



Tarea 1

# AFI-01

ANÁLISIS FORENSE INFORMÁTICO (Análisis de Memoria RAM)

JOSÉ ANTONIO MORENO ARANDA



## Caso práctico



[Pixabay](#) (Dominio público)

evidencia.

María está trabajando en un caso y ha recibido la imagen de memoria RAM de un servidor que ha tenido un comportamiento anómalo.

Un compañero sobre el terreno ha capturado la memoria RAM de la máquina antes de que la apagasen y se la ha enviado al laboratorio para ser analizada por María.

El coordinador de la investigación le ha hecho varias preguntas a María que deberá responder sobre la

- **Apartado 1: Analiza la memoria RAM**

Lo ideal es usar la herramienta Volatility (versión 2), la tienes disponible en [Volatility](#)

- La memoria RAM está disponible en este enlace ([https://mega.co.nz/#!1UpjkTab!RP\\_QeooLaxA7bixLxkHLIqhWKfQ9G\\_0M58NSUchRn68](https://mega.co.nz/#!1UpjkTab!RP_QeooLaxA7bixLxkHLIqhWKfQ9G_0M58NSUchRn68) )
- Descomprime la memoria RAM
- Debes de ejecutar Volatility desde consola ya sea en Windows o Linux
- Tienes varias guías de vídeo que te pueden ayudar en el proceso:
  - <https://www.youtube.com/watch?v=RFYbevW6hxl>
  - <https://www.youtube.com/watch?v=iU9mqB4h3Tg>
- Otras herramientas que te pueden ser útiles
  - Floss: <https://github.com/mandiant/flare-floss>

- **Apartado 2: Contestando a las preguntas**

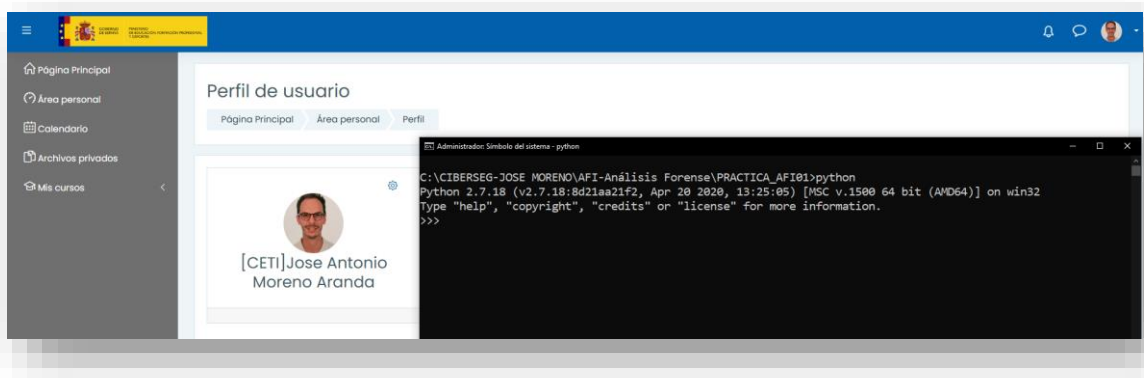
- ¿Qué pasaría si se hubiera apagado este servidor?
- ¿Qué tipo de comandos ha ejecutado el cibercriminal? ¿Qué sugiere?
- ¿Cómo se han ejecutado los comandos?
- ¿Qué actividad maliciosa has visto?
- ¿Puedes identificar desde que IP vino el ataque?
- ¿Qué tipo de ataque pudo ser? ¿Qué tipo de malware se ha encontrado?

## APARTADO 1: ANALIZA LA MEMORIA RAM

- **Proceso de Instalación Python**
  - Realizaremos las comprobaciones en el CMD como Administrador

