

<https://github.com/aguayro>

@9v@yr0

Nos entregan un volcado de memoria que debemos estudiar en búsqueda de evidencias sobre actividad delictiva

Pasos seguidos en el análisis de la memoria.

1.- Compruebo que el hash del archivo.
Obtengo con el comando shasum el hash del fichero que se ha entregado para su comprobación con el documento de custodia.

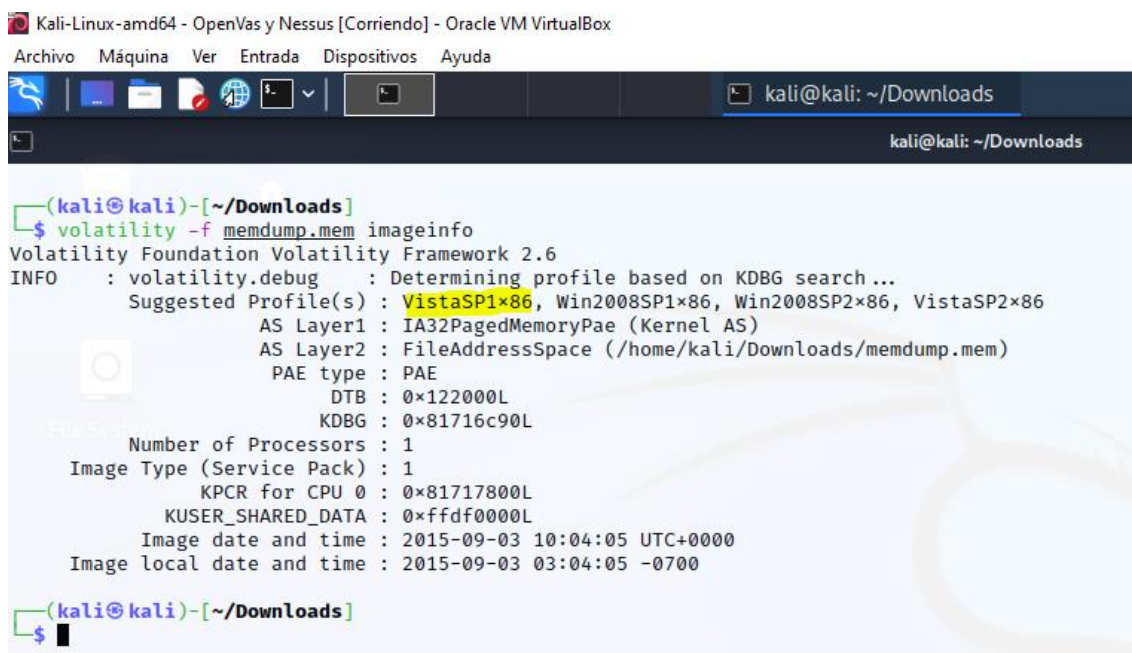
```
shasum memdump.mem
```

```
(kali@kali)-[~/Downloads]
$ shasum memdump.mem
5f3fc1682f0cc969240627be9241dd59c1fdb833  memdump.mem
```

2.- Averiguo el sistema operativo de la memoria:

Ejecuto el comando siguiente:

```
$ volatility -f memdump.mem imageinfo
```



```
(kali@kali)-[~/Downloads]
$ volatility -f memdump.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : VistaSP1x86, Win2008SP1x86, Win2008SP2x86, VistaSP2x86
      AS Layer1 : IA32PagedMemoryPae (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/kali/Downloads/memdump.mem)
      PAE type : PAE
      DTB : 0x122000L
      KDBG : 0x81716c90L
      Number of Processors : 1
      Image Type (Service Pack) : 1
      KPCR for CPU 0 : 0x81717800L
      KUSER_SHARED_DATA : 0xffdf0000L
      Image date and time : 2015-09-03 10:04:05 UTC+0000
      Image local date and time : 2015-09-03 03:04:05 -0700

(kali@kali)-[~/Downloads]
$
```

Volatility nos sugiere usar el profile VistaSP1x86, Win2008SP1x86, Win2008SP2x86 y VistaSP2x86.

Me decanto por usar el primer profile **VistaSP1x86**.

<https://github.com/aguayro>

@9v@yr0

3.- Obtener los procesos que se estaban ejecutando en la máquina con el comando pslist y pstree:

\$ volatility -f memdump.mem --profile VistaSP1x86 pslist

Kali-Linux-amd64 - OpenVas y Nessus [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

