413772644:::
hacker:1006:aad3b435b51404eeaad3b435b51404ee:817875ce4794a9262159186413772644:::
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~#
```

Hay 4 usuarios en total: Administrator, Guest, User1 y hacker.

- ¿Cuál es el código hash de los passwords “encriptados” de los usuarios?

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:63d6a39b8467b94ae92ab1931d4079dd:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
user1:1005:aad3b435b51404eeaad3b435b51404ee:817875ce4794a9262159186413772644:::
hacker:1006:aad3b435b51404eeaad3b435b51404ee:817875ce4794a9262159186413772644:::
```

- ¿Con qué programa podría intentar, por fuerza bruta, conseguir las claves de los usuarios?

Con John the Ripper.

He creado un archivo y he metido el usuario y su hash.

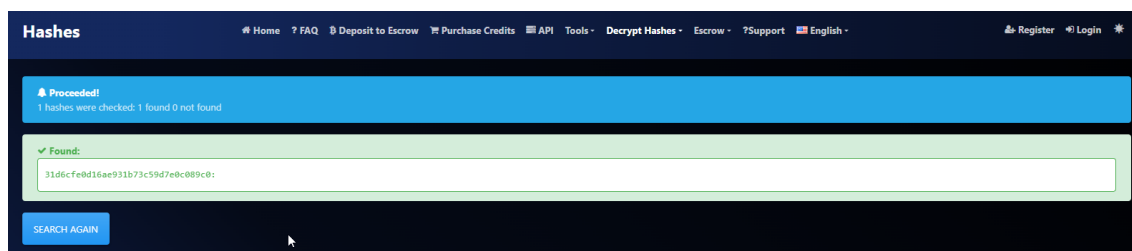
```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# cat john.txt
Guest:31d6cfe0d16ae931b73c59d7e0c089c0root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~#
```

Y ahora he ejecutado el comando john, he abortado, ya que iba a tardar bastante.

```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# john john.txt
Created directory: /root/.john
Loaded 2 password hashes with no different salts (LM [DES 128/128 SSE2-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:58 3/3 0g/s 61698Kp/s 61698Kc/s 123630Kc/s 0479NY4..0476GOS
Session aborted
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~#
```

- ¿Qué web online le indica el password del usuario a través del hash de manera automática?

<https://hashes.com/en/decrypt/hash>



## 7. Indique la IP origen del PC.

- Muestre únicamente las líneas que tengan una IP diferente de 0.0.0.0 (tanto en origen como destino).

`vol.py -f memdump --profile Win2008SP2x86 netscan > netscan.txt`

```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f memdump.mem --profile Win2008SP2x86 netscan > netscan.txt
```

`cat netscan.txt | sort -k3`

```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# cat netscan.txt | sort -k3
```

0x3f3258d8	UDPv4	127.0.0.1:57557	**	1204	svchost.exe	2015-08-23 10:30:07 UTC+0000
0x3f1e1438	UDPv4	192.168.56.101:137	**	4	System	2015-09-03 06:08:35 UTC+0000
0x3ef710f0	UDPv4	192.168.56.101:138	**	4	System	2015-09-03 06:08:35 UTC+0000
0x196d320	TCPv4	192.168.56.101:139	0.0.0.0:0	LISTENING	4	System
0x3f22c008	TCPv4	192.168.56.101:51157	192.168.56.1:5357	ESTABLISHED	1108	svchost.exe
0x3ff40008	TCPv4	192.168.56.101:51159	192.168.56.1:139	CLOSED	4	System
0x3ffc88f0	TCPv4	192.168.56.101:51160	192.168.56.1:139	CLOSED	4	System

La ip origen del PC es 192.168.56.101.

➤ ¿Cuál es la IP origen del posible “hacker”?

IP del host			
127.0.0.1	57557		
192.168.56.101	137		
192.168.56.101	138		
192.168.56.101	139		
192.168.56.101	51157		
192.168.56.101	51159		
192.168.56.101	51160		
:::1	14147		
:::0			
Atacante			
0.0.0.0			LISTENING
0.0.0.0			LISTENING
0.0.0.0			LISTENING
0.0.0.0			LISTENING
192.168.56.1	5357		ESTABLISHED
192.168.56.1	139		CLOSED
192.168.56.1	139		CLOSED
:::0			LISTENING

Debería ser la 192.168.56.1, esto suponiendo que no es el router.