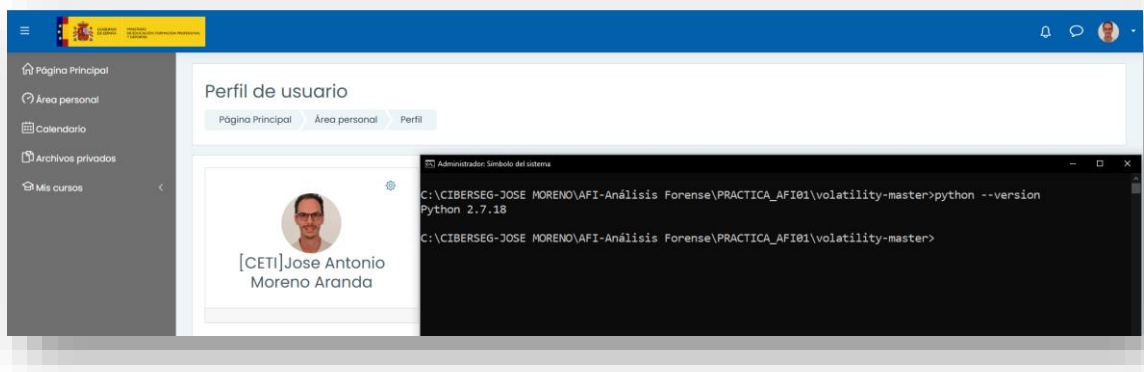
Instalación de Python 2.7.18 para el uso correcto de Volatility, usaremos el CMD con permisos de Administrador

- Comando: `python`



Usaremos el comando Python version para determinar la versión instalada de Python

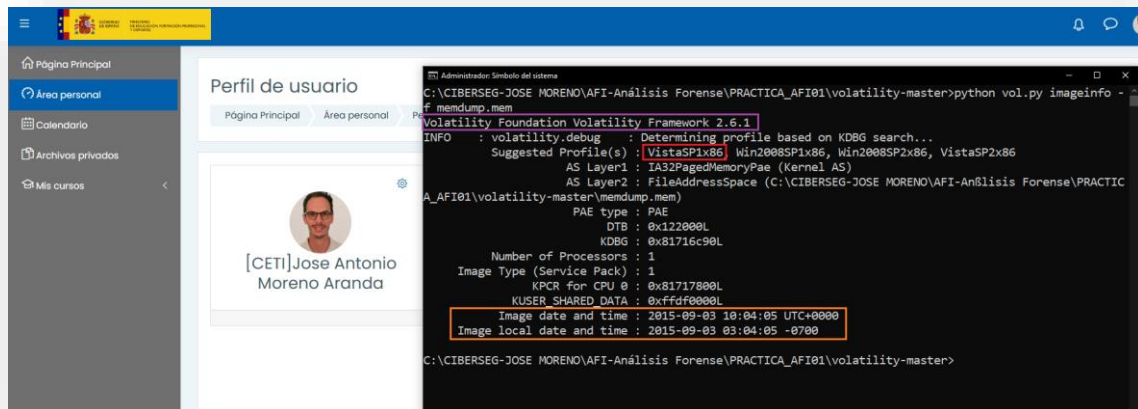
- Comando: `python --version`



Ejecutaremos el comando para el volcado de *memdump.mem* y obtener indicios en la información de la memoria. Este comando también nos indicará información importante a nivel de análisis forense, por ejemplo, el sistema operativo

- `python vol.py imageinfo -f memdump.mem`

Realizaremos las pruebas sobre el perfil **VistaSP1x86**, que indicamos en **rojo** en la captura, marcamos en **naranja** la fecha y hora exactas cuando se capturó el volcado de memoria. Se indica en **morado** la versión usada de Volatility.