kali@kali: ~/Downloads

kali@kali: ~/Downloads

```

L$ volatility -f memdump.mem --profile VistaSP1x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                PID  PPID  Thds  Hnds  Sess  Wow64  Start                Exit
-----
0x82f57910 System              4    0    105   504   0     0     2015-08-23 20:27:20 UTC+0000
0x838382d0 smss.exe          420   4     4     28   0     0     2015-08-23 20:27:20 UTC+0000
0x83912208 csrss.exe          484  472    11   400   0     0     2015-08-23 20:27:22 UTC+0000
0x8392d530 csrss.exe          524  516     9   536   1     0     2015-08-23 20:27:28 UTC+0000
0x8392c9f8 wininit.exe       532  472     3   102   0     0     2015-08-23 20:27:28 UTC+0000
0x8387ed90 winlogon.exe     560  516     4   125   1     0     2015-08-23 20:27:28 UTC+0000
0x8393bd90 services.exe    608  532     7   238   0     0     2015-08-23 20:29:06 UTC+0000
0x83942020 lsass.exe      620  532    19   628   0     0     2015-08-23 20:29:18 UTC+0000
0x83945d90 lsm.exe          628  532    10   166   0     0     2015-08-23 20:29:19 UTC+0000
0x839d4020 svchost.exe      792  608     8   305   0     0     2015-08-23 20:29:45 UTC+0000
0x839ded90 VBoxService.exe    836  608     8   115   0     0     2015-08-23 20:29:46 UTC+0000
0x839f0020 svchost.exe      892  608     7   262   0     0     2015-08-23 10:29:52 UTC+0000
0x83a06020 svchost.exe      984  608    15   306   0     0     2015-08-23 10:29:52 UTC+0000
0x83a18020 svchost.exe     1012 608     6   147   0     0     2015-08-23 10:29:53 UTC+0000
0x83a0eb88 svchost.exe     1024 608    37   913   0     0     2015-08-23 10:29:53 UTC+0000
0x83a1e020 SLsvc.exe      1040 608     4    75   0     0     2015-08-23 10:29:53 UTC+0000
0x83a35630 svchost.exe     1108 608    23   450   0     0     2015-08-23 10:29:54 UTC+0000
0x83a365d0 svchost.exe     1176 608    22   257   0     0     2015-08-23 10:29:56 UTC+0000
0x83a3e020 svchost.exe     1204 608    18   518   0     0     2015-08-23 10:29:56 UTC+0000
0x838ed8c8 svchost.exe     1352 608    18   271   0     0     2015-08-23 10:29:58 UTC+0000
0x83acadb0 spoolsv.exe    1476 608    17   282   0     0     2015-08-23 10:30:04 UTC+0000
0x83adfd90 svchost.exe     1512 608     9   117   0     0     2015-08-23 10:30:04 UTC+0000
0x83ae4af0 svchost.exe     1556 608     5   123   0     0     2015-08-23 10:30:05 UTC+0000
0x83ae6c28 svchost.exe     1568 608     3    73   0     0     2015-08-23 10:30:05 UTC+0000
0x83af2d90 svchost.exe     1680 608     5    44   0     0     2015-08-23 10:30:05 UTC+0000
0x83dca020 taskeng.exe      1984 1024     5   135   0     0     2015-08-23 10:30:08 UTC+0000
0x83b2b020 taskeng.exe     1444 1024    10   245   1     0     2015-08-23 10:30:34 UTC+0000
0x83e2f168 dwm.exe          1688 1176     3    77   1     0     2015-08-23 10:30:34 UTC+0000
0x83e368e0 explorer.exe      816  676    22   756   1     0     2015-08-23 10:30:34 UTC+0000
0x83e652a0 VBoxTray.exe 1816  816     8   114   1     0     2015-08-23 10:30:38 UTC+0000
0x83e7b7f8 cmd.exe           612  816     1    72   1     0     2015-08-23 10:30:44 UTC+0000
0x83f84d90 svchost.exe     2424 608     9   227   0     0     2015-08-23 10:31:51 UTC+0000
0x83f8e5d0 msdtc.exe      2620 608    11   165   0     0     2015-08-23 10:32:10 UTC+0000
0x83faa020 xampp-control.e  2768  816     2   119   1     0     2015-08-23 10:32:17 UTC+0000
0x83e4d7c0 httpd.exe        2796 2768     1    92   1     0     2015-08-23 10:32:21 UTC+0000
0x83f9ec70 mysqld.exe      2804 2768    23   570   1     0     2015-08-23 10:32:23 UTC+0000
0x83fd5200 FileZillaServer 2856 2768     5    35   1     0     2015-08-23 10:32:25 UTC+0000
0x83fd77a8 httpd.exe      2880 2796   155   483   1     0     2015-08-23 10:32:26 UTC+0000
0x8427c730 wuaucnt.exe      2516 1024     2   140   1     0     2015-09-02 09:01:13 UTC+0000
0x84259100 cmd.exe          1972  816     1    19   1     0     2015-09-02 09:28:30 UTC+0000
0x8324cb70 TrustedInstalle 3848  608     5   110   0     0     2015-09-03 10:03:06 UTC+0000
0x83f68300 FTK Imager.exe   2120  816    13   382   1     0     2015-09-03 10:03:37 UTC+0000
  
```

(kali@kali)~-[~/Downloads]

\$

<https://github.com/aguayro>

@9v@yr0

Agrupamos los procesos por dependencias para averiguar sus procesos padres con el comando:

\$ volatility -f memdump.mem --profile VistaSP1x86 pstree

```

kali@kali: ~/Downloads
$ volatility -f memdump.mem --profile VistaSP1x86 pstree
Volatility Foundation Volatility Framework 2.6
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:TrustedInstalle        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:lsass.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

(kali@kali)-[~/Downloads]
$
  
```

Se identifican varios procesos un tanto anómalos, por un lado:

El servicio svchost.exe tiene arrancados dos procesos **taskeng.exe** con **pid 1984** y **1444** y por otro lado el servicio **httpd.exe** tiene el proceso con **pid 2796** y **2880**. Éste último es proceso hijo del mismo servicio.