8. Detecte el proceso en el cual se haya establecido una conexión del posible “hacker” y descargue la porción de memoria que utiliza este proceso (memdump).

0x196d320	TCPv4	192.168.56.101:139	0.0.0.0:0	LISTENING	4	System
0x3f22c008	TCPv4	192.168.56.101:51157	192.168.56.1:5357	ESTABLISHED	1108	svchost.exe
0x3ffd4008	TCPv4	192.168.56.101:51159	192.168.56.1:139	CLOSED	4	System

Ya sabemos que el PID es 1108.

`vol.py -f memdump.mem --profile Win2008SP2x86 memdump -p 1108 -D ./dump`

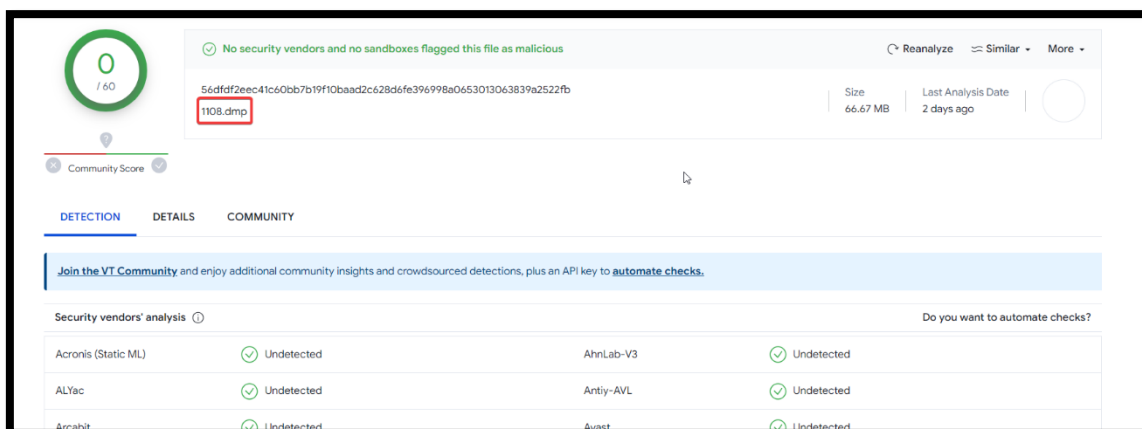
```

root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f memdump.mem --profile Win2008SP2x86 memdump -p 1108 -D ./dump
Volatility Foundation Volatility Framework 2.6.1
*****
Writing svchost.exe [ 1108] to 1108.dmp
Traceback (most recent call last):
  File "/usr/bin/vol.py", line 192, in <module>
    main()
  File "/usr/bin/vol.py", line 183, in main
    command.execute()
  File "/opt/volatility/volatility/commands.py", line 147, in execute
    func(outfd, data)
  File "/opt/volatility/volatility/plugins/taskmods.py", line 373, in render_text
    data = task.space.read(p[0], p[1])
  File "/opt/volatility/volatility/addrspace.py", line 276, in read
    return self._read(addr, length, False)
  File "/opt/volatility/volatility/addrspace.py", line 268, in _read
    assert (position - addr == len(buff), "Position - address != len(buff) (" + str(position - addr) + " != " + str(len(buff)) + ") in " + self.base.__class__.__name__)
AssertionError: Position - address != len(buff) (4096 != 2) in FileAddressSpace

```

➤ **Analice la memoria del proceso con:**

- VirusTotal.

