ANÁLISIS FORENSE INFORMÁTICO

Tarea 1

ESTHER CARRILLO GÁLVEZ

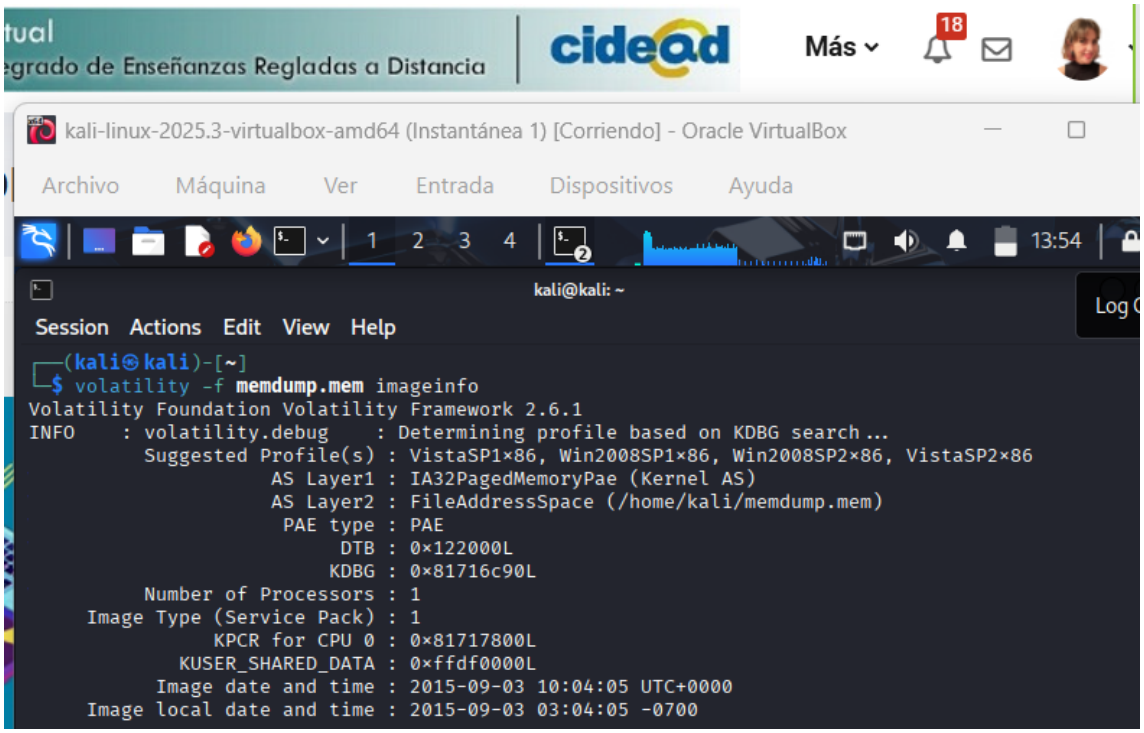
Contenido

¿QUÉ PASARÍA SI SE HUBIERA APAGADO ESTE SERVIDOR?

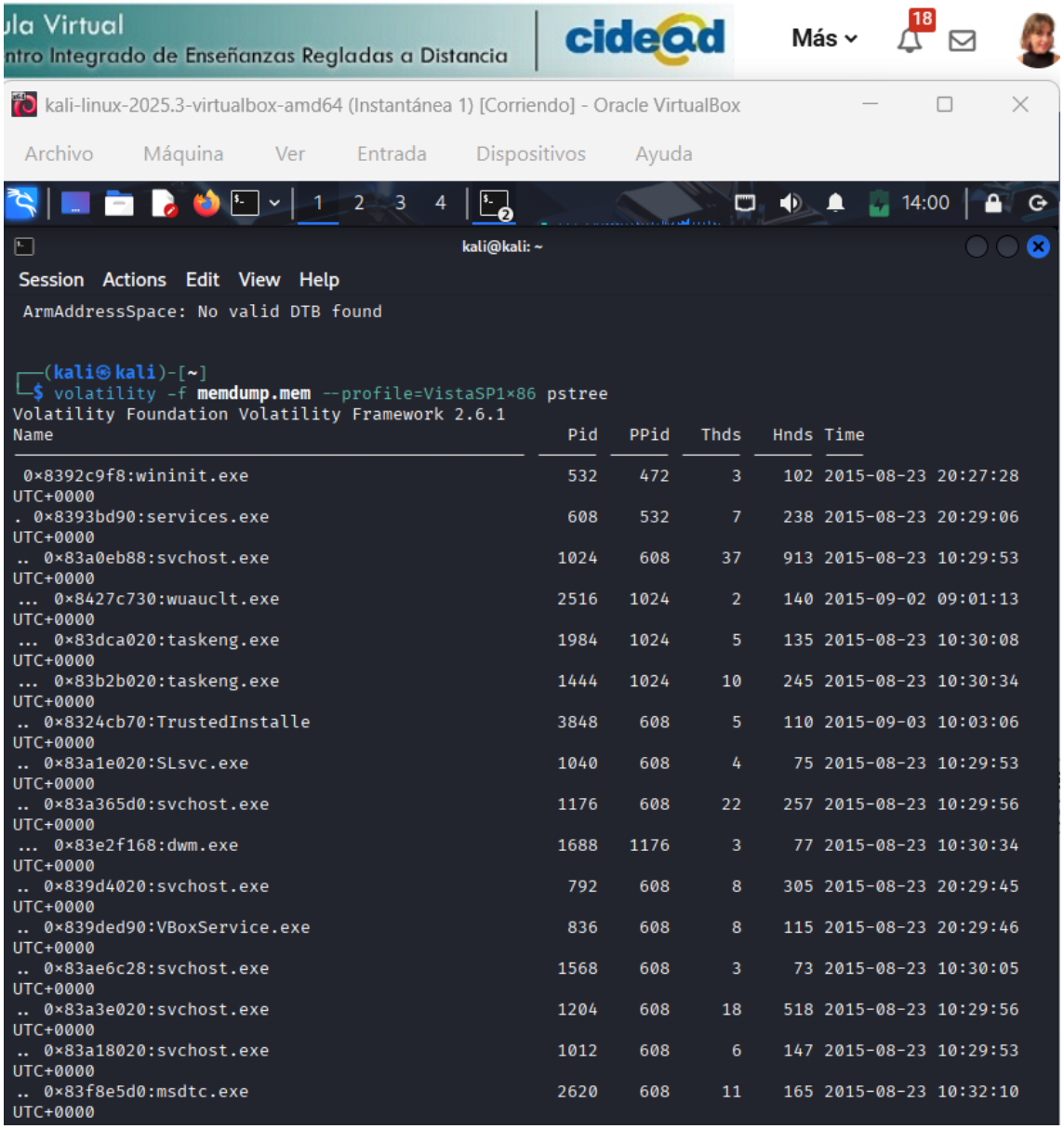
La memoria RAM es volátil esto significa que necesita energía eléctrica para retener los datos. Si se hubiera apagado el servidor, toda la información de *memdump.mem* se hubiera perdido, así como las conexiones de red, las listas de procesos y cualquier información contenida en ella. Además de haber alterado los archivos temporales o haber alterado los *timestamps*. Por tanto, si se hubiera apagado no habría datos en la memoria RAM y, por consiguiente, no se habría conseguido su imagen.