<https://github.com/aguayro>

@9v@yr0

4.- Investigo si hay algún proceso oculto y posibles positivos

Ejecuto el comando siguiente y filtro para que sólo me muestre los posibles positivos (marcados como false).

\$ volatility -f memdump.mem --profile VistaSP1x86 psxview | grep "False"

```
L$ volatility -f memdump.mem --profile VistaSP1x86 psxview
Volatility Foundation Volatility Framework 2.6
Offset(P) Name PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
0x3efd5200 FileZillaServer 2856 True True True True True True True True
0x019c1100 cmd.exe 1972 True True True True True True True False
0x3f20eb88 svchost.exe 1024 True True True True True True True True
0x3ef9ec70 mysqld.exe 2804 True True True True True True True True
0x3f53bd90 services.exe 608 True True True True True True True False
0x3f1ca020 taskeng.exe 1984 True True True True True True True True
0x3f545d90 lsm.exe 628 True True True True True True True True
0x3ef8e5d0 msdtc.exe 2620 True True True True True True True True
0x3f5ded90 VBoxService.exe 836 True True True True True True True True
0x3f2dfd90 svchost.exe 1512 True True True True True True True True
0x3ef68300 FTK Imager.exe 2120 True True True True True True True True
0x3f5d4020 svchost.exe 792 True True True True True True True True
0x3fa4cb70 TrustedInstall.exe 3848 True True True True True True True True
0x3f2e6c28 svchost.exe 1568 True True True True True True True False
0x3ef84d90 svchost.exe 2424 True True True True True True True True
0x3f235630 svchost.exe 1108 True True True True True True True True
0x3efaa020 xampp-control.e 2768 True True True True True True True True
0x3f32b020 taskeng.exe 1444 True True True True True True True True
0x3ee4d7c0 httpd.exe 2796 True True True True True True True True
0x3f21e020 SLsvc.exe 1040 True True True True True True True True
0x3f218020 svchost.exe 1012 True True True True True True True True
0x3f5f0020 svchost.exe 892 True True True True True True True True
0x3f4ed8c8 svchost.exe 1352 True True True True True True True True
0x3f2365d0 svchost.exe 1176 True True True True True True True True
0x3ee7b7f8 cmd.exe 612 True True True True True True True False
0x3f2cad90 spoolsv.exe 1476 True True True True True True True True
0x3ee652a0 VBoxTray.exe 1816 True True True True True True True True
0x3f23e020 svchost.exe 1204 True True True True True True True True
0x29e02730 wuauclt.exe 2516 True True True True True True True True
0x3ee368e0 explorer.exe 816 True True True True True True True True
0x3f2f2d90 svchost.exe 1680 True True True True True True True False
0x3ee2f168 dwm.exe 1688 True True True True True True True True
0x3f542020 lsass.exe 620 True True True True True True True False
0x3f2e4af0 svchost.exe 1556 True True True True True True True True
0x3efd77a8 httpd.exe 2880 True True True True True True True True
0x3f52c9f8 wininit.exe 532 True True True True True True True True
0x3f206020 svchost.exe 984 True True True True True True True True
0x3f47ed90 winlogon.exe 560 True True True True True True True True
0x3f512208 csrss.exe 484 True True True True False True True True
0x02f57910 System 4 True True True True False False False False
0x3f52d530 csrss.exe 524 True True True True False True True True
0x3f4382d0 smss.exe 420 True True True True False False False False

(kali@kali)~/Downloads$
```

No aparece nada anormal, con los pids anteriormente indicados. Las dos primeras columnas del pslist y psscan están en true.

<https://github.com/aguayro>

@9v@yr0

4.- Reviso las conexiones de red existentes

```
(kali@kali)~[/Downloads]
$ volatility -f memdump.mem --profile VistaSPI-86 connscan
Volatility Foundation Volatility Framework 2.6
ERROR : volatility.debug : This command does not support the profile VistaSPI-86

(kali@kali)~[/Downloads]
$ volatility -f memdump.mem --profile VistaSPI-86 sockets
Volatility Foundation Volatility Framework 2.6
ERROR : volatility.debug : This command does not support the profile VistaSPI-86

(kali@kali)~[/Downloads]
$ volatility -f memdump.mem --profile VistaSPI-86 netscan
Volatility Foundation Volatility Framework 2.6
```

Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner	Created
0x1972938	UDPv4	0.0.0.0:123	*	*	1108	svchost.exe	2015-09-03 06:06:35 UTC+0000
0x1972938	UDPv6	:::123	*	*	1108	svchost.exe	2015-09-03 06:06:35 UTC+0000
0x1974a88	UDPv4	0.0.0.0:3782	*	*	1108	svchost.exe	2015-09-03 10:03:20 UTC+0000
0x196d328	TCPv4	192.168.56.101:139	0.0.0.0:0	LISTENING	4	System	
0x3ee45448	UDPv4	0.0.0.0:123	*	*	1108	svchost.exe	2015-09-03 06:06:35 UTC+0000
0x3ee554a8	UDPv4	0.0.0.0:5355	*	*	1204	svchost.exe	2015-09-03 06:06:37 UTC+0000
0x3ee554a8	UDPv6	:::5355	*	*	1204	svchost.exe	2015-09-03 06:06:37 UTC+0000
0x3ee88e48	UDPv4	0.0.0.0:0	*	*	1176	svchost.exe	2015-08-23 10:30:48 UTC+0000
0x3ee99a98	UDPv4	0.0.0.0:62184	*	*	1108	svchost.exe	2015-09-03 10:03:20 UTC+0000
0x3ef33988	UDPv4	0.0.0.0:3782	*	*	1108	svchost.exe	2015-09-03 10:03:20 UTC+0000
0x3ef33988	UDPv6	:::3782	*	*	1108	svchost.exe	2015-09-03 10:03:20 UTC+0000
0x3ef326f8	UDPv4	0.0.0.0:62185	*	*	1108	svchost.exe	2015-09-03 10:03:20 UTC+0000
0x3ef326f8	UDPv6	:::62185	*	*	1108	svchost.exe	2015-09-03 10:03:20 UTC+0000
0x3ef710f8	UDPv4	192.168.56.101:138	*	*	4	System	2015-09-03 06:06:35 UTC+0000
0x3f1e1438	UDPv4	192.168.56.101:137	*	*	4	System	2015-09-03 06:06:35 UTC+0000
0x3f1e03d8	UDPv4	0.0.0.0:0	*	*	836	VBoxService.exe	2015-09-03 10:04:08 UTC+0000
0x3efccb88	TCPv4	0.0.0.0:80	0.0.0.0:0	LISTENING	2796	httpd.exe	
0x3efccb88	TCPv6	:::80	0.0.0.0:0	LISTENING	2796	httpd.exe	
0x3efcde18	TCPv4	0.0.0.0:443	0.0.0.0:0	LISTENING	2796	httpd.exe	
0x3efcde18	TCPv4	0.0.0.0:443	0.0.0.0:0	LISTENING	2796	httpd.exe	
0x3efcde18	TCPv6	:::443	0.0.0.0:0	LISTENING	2796	httpd.exe	
0x3efcdff8	TCPv4	0.0.0.0:80	0.0.0.0:0	LISTENING	2796	httpd.exe	
0x3f1f8328	TCPv4	0.0.0.0:49157	0.0.0.0:0	LISTENING	688	services.exe	
0x3f1f9328	TCPv4	0.0.0.0:49157	0.0.0.0:0	LISTENING	688	services.exe	
0x3f1f9328	TCPv6	:::49157	0.0.0.0:0	LISTENING	688	services.exe	
0x3ef81c18	TCPv6	fe80::3816:d72e:759b:76b9:3386	ff02::1:3:51128	CLOSED	2884	mysqld.exe	
0x3f258678	UDPv4	0.0.0.0:580	*	*	1824	svchost.exe	2015-08-23 10:30:05 UTC+0000
0x3f26c388	UDPv4	0.0.0.0:4580	*	*	1824	svchost.exe	2015-08-23 10:30:05 UTC+0000
0x3f26d988	UDPv4	0.0.0.0:5355	*	*	1204	svchost.exe	2015-09-03 06:06:37 UTC+0000
0x3f28e2a8	UDPv4	0.0.0.0:580	*	*	1824	svchost.exe	2015-08-23 10:30:05 UTC+0000
0x3f28e2a8	UDPv6	:::580	*	*	1824	svchost.exe	2015-08-23 10:30:05 UTC+0000
0x3f2e3188	UDPv4	0.0.0.0:0	*	*	1824	svchost.exe	2015-08-23 10:30:05 UTC+0000
0x3f2e3188	UDPv6	:::0	*	*	1824	svchost.exe	2015-08-23 10:30:05 UTC+0000
0x3f2ead98	UDPv4	0.0.0.0:0	*	*	1824	svchost.exe	2015-08-23 10:30:05 UTC+0000
0x3f2f49b8	UDPv4	0.0.0.0:55813	*	*	1204	svchost.exe	2015-09-03 10:03:55 UTC+0000
0x3f2fc9f8	UDPv4	0.0.0.0:0	*	*	1356	svchost.exe	2015-08-23 10:30:05 UTC+0000
0x3f2fc9f8	UDPv6	:::0	*	*	1356	svchost.exe	2015-08-23 10:30:05 UTC+0000
0x3f2fe078	UDPv4	0.0.0.0:0	*	*	1356	svchost.exe	2015-08-23 10:30:05 UTC+0000
0x3f2ff288	UDPv4	0.0.0.0:0	*	*	1108	svchost.exe	2015-08-23 10:30:05 UTC+0000
0x3f308e48	UDPv4	0.0.0.0:0	*	*	1108	svchost.exe	2015-08-23 10:30:05 UTC+0000
0x3f308e48	UDPv6	:::0	*	*	1108	svchost.exe	2015-08-23 10:30:05 UTC+0000
0x3f3258d8	UDPv4	127.0.0.1:57557	*	*	1204	svchost.exe	2015-08-23 10:30:07 UTC+0000
0x3f352998	UDPv4	0.0.0.0:3782	*	*	1108	svchost.exe	2015-09-03 10:03:20 UTC+0000
0x3f352998	UDPv6	:::3782	*	*	1108	svchost.exe	2015-09-03 10:03:20 UTC+0000
0x3f353338	UDPv4	0.0.0.0:3782	*	*	1108	svchost.exe	2015-09-03 10:03:20 UTC+0000
0x3fa91948	UDPv4	0.0.0.0:0	*	*	1204	svchost.exe	2015-09-03 06:06:37 UTC+0000
0x3fa91948	UDPv6	:::0	*	*	1204	svchost.exe	2015-09-03 06:06:37 UTC+0000
0x3f284188	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	984	svchost.exe	
0x3f284188	TCPv6	:::49153	0.0.0.0:0	LISTENING	984	svchost.exe	
0x3f288b78	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	620	lsass.exe	
0x3f288b78	TCPv6	:::49154	0.0.0.0:0	LISTENING	620	lsass.exe	
0x3f288f98	TCPv4	0.0.0.0:49154	0.0.0.0:0	LISTENING	620	lsass.exe	
0x3f3085c8	TCPv4	0.0.0.0:49156	0.0.0.0:0	LISTENING	1356	svchost.exe	
0x3f3085c8	TCPv6	0.0.0.0:49156	0.0.0.0:0	LISTENING	1356	svchost.exe	
0x3f383cc8	TCPv6	:::49156	0.0.0.0:0	LISTENING	1356	svchost.exe	
0x3f321c88	TCPv4	0.0.0.0:445	0.0.0.0:0	LISTENING	4	System	
0x3f321c88	TCPv6	:::445	0.0.0.0:0	LISTENING	4	System	
0x3f495e38	TCPv6	:::14147	0.0.0.0:0	LISTENING	2856	FileZillaServer	
0x3f4a84c8	TCPv4	127.0.0.1:14147	0.0.0.0:0	LISTENING	2856	FileZillaServer	
0x3f58e648	TCPv4	0.0.0.0:21	0.0.0.0:0	LISTENING	2856	FileZillaServer	
0x3f516bd8	TCPv4	0.0.0.0:21	0.0.0.0:0	LISTENING	2856	FileZillaServer	
0x3f516bd8	TCPv6	:::21	0.0.0.0:0	LISTENING	2856	FileZillaServer	
0x3f5354b8	TCPv4	0.0.0.0:49155	0.0.0.0:0	LISTENING	1824	svchost.exe	
0x3f5e8688	TCPv4	0.0.0.0:49153	0.0.0.0:0	LISTENING	984	svchost.exe	
0x3f5f5328	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	892	svchost.exe	
0x3f5f5328	TCPv6	:::135	0.0.0.0:0	LISTENING	892	svchost.exe	
0x3f5f5e38	TCPv4	0.0.0.0:135	0.0.0.0:0	LISTENING	892	svchost.exe	

