## **Hash del fichero**

Ejecutamos CertUtil -hashfile Win10\_PC001.vmdk SHA256

SHA256 hash: **4446e9c42345a32fa78a8ce20834faa047a3b161eba986f894d2230fcf6b0cbe**

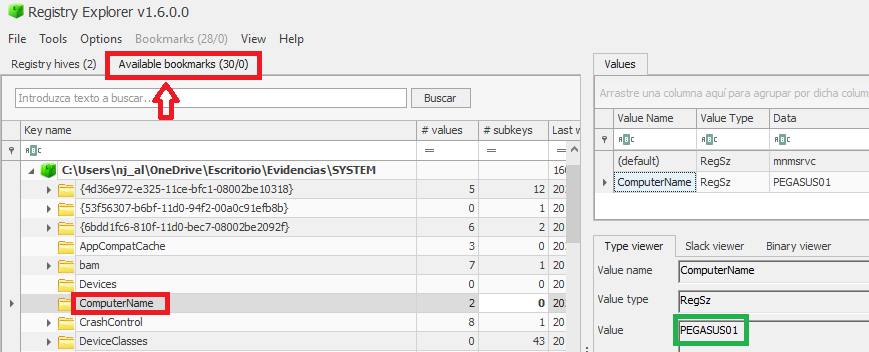
## 

## **Nombre de la maquina**

Encontrar el nombre de la máquina de la que se está realizando el análisis.

Utilizando la herramienta *AccessDataFTK* vamos a la carpeta */root/Windows/system32/config* , extraemos el archivo *SYSTEM.*

Con *Registry Explorer,* cargamos el archivo *SYSTEM*, vamos a la pestaña *Available boomarks* y en *ComputerName* nos aparece el nombre de la máquina, **PEGASUS01**.



## **Descarga fichero de control remoto y Fecha descarga**

Encontrar el nombre del fichero .exe de un programa de control remoto que se ha descargado el usuario y la fecha de su descarga

Utilizamos la herramienta *RegRipper* con el archivo *SYSTEM*. Tenemos que encontrar el nombre del fichero .exe de un programa de control remoto que se ha descargado el usuario.

Buscamos en carpetas de descargas:

* C:\Users\...Downloads\
* C:\Users\...\AppData\Local\Temp\
* C:\Users\...\AppData\Roaming\
* C:\Users\...\Desktop\



**Evidencia:**

**C:\Users\IEUser\Downloads\TeamViewer\_Setup\_x64.exe [2022-04-29 17:11:34]**

* Este archivo fue descargado directamente por el usuario.
* **TeamViewer** es un conocido programa de **control remoto**, usado tanto legítimamente como en campañas maliciosas.
* Está en la carpeta **Downloads**, lo que confirma que **fue descargado manualmente**.

## **Conexión programa control remoto**

Existe la sospecha de que se hayan conectado al equipo desde un programa de control remoto.

Hay que encontrar el ID desde el que se conecta el atacante.

Con *AccesData FTK Imager* nos dirigimos a la carpeta */root/ProgramFiles/TeamViewer ,* descargamos los archivos de esa carpeta e indagamos en el archivo *Connections\_incoming.txt.*

* La **primera columna** es el **TeamViewer ID remoto del atacante: 765418952**
* El equipo comprometido se llama **WIN-MORENIN** y el usuario es **IEUser**.

## **Fecha de ejecución programa de control remoto**

Encontrar la fecha en la que se ejecuto Team Viewer en el equipo.

Buscamos *Connection incoming* en el archivo *TeamViewer15\_Logfile.log* y hallamos la fecha en la que se ejecutó: **29/04/2022**



## **Ficheros eliminados**

Encontrar el fichero .zip eliminado.

Extraemos el archivo *$Logfile* de *root* con *AccessDataFTK.*

Interfaz de usuario gráfica, Texto, Aplicación

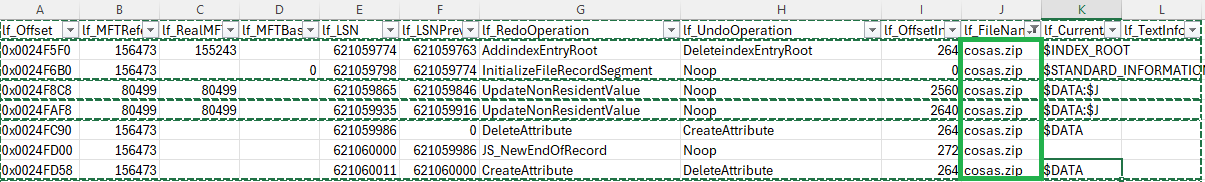
El contenido generado por IA puede ser incorrecto.

Utilizamos la herramienta LogFileParser para extraer de forma legible la información de *$Logfile.*

Accedemos al archivo *Logfile.csv* que se genera y observamos que hay un archivo que cumple todas las condiciones de que ha sido eliminado.

**Operaciones de eliminación registradas**:

* En la fila con *lf\_RedoOperation="DeleteAttribute"* en *lf\_CurrentAttribute="$DATA",* se muestra que el atributo de datos del archivo **"cosas.zip"** fue eliminado.
* También aparece una entrada con *lf\_RedoOperation="DeleteindexEntryRoot"* en *lf\_CurrentAttribute="$INDEX\_ROOT",* indicando que el archivo fue eliminado del índice del sistema de archivos.

