Apartado 1 - Análisis Memoria RAM

Partiremos de una imagen de memoria RAM en formato *dump*, es decir de un volcado de memoria.

La imagen de memoria se encuentra disponible en:

https://mega.co.nz/#!1UpjkTab!RP_QeooLaxA7bixLxkHLIqhWKfQ9G_0M58NSUchRn68

La descomprimimos hasta que tengamos el fichero memdump.mem

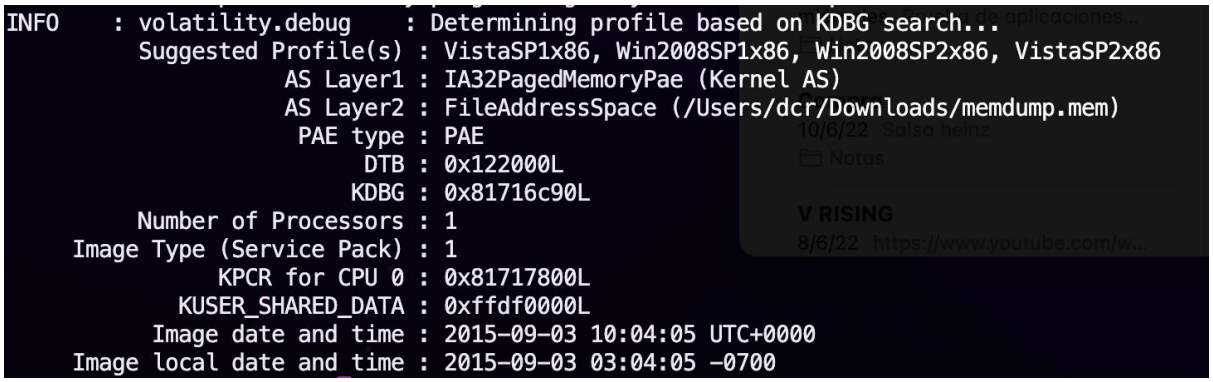
Tenemos varias herramientas para trabajar con la memoria RAM pero casi el estándar a nivel forense es Volatility (tanto la versión 2 como la 3 están disponible en la web oficial de Volatility https://www.volatilityfoundation.org/releases)

Respecto a que versión usar, volatilit3 tiene algunas ventajas como veremos a continuación pero la versión 2 como ha estado más tiempo en desarrollo hay mas plugin y complementos creados. Usaremos la versión durante esta práctica.

Lo primero de todo trataremos de identificar a que sistema operativo pertenece la imagen (si usamos volatility3 no será necesario), para eso usaremos el módulo de imageinfo de volatility.

El comando para hacerlo es:

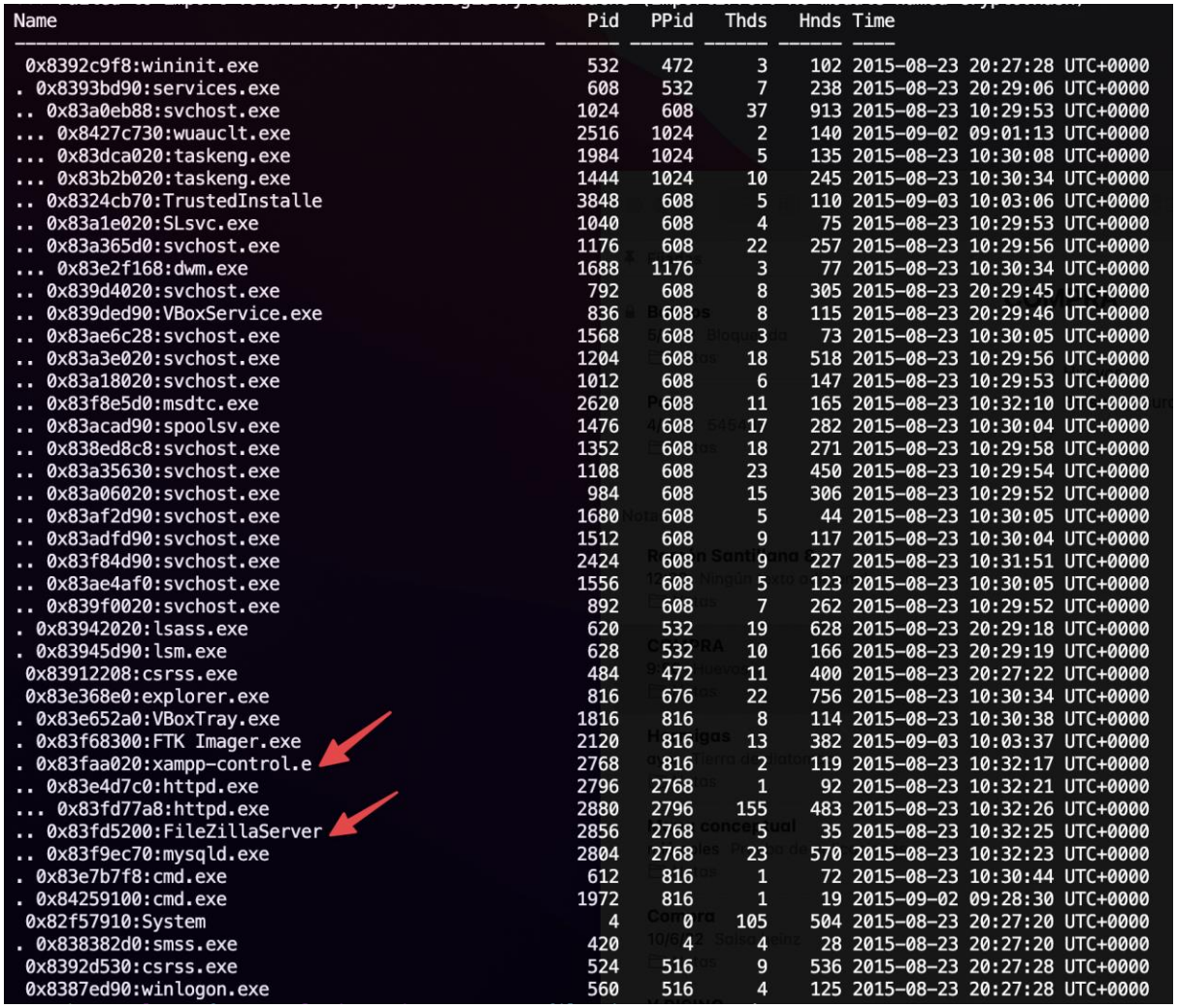
python2 vol.py -f <*ruta de la imagen de memoria RAM descargada*> imageinfo



La búsqueda mediante KDBG sugiere varias opciones probables, probaremos la primera de ellas que es VistaSP1x86.

Un buen punto de partida es ver qué los procesos que había activos cuando se sacó la captura de la memoria. Podemos hacerlo de varias formas pero recomendamos sacar la jerarquía de los procesos y ver la relación entre procesos padres-hijos. Para ello lo haremos con el siguiente comando.

Nos devolverá el listado de procesos en modo árbol (lo que quiere decir que el perfil es correcto o al menos compatible)