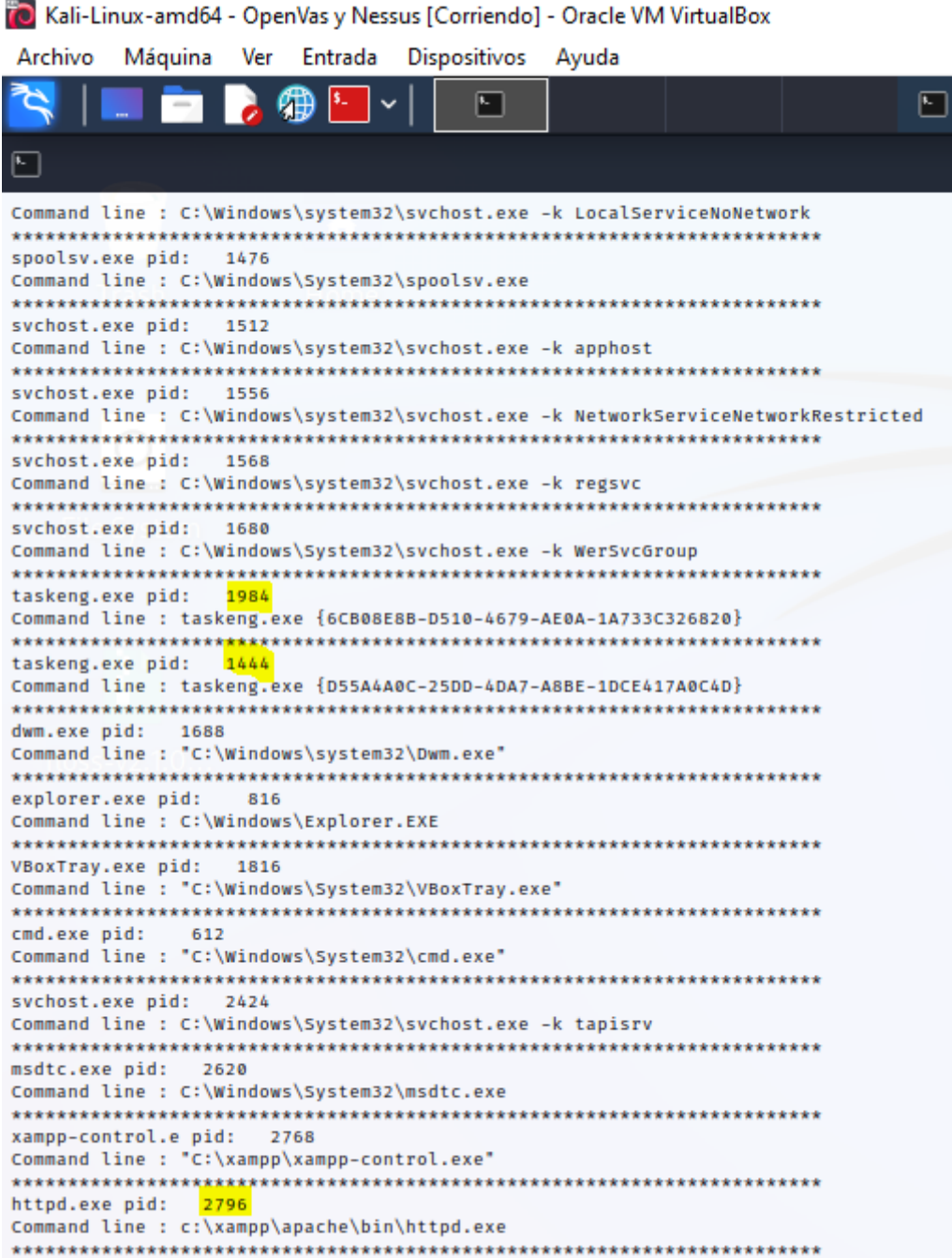
No hay nada relevante en el momento de la captura de memoria.