## APARTADO 2: CONTESTANDO A LAS PREGUNTAS:

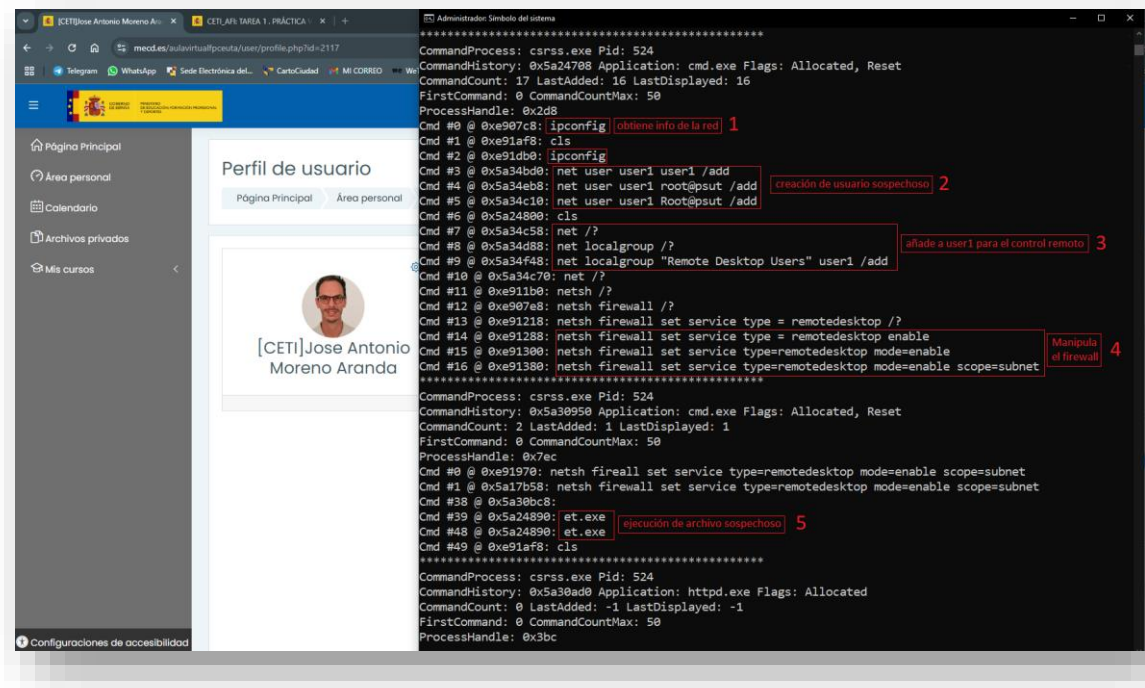
**¿Qué pasaría si se hubiera apagado este servidor?**

- Si el servidor se hubiera apagado antes de realizar la captura de memoria RAM, toda la información volátil se habría perdido. Dificultaría la capacidad de reconstruir los incidentes en gran parte.



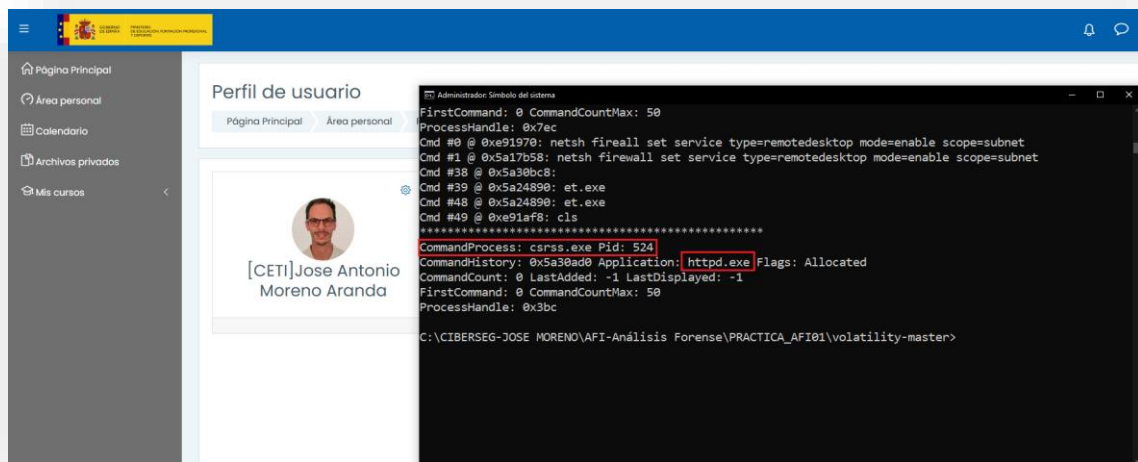
## ¿Qué tipo de comandos ha ejecutado el cibercriminal? ¿Qué sugiere?

- Usaremos el comando cmdscan para determinar cuáles fueron los últimos comandos sospechosos que se realizaron.
  - `python vol.py cmdscan -f memdump.mem --profile=VistaSP1x86`



Los comandos ejecutados por el cibercriminal:

1. Comando: **ipconfig** → Obtiene la información sobre la configuración de la red del sistema.
2. Comando: **net user user1 user1 /add , net user user1 root@psut /add , net user user1Root@psut /add** → Crea usuario sospechoso, el usuario user1
3. Comando: **net /? , net localgroup /? , net localgroup "Remote Desktop Users" user1 /add** → Le da permisos a user1 para acceder mediante escritorio remoto
4. Comando: **netsh firewall set service type = remotedesktop enable , netsh firewall set service type=remotedesktop mode=enable , netsh firewall set service type=remotedesktop mode=enable scope=subnet** → Permite Firewall aceptar conexiones en Escritorio Remoto
5. Comando: **et.exe**, repite la ejecución de un archivo sospechoso
6. Comando: **csrss.exe** Pid:524 → Ejecuta el archivo **httpd.exe** (imagen abajo) también lo consideraremos como potencialmente sospechoso.

