IMF Smart Education

Plantilla de respuestas
Ejercicio análisis forense

Módulo	ANÁLISIS FORENSE
Nombre y apellidos	David Fernández Alejo
Fecha entrega	

Para la resolución del ejercicio se deberá responder a las siguientes preguntas **sobre esta plantilla.** Será necesario atender a los siguientes puntos:

- Contestar a las preguntas en el orden establecido.
- Limitarse a contestar a las preguntas planteadas mediante una respuesta directa que posteriormente se deberá argumentar y desarrollar con detalle así como utilizar, cuando proceda, las evidencias facilitadas para el análisis
- El ejercicio se puede resolver bien analizando los resultados de la ejecución de la herramienta WLR que se incluyen en el fichero comprimido, bien analizando el disco facilitado del equipo víctima (mediante una herramienta forense, tipo Autopsy, Caine o similar). Ambas opciones son válidas. Para la opción de análisis con herramienta forense no es necesario saber la cuenta de administrador del equipo víctima.
- Como orientación, el ejercicio debe tener una extensión comprendida entre 10 y 15 páginas.

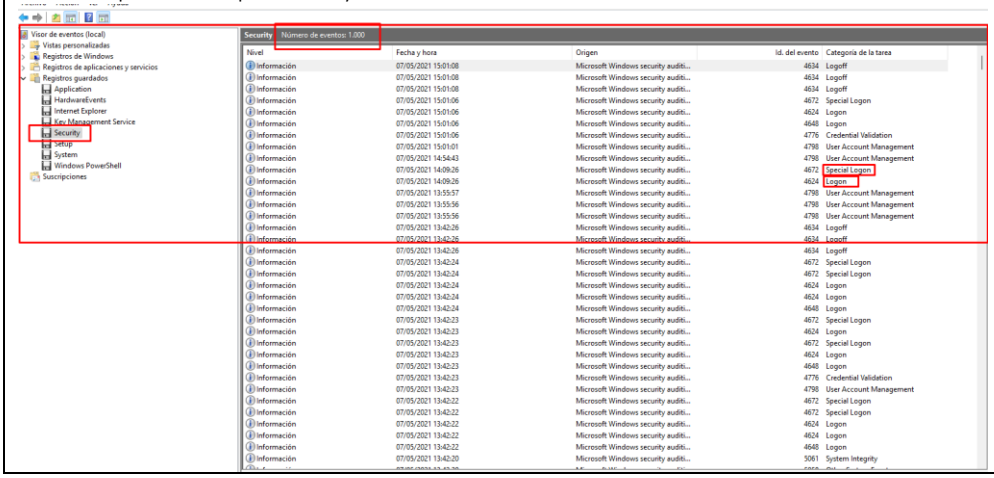
Pregunta 1 (2 puntos):

¿Cómo, cuándo y desde dónde accedió el intruso al servidor? Indique el detalle de las evidencias (archivo, evento, etc.) de las que se deduce esta información.

Respuesta:

En primer lugar, para poder realizar un analisis de los datos , se importarán los distintos eventos al visor de eventos de Windows para poder comprobar los eventos de tipo Security y comprobar los distintos accesos al servidor.

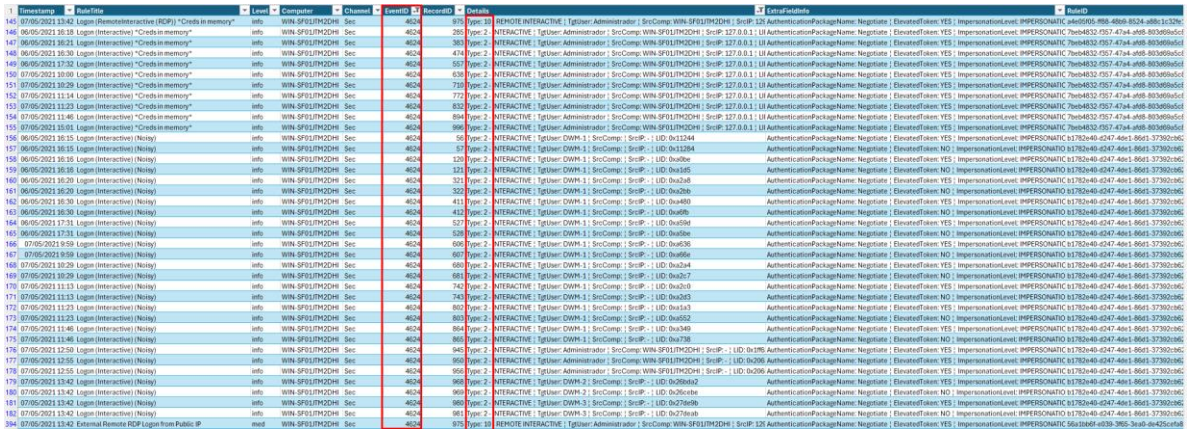
Como se puede comprobar hay numerosos eventos:



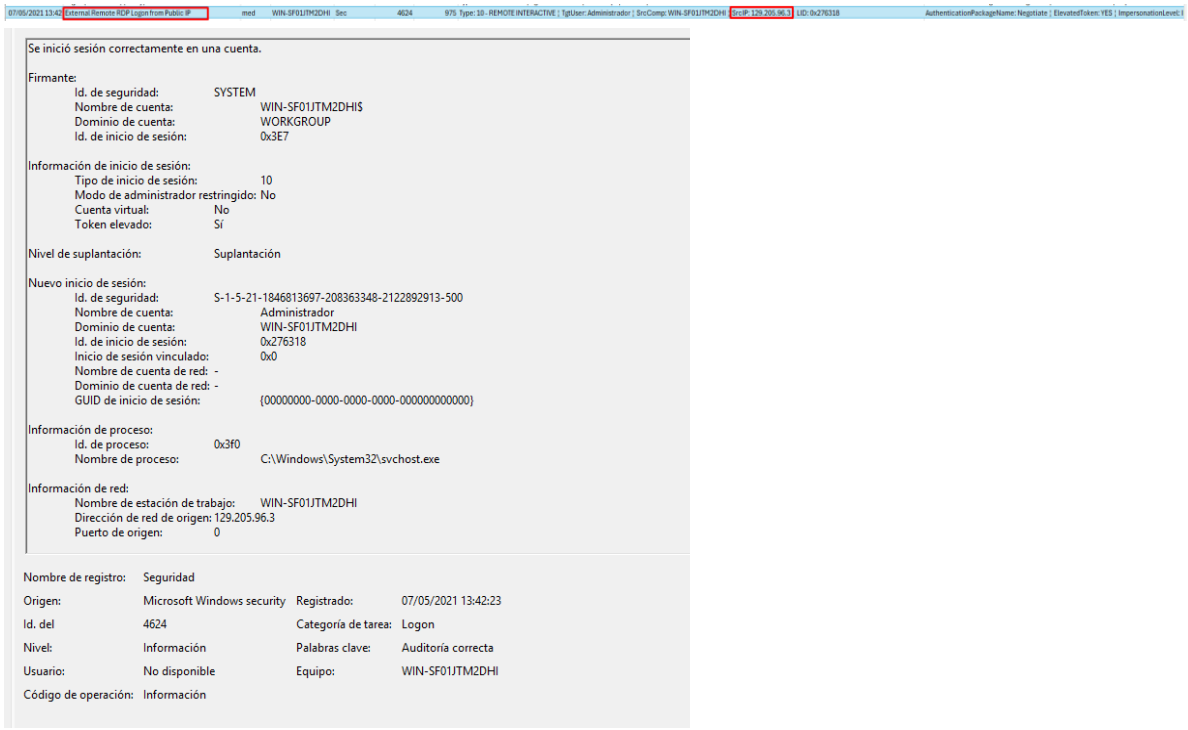
Para poder filtrar los eventos y ver la información de una manera mas visual, se utilizará la herramienta hayabusa, para exportar los distintos eventos a un csv.

Como se puede observar, en el reporte que nos da la herramienta nos indica el número de accesos, así como los eventos sospechosos.

Posteriormente, se filtrará por los eventos 4624 que son los inicios de sesión, que además tengan un id 2 (interactivo, acceso local) y 10 (acceso remoto, por ejemplo, RDP).



Como se puede observar hay numerosos accesos de este tipo al servidor, pero según el enunciado de la práctica, se indica: "... se cree que pudo haber sido un trabajador descontento del departamento de informática. Este trabajador podría conocer la dirección IP privada del servidor y conectarse a él.". Es por ello por lo que el acceso de 13:42:23 sería el acceso vía IP pública desde la IP remota indicada en el evento.