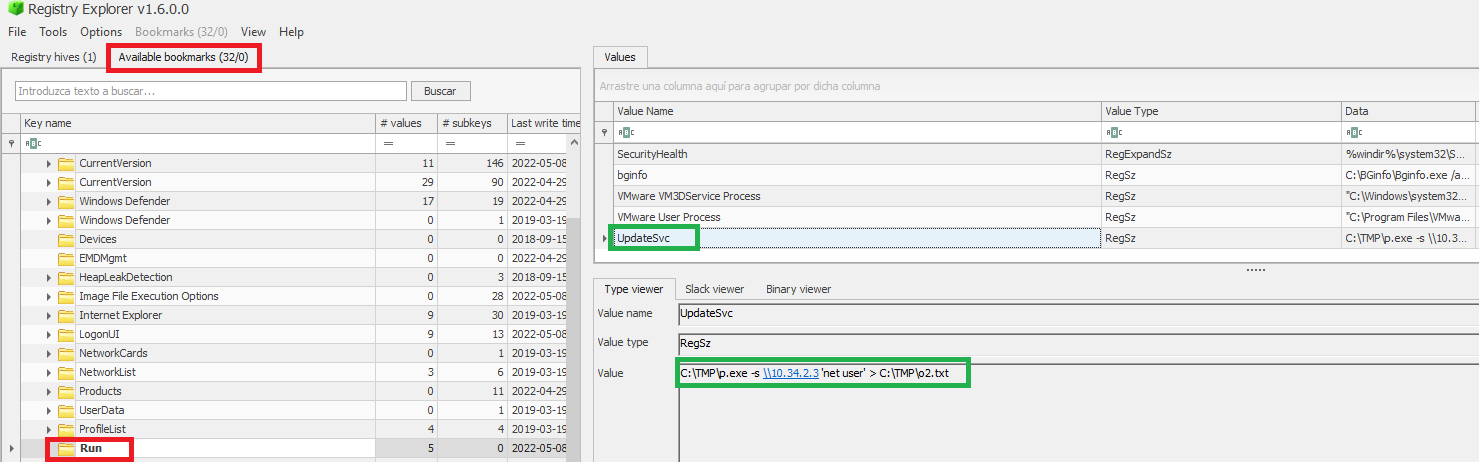


## **Ficheros maliciosos**

En la máquina se han encontrado varios ficheros maliciosos.

En que carpeta (solamente el nombre de la carpeta) se encuentran dichos ficheros ?

Con el programa *Registry Explorer* cargarmos el *hive SOFTWARE* de la carpeta */Windows/system32/config,* accedemos a *Run* y observamos que hay un fichero malicioso.



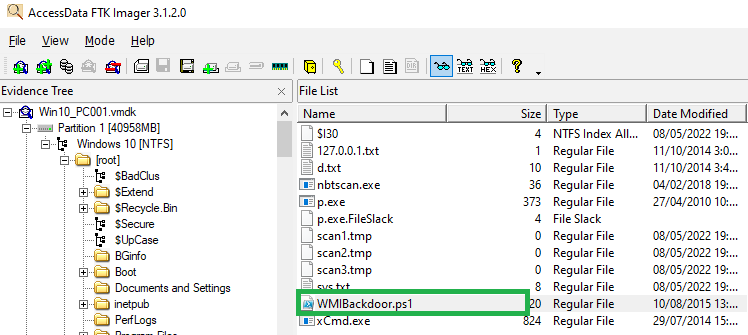
La información que sacamos es:

* **c:\TMP\p.exe -s** → Se ejecuta un ejecutable p.exe con el argumento -s.
* **\\10.34.2.3 'net user'** → Parece que p.exe está intentando conectarse a la IP 10.34.2.3 y ejecutar el comando net user, que lista los usuarios del sistema.
* **> C:\TMP\o2.txt** → Guarda la salida del comando en C:\TMP\o2.txt.

## **Powershell maliciosa**

Encontrar script de powershell malicioso con extensión .ps1

Buscamos en la carpeta TMP donde se encontraba el archivo malicioso de la anterior pregunta y encontramos **WMIBackdoor.ps1**



**Opción 2: Usar Mimikatz**

Si tienes acceso a Windows y puedes ejecutar **Mimikatz**, usa:

mimikatz

CopiarEditar

privilege::debug

lsadump::sam

Esto también te dará los hashes NTLM.

## **Contraseñas débiles**

Existen sospechas de que la contraseña del usuario IEUser es una contraseña débil, lo que ha permitido al atacante acceder a ella.

Indicar la contraseña del usuario.

Con *mimikatz* ejecutamos el comando:

mimikatz # privilege::debug

mimikatz # lsadump::sam /system:"C:\Users\nj\_al\OneDrive\Escritorio\Evidencias\SYSTEM" /sam:"C:\Users\nj\_al\OneDrive\Escritorio\Evidencias\SAM"

Buscamos el HASH:

Texto

El contenido generado por IA puede ser incorrecto.

Y con la página <https://crackstation.net/> comprobamos si la contraseña ha sido “crackeada”.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

## **Conexión RDP y Puerto de conexión máquina atacante**

Se ha detectado actividad sospechosa en la red, indicar la IP desde la que se ha conectado a la máquina por RDP y el puerto sobre el que se produce la conexión

Nos descargamos el archivo *Security.evtx* de la ubicación *C:\Windows\System32\winevt\Logs\* con el *AccessData FTK*

Desde el CMD ejecutamos *EvtxECmd.exe* y corremos el siguiente comando:

EvtxECmd.exe -f "C:\Users\nj\_al\OneDrive\Escritorio\Evidencias\Security.evtx" --csv "C:\Users\nj\_al\OneDrive\Escritorio\Evidencias\salida"

Filtramos los datos para los siguientes EventID:

* ID 4624 → Inicio de sesión exitoso -> No se observan conexiones
* ID 4648 → Se usaron credenciales explícitas -> Se hallan resultados