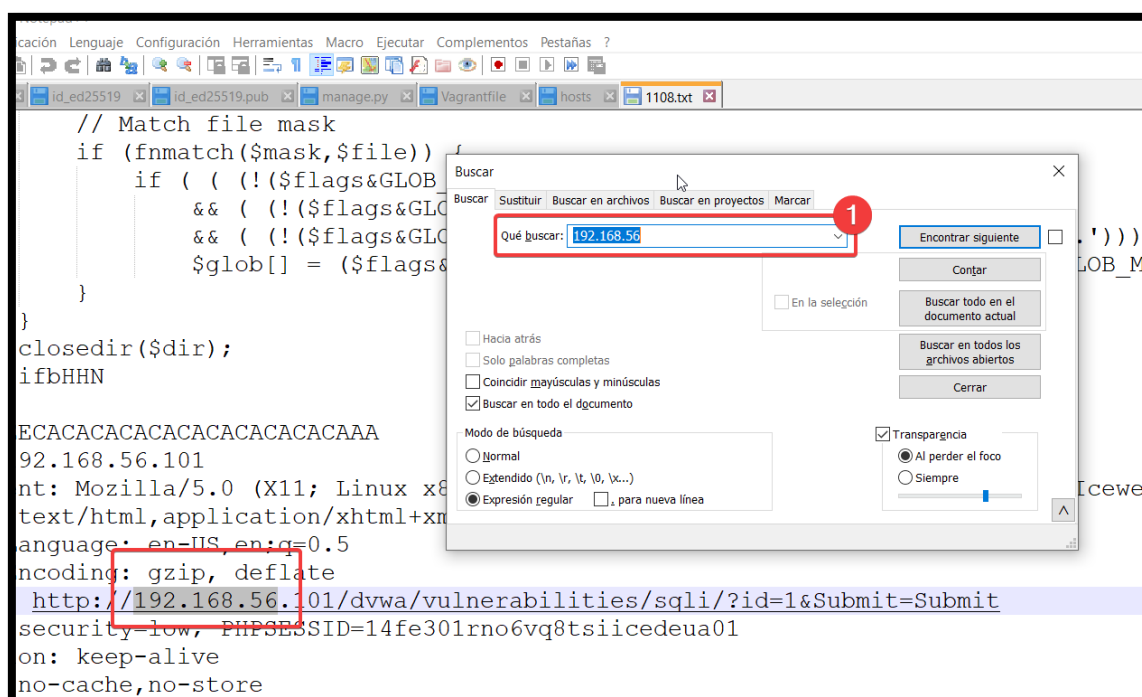


- strings

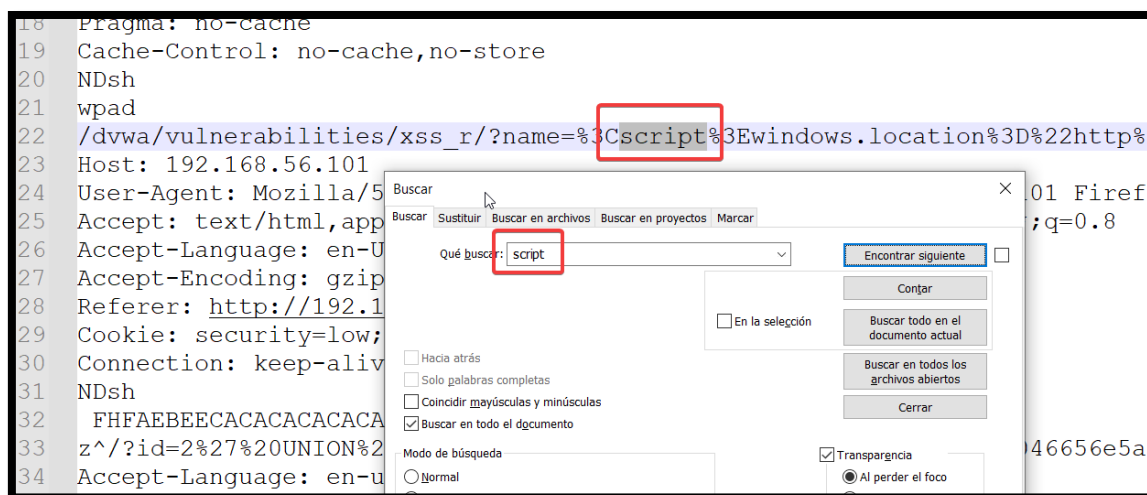
*strings 1108.dmp > 1108.txt*

```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~/dump# strings 1108.dmp > 1108.txt
```

Podemos buscar en notepad++ por IP y encontrar cosas curiosas, como este enlace, que parece estar solicitando una página que podría ser vulnerable a la inyección SQL. La parte `id=1&Submit=Submit` indica que se está enviando un parámetro "id" con el valor "1" a través de un formulario y se está enviando para procesamiento.