<https://github.com/aguayro>

@9v@yr0

5.- Revisar la línea de comandos que se ha están ejecutando

\$ volatility -f memdump.mem --profile VistaSP1x86 cmdline



```

Kali-Linux-amd64 - OpenVas y Nessus [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

Command line : C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
*****
spoolsv.exe pid: 1476
Command line : C:\Windows\System32\spoolsv.exe
*****
svchost.exe pid: 1512
Command line : C:\Windows\system32\svchost.exe -k apphost
*****
svchost.exe pid: 1556
Command line : C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted
*****
svchost.exe pid: 1568
Command line : C:\Windows\system32\svchost.exe -k regsvc
*****
svchost.exe pid: 1680
Command line : C:\Windows\System32\svchost.exe -k WerSvcGroup
*****
taskeng.exe pid: 1984
Command line : taskeng.exe {6CB08E8B-D510-4679-AE0A-1A733C326820}
*****
taskeng.exe pid: 1444
Command line : taskeng.exe {D55A4A0C-25DD-4DA7-ABBE-1DCE417A0C4D}
*****
dwm.exe pid: 1688
Command line : "C:\Windows\system32\Dwm.exe"
*****
explorer.exe pid: 816
Command line : C:\Windows\Explorer.EXE
*****
VBoxTray.exe pid: 1816
Command line : "C:\Windows\System32\VBoxTray.exe"
*****
cmd.exe pid: 612
Command line : "C:\Windows\System32\cmd.exe"
*****
svchost.exe pid: 2424
Command line : C:\Windows\System32\svchost.exe -k tapisrv
*****
msdtc.exe pid: 2620
Command line : C:\Windows\System32\msdtc.exe
*****
xampp-control.e pid: 2768
Command line : "C:\xampp\xampp-control.exe"
*****
httpd.exe pid: 2796
Command line : c:\xampp\apache\bin\httpd.exe
*****

```

Los procesos con **pid 1984** y **pid 1444** hacen llamadas a claves del registro de windows que son un poco sospechosas. El proceso con **pid 2796** que se está ejecutando dos veces se corresponde con el servidor apache de xampp.

<https://github.com/aguayro>

@9v@yr0

6.- Volcado de los comandos ejecutados desde la consola

\$ Volatility -f memdump.mem --profile VistaSP1x86 cmdscan

```

Kali-Linux-amd64 - OpenVas y Nessus [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

(kali@kali)-[~/Downloads]
$ volatility -f memdump.mem --profile VistaSP1x86 cmdscan
Volatility Foundation Volatility Framework 2.6
*****
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 fireall 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

(kali@kali)-[~/Downloads]
$