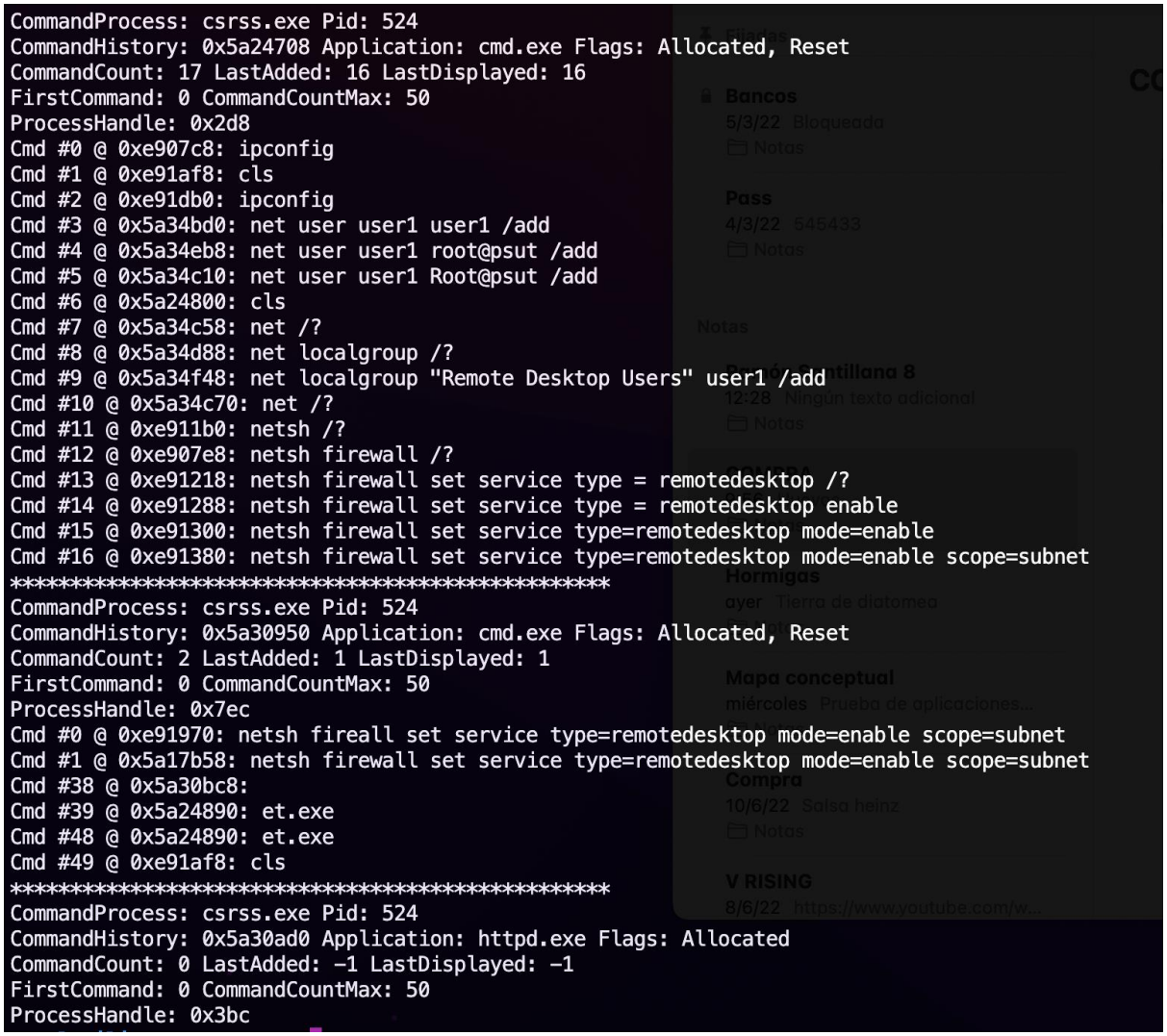


Name	Pid	PPid	Thds	Hnds	Time
0x8392c9f8:wininit.exe	532	472	3	102	2015-08-23 20:27:28 UTC+0000
. 0x8393bd90:services.exe	608	532	7	238	2015-08-23 20:29:06 UTC+0000
.. 0x83a0eb88:svchost.exe	1024	608	37	913	2015-08-23 10:29:53 UTC+0000
... 0x8427c730:wuauclt.exe	2516	1024	2	140	2015-09-02 09:01:13 UTC+0000
... 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: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:mysqld.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

Hay algunos procesos que nos llaman la atención, podemos comprobar como efectivamente es un servidor ejecutando XAMPP (suite de aplicativos web con BBDD, servidor web, etc) tenemos una instancia hija y otra hija de esta última del daemon del servicio http.

Para ello vamos a correlar esta información para revisar que comandos se han ejecutado en la máquina mediante el siguiente comando.

```
> python2 vol.py -f ../Downloads/memdump.mem --profile=VistaSP1x86 cmdscan
```



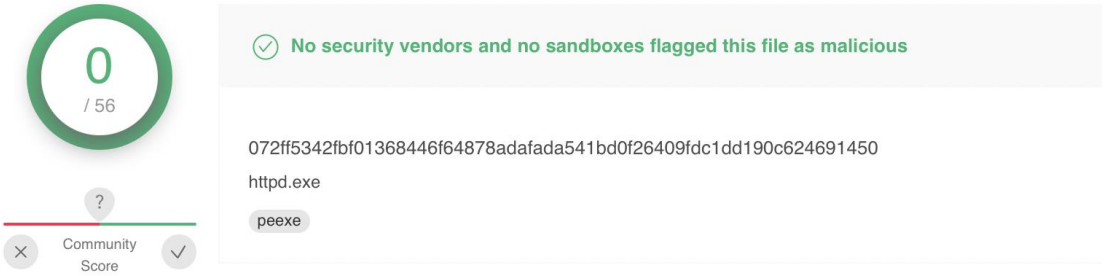
Como vemos se han ejecutado varios comandos en la máquina, se han creado usuarios, se les ha añadido al grupo de remotedesktop, se ha permitido el acceso desde fuera mediante remotedesktop…

Vamos a inspeccionar que ha sucedido en los procesos de httpd, su identificador de proceso es el 2796 y 2880.