¿QUÉ TIPO DE COMANDOS HA EJECUTADO EL CIBERCRIMINAL? ¿QUÉ SUGIERE?

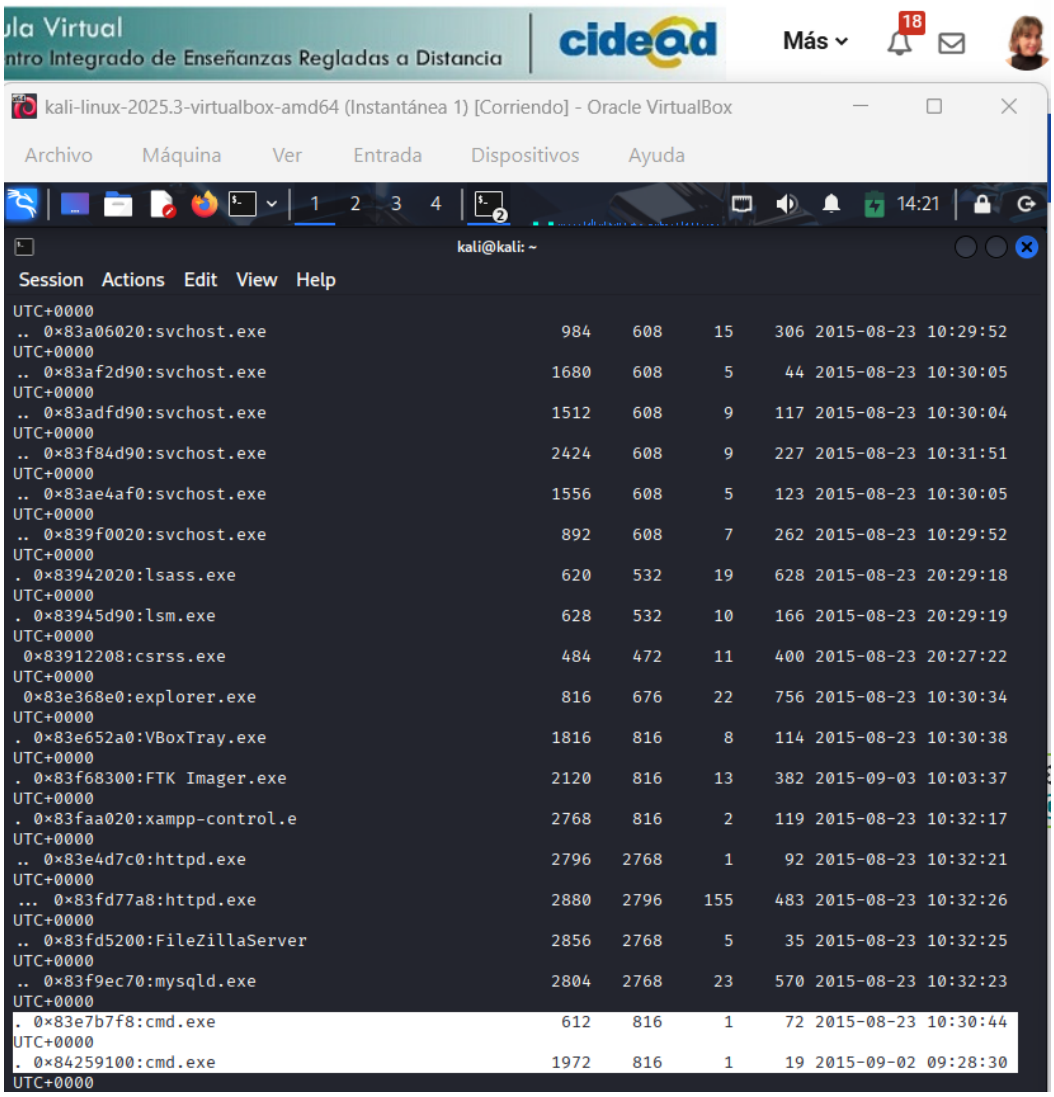
Para determinar el tipo de comandos que ha ejecutado el cibercriminal, se deberá "interpretar" los datos binarios de la imagen de la memoria RAM mediante la herramienta Volatility. A continuación, mediante el plugin *imageinfo*, se determinará el sistema operativo que usó el cibercriminal desde el equipo del que se extrajo la memoria RAM, en este caso *Windows VistaSP1x86*.



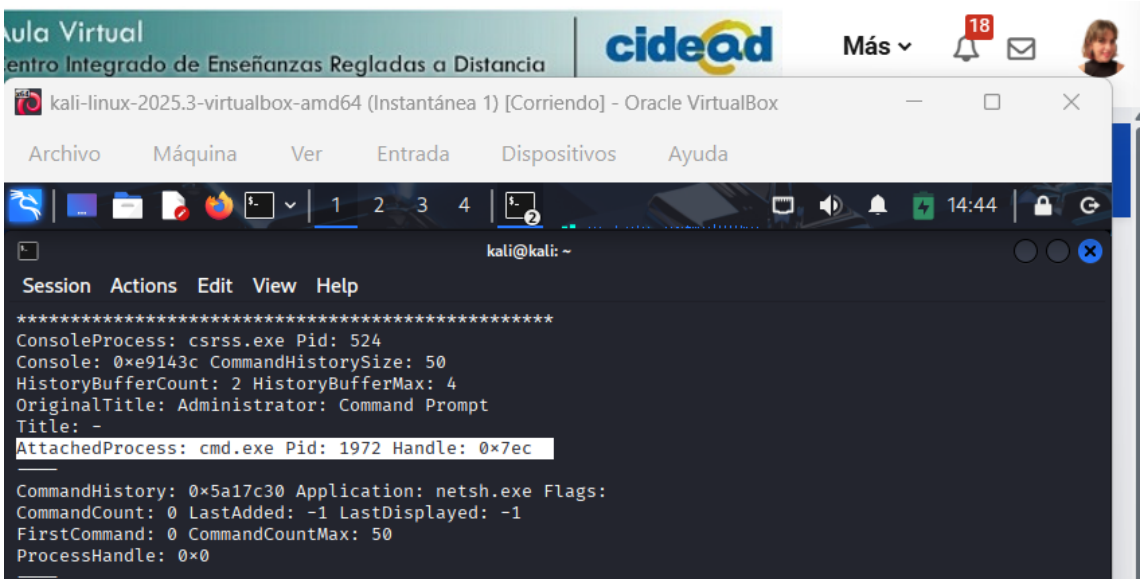
Un plugin importante de Volatility es *pstree* que muestra una lista jerárquica de los procesos del sistema operativo, indicando los procesos padres y los procesos hijos.