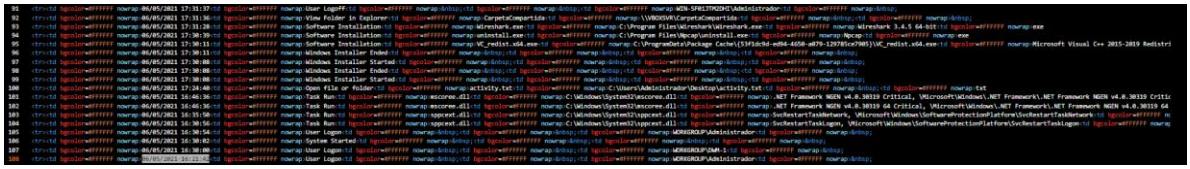
Este es el evento asociado al acceso vía RDP del usuario Administrador desde la ip 129.205.96.3.

Este acceso es el primero vía RDP con la IP pública del servidor, sin embargo, se puede constatar que dicho usuario había accedido previamente, ya que cómo se puede comprobar en el NTSUSERDAT (para visualizar dicha información se ha utilizado la herramienta RegRipper), se lanzó un Netscan previo a dicho acceso:

Fri May 7 11:44:00 2021 Z

{6D809377-6AF0-444B-8957-A3773F02200E}\SoftPerfect Network Scanner\netscan.exe (1)

Además, según los reportes del archivo "LasActivityView.html", después del acceso registrado a las 16:21:42 del 06/05/2021, se realizan las siguientes acciones:



Como se puede comprobar, se instalan varios Softwares, entre ellos Wireshark, y se desinstala Npcap para posteriormente reiniciar el servidor.

Además, como se puede observar se descarga el zip "2.2.0 20200918 Zerologon encrypted.zip".

Por lo tanto, se puede constatar, que el usuario sospechoso accedió de forma local al servidor para instalar una serie de herramientas, para posteriormente, loguearse via RDP desde la ip 129.205.96.3 como se indica en los eventos del sistema.

Pregunta 2 (3 puntos):

¿Qué acciones fueron realizadas por el intruso a partir de su acceso? Indique el detalle de las evidencias (archivo, evento, etc.) de las que se deduce esta información.

Respuesta:

Como se ha indicado en la pregunta anterior, las acciones realizadas por el intruso son varias:

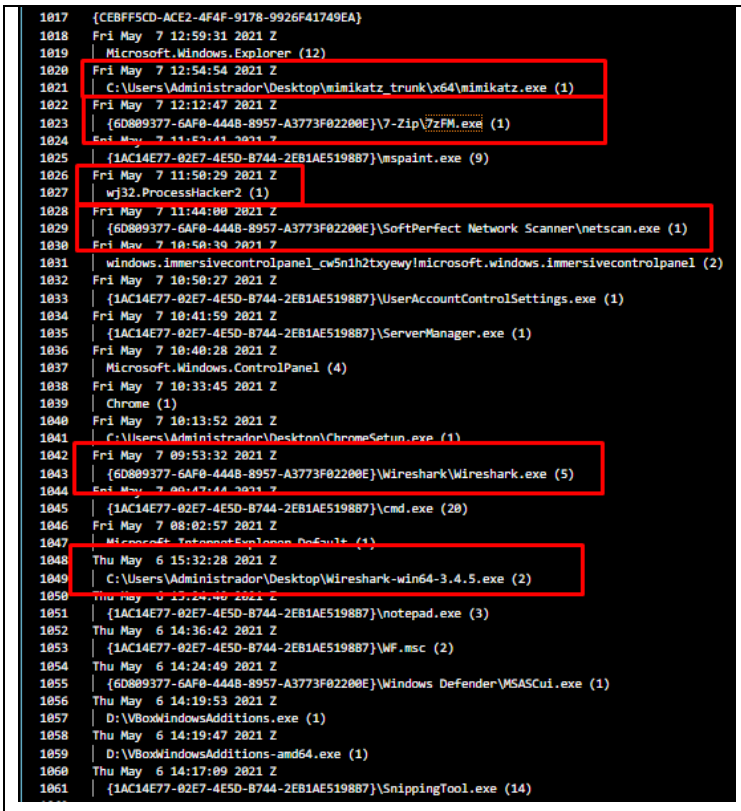
En primer lugar, presuntamente, instaló Wireshark y desinstaló Npcap:

Hay varios accesos del usuario Administrador, por lo que no se puede saber si está acción fue realizada por el usuario sospechoso o fue parte del mantenimiento del servidor.

Posteriormente según el archivo "LasActivityView.html", se realizaron las siguientes acciones:

Se descargó el Chrome, además del archivo "2.2.0 20200918 Zerologon encrypted.zip" para posteriormente ejecutar Mimikatz (herramienta de post-explotación poderosa con la cual se puede obtener contraseñas en texto claro, obtener hashes NTLM, así como extraer credenciales de sesiones actuales o pasadas entre otras funciones.)

Además, como se puede observar en el NTUSERDAT se ha realizado los siguiente:



Dicha imagen identifica los distintos softwares instalados en el sistema, así como las veces que se ha ejecutado cada uno de ellos, registrando la hora en la que se ha realizado la última ejecución.

Pregunta 3 (1 puntos):

¿Cuándo termina las acciones del intruso? Indique el detalle de las evidencias (archivo, evento, etc.) de las que se deduce esta información.

Respuesta:

Las acciones del intruso finalizan (al menos visiblemente) a las 15:01:08 del 07/05/2021, con la ejecución de la tarea programada CreateObjectTask mediante shell32.dll. Esta acción puede indicar un intento de establecer persistencia en el sistema. Es el último evento asociado al usuario Administrador en el fichero "LastActivityView.html".

Pregunta 4 (2 puntos):

Realice una línea de tiempos de lo ocurrido el día 7/5/2021bcon la hora y el evento ocurrido.

Respuesta:

Hora	Evento
11:44:00	Netscan.exe (UserAssist- NTUSER.DAT)
12:44:44	Instalación de chrome.exe
12:19:45	Se abre Zerologon encrypted.zip

12:36:25	Selección de curriculum1.pdf
13:42:23	Logon remoto RDP desde IP 129.205.96.3
13:52:42	Acceso carpeta Mimikatz
14:54:29	Acceso a Z:\ (posible red compartida)
14:54:36	Se abre mimikatz_trunk.zip
15:01:08	Se ejecuta tarea programada CreateObjectTask (persistencia)

Pregunta 5 (2 puntos):

Realice un resumen forense con los siguientes apartados:

1. **Antecedentes del caso.**
   En este apartado se deberán explicar los motivos que han llevado a la empresa a pensar que el equipo ha sido atacado.
2. **Informe ejecutivo.**
   a. Introducción.
   b. Descripción.
   c. Recomendaciones.
3. **Informe técnico.**
   a. Objetivos y alcance.
   b. Metodología del análisis.
   c. Listado de evidencias.
   d. Proceso de análisis forense.
   e. Conclusiones.
   f. Recomendaciones.

El informe no debe tener una extensión superior a 1 o 2 hojas y debe realizarse dentro de la siguiente casilla de respuesta.

Respuesta:

1. **Antecedentes del caso**
   Se piensa que la empresa puede haber sido atacada ya que, en el archivo de recursos compartidos, en vez de encontrar un archivo con el curriculum vitae de varios empleados, un trabajador, se encontró un archivo comprimido con contraseña, además de una instancia de NetScan ejecutándose en segundo plano. El sistema presentaba actividades no autorizadas, como el acceso con cuentas privilegiadas, ejecución de herramientas ofensivas y conexiones remotas desde una IP externa desconocida. Esto motivó el análisis forense.

2. **Informe ejecutivo**
   a. **Introducción.**
      Se realiza un análisis forense sobre el servidor WIN-SF01JTM2DHI ante la sospecha de un acceso y ejecución de software malicioso por parte de un usuario con conocimientos avanzados al sistema.

   b. **Descripción.**
      Durante la investigación se identificaron accesos locales con la cuenta del Administrador, así como accesos via RDP. Se realizó la apertura/ejecución de herramientas de explotación: Zerologon y mimikatz, así como la ejecución de herramientas de escaneo de red como NetScan asi como wireshark. Además, se constató el acceso via RDP desde una ip pública.

c. Recomendaciones.

- Revisión de las cuentas privilegiadas.
- Auditoria del acceso remoto RDP.
- Remplazo de las contraseñas de cuentas con permisos de Administración.
- Revisar las políticas de red para evitar accesos no deseados.

3. Informe técnico

a. Objetivos y alcance.

El objetivo de dicho informe es confirmar si el sistema ha sido comprometido, identificar cómo y cuándo sucedió, así como identificar las acciones realizadas por el sospechoso para poder evaluar el alcance del ataque.

b. Metodología del análisis.

Para realizar el análisis del sistema, se realizará un análisis de las distintas evidencias del sistema. Para ello se analizarán distintos ficheros, entre otros, LastActivityView.txt y NTUSER.DAT, para poder determinar las acciones llevadas a cabo por el sospechoso.
Se revisarán los logs del sistema, así como los distintos eventos del sistema para determinar las acciones llevadas a cabo en el servidor.

c. Listado de evidencias.

```
└── LiveResponseData
    ├── BasicInfo
    │   ├── DiskDriveList_wmic.txt
    │   ├── DiskDriveList_wmic.txt:Zone.Identifier
    │   ├── Full_file_listing.txt
    │   ├── Full_file_listing.txt:Zone.Identifier
    │   ├── Hashes_md5_Startup_and_Dates.txt
    │   ├── Hashes_md5_Startup_and_Dates.txt:Zone.Identifier
    │   ├── Hashes_md5_System32_AllFiles_and_Dates.txt
    │   ├── Hashes_md5_System32_AllFiles_and_Dates.txt:Zone.Identifier
    │   ├── Hashes_md5_System_TEMP_AllFiles_and_Dates.txt
    │   ├── Hashes_md5_System_TEMP_AllFiles_and_Dates.txt:Zone.Identifier
    │   ├── Hashes_md5_User_TEMP_AllFiles_and_Dates.txt
    │   ├── Hashes_md5_User_TEMP_AllFiles_and_Dates.txt:Zone.Identifier
    │   ├── Hashes_sha256_Startup_and_Dates.txt
    │   ├── Hashes_sha256_Startup_and_Dates.txt:Zone.Identifier
    │   ├── Hashes_sha256_System32_AllFiles_and_Dates.txt
    │   ├── Hashes_sha256_System32_AllFiles_and_Dates.txt:Zone.Identifier
    │   ├── Hashes_sha256_System_TEMP_AllFiles_and_Dates.txt
    │   ├── Hashes_sha256_System_TEMP_AllFiles_and_Dates.txt:Zone.Identifier
    │   ├── Hashes_sha256_User_TEMP_AllFiles_and_Dates.txt
    │   ├── Hashes_sha256_User_TEMP_AllFiles_and_Dates.txt:Zone.Identifier
    │   ├── Installed_software_wmic.txt
    │   ├── Installed_software_wmic.txt:Zone.Identifier
    │   ├── LastActivityView.html
    │   ├── LastActivityView.html:Zone.Identifier
    │   ├── List_hidden_directories.txt
    │   ├── List_hidden_directories.txt:Zone.Identifier
    │   ├── Loaded_system_drivers_wmic.txt
    │   ├── Loaded_system_drivers_wmic.txt:Zone.Identifier
    │   ├── LogicalDisk_name_wmic.txt
    │   ├── LogicalDisk_name_wmic.txt:Zone.Identifier
    │   ├── LogicalDisk_size_caption_wmic.txt
    │   ├── LogicalDisk_size_caption_wmic.txt:Zone.Identifier
    │   ├── Possible_unicode_files_and_directories.txt
```

```
|   ├── Possible_unicode_files_and_directories.txt:Zone.Identifier
|   ├── PrcView_extended_long.txt
|   ├── PrcView_extended_long.txt:Zone.Identifier
|   ├── PrcView_extended.txt
|   ├── PrcView_extended.txt:Zone.Identifier
|   ├── psfile.txt
|   ├── psfile.txt:Zone.Identifier
|   ├── psinfo.txt
|   ├── psinfo.txt:Zone.Identifier
|   ├── PsList.txt
|   ├── PsList.txt:Zone.Identifier
|   ├── PsLoggedon.txt
|   ├── PsLoggedon.txt:Zone.Identifier
|   ├── PsLoglist.txt
|   ├── PsLoglist.txt:Zone.Identifier
|   ├── Running_processes.txt
|   ├── Running_processes.txt:Zone.Identifier
|   ├── system_date_time_tz.txt
|   ├── system_date_time_tz.txt:Zone.Identifier
|   ├── system_info.txt
|   ├── system_info.txt:Zone.Identifier
|   ├── system_info_wmic.txt
|   ├── system_info_wmic.txt:Zone.Identifier
|   ├── Windows_codepage.txt
|   ├── Windows_codepage.txt:Zone.Identifier
|   ├── Windows_Version.txt
|   └── Windows_Version.txt:Zone.Identifier
├── CopiedFiles
|   ├── amcache
|   |   ├── Amcache.hve
|   |   ├── Amcache.hve:Zone.Identifier
|   |   ├── info_amcache.log
|   |   └── info_amcache.txt
|   ├── chrome
|   |   └── Administrador
|   |       ├── cache
|   |       |   ├── data_0
|   |       |   ├── data_0:Zone.Identifier
|   |       |   ├── data_1
|   |       |   ├── data_1:Zone.Identifier
|   |       |   ├── data_2
|   |       |   ├── data_2:Zone.Identifier
|   |       |   ├── data_3
|   |       |   └── data_3:Zone.Identifier
|   |       ├── cookies
|   |       |   ├── Cookies
|   |       |   └── Cookies:Zone.Identifier
|   |       └── history
|   |           ├── History
|   |           └── History:Zone.Identifier
|   ├── eventlogs
|   |   └── Logs
|   |       ├── Application.evtx
|   |       ├── Application.evtx:Zone.Identifier
|   |       ├── HardwareEvents.evtx
|   |       ├── HardwareEvents.evtx:Zone.Identifier
|   |       ├── Internet Explorer.evtx
|   |       ├── Internet Explorer.evtx:Zone.Identifier
|   |       ├── Key Management Service.evtx
|   |       ├── Key Management Service.evtx:Zone.Identifier
|   |       ├── Microsoft-Client-Licensing-Platform%4Admin.evtx
|   |       ├── Microsoft-Client-Licensing-Platform%4Admin.evtx:Zone.Identifier
|   |       ├── Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx
|   |       ├── Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx:Zone.Identifier
|   |       ├── Microsoft-Windows-Application-Experience%4Program-Compatibility-Troubleshooter.evtx
```

```
│   │   ├── Microsoft-Windows-Application-Experience%4Program-Compatibility-
Troubleshooter.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Application-Experience%4Program-Inventory.evtx
│   │   ├── Microsoft-Windows-Application-Experience%4Program-Inventory.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Application-Experience%4Program-Telemetry.evtx
│   │   ├── Microsoft-Windows-Application-Experience%4Program-Telemetry.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Application-Experience%4Steps-Recorder.evtx
│   │   ├── Microsoft-Windows-Application-Experience%4Steps-Recorder.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-ApplicationResourceManagementSystem%4Operational.evtx
│   │   ├── Microsoft-Windows-ApplicationResourceManagementSystem%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-AppModel-Runtime%4Admin.evtx
│   │   ├── Microsoft-Windows-AppModel-Runtime%4Admin.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-AppReadiness%4Admin.evtx
│   │   ├── Microsoft-Windows-AppReadiness%4Admin.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-AppReadiness%4Operational.evtx
│   │   ├── Microsoft-Windows-AppReadiness%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-AppXDeployment%4Operational.evtx
│   │   ├── Microsoft-Windows-AppXDeployment%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-AppXDeploymentServer%4Operational.evtx
│   │   ├── Microsoft-Windows-AppXDeploymentServer%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-AppXDeploymentServer%4Restricted.evtx
│   │   ├── Microsoft-Windows-AppXDeploymentServer%4Restricted.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-BackgroundTaskInfrastructure%4Operational.evtx
│   │   ├── Microsoft-Windows-BackgroundTaskInfrastructure%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Biometrics%4Operational.evtx
│   │   ├── Microsoft-Windows-Biometrics%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Bits-Client%4Operational.evtx
│   │   ├── Microsoft-Windows-Bits-Client%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-CodeIntegrity%4Operational.evtx
│   │   ├── Microsoft-Windows-CodeIntegrity%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Containers-Wcifs%4Operational.evtx
│   │   ├── Microsoft-Windows-Containers-Wcifs%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Containers-Wcnfs%4Operational.evtx
│   │   ├── Microsoft-Windows-Containers-Wcnfs%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Crypto-DPAPI%4BackUpKeySvc.evtx
│   │   ├── Microsoft-Windows-Crypto-DPAPI%4BackUpKeySvc.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Crypto-DPAPI%4Operational.evtx
│   │   ├── Microsoft-Windows-Crypto-DPAPI%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-Provider%4Admin.evtx
│   │   ├── Microsoft-Windows-DeviceManagement-Enterprise-Diagnostics-
Provider%4Admin.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-DeviceSetupManager%4Admin.evtx
│   │   ├── Microsoft-Windows-DeviceSetupManager%4Admin.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-DeviceSetupManager%4Operational.evtx
│   │   ├── Microsoft-Windows-DeviceSetupManager%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Dhcp-Client%4Admin.evtx
│   │   ├── Microsoft-Windows-Dhcp-Client%4Admin.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Dhcpv6-Client%4Admin.evtx
│   │   ├── Microsoft-Windows-Dhcpv6-Client%4Admin.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Diagnosis-PLA%4Operational.evtx
│   │   ├── Microsoft-Windows-Diagnosis-PLA%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Diagnosis-Scheduled%4Operational.evtx
│   │   ├── Microsoft-Windows-Diagnosis-Scheduled%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-FileServices-ServerManager-EventProvider%4Admin.evtx
│   │   ├── Microsoft-Windows-FileServices-ServerManager-EventProvider%4Admin.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-FileServices-ServerManager-EventProvider%4Operational.evtx
│   │   ├── Microsoft-Windows-FileServices-ServerManager-EventProvider%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-GroupPolicy%4Operational.evtx
│   │   ├── Microsoft-Windows-GroupPolicy%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-HomeGroup Control Panel%4Operational.evtx
│   │   ├── Microsoft-Windows-HomeGroup Control Panel%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-IKE%4Operational.evtx
│   │   ├── Microsoft-Windows-IKE%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-International%4Operational.evtx
│   │   ├── Microsoft-Windows-International%4Operational.evtx:Zone.Identifier
```

```
|   |   ├── Microsoft-Windows-Iphlpsvc%4Operational.evtx
|   |   ├── Microsoft-Windows-Iphlpsvc%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Kernel-Boot%4Operational.evtx
|   |   ├── Microsoft-Windows-Kernel-Boot%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Kernel-IO%4Operational.evtx
|   |   ├── Microsoft-Windows-Kernel-IO%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Kernel-PnP%4Configuration.evtx
|   |   ├── Microsoft-Windows-Kernel-PnP%4Configuration.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Kernel-Power%4Thermal-Operational.evtx
|   |   ├── Microsoft-Windows-Kernel-Power%4Thermal-Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Kernel-ShimEngine%4Operational.evtx
|   |   ├── Microsoft-Windows-Kernel-ShimEngine%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Kernel-StoreMgr%4Operational.evtx
|   |   ├── Microsoft-Windows-Kernel-StoreMgr%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Kernel-WHEA%4Errors.evtx
|   |   ├── Microsoft-Windows-Kernel-WHEA%4Errors.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Kernel-WHEA%4Operational.evtx
|   |   ├── Microsoft-Windows-Kernel-WHEA%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Known Folders API Service.evtx
|   |   ├── Microsoft-Windows-Known Folders API Service.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-LiveId%4Operational.evtx
|   |   ├── Microsoft-Windows-LiveId%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-MUI%4Admin.evtx
|   |   ├── Microsoft-Windows-MUI%4Admin.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-MUI%4Operational.evtx
|   |   ├── Microsoft-Windows-MUI%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-NCSI%4Operational.evtx
|   |   ├── Microsoft-Windows-NCSI%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-NetworkProfile%4Operational.evtx
|   |   ├── Microsoft-Windows-NetworkProfile%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-NlaSvc%4Operational.evtx
|   |   ├── Microsoft-Windows-NlaSvc%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Ntfs%4Operational.evtx
|   |   ├── Microsoft-Windows-Ntfs%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Ntfs%4WHC.evtx
|   |   ├── Microsoft-Windows-Ntfs%4WHC.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-PrintService%4Admin.evtx
|   |   ├── Microsoft-Windows-PrintService%4Admin.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Program-Compatibility-Assistant%4CompatAfterUpgrade.evtx
|   |   ├── Microsoft-Windows-Program-Compatibility-Assistant%4CompatAfterUpgrade.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-PushNotification-Platform%4Admin.evtx
|   |   ├── Microsoft-Windows-PushNotification-Platform%4Admin.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-PushNotification-Platform%4Operational.evtx
|   |   ├── Microsoft-Windows-PushNotification-Platform%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Admin.evtx
|   |   ├── Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Admin.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx
|   |   ├── Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-RemoteDesktopServices-SessionServices%4Operational.evtx
|   |   ├── Microsoft-Windows-RemoteDesktopServices-SessionServices%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Resource-Exhaustion-Detector%4Operational.evtx
|   |   ├── Microsoft-Windows-Resource-Exhaustion-Detector%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-RestartManager%4Operational.evtx
|   |   ├── Microsoft-Windows-RestartManager%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Security-SPP-UX-Notifications%4ActionCenter.evtx
|   |   ├── Microsoft-Windows-Security-SPP-UX-Notifications%4ActionCenter.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-ServerManager-DeploymentProvider%4Operational.evtx
|   |   ├── Microsoft-Windows-ServerManager-DeploymentProvider%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-ServerManager-MgmtProvider%4Operational.evtx
|   |   ├── Microsoft-Windows-ServerManager-MgmtProvider%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-ServerManager-MultiMachine%4Admin.evtx
|   |   ├── Microsoft-Windows-ServerManager-MultiMachine%4Admin.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-ServerManager-MultiMachine%4Operational.evtx
|   |   ├── Microsoft-Windows-ServerManager-MultiMachine%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-SettingSync%4Debug.evtx
```

```
│   │   ├── Microsoft-Windows-SettingSync%4Debug.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-SettingSync%4Operational.evtx
│   │   ├── Microsoft-Windows-SettingSync%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Shell-ConnectedAccountState%4ActionCenter.evtx
│   │   ├── Microsoft-Windows-Shell-ConnectedAccountState%4ActionCenter.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Shell-Core%4ActionCenter.evtx
│   │   ├── Microsoft-Windows-Shell-Core%4ActionCenter.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Shell-Core%4AppDefaults.evtx
│   │   ├── Microsoft-Windows-Shell-Core%4AppDefaults.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Shell-Core%4LogonTasksChannel.evtx
│   │   ├── Microsoft-Windows-Shell-Core%4LogonTasksChannel.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Shell-Core%4Operational.evtx
│   │   ├── Microsoft-Windows-Shell-Core%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-SmartCard-DeviceEnum%4Operational.evtx
│   │   ├── Microsoft-Windows-SmartCard-DeviceEnum%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-SmbClient%4Connectivity.evtx
│   │   ├── Microsoft-Windows-SmbClient%4Connectivity.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-SMBClient%4Operational.evtx
│   │   ├── Microsoft-Windows-SMBClient%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-SmbClient%4Security.evtx
│   │   ├── Microsoft-Windows-SmbClient%4Security.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-SMBServer%4Audit.evtx
│   │   ├── Microsoft-Windows-SMBServer%4Audit.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-SMBServer%4Connectivity.evtx
│   │   ├── Microsoft-Windows-SMBServer%4Connectivity.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-SMBServer%4Operational.evtx
│   │   ├── Microsoft-Windows-SMBServer%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-SMBServer%4Security.evtx
│   │   ├── Microsoft-Windows-SMBServer%4Security.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-SMBWitnessClient%4Admin.evtx
│   │   ├── Microsoft-Windows-SMBWitnessClient%4Admin.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-SMBWitnessClient%4Informational.evtx
│   │   ├── Microsoft-Windows-SMBWitnessClient%4Informational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-StateRepository%4Operational.evtx
│   │   ├── Microsoft-Windows-StateRepository%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-StateRepository%4Restricted.evtx
│   │   ├── Microsoft-Windows-StateRepository%4Restricted.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-StorageSpaces-ManagementAgent%4WHC.evtx
│   │   ├── Microsoft-Windows-StorageSpaces-ManagementAgent%4WHC.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-Store%4Operational.evtx
│   │   ├── Microsoft-Windows-Store%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-TaskScheduler%4Maintenance.evtx
│   │   ├── Microsoft-Windows-TaskScheduler%4Maintenance.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-TerminalServices-LocalSessionManager%4Admin.evtx
│   │   ├── Microsoft-Windows-TerminalServices-LocalSessionManager%4Admin.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx
│   │   ├── Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-TerminalServices-Printers%4Admin.evtx
│   │   ├── Microsoft-Windows-TerminalServices-Printers%4Admin.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-TerminalServices-Printers%4Operational.evtx
│   │   ├── Microsoft-Windows-TerminalServices-Printers%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Admin.evtx
│   │   ├── Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Admin.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Operational.evtx
│   │   ├── Microsoft-Windows-TerminalServices-
RemoteConnectionManager%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-TWinUI%4Operational.evtx
│   │   ├── Microsoft-Windows-TWinUI%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-UniversalTelemetryClient%4Operational.evtx
│   │   ├── Microsoft-Windows-UniversalTelemetryClient%4Operational.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-UserPnp%4ActionCenter.evtx
│   │   ├── Microsoft-Windows-UserPnp%4ActionCenter.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-UserPnp%4DeviceInstall.evtx
│   │   ├── Microsoft-Windows-UserPnp%4DeviceInstall.evtx