Procedemos a volcar los procesos de httpd tanto el 2796 como el 2880 mediante el comando:

Con eso conseguiremos una imagen del proceso httpd.

Vamos a ver si esta info es realmente de ayuda, si probamos a ver si es malicioso en Virustotal.com veremos cómo nos dice que está limpio (es normal es la imagen legítima del servidor web en este caso de Apache)



Entonces lo que necesitamos es buscar en la memoria asociada a ese proceso y no el proceso en sí. Para ello en vez de usar el módulo de procdump usaremos el módulo de memdump.

Esto es normal no es mas que la imagen del servicio de apache, por lo que realmente necesitamos no es la imagen del proceso sino el espacio de memoria con el que estaba trabajando. En este caso mediante el comando

```
~/volatility master !1 ?2 > python2 vol.py -f ../Downloads/memdump.mem --profile=VistaSP1x86 mempdump -p 2796 --dump-dir .
```

Esto nos generará un fichero del formato 2796.dump

Ahora buscaremos cosas sospechosas en este fichero (recordemos es el contenido de memoria que estaba usando el proceso 2796)

Normalmente podríamos usar strings para buscar cadenas o patrones pero usaremos floss que es una versión vitaminada de strings

Encontramos varias referencias curiosas, por ejemplo vemos como hay referencias a *hacker*

```
WebWhacker*
WebWhacker*
WebWhacker
Zp6.102+%26%26+net+user+hacker+hacker+/add&submit=submit
ip=192.168.56.102+%26%26+net+localgroup+%22Remote+Desktop+Users%22+hacker+%2Fadd&submit=submit$
hackerLo
```

Y si nos fijamos tanto aquí como en varias cadenas más vemos una IP que se repite (192.168.56.102)

```
~/volatility master !1 ?2 > floss 2796.dmp | grep "192.168.56.102"
```

```
192.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=ext_md HTTP/1.1" 200 1034 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
192.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=ext_txt HTTP/1.1" 200 132 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
192.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=ext_php HTTP/1.1" 200 79 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
192.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=forward HTTP/1.1" 200 119 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
192.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=up HTTP/1.1" 200 199 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
192.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=ext_ico HTTP/1.1" 200 175 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
192.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=arrow_ltr HTTP/1.1" 200 88 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
192.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=refresh HTTP/1.1" 200 200 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
192.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=ext_ini HTTP/1.1" 200 134 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
192.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=ext_zip HTTP/1.1" 200 577 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
192.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php HTTP/1.1" 200 34708 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.2.0"
192.168.56.102 - - [03/Sep/2015:00:20:59 -0700] "GET /dvwa/c99.php?act=img&img=back HTTP/1.1" 200 119 "http://192.168.56.101/dvwa/c99.php" "Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Ic
```

Si nos fijamos está haciendo varias peticiones extrañas, involucrando un módulo de php llamado c99.php

Si buscamos algo mas de info sobre este módulo vemos que es una pieza de malware, en concreto una webshell (es decir una pieza de malware que se pone en un servidor para ejecutar comandos maliciosos de forma remota)