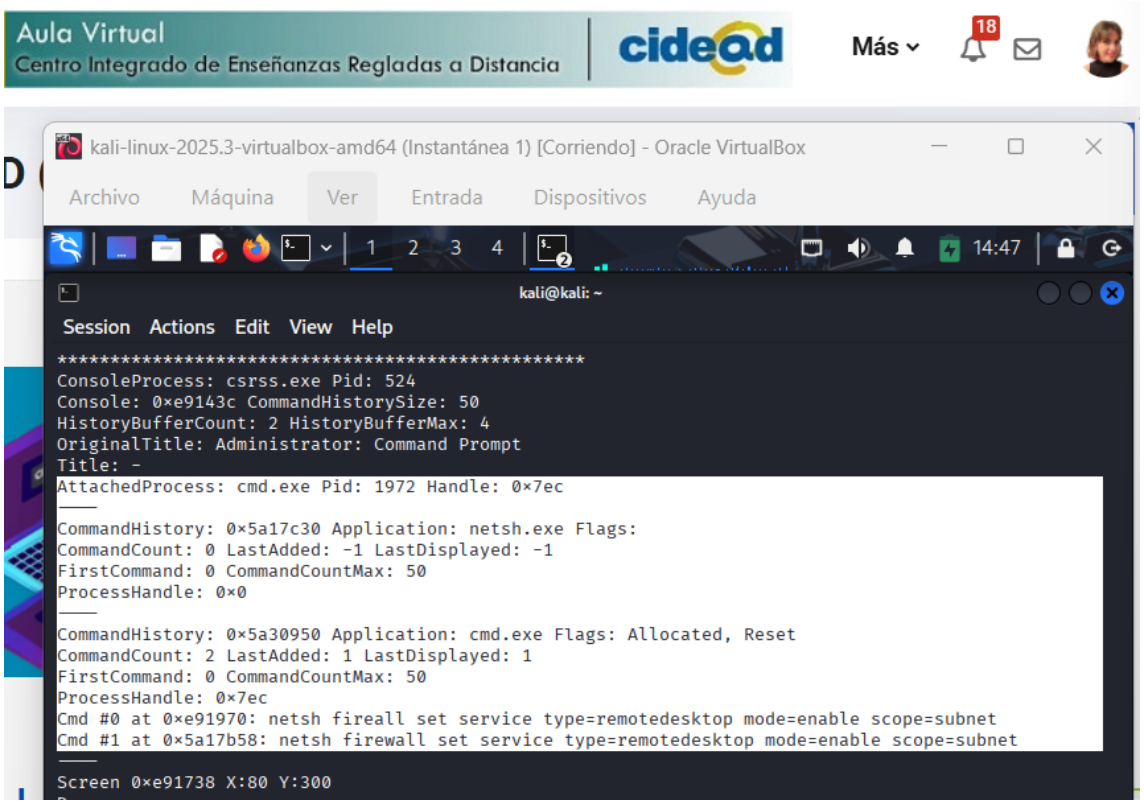

ula Virtual
ntro Integrado de Enseñanzas Regladas a Distancia
cidead
Más
18
kali-linux-2025.3-virtualbox-amd64 (Instantánea 1) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
14:00
kali@kali: ~
Session Actions Edit View Help
ArmAddressSpace: No valid DTB found
(kali㉿kali)-[~]
$ volatility -f memdump.mem --profile=VistaSP1x86 pstree
Volatility Foundation Volatility Framework 2.6.1
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

Se observan procesos sospechosos en la lista recogida en la imagen. Entre ellos se encuentran dos procesos *cmd.exe* cuyos PID son *612* y *1972*, respectivamente.

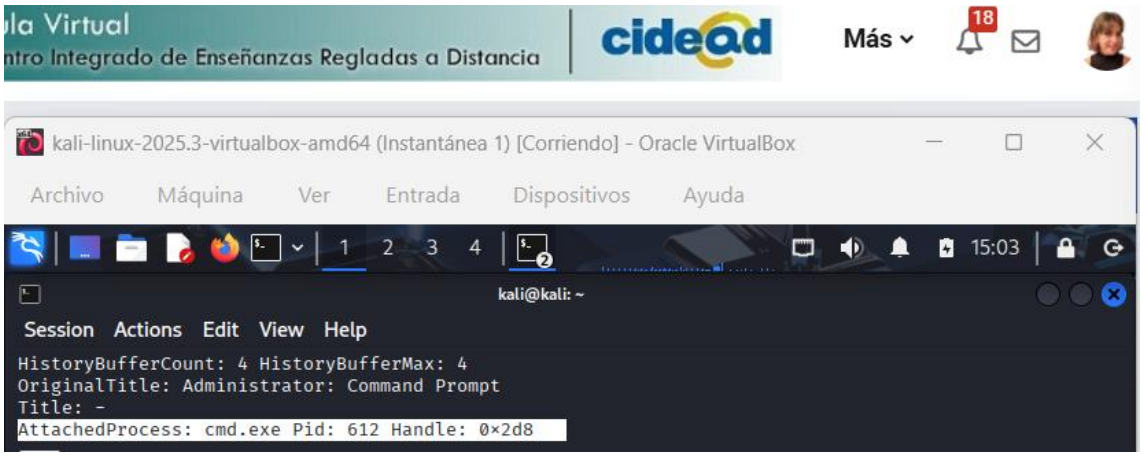


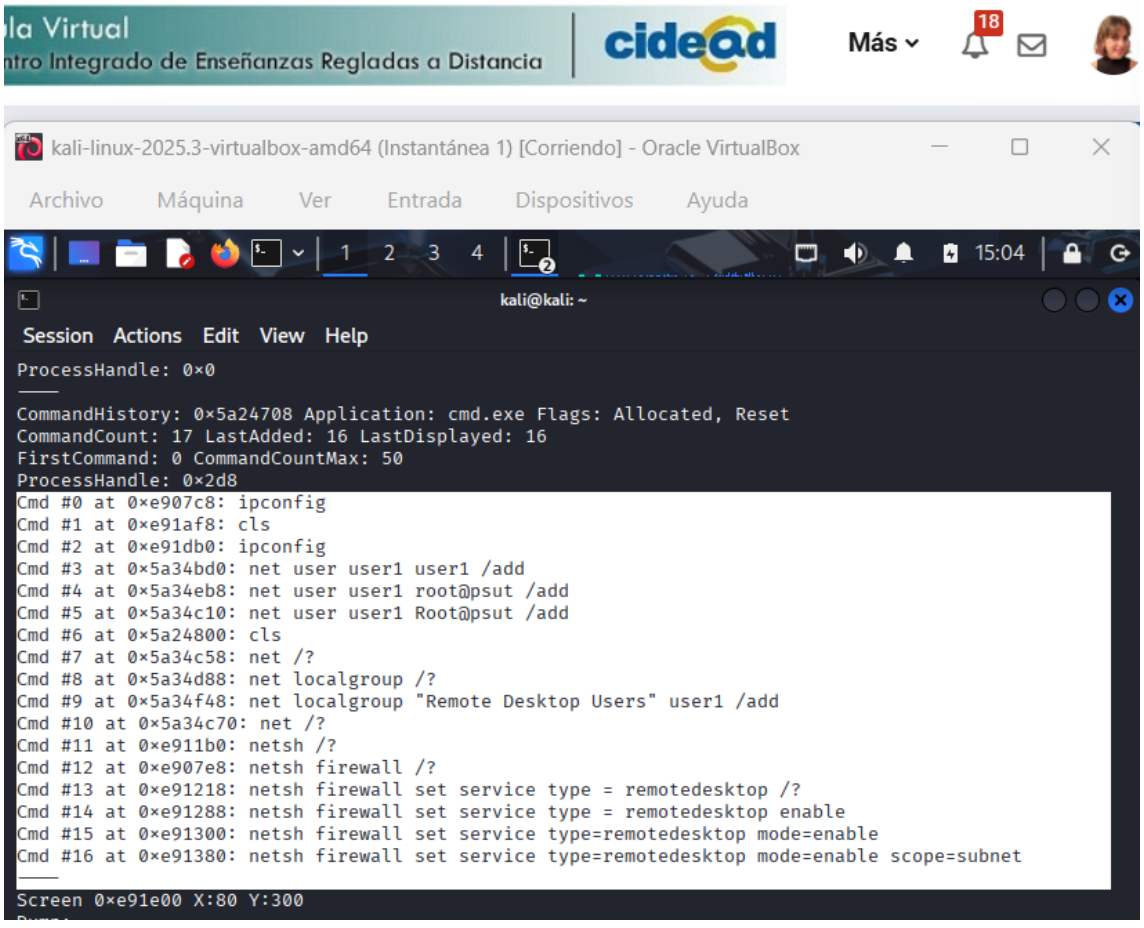
El plugin *consoles* combina la funcionalidad de *cmdscan* con información de los procesos de la consola. Es decir, extrae el historial de comandos ejecutados dentro de las consolas activas al momento del volcado. Se revela que dentro del proceso *1972* se ejecutaron comandos para abrir el firewall y permitir conexiones *remotedesktop*.