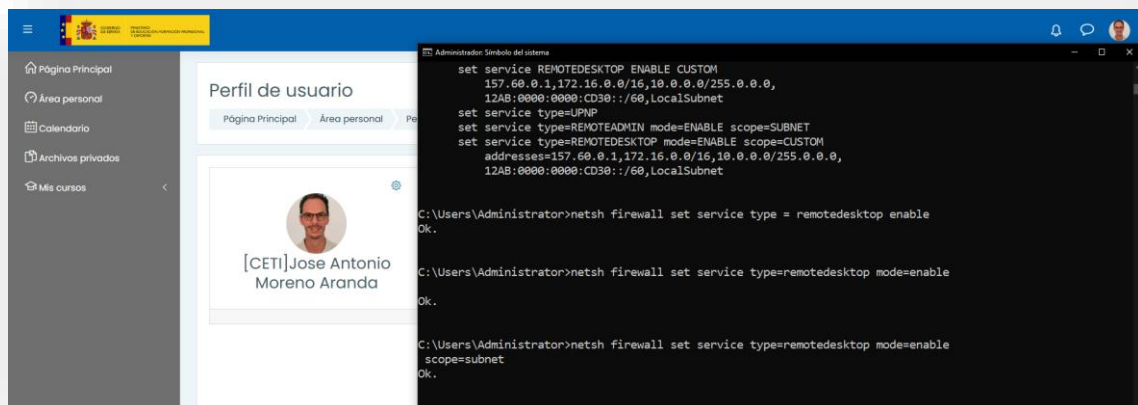


El archivo encontrado en la memoria llamado httpd.exe es sospechoso y podemos dar por hecho que las intenciones no son éticas ni profesionales.

También ejecutamos el comando siguiente como admin en el CMD:

- `python vol.py -f memdump.mem --profile=VistaSP1x86 consoles`

Este comando es utilizado en Volatility para analizar el contenido de las consolas (cmd) que estaban activas en el momento de la captura de memoria, nos proporciona un contexto.

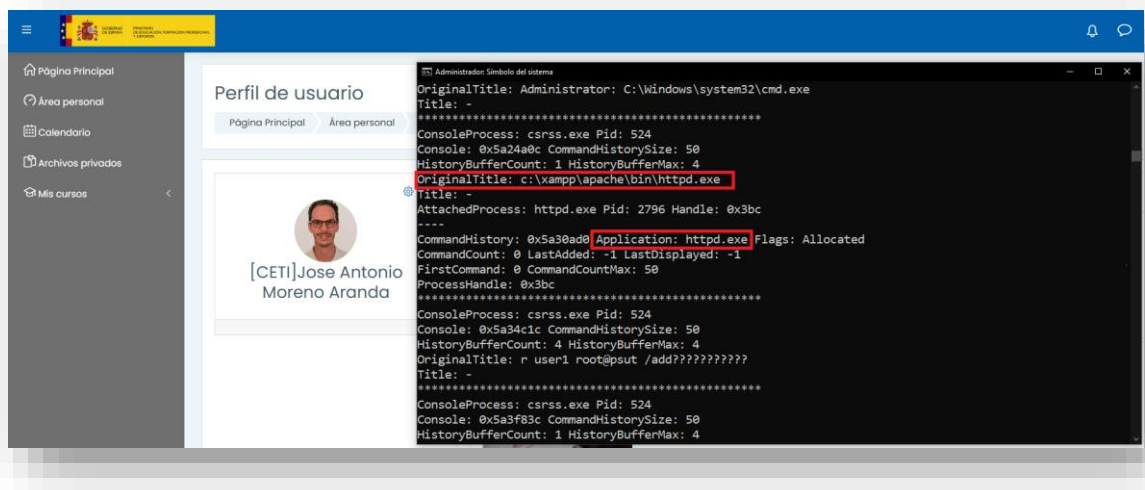


### ¿Cómo se han ejecutado los comandos?

Desde el punto de vista del cibercriminal los comando que se ejecutaron fueron realizados desde el cmd.exe, preparando el entorno de red a su disposición, mediante este comando:

- `python vol.py consoles -f memdump.mem --profile=VistaSP1x86`

Este comando nos permite ver la actividad en la consola. Podemos observar en la captura como está vinculado el archivo **httpd.exe** como ejecutable del Apache HTTP Server que es **xampp** a su vez.



