**INFORMACIÓN DEL SISTEMA**

Mediante el software OSForensics se ha obtenido la siguiente información del sistema:

<https://drive.google.com/file/d/17GeX8rcvSNEHLNfx4DZevmI5tYC8IEvb/view?usp=share_link> (descargar y abrir con html)

También se puede obtener información sobre el sistema con WRR mediante el archivo SYSTEM.

<https://drive.google.com/drive/folders/1xRBN_7SGzPg34jdxnhq7gOt3yLueXbW-?usp=share_link>

**OBTENCIÓN Y ANÁLISIS DE VOLCADO DE MEMORIA RAM**

Se ha obtenido un volcado de la memoria RAM mediante Dumpit, con el objetivo de analizarlo posteriormente con Volatility (v2.6.1). Para ello se va a utilizar una máquina virtual con Ubuntu 20.04.3 con el software Volatility instalado.

Para el análisis del volcado de memoria, se seguirán los siguientes pasos:

1. Enviar el volcado de memoria RAM de la máquina WS01 a la máquina linux con Volatility, mediante la utilización de carpetas compartidas.
2. Una vez tengamos el volcado de memoria, se debe obtener el perfil de el volcado para su análisis, mediante el plugin **imageinfo.**

****

1. Una vez obtenido el perfil, procederemos al análisis mediante los plugins que ofrece Volatility:

* Procesos en ejecución: **pslist, pstree, psxview**
* Bibliotecas relacionadas con procesos: **dlllist**
* Drivers en ejecución: **modscan**
* Información de subprocesos: **threads**
* Comandos ejecutados: **cmd\_scan, consoles**
  + No se ha obtenido información mediante estos comandos, posiblemente porque no se ejecutó ninguno.
* Ficheros relacionados con procesos: **handles**
* Alteraciones en flujos normales de una aplicación: **apihooks**
* Listado de hashes de usuarios: **hashdump**
* Información sobre nodos vad: **vadinfo**
* Artefactos de red en el volcado de memoria: **netscan**
* Servicios en ejecución: **svcscan**
* Privilegios: **privs**
* Identificadores de seguridad: **getsids**
* Logins RDP: **sessions**

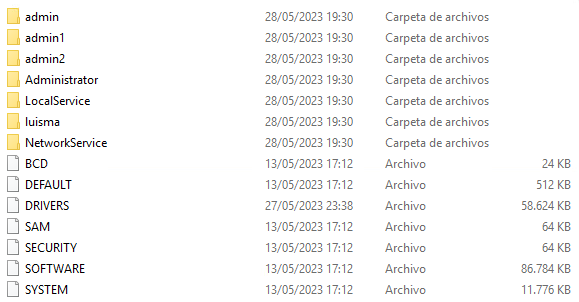
Los resultados obtenidos están disponibles en:

<https://drive.google.com/drive/folders/1FpXxy9ddxqm0nXGZiobfLYlJl2dndMhO?usp=share_link>

Se ha analizado la información obtenida y no parece haber nada raro.

**OBTENCIÓN Y ANÁLISIS DE ARCHIVOS DE REGISTRO**

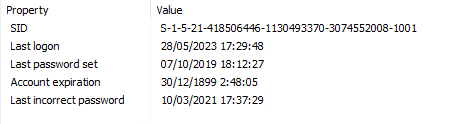
Mediante el software WRR se han obtenido los ficheros de registro de la máquina WS01 para su posterior análisis.Se han obtenido los siguientes archivos:



Fichero **SAM:**

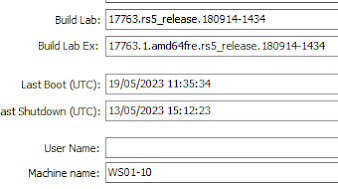
****

Información sobre usuario ‘admin’:



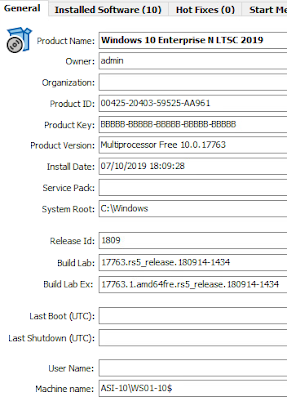
Fichero **SYSTEM:**

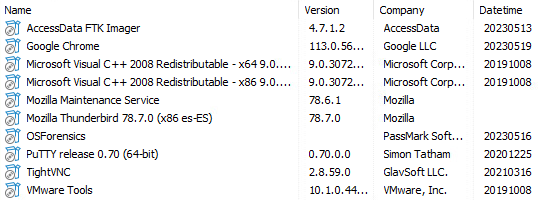
Obtenemos información sobre el equipo

****

Fichero **SOFTWARE**

Información sobre la máquina, programas instalados, etc.