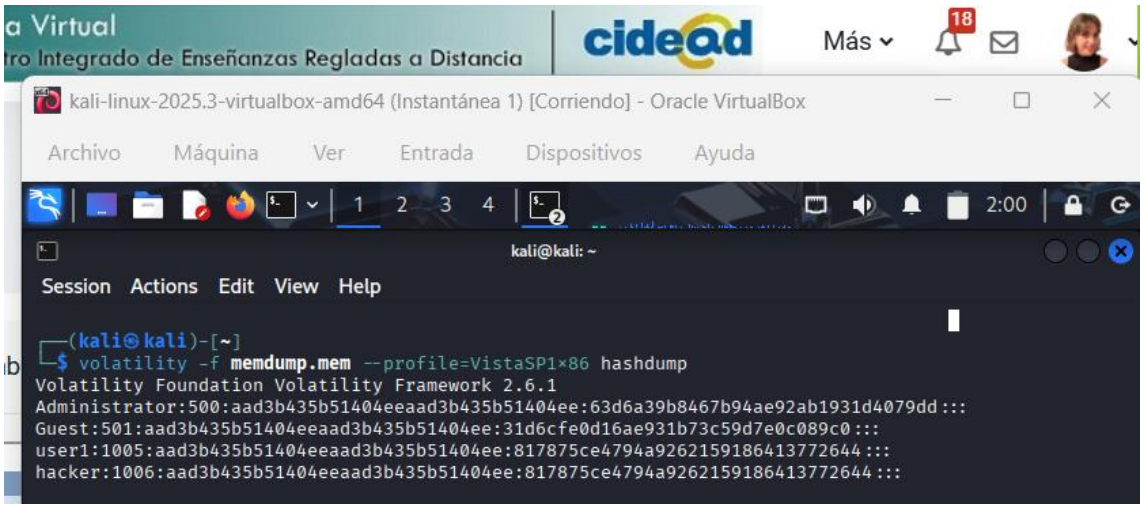


Así como también se ha encontrado evidencia de actividad maliciosa con la creación de un nuevo usuario *user1* con contraseña *user1* y es añadido al grupo *remotedesktop* para darle permisos en el firewall y acceder al escritorio remoto.


la Virtual
ntro Integrado de Enseñanzas Regladas a Distancia
cidead
Más
18
kali-linux-2025.3-virtualbox-amd64 (Instantánea 1) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
15:03
kali@kali: ~
Session Actions Edit View Help
HistoryBufferCount: 4 HistoryBufferMax: 4
OriginalTitle: Administrator: Command Prompt
Title: -
AttachedProcess: cmd.exe Pid: 612 Handle: 0×2d8

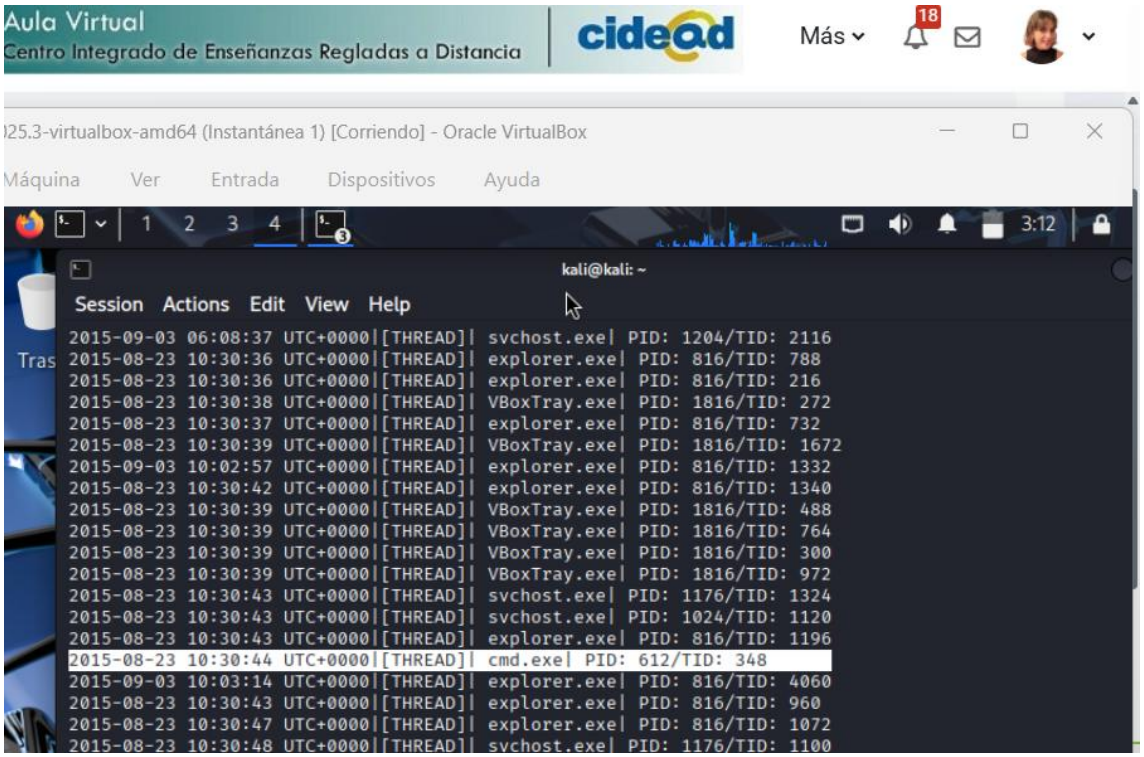

la Virtual
ntro Integrado de Enseñanzas Regladas a Distancia
cidead
Más
18
kali-linux-2025.3-virtualbox-amd64 (Instantánea 1) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
15:04
kali@kali: ~
Session Actions Edit View Help
ProcessHandle: 0×0
CommandHistory: 0×5a24708 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 17 LastAdded: 16 LastDisplayed: 16
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0×2d8
Cmd #0 at 0×e907c8: ipconfig
Cmd #1 at 0×e91af8: cls
Cmd #2 at 0×e91db0: ipconfig
Cmd #3 at 0×5a34bd0: net user user1 user1 /add
Cmd #4 at 0×5a34eb8: net user user1 root@psut /add
Cmd #5 at 0×5a34c10: net user user1 Root@psut /add
Cmd #6 at 0×5a24800: cls
Cmd #7 at 0×5a34c58: net /?
Cmd #8 at 0×5a34d88: net localgroup /?
Cmd #9 at 0×5a34f48: net localgroup "Remote Desktop Users" user1 /add
Cmd #10 at 0×5a34c70: net /?
Cmd #11 at 0×e911b0: netsh /?
Cmd #12 at 0×e907e8: netsh firewall /?
Cmd #13 at 0×e91218: netsh firewall set service type = remotedesktop /?
Cmd #14 at 0×e91288: netsh firewall set service type = remotedesktop enable
Cmd #15 at 0×e91300: netsh firewall set service type=remotedesktop mode=enable
Cmd #16 at 0×e91380: netsh firewall set service type=remotedesktop mode=enable scope=subnet
Screen 0×e91e00 X:80 Y:300