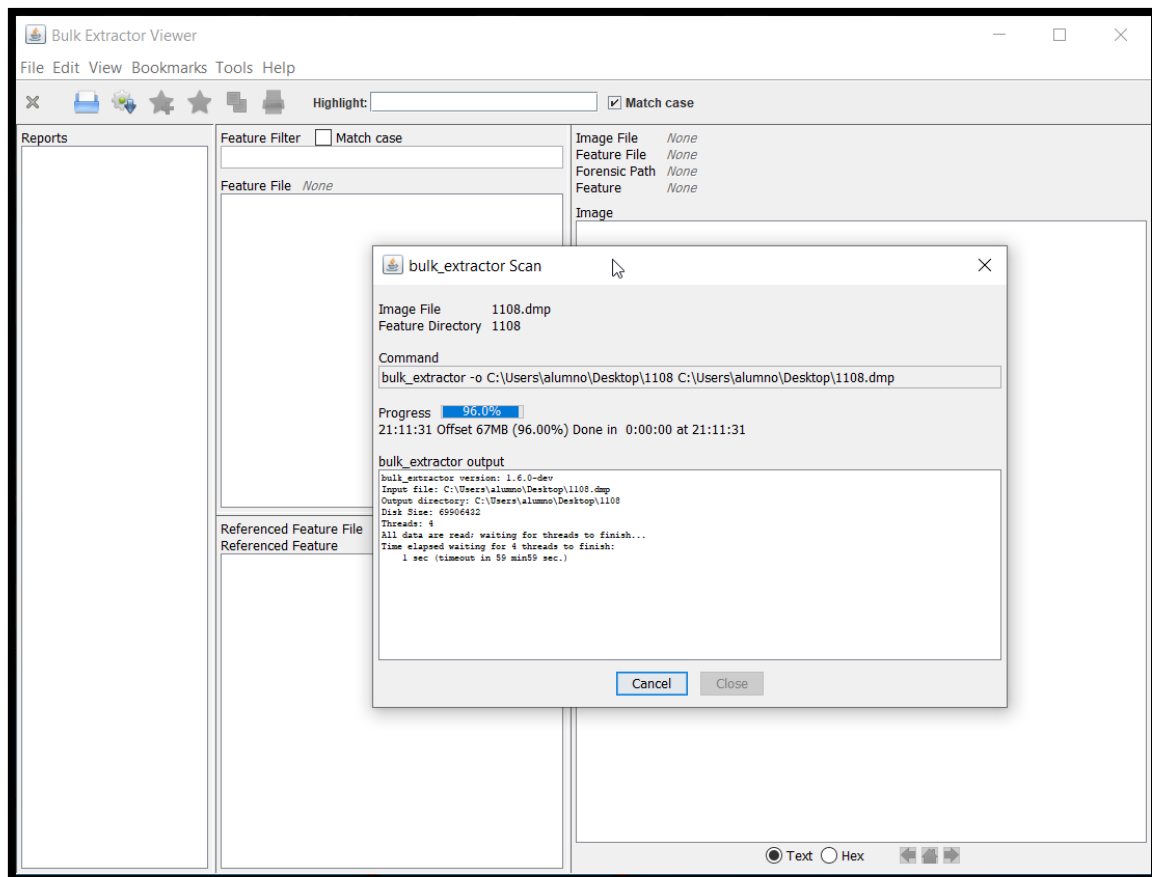
Buscando por script, encontramos lo siguiente:  
/dvwa/vulnerabilities/xss\_r/?name=%3Cscript%3Ewindows.location%3D%22http%  
p%3A%2F%2F192.168.56.102%22%3C%2Fscript%3E HTTP/1.1