Xampp es un software para instalación y configuración de un entorno de desarrollo web, su nombre es acrónimo: X indica multiplataforma, A indica servidor Apache, M indica MariaDB-MySQL, P indica PHP y P indica Perl.



Para listar los procesos activos (padres e hijos) en Volatility, detectar las relaciones entre procesos, utilizamos este comando:

- `python vol.py pstree -f memdump.mem --profile=VistaSP1x86`

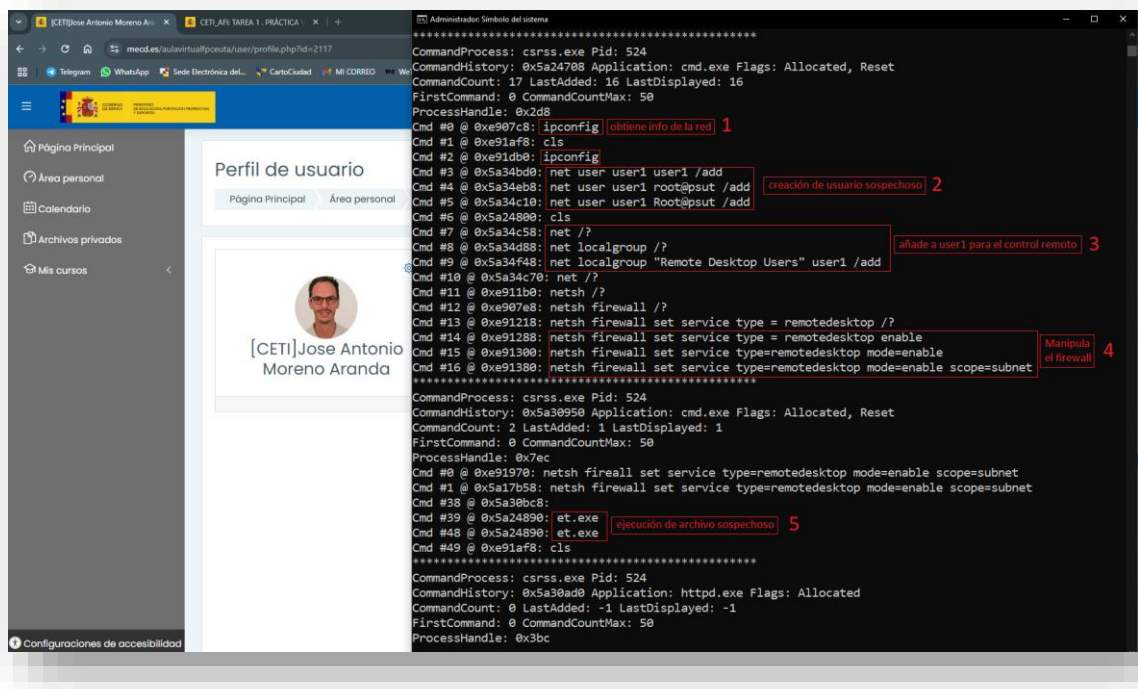
Process Name	PID	PPID	Session ID	Architecture	Start Time	End Time
csrss.exe	484	472	11	400	2015-08-23 20:27:22 UTC+0000	
explorer.exe	816	676	22	756	2015-08-23 10:30:34 UTC+0000	
VBoxTray.exe	1816	816	8	114	2015-08-23 10:30:38 UTC+0000	
FTK Imager.exe	2120	816	13	382	2015-09-03 10:03:37 UTC+0000	
xampp-control.e	2768	816	2	119	2015-08-23 10:32:17 UTC+0000	
httpd.exe	2796	2768	1	92	2015-08-23 10:32:21 UTC+0000	
httpd.exe	2880	2796	155	483	2015-08-23 10:32:26 UTC+0000	
FileZillaServer	2856	2768	5	35	2015-08-23 10:32:25 UTC+0000	
mysqld.exe	2804	2768	23	570	2015-08-23 10:32:23 UTC+0000	
cmd.exe	612	816	1	72	2015-08-23 10:30:44 UTC+0000	
cmd.exe	1972	816	1	19	2015-09-02 09:28:30 UTC+0000	
System	4	0	105	504	2015-08-23 20:27:20 UTC+0000	
smss.exe	420	4	4	28	2015-08-23 20:27:20 UTC+0000	
csrss.exe	524	516	9	536	2015-08-23 20:27:28 UTC+0000	
winlogon.exe	560	516	4	125	2015-08-23 20:27:28 UTC+0000	