Con el plugin *hashdump* se extraen los hashes de las contraseñas de usuarios, entre los cuales se incluye el usuario hacker. Este usuario activa todas las alarmas ante actividad maliciosa.



¿CÓMO SE HAN EJECUTADO LOS COMANDOS?

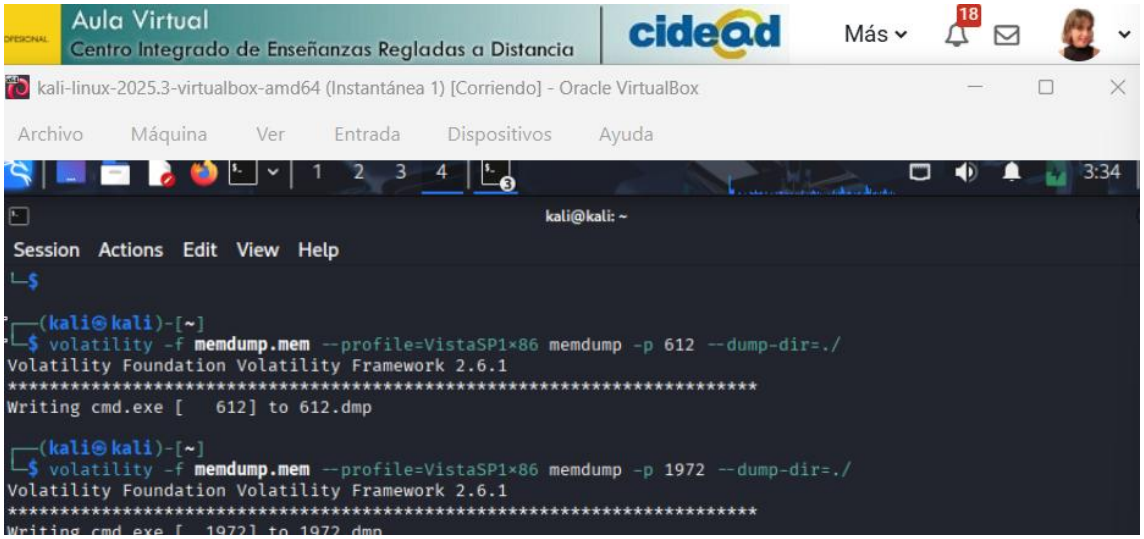
El atacante ejecutó los comandos mediante el *cmd.exe* con privilegios de administrador, de modo que debió tener acceso al equipo víctima. Con el plugin *timeliner* se puede observar un ejemplo claro de en qué momento exacto se ejecutaron los procesos, como es en el caso del primer *cmd.exe* que se ejecutó el 23 de agosto de 2015 a las 10:30:44.



¿QUÉ ACTIVIDAD MALICIOSA HAS VISTO?

Hasta ahora la actividad maliciosa que se ha observado es que el atacante mediante el *cmd.exe* y con privilegios de administrador, creó el usuario *hacker* con permisos y para abrir el firewall con conexiones remotas.

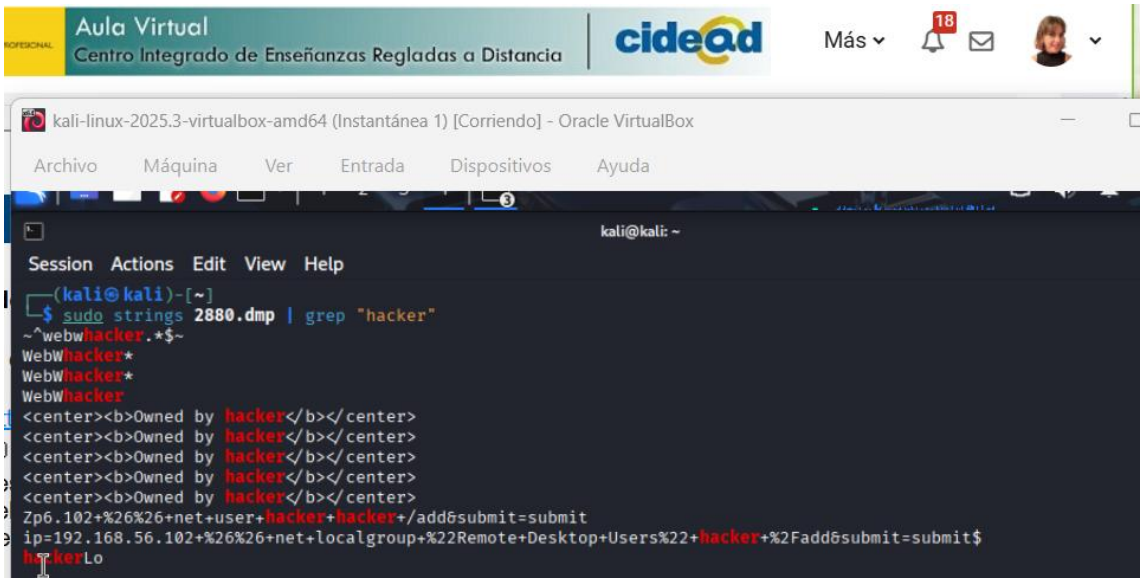
Pero para ir más allá, se analizarán los dos procesos *cmd* sospechosos vistos anteriormente con el plugin *memdump*.