**OBTENCIÓN DE ARTEFACTOS DE WINDOWS**

Listas MRU / Última actividad del sistema

Para la obtención de las listas MRU se ha utilizado el software LastActivityView y se han exportado los resultados a un archivo en formato html para su posterior análisis.

<https://drive.google.com/file/d/1D3My3widQZF1WxbE-5-Srv_1ViM-EvI1/view?usp=share_link>

Prefetchs

<https://drive.google.com/file/d/1Vzr2d3i6u-aLqepqu-S_GFj3smx7b0Jk/view?usp=share_link>

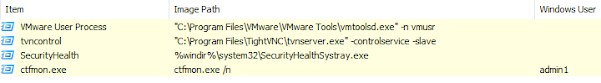
Eventos EVTX y logs del sistema

<https://drive.google.com/file/d/1mSVbFJWvXBnOHx9MagDuvM1mhXrYMLxl/view?usp=share_link>

**OTROS**

Listado de comandos automáticos

Mediante OSForensics se han obtenido los comandos automáticos del sistema:



El comando **ctfmon.exe** está asociado al usuario ‘admin1’, por lo que puede haber sido configurado por un posible atacante.

El objetivo de ctfmon.exe es el de monitorear de forma constante todas las ventanas activas, además de proporcionar soporte de servicio de entrada y también texto para reconocimiento de voz, además de esto: Reconocimiento de escritura. Teclado. Traducción y muchas otras funciones.

Se va a proceder a analizar el ejecutable con la herramienta Volatility, siguiendo los siguientes pasos:

1. Al obtener el listado de procesos, filtramos con **grep** para obtener información sobre el proceso:



PID: 3500 - PPID: 450 - Segmento de memoria del proceso: 0xffff8f0ec66e3080

1. Ejecutamos el plugin **pstree** para obtener el proceso padre de ctfmon.exe.



El proceso ctfmon.exe es hijo del proceso svchost.exe, que tiene como padre el proceso con PID 600, es decir, el proceso services.exe, hijo del proceso wininit.exe, que se encarga del proceso de inicialización de Windows.

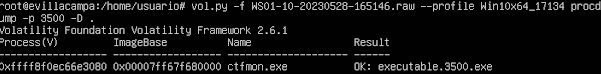


1. Ahora analizaremos si existe código malicioso en el proceso **ctfom.exe.** Para ello, usaremos el plugin **malfind**:



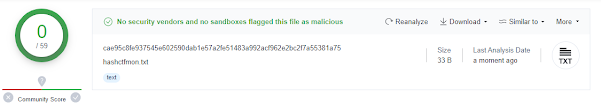
No muestra ningún resultado, por lo que no existe código malicioso.

1. Ahora vamos a extraer el proceso y a obtener el hash, para posteriormente subir el resultado a virustotal para que lo analice:



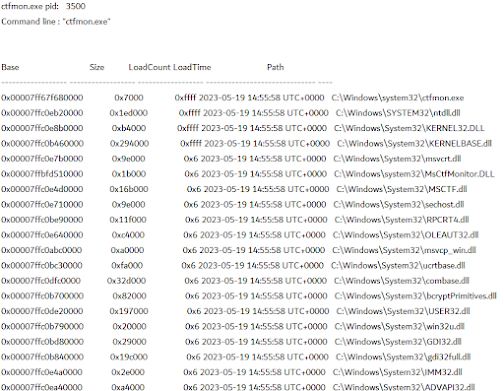






No es detectado por ninguno de los motores de virustotal.

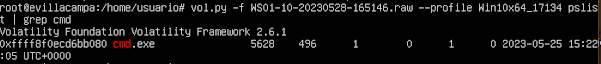
1. Mediante el plugin dlllist podemos obtener las bibliotecas asociadas al proceso. Algunas son:



1. Tras los resultados obtenidos, podemos llegar a la conclusión de que no es un proceso dañino.

Otro proceso a analizar es el **cmd.exe:**

1. Obtención de información del proceso



PID: 5628

PPID: 496

Segmento de memoria del proceso: 0xffff8f0ecd6bb080

Árbol del proceso:







1. Vamos a realizar un volcado del proceso con el objetivo de extraer cadenas de texto legibles para realizar búsquedas. Utilizaremos el plugin memdump y el comando strings:

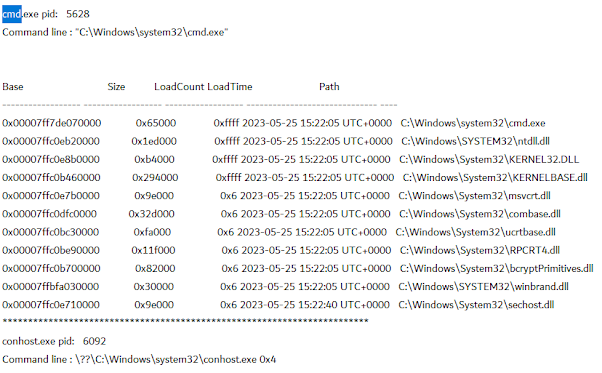




Para visualizar el fichero se puede ejecutar el comando **less** o podemos pasar el fichero a la máquina anfitrión y abrirlo con el bloc de notas.