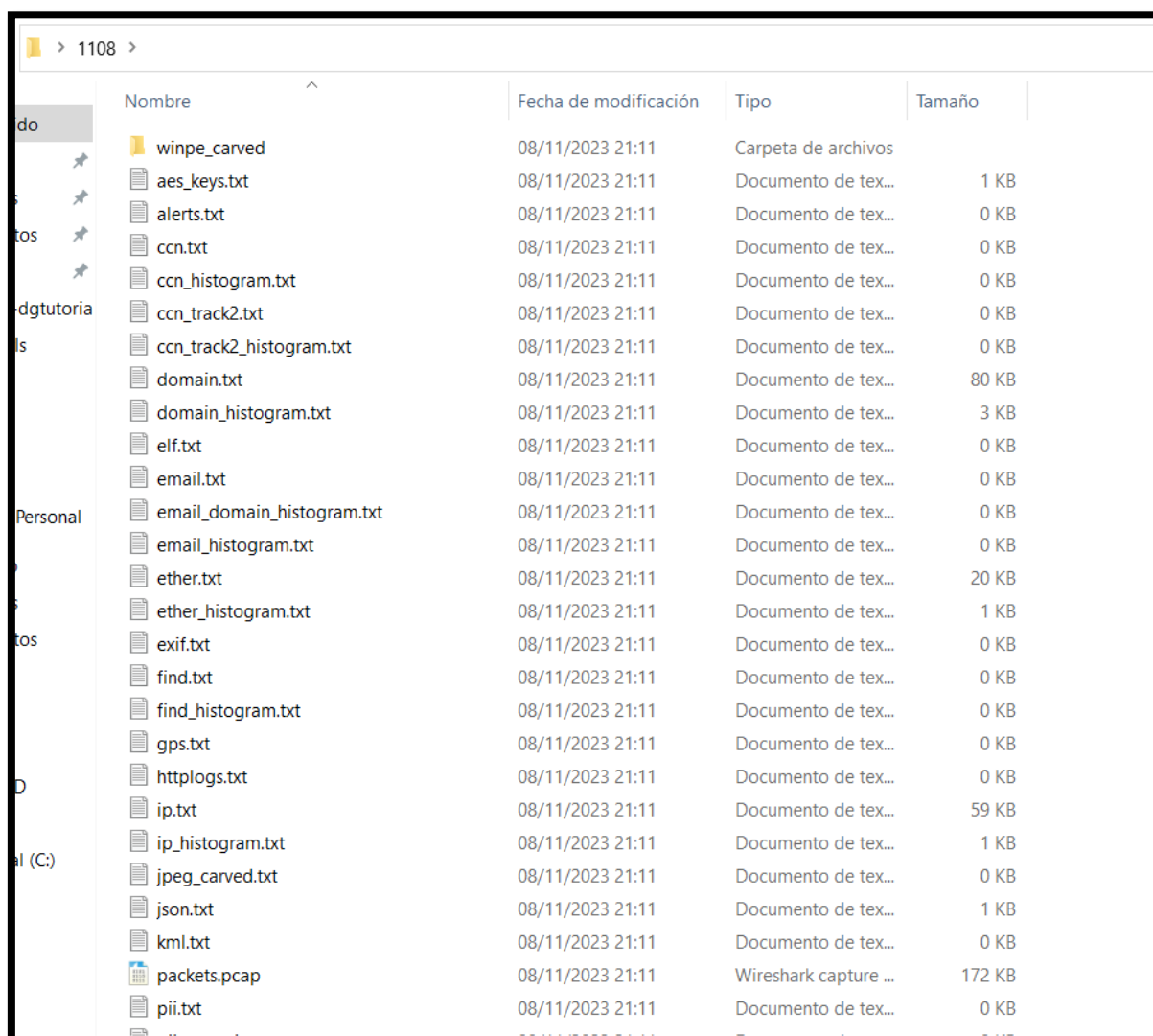
Parece ser otra solicitud a una aplicación web DVWA (Damn Vulnerable Web Application) pero esta vez relacionada con una vulnerabilidad de Cross-Site Scripting (XSS). La parte name=%3Cscript.... es un parámetro en la URL. En este caso, parece que el parámetro "name" está siendo utilizado para introducir código JavaScript malicioso. El código JavaScript en cuestión redirige la página actual a la URL <http://192.168.56.102>.

*“Esta vulnerabilidad ocurre cuando una aplicación web permite la ejecución de scripts en el navegador del usuario sin la debida validación o filtrado. Esto puede llevar a ataques como el robo de sesiones, redirecciones maliciosas y otros problemas de seguridad”.*