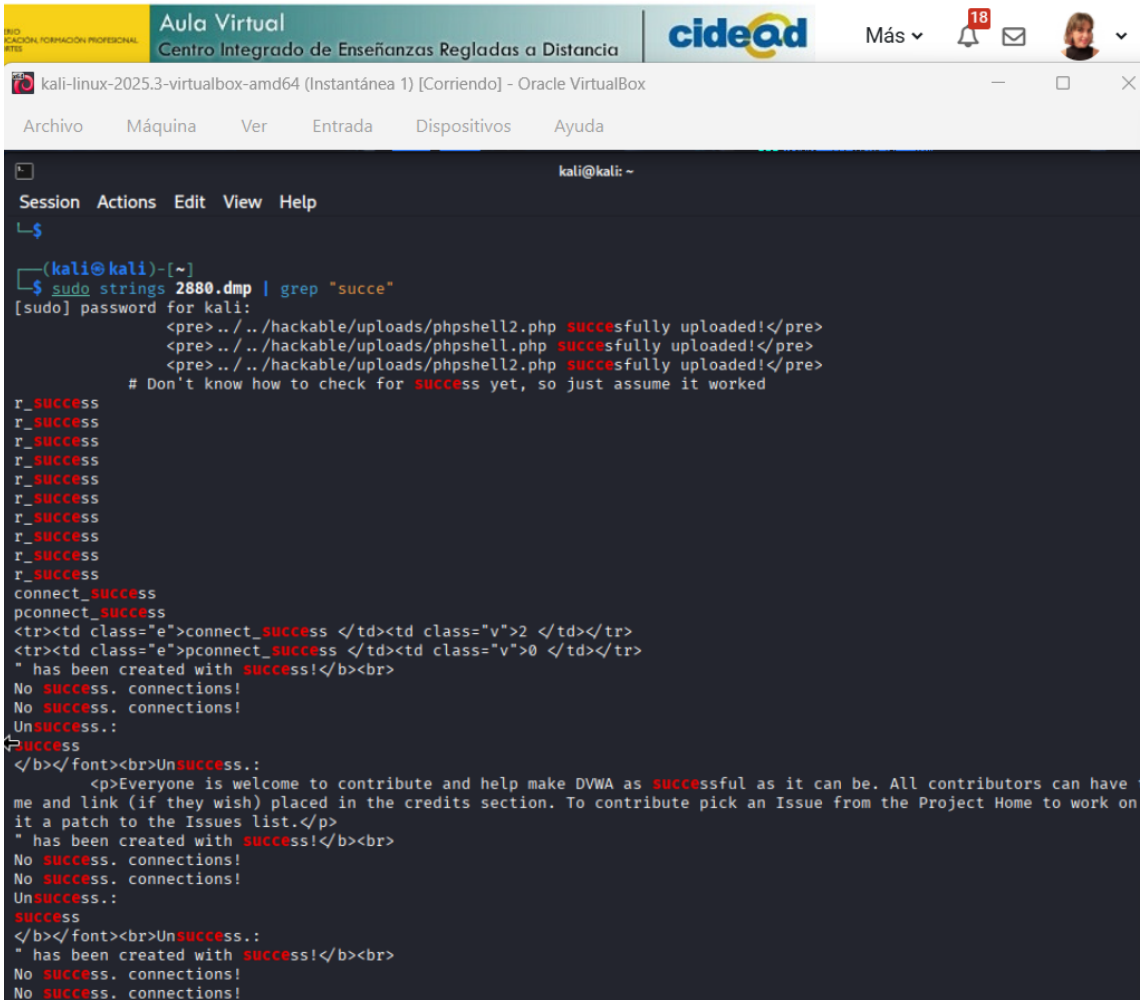
A continuación, se ejecuta el plugin *strings* para extraer todas las cadenas de texto legible del proceso *2880* y que se identificó como *httpd.exe*. Con *grep hacker*, el programa filtra por las líneas que contienen la palabra *hacker*.

Nota: para los procesos 612 y 1972 no se encontró ninguna cadena.

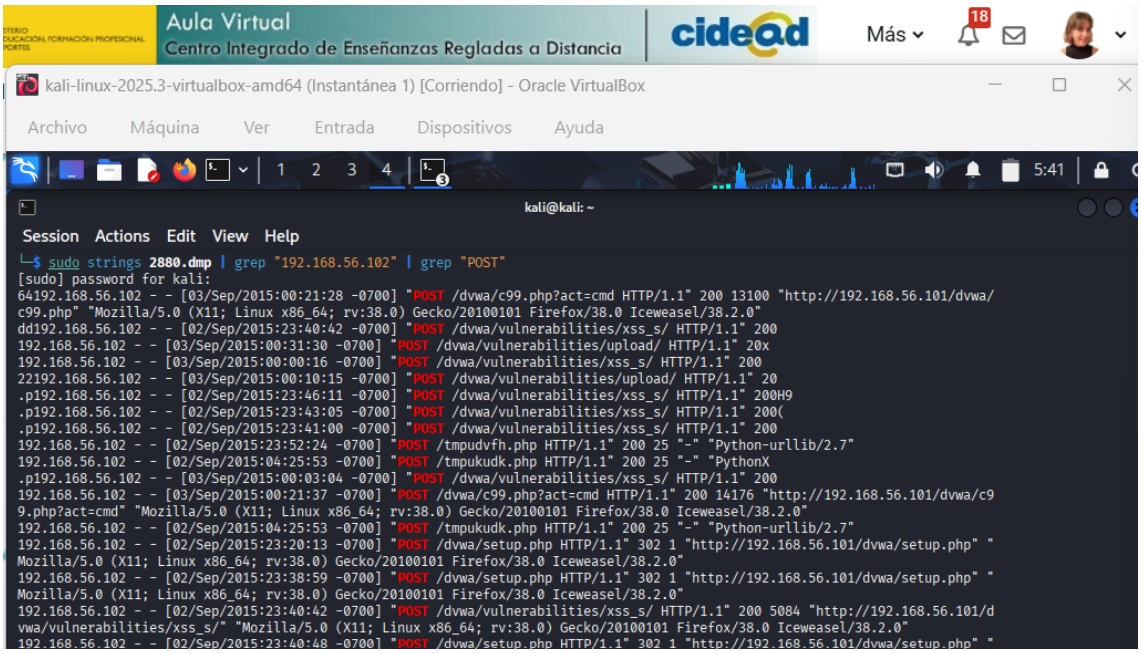
Este resultado indica que el atacante utilizó el servidor web *httpd.exe* para el ataque desde una IP privada 192.168.56.102.



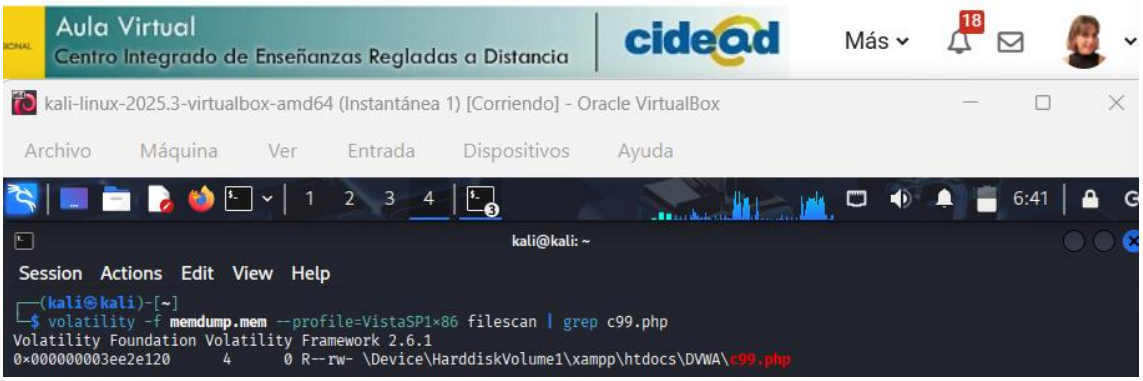
Por consiguiente, para comprobar si el servidor web devolvió algún mensaje de éxito después de que el atacante ejecutara sus comandos, se busca la cadena *succe*. Definitivamente el atacante subió un webshell *phpshell2.php* al servidor web. De modo que con este script, consigue abrir una consola de comandos remota.