No aparece información relevante.

1. Bibliotecas asociadas al proceso:



Logs de conexiones RDP al equipo

Mediante el análisis del listado de archivos MRU, se observaron eventos sobre conexiones RDP al equipo desde la IP **10.220.9.112 por el puerto 63562.**

**Conexiones RDP 1:** [**https://drive.google.com/file/d/1ztJWIILhFas-oT2RyGn2SR47qUzLWfvU/view?usp=share\_link**](https://drive.google.com/file/d/1ztJWIILhFas-oT2RyGn2SR47qUzLWfvU/view?usp=share_link)

**Conexiones RDP 2:**

[**https://drive.google.com/file/d/1nebjrfQ4czNjeo4OI5SNqlr0mhLS0dx5/view?usp=share\_link**](https://drive.google.com/file/d/1nebjrfQ4czNjeo4OI5SNqlr0mhLS0dx5/view?usp=share_link)

Podemos obtener más información sobre las conexiones RDP, ejecutando el siguiente script en powershell:

$RDPAuths = Get-WinEvent -LogName 'Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational' -FilterXPath '<QueryList><Query Id="0"><Select>\*[System[EventID=1149]]</Select></Query></QueryList>'

[xml[]]$xml=$RDPAuths|Foreach{$\_.ToXml()}

$EventData = Foreach ($event in $xml.Event)

{ New-Object PSObject -Property @{

TimeCreated = (Get-Date ($event.System.TimeCreated.SystemTime) -Format 'yyyy-MM-dd hh:mm:ss K')

User = $event.UserData.EventXML.Param1

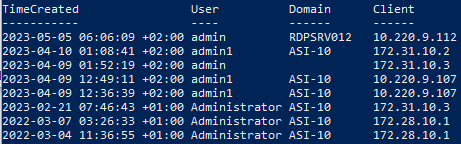
Domain = $event.UserData.EventXML.Param2

Client = $event.UserData.EventXML.Param3

}

} $EventData | FT

Últimas conexiones RDP:



Conexiones TCP al equipo

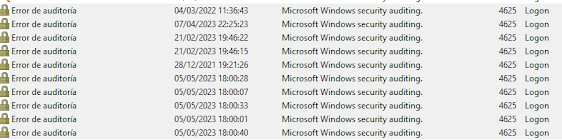
Si accedemos al Administrador de Tareas y vamos a *Rendimiento → Abrir monitor de recursos → Red → Conexiones TCP* vemos las conexiones TCP activas:



**svchost.exe** es un proceso de servicio compartido que Windows usa para cargar archivos DLL. Aparece repetidas cuando se han analizado los procesos del volcado de memoria con Volatility.

Intentos de acceso fallidos al sistema

Se ha accedido al visor de eventos de windows con el objetivo de ver los intentos de acceso fallidos en el sistema. Para ello, se debe acceder a *Registros de Windows → Seguridad* y filtrar por la columna *ID del evento.* Una vez ordenados por Id, buscaremos los que tengan el valor 4625 en esta columna.

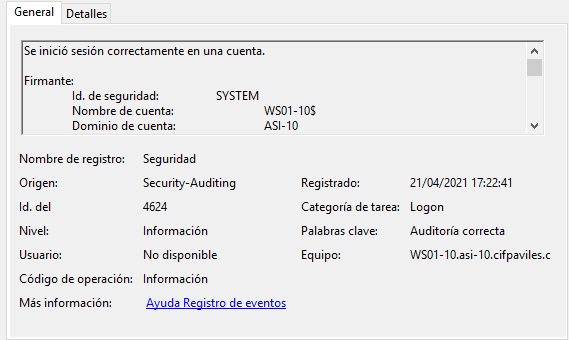


No aparece información relevante.

Acceso al registro: <https://drive.google.com/file/d/1xJbXlvCS5DF8MHf-yYcGM_ZepekpfhAS/view?usp=share_link>

Registro de accesos al sistema

Aparecen accesos al equipo con el usuario ‘WS-01$’



Se perdió el acceso a la máquina al ser cambiada la contraseña por un posible atacante. Para volver a conseguir acceso, se volvió a cambiar la contraseña mediante el proceso explicado en el siguiente enlace:

[Reset Administrator's password in Windows Server 2012 R2 (forgot password)](https://www.youtube.com/watch?v=BW1yZfjdyRY)