```

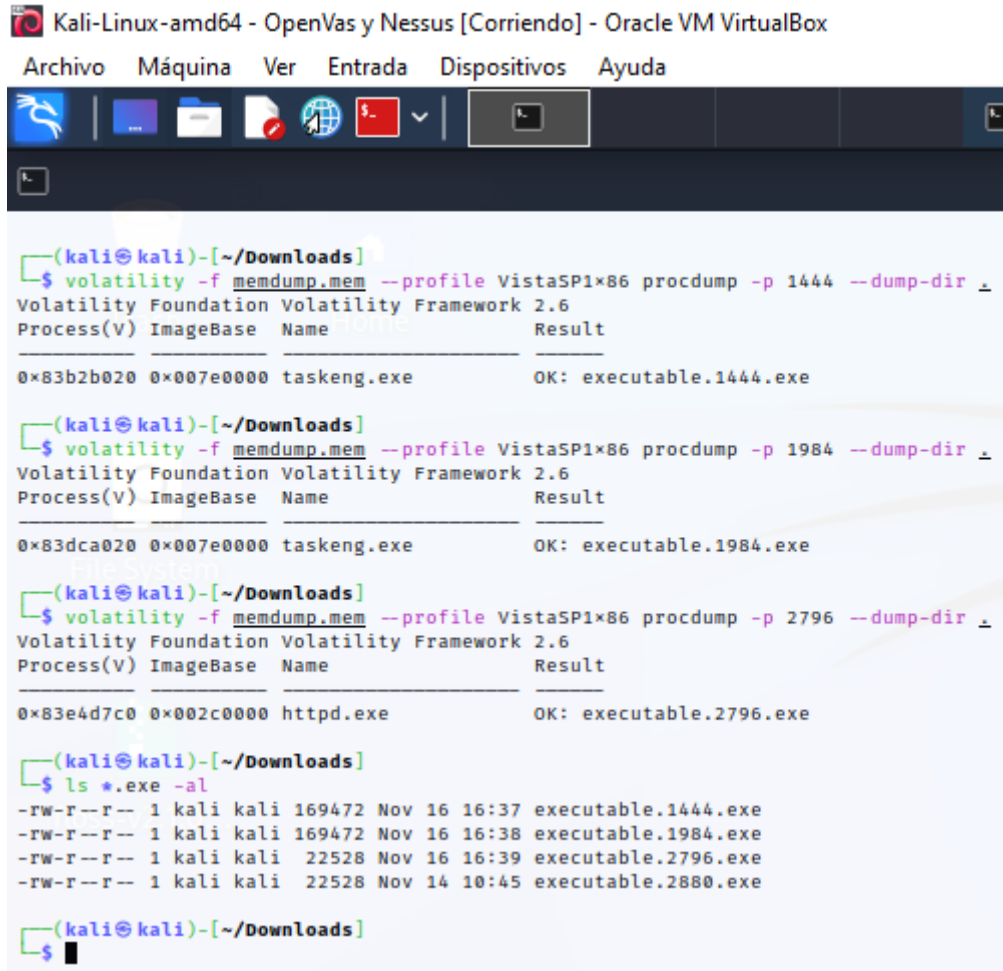
Obtengo los comandos que se han ejecutado desde la consola con el **pid 524**, cuyo servicio es el **csrss.exe** según el listado de procesos que obtuvimos del pslist se está ejecutando desde el **23 de agosto de 2.015**

<https://github.com/aguayro>

@9v@yr0

7.- Realizo un volcado memoria a disco del ejecutable con pid 1444, pid 1984 y pid 2796 para su analisis en virustotal

\$ volatility -f memdump.mem --profile VistaSP1x86 procdump -p 1444 --dump-dir .



```
(kali㉿kali)-[~/Downloads]
$ volatility -f memdump.mem --profile VistaSP1x86 procdump -p 1444 --dump-dir .
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase Name Result
-----
0x83b2b020 0x007e0000 taskeng.exe OK: executable.1444.exe

(kali㉿kali)-[~/Downloads]
$ volatility -f memdump.mem --profile VistaSP1x86 procdump -p 1984 --dump-dir .
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase Name Result
-----
0x83dca020 0x007e0000 taskeng.exe OK: executable.1984.exe

(kali㉿kali)-[~/Downloads]
$ volatility -f memdump.mem --profile VistaSP1x86 procdump -p 2796 --dump-dir .
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase Name Result
-----
0x83e4d7c0 0x002c0000 httpd.exe OK: executable.2796.exe

(kali㉿kali)-[~/Downloads]
$ ls *.exe -al
-rw-r--r-- 1 kali kali 169472 Nov 16 16:37 executable.1444.exe
-rw-r--r-- 1 kali kali 169472 Nov 16 16:38 executable.1984.exe
-rw-r--r-- 1 kali kali 22528 Nov 16 16:39 executable.2796.exe
-rw-r--r-- 1 kali kali 22528 Nov 14 10:45 executable.2880.exe

(kali㉿kali)-[~/Downloads]
$
```


<https://github.com/aguayro>

@9v@yr0

Analizo el contenido de los ficheros ejecutables en la web de virustotal.com

Kali-Linux-amd64 - OpenVas y Nessus [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

VirusTotal - File - ac6b716fb9755b71684a3795e2f756f161011674b5830c9a354cb0a61586158f

https://www.virustotal.com/gui/file/ac6b716fb9755b71684a3795e2f756f161011674b5830c9a354cb0a61586158f

ac6b716fb9755b71684a3795e2f756f161011674b5830c9a354cb0a61586158f

1 / 59

taskeng.exe

165.50 KB Size

2017-02-27 02:25:50 UTC 5 years ago

Community Score

DETECTION DETAILS COMMUNITY

Security Vendors' Analysis

CrowdStrike Falcon	Malicious_confidence_77% (D)	Ad-Aware	Undetected
--------------------	------------------------------	----------	------------

De los ficheros escaneado por virus total, tanto el id 1984 como id 1444 dan el fichero executable.1444.exe y executable.1984.exe como software ad-ware. Del fichero executable.2796.exe no detecta nada de virus en el fichero.

8.- Realizo un volcado de memoria del proceso del proceso con pid 2796 para su análisis con floss

\$ volatility -f memdump.mem --profile VistaSP1x86 memdump -p 1984 --dump-dir .

<https://github.com/aguayro>

@9v@yr0

Kali-Linux-amd64 - OpenVas y Nessus [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
(kali@kali)-[~/Downloads]
$ volatility -f memdump.mem --profile VistaSP1x86 memdump -p 2796 --dump-dir .
Volatility Foundation Volatility Framework 2.6
*****
Writing httpd.exe [ 2796] to 2796.dmp

(kali@kali)-[~/Downloads]
$ ls 2796* -al
-rw-r--r-- 1 kali kali 207925248 Nov 16 16:50 2796.dmp

(kali@kali)-[~/Downloads]
$
```

9.- Obtengo los offset del proceso pid 2796

\$ volatility -f memdump.mem --profile VistaSP1x86 psscan | grep "httpd.exe"

Kali-Linux-amd64 - OpenVas y Nessus [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
(kali@kali)-[~/Downloads]
$ volatility -f memdump.mem --profile VistaSP1x86 psscan | grep "httpd.exe"
Volatility Foundation Volatility Framework 2.6
0x000000003ee4d7c0 httpd.exe 2796 2768 0x3f4a74c0 2015-08-23 10:32:21 UTC+0000
0x000000003efd77a8 httpd.exe 2880 2796 0x3f4a7520 2015-08-23 10:32:26 UTC+0000

(kali@kali)-[~/Downloads]
$
```

Confirmamos que el proceso de httpd.exe se está ejecutando desde el 23 de agosto de 2.015, coincidiendo con la ejecución de comandos en la consola de la sección 6 de este documento.

10.- Analizo el fichero ejecutable con pid 2796 con floss

```
(kali@kali)-[~/Downloads]
$ ./floss -v executable.2796.exe --profile VistaSP1x86
INFO: Floss: extracting static strings ...
finding decoding function features: 100% | 48/48 [00:00:00:00, 535.36 functions/s, skipped 10 library functions (20%)]
INFO: Floss: stackstrings: extracting stackstrings from 10 functions
extracting stackstrings: 100% | 18/18 [00:00:00:00, 42.83 functions/s]
INFO: Floss: tightstrings: extracting tightstrings from 0 functions ...
extracting tightstrings: 0 functions [00:00, 7 functions/s]
INFO: Floss: string_decoder: decoding strings
emulating function 0x2c2b56 (call 1/1): 100% | 18/18 [00:05:00:00, 3.40 functions/s]
INFO: Floss: finished execution after 18.41 seconds

FLARE FLOSS RESULTS (version v2.1.0-0-gbf2bf1c)
+-----+-----+
| file path | file | executable.2796.exe |
| start date | date | 2022-11-17 05:51:54 |
| runtime | time | 00:18 |
| version | version | v2.1.0-0-gbf2bf1c |
| imagebase | imagebase | 0x2c0000 |
| min string length | min string length | 4 |
| extracted strings | extracted strings | 401 |
| static strings | static strings | 0 |
| stack strings | stack strings | 0 |
| tight strings | tight strings | 0 |
| decoded strings | decoded strings | 0 |
| analyzed functions | analyzed functions | 48 |
| discovered | discovered | 18 |
| library | library | 10 |
| stack strings | stack strings | 18 |
| tight strings | tight strings | 0 |
| decoded strings | decoded strings | 18 |
| identified decoding functions | identified decoding functions | 0 |
| (offset and score) | (offset and score) | 0 |
+-----+-----+
| 0x2c1330 (0.924), 0x2c11b0 (0.886), 0x2c1200 (0.819), 0x2c1cf0 (0.669), 0x2c2b74 |
| (0.584), 0x2c2762 (0.561), 0x2c2842 (0.560), 0x2c1de0 (0.554), 0x2c1150 (0.440), |
| 0x2c1e90 (0.437), 0x2c2a69 (0.414), 0x2c1000 (0.360), 0x2c1100 (0.300), 0x2c2b56 |
| (0.214), 0x2c2a7b (0.157), 0x2c1120 (0.100), 0x2c1130 (0.100), 0x2c1140 (0.100) |
+-----+-----+
```

<https://github.com/aguayro>

@9v@yr0

No se detecta ninguna cadena de texto anómala en el fichero ejecutable.

11.- Análisis del volcado de memoria con el proceso pid 2796.

Busco algún patrón a partir de la fecha del proceso pid 2796 y 2880 de fecha 23/08/2015, a partir de dicha fecha.

```
$ Strings 2796.dmp | grep "GET /"
```

[illegible]

Aquí hay evidencias de posible ataque con fecha 02 de septiembre de 2.015, desde la dirección ip 192.168.56.102. Realizamos una búsqueda más concreta filtrando por dicha ip.

[illegible]

Se observa conexión desde la ip 192.168.56.102 acceso por web contra el servidor web xamp explotando una vulnerabilidad usando técnicas de sql inyección.

<https://github.com/aguayro>

@9v@yr0

Software:

Volatility 2