➤ **Bulk\_extractor 1.6**







Nombre	Fecha de modificación	Tipo	Tamaño
winpe_carved	08/11/2023 21:11	Carpeta de archivos	
aes_keys.txt	08/11/2023 21:11	Documento de tex...	1 KB
alerts.txt	08/11/2023 21:11	Documento de tex...	0 KB
ccn.txt	08/11/2023 21:11	Documento de tex...	0 KB
ccn_histogram.txt	08/11/2023 21:11	Documento de tex...	0 KB
ccn_track2.txt	08/11/2023 21:11	Documento de tex...	0 KB
ccn_track2_histogram.txt	08/11/2023 21:11	Documento de tex...	0 KB
domain.txt	08/11/2023 21:11	Documento de tex...	80 KB
domain_histogram.txt	08/11/2023 21:11	Documento de tex...	3 KB
elf.txt	08/11/2023 21:11	Documento de tex...	0 KB
email.txt	08/11/2023 21:11	Documento de tex...	0 KB
email_domain_histogram.txt	08/11/2023 21:11	Documento de tex...	0 KB
email_histogram.txt	08/11/2023 21:11	Documento de tex...	0 KB
ether.txt	08/11/2023 21:11	Documento de tex...	20 KB
ether_histogram.txt	08/11/2023 21:11	Documento de tex...	1 KB
exif.txt	08/11/2023 21:11	Documento de tex...	0 KB
find.txt	08/11/2023 21:11	Documento de tex...	0 KB
find_histogram.txt	08/11/2023 21:11	Documento de tex...	0 KB
gps.txt	08/11/2023 21:11	Documento de tex...	0 KB
httplogs.txt	08/11/2023 21:11	Documento de tex...	0 KB
ip.txt	08/11/2023 21:11	Documento de tex...	59 KB
ip_histogram.txt	08/11/2023 21:11	Documento de tex...	1 KB
jpeg_carved.txt	08/11/2023 21:11	Documento de tex...	0 KB
json.txt	08/11/2023 21:11	Documento de tex...	1 KB
kml.txt	08/11/2023 21:11	Documento de tex...	0 KB
packets.pcap	08/11/2023 21:11	Wireshark capture ...	172 KB
pii.txt	08/11/2023 21:11	Documento de tex...	0 KB

### ➤ Ejercicio sobre Volatility

- <https://github.com/mandiant/flare-floss>

He intentado de muchas formas usar flare-floss, tanto en Linux como en Windows y no he podido, dejo aquí un gif de los comandos que he puesto en Linux, para que se vea que lo he intentado: <https://i.imgur.com/4rfW5ZJ.gif>

Probando en Windows: <https://i.imgur.com/TUZeKR4.gif> también he probado por comandos, pero cerré la terminal y ya no aparece el historial.



## 9. ¿Qué tipo de comandos ha ejecutado el cibercriminal?

El cibercriminal ha usado comandos para crear usuarios adicionales, cambiar contraseñas y habilitar acceso remoto, cosas que podría realizar un cibercriminal para comprometer la seguridad de un sistema.

## 10. ¿En qué fecha sucedió?

*vol3.py -f memdump.mem windows.info*

Sucedió el 03/09/2015.

```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol3.py -f memdump.mem windows.info
Volatility 3 Framework 2.5.2
Progress: 100.00 PDB scanning finished
Variable Value
Kernel Base 0x8161f000
DTB 0x122000
Symbols file:///opt/volatility3/volatility3/symbols/windows/ntkrpamp.pdb/37D328F51D-2.json.xz
Is64Bit False
IsPAE True
layer_name 0 WindowsIntelPAE
memory_layer 1 FileLayer
KdDebuggerDataBlock 0x81716c90
NTBuildLab 6001.18000.x86fre.longhorn_rtm.050826
CSDVersion 1
KdVersionBlock 0x81716c68
Major/Minor 15.6001
MachineType 332
NumberProcessors 2405840385
SystemTime 2015-09-03 10:04:05
NtSystemRoot C:\Windows
NtProductType NtProductServer
NtMajorVersion 6
NtMinorVersion 0
PE MajorOperatingSystemVersion 6
PE MinorOperatingSystemVersion 0
PE Machine 332
PE TimeDateStamp Sat Jan 19 05:30:58 2008
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~#
```

## 11. ¿Que sugiere que ha sucedido?

**Inyeccion SQL:** por los comandos sobre creación y modificación de usuarios junto con la evidencia de SQL injection de (dvwa/vulnerabilities/sqli/?....).

**Cross-Site Scripting (XSS):** por la evidencia encontrada al buscar script en el archivo (name=%3Cscript%3...), ya que indica un intento de explotar una vulnerabilidad XSS para ejecutar código JavaScript malicioso en el navegador del usuario.

## 12. ¿Cómo se han ejecutado los comandos?

Ha ejecutado los comandos entrando al PC por RDP.

## 13. ¿Qué actividad maliciosa has visto?

He visto un intento de explotar vulnerabilidades, establecer acceso no autorizado y mantener el control del sistema. Ha habido una combinación de inyección SQL, manipulación de usuarios y configuración de firewall para permitir conexiones remotas, y por último un intento de explotar vulnerabilidad XSS.