También si queremos saber más de cómo ha entrado podemos obtenerlo del filtrado anterior.

```
192.168.56.102 - - [02/Sep/2015:04:24:34 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2%27%20UNION%20ALL%20SELECT%20NULL%2CCONCAT%280x717a717871%2CIFNULL%28CAST%28COUNT%28%2A%29%20AS%20CHAR%29%2C0x20%29%2C0x7170706271%29%20FROM%20phpmyadmin.pma_userconfig--%20&Submit=Submit HTTP/1.1" 200 5078 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
192.168.56.102 - - [02/Sep/2015:04:24:34 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2%27%20AND%200RD%28MID%28%28SELECT%20IFNULL%28CAST%28COUNT%28%2A%29%20AS%20CHAR%29%2C0x20%29%20FROM%20phpmyadmin.pma_user%29%2C1%2C1%29%29%3E51%20AND%20%27EDUh%27%3D%27EDUh&Submit=Submit HTTP/1.1" 200 4712 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
192.168.56.102 - - [02/Sep/2015:04:24:34 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2%27%20AND%200RD%28MID%28%28SELECT%20IFNULL%28CAST%28COUNT%28%2A%29%20AS%20CHAR%29%2C0x20%29%20FROM%20phpmyadmin.pma_user%29%2C1%2C1%29%29%3E48%20AND%20%27EDUh%27%3D%27EDUh&Submit=Submit HTTP/1.1" 200 4712 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
192.168.56.102 - - [02/Sep/2015:04:24:34 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2%27%20AND%200RD%28MID%28%28SELECT%20IFNULL%28CAST%28COUNT%28%2A%29%20AS%20CHAR%29%2C0x20%29%20FROM%20phpmyadmin.pma_user%29%2C1%2C1%29%29%3E1%20AND%20%27EDUh%27%3D%27EDUh&Submit=Submit HTTP/1.1" 200 4882 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
192.168.56.102 - - [02/Sep/2015:04:24:34 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2%27%20AND%200RD%28MID%28%28SELECT%20IFNULL%28CAST%28COUNT%28%2A%29%20AS%20CHAR%29%2C0x20%29%20FROM%20phpmyadmin.pma_user%29%2C1%2C1%29%29%3E47%20AND%20%27EDUh%27%3D%27EDUh&Submit=Submit HTTP/1.1" 200 4883 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
192.168.56.102 - - [02/Sep/2015:04:24:34 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2%27%20AND%200RD%28MID%28%28SELECT%20IFNULL%28CAST%28COUNT%28%2A%29%20AS%20CHAR%29%2C0x20%29%20FROM%20phpmyadmin.pma_user%29%2C2%2C1%29%29%3E51%20AND%20%27EDUh%27%3D%27EDUh&Submit=Submit HTTP/1.1" 200 4712 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
192.168.56.102 - - [02/Sep/2015:04:24:34 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2%27%20AND%200RD%28MID%28%28SELECT%20IFNULL%28CAST%28COUNT%28%2A%29%20AS%20CHAR%29%2C0x20%29%20FROM%20phpmyadmin.pma_user%29%2C2%2C1%29%29%3E48%20AND%20%27EDUh%27%3D%27EDUh&Submit=Submit HTTP/1.1" 200 4712 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
192.168.56.102 - - [02/Sep/2015:04:24:34 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2%27%20AND%200RD%28MID%28%28SELECT%20IFNULL%28CAST%28COUNT%28%2A%29%20AS%20CHAR%29%2C0x20%29%20FROM%20phpmyadmin.pma_user%29%2C2%2C1%29%29%3E1%20AND%20%27EDUh%27%3D%27EDUh&Submit=Submit HTTP/1.1" 200 4712 "-" "sqlmap/1.0-dev-nongit-20150902 (http://sqlmap.org)"
192.168.56.102 - - [02/Sep/2015:04:24:34 -0700] "GET /dvwa/vulnerabilities/sqli/?id=2%27%20UNION%20ALL%20SELECT%20NULL%2CCONCAT%280x717a717871%2CIFNULL%28CAST%28column_name%20AS%20CHAR%29%2C0x20%29%2C0x7179%2CIFNULL%28CAST%28column_type%20AS%20CHAR%29%2C0x20%29%2C0x7170706271%29%20FROM%20INFORMATION_SCHEMA.COLUMNS%20WHERE%20table_name%3D0x706d615f747261636b696e67%20AND%20table_schema%3D0x7068706d7961646d
```

Ha intentado un ataque de tipo SQL Injection contra DVWA, software vulnerable. Con esto habrá podido conseguir permisos de administrador, ha ejecutado los comandos maliciosos y ha desplegado una webshell.

Apartado 2 – Preguntas finales

Están todas las respuestas desarrolladas punto 1, se incluyen aquí el resumen de las respuestas.

1. ¿Qué pasaría si se hubiera apagado este servidor?
    - Que se hubiera perdido el contenido de la memoria RAM

2. ¿Qué tipo de comandos ha ejecutado el cibercriminal? ¿Qué sugiere?
    - Ha ejecutado varios comandos maliciosos (ver punto 1) como son la creación de usuarios, añadirlo al grupo de protocolo de administración remota, crear reglas para permitir estas conexiones en el firewall, etc

3. ¿Cómo se han ejecutado los comandos?
    - Mediante consola (cmd.exe)

4. ¿Qué actividad maliciosa has visto?
    - Acceso mediante SQL Injection, despliegue de webshell, comandos maliciosos, etc

5. ¿Puedes identificar desde que IP vino el ataque?
    - 192.168.56.102

6. ¿Qué tipo de ataque pudo ser? ¿Qué tipo de malware se ha encontrado?
    - Ataque de tipo SQL Injection para desplegar después una webshell.