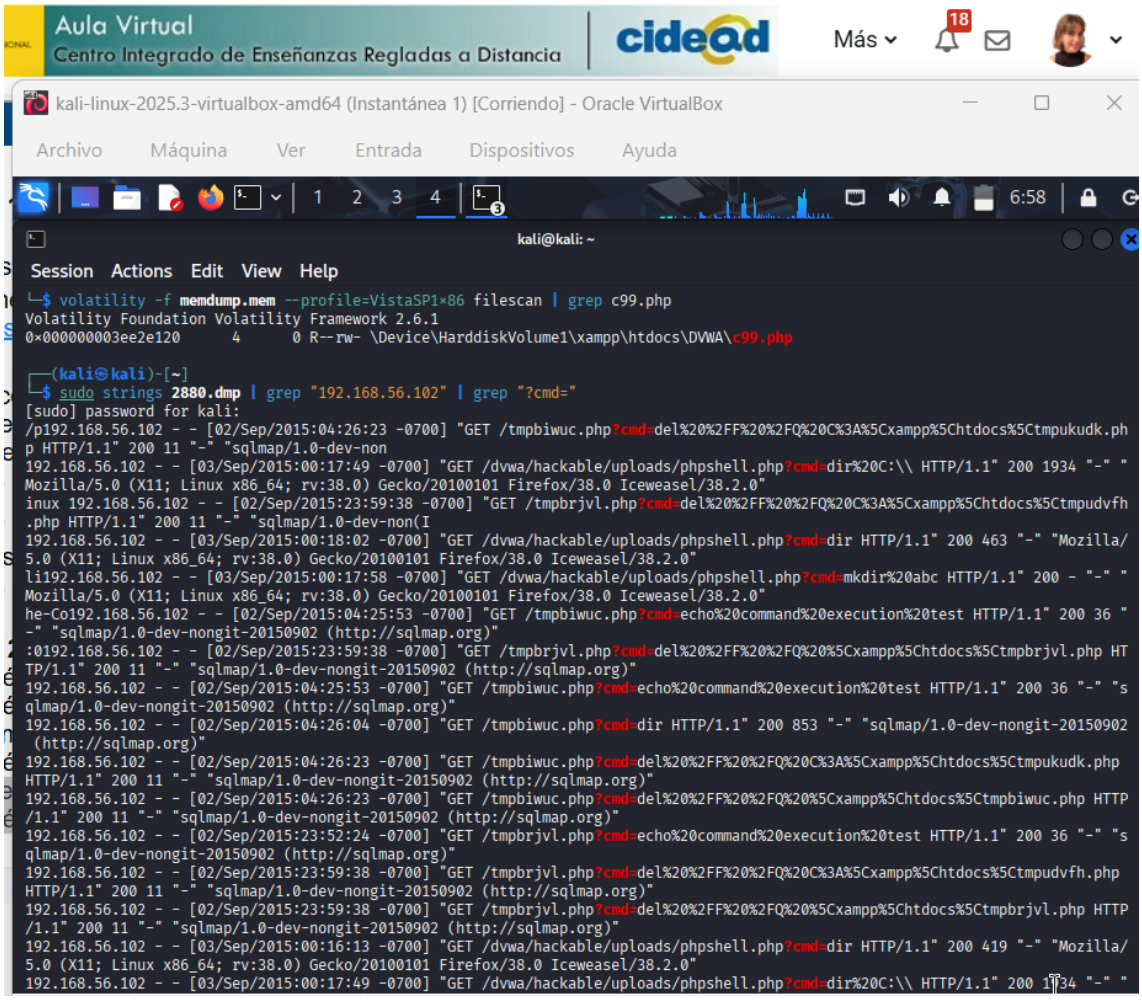
Una vez localizada la IP desde la que atacó el cibercriminal, se filtra por la cadena *192.168.56.102* para rastrear su actividad en el servidor web. Además, se utiliza el método *POST* para enviar datos desde el cliente al servidor y comprobar que el atacante utilizó su dirección IP para enviar al servidor *httpd.exe* comandos y exploits.



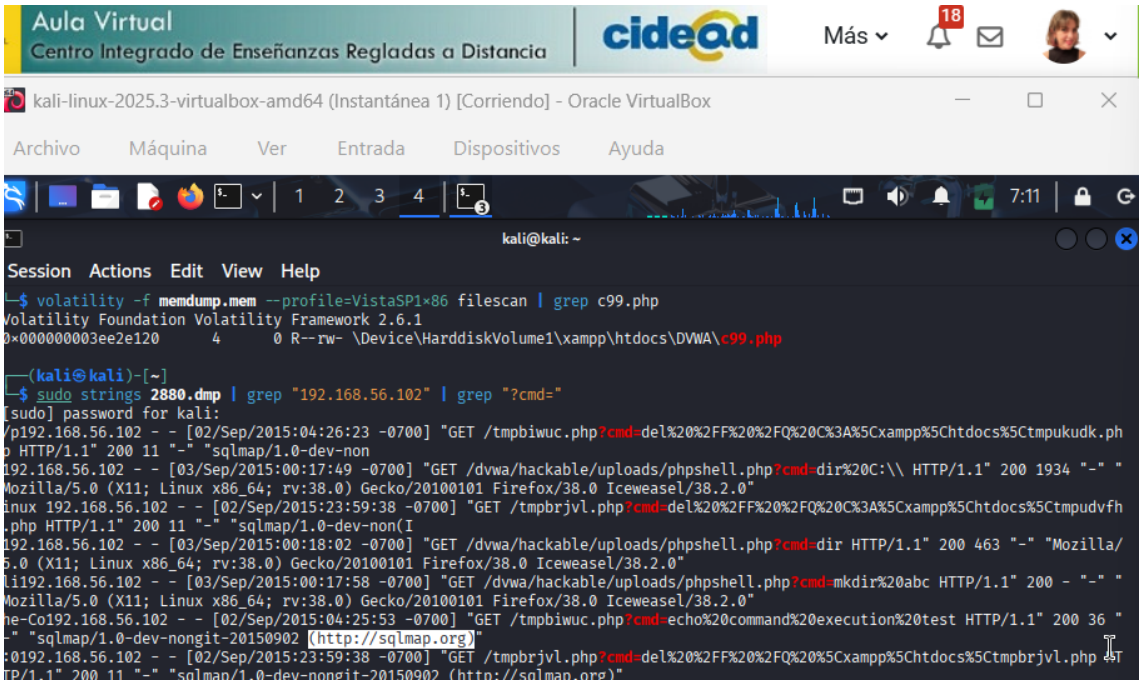
Se observa que el atacante ha interaccionado con la puerta trasera haciendo una petición *POST* contra el fichero *c99.php*. Mediante un *filescan | grep c99.php* se confirma que el archivo *c99.php* se subió a la aplicación vulnerable DVWA dentro de XAMPP.



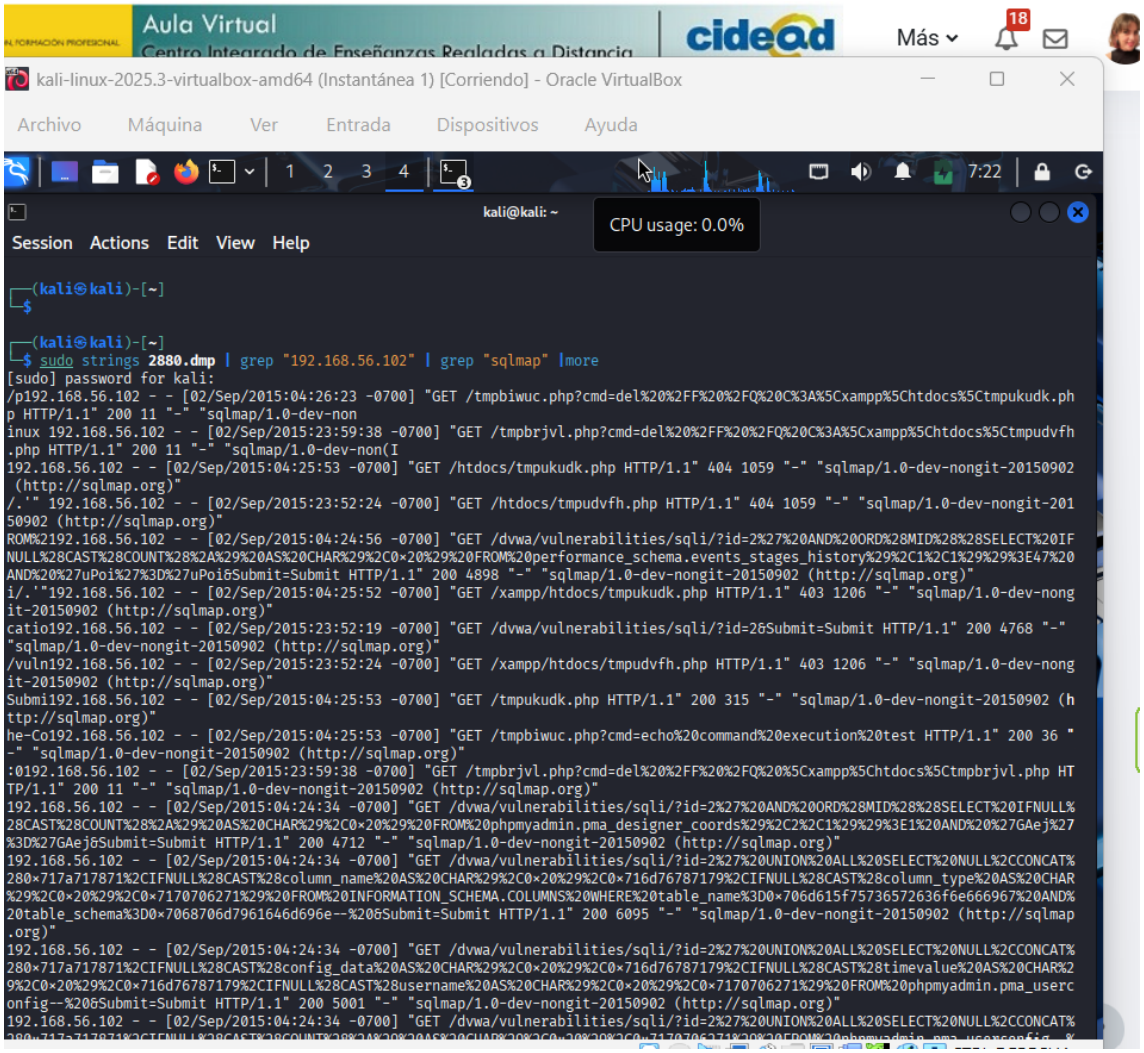
Se vuelve a ejecutar el plugin *strings* filtrando por *?cmd=* para revelar la interacción entre el atacante y la web shell.



La salida muestra peticiones *GET* y *POST* provenientes de la IP del atacante. En las respuestas *GET* aparece la url *sqlmap.org* confirmando que el atacante utilizó la herramienta *sqlmap* para detectar y explotar vulnerabilidades de inyección SQL.

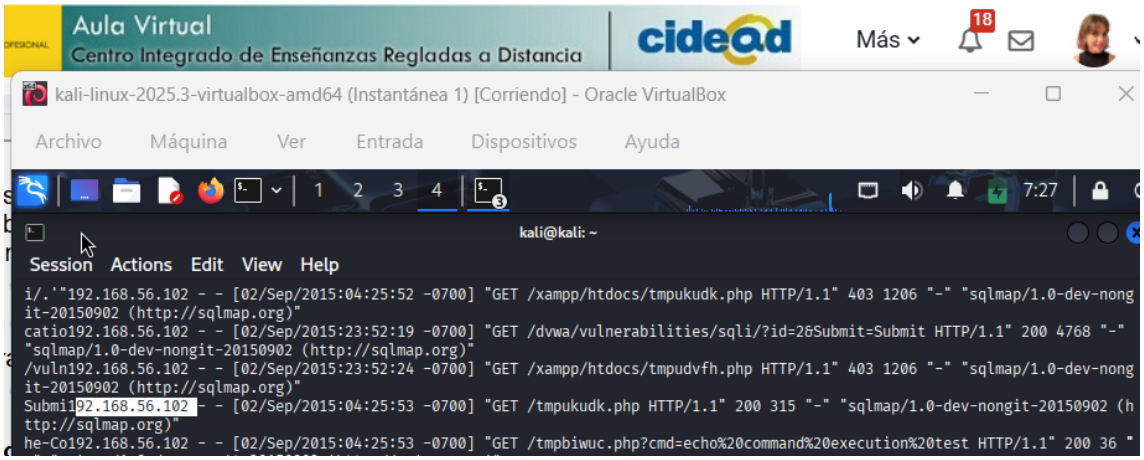


Finalmente se vuelve a filtrar por la cadena *sqlmap* para revelar las peticiones *http* y se observan sentencias SQL de tipo *SELECT*, confirmando que el atacante realizó consultas contra el servidor *mysql*.



¿PUEDES IDENTIFICAR DESDE QUE IP VINO EL ATAQUE?

El ataque vino desde la IP 192.168.56.102.



¿QUÉ TIPO DE ATAQUE PUDO SER? ¿QUÉ TIPO DE MALWARE SE HA ENCONTRADO?

El tipo de ataque se denomina SQL Injection. Se identificó un malware *phpshell2.php* y *c99.php* lo que permitió al atacante ejecutar comandos a través de un navegador web a través de un servidor vulnerable o comprometido.

BIBLIOGRAFÍA

Volatility Foundation. (s.f.). *Command Reference*. GitHub: Volatility Foundation. Recuperado el 14 de diciembre de 2025, de https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#pslist

Ergo, Hackers. (2021, 8 de marzo). *VOLATILITY // Cómo hacer un análisis de memoria y determinar si una maquina esta infectada* [Video]. YouTube. http://www.youtube.com/watch?v=RFYbevw6hxI

Behackerpro. (2021, 3 de septiembre). *Encontrando Secretos en la memoria del computador con Volatility Instalación No Standalone en Win10* [Video]. YouTube. http://www.youtube.com/watch?v=iU9mqB4h3Tg

Hackavis. (2025, 6 de abril). *Como Usar Volatility para Analizar Memoria RAM en Windows. [Guía Completa]* [Video]. YouTube. http://www.youtube.com/watch?v=QeE6asCnD6E

https://github.com/volatilityfoundation/volatility/wiki/Command-Reference#pslist