## ¿Qué actividad maliciosa has visto?

Se dan crean nuevos usuarios, se dan permisos a estos, se indaga sobre la configuración de red del sistema, se habilita el control remoto, se altera el Firewall, se ejecute archivos maliciosos.

Desde mi punto de vista el sistema se afectado; la presencia de httpd.exe y el uso de servicios como MySQL y FileZilla para el almacenamiento y transferencia de datos de forma maliciosa.

Indicios de que el atacante utilizo las técnicas para comprometer el sistema y facilitar el acceso remoto.

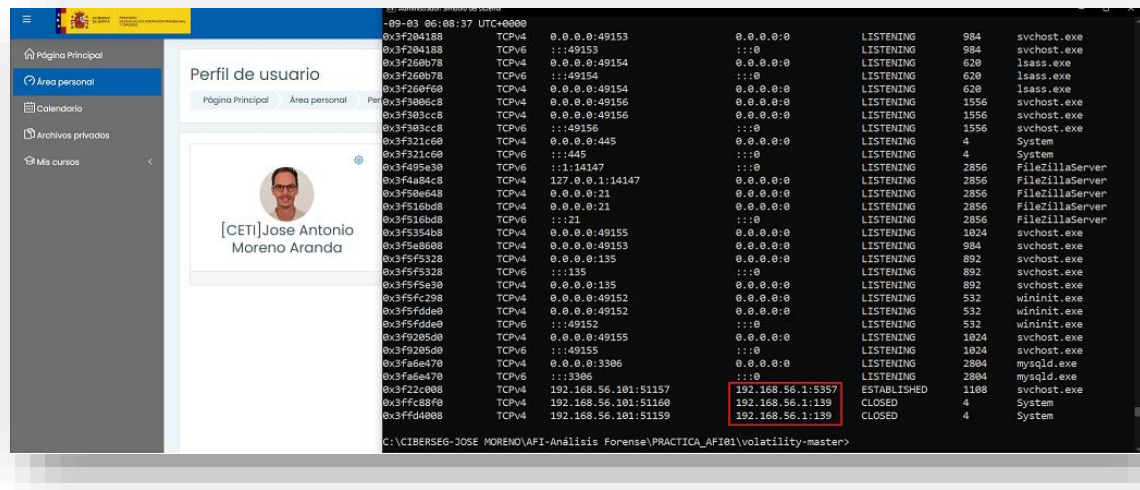


## ¿Puedes identificar desde que IP vino el ataque?

El comando utilizado en este caso para detectar la IP desde donde vino el ataque, es:

- `python vol.py netscan -f memdump.mem --profile=VistaSP1x86`

Considero que es la IP: **192.168.56.1**



Las razones son, 192.168.56.1 tiene conexión activa con svchost.exe, los puertos abiertos en este caso son el 80 que es el HTTP y el puerto 443 que es el HTTPS

## ¿Qué tipo de ataque pudo ser? ¿Qué tipo de malware se ha encontrado?

Parece un ataque persistente y dirigido al sistema, hay indicios de que se crean usuarios maliciosos los cuales se incluyen para el control remoto, facilitándoles la configuración a su favor del Firewall con esto el atacante puede tener acceso continuo a nuestra máquina.

Se hace mal uso de los servicios de xampp, por ej: el archivo **httpd.exe** potencialmente malicioso que hace referencia a Apache, MySQL y PHP; puertos abiertos (listening) 80-443-3306, explotando estos puertos con **backdoors** para su beneficio.

Parece que hay comunicación externa con un servidor externo, 192.168.52.1 la considero vinculante, destacar la conexión activa con archivo **svchost.exe**

**Combina técnicas de modificación de privilegios, backdoor y modificación de red que comprometería al sistema.**