## 14. ¿Qué tipo de ataque pudo ser?

Por las evidencias conocidas me decanto a que ha habido ataques SQL injection y XSS.

## 15. Plugin MFTParser en Volatility.

```
vol.py -f memdump.mem --profile Win2008SP2x86 mftparser > memdumpMFTPARSER.txt
```

```
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# vol.py -f memdump.mem --profile Win2008SP2x86 mftparser > memdumpMFTPARSER.txt
Volatility Foundation Volatility Framework 2.6.1
root@CIBER-LXC-Ubuntu20-EricSerranoMarin:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.22.236.146 netmask 255.255.0.0 broadcast 172.22.255.255
    inet6 fe80::846f:1fff:feef:b9b4 prefixlen 64 scopeid 0x20<link>
    ether 86:6f:1f:ef:b9:b4 txqueuelen 1000 (Ethernet)
    RX packets 11408 bytes 744616 (744.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 27 bytes 3283 (3.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

## Archivo mftparser.

```
memdumpMFTPARSER: Bloc de notas
Archivo Edición Formato Ver Ayuda
Scanning for MFT entries and building directory, this can take a while
*****
MFT entry found at offset 0xa000
Attribute: In Use & File
Record Number: 0
Link count: 1

$STANDARD_INFORMATION
Creation          Modified          MFT Altered          Access Date          Type
-----
2015-08-24 07:42:51 UTC+0000 2015-08-24 07:42:51 UTC+0000 2015-08-24 07:42:51 UTC+0000 2015-08-24 07:42:51 UTC+0000 Hidden & System

$FILE_NAME
Creation          Modified          MFT Altered          Access Date          Name/Path
-----
2015-08-24 07:42:51 UTC+0000 2015-08-24 07:42:51 UTC+0000 2015-08-24 07:42:51 UTC+0000 2015-08-24 07:42:51 UTC+0000 $MFT

$DATA

$OBJECT_ID
Object ID: 40000000-0000-0000-0000-b00300000000
Birth Volume ID: 0000b003-0000-0000-0000-b00300000000
Birth Object ID: 32003b00-000c-0007-b000-000050000000
Birth Domain ID: 01004000-0000-0500-0000-000000000000

*****
MFT entry found at offset 0xa808
Attribute: In Use & Directory
Record Number: 5
Link count: 1

$STANDARD_INFORMATION
Creation          Modified          MFT Altered          Access Date          Type
-----
2008-01-19 08:41:23 UTC+0000 2015-08-23 21:44:01 UTC+0000 2015-08-23 21:44:01 UTC+0000 2015-08-23 21:44:01 UTC+0000 Hidden & System

$FILE_NAME
Creation          Modified          MFT Altered          Access Date          Name/Path
-----
2015-08-24 07:42:51 UTC+0000 2015-08-24 07:42:51 UTC+0000 2015-08-24 07:42:51 UTC+0000 2015-08-24 07:42:51 UTC+0000 .

*****
MFT entry found at offset 0xb408
Attribute: In Use & File
Record Number: 42037
Link count: 1

$STANDARD_INFORMATION
Creation          Modified          MFT Altered          Access Date          Type
-----
2015-08-24 07:50:02 UTC+0000 2008-01-19 07:45:45 UTC+0000 2015-08-24 07:50:02 UTC+0000 2015-08-24 07:50:02 UTC+0000 Read Only & Hidden & System & Archive

$FILE_NAME
Creation          Modified          MFT Altered          Access Date          Name/Path
-----
2015-08-24 07:50:02 UTC+0000 2015-08-24 07:50:02 UTC+0000 2015-08-24 07:50:02 UTC+0000 2015-08-24 07:50:02 UTC+0000 bootmgr

$DATA

$OBJECT_ID
Object ID: 40000000-0000-0000-0020-050000000000
Birth Volume ID: 93150500-0000-0000-9315-050000000000
Birth Object ID: 31522b4d-1700-0000-ffff-ffff82794711
Birth Domain ID: 00000000-0000-0000-0000-000000000000

*****
```

Aquí podríamos encontrar la estructura del sistema de archivos, así como identificar posibles artefactos relacionados con actividad maliciosa, como nombres de archivos inusuales, cambios de timestamp sospechosos o ubicaciones diferentes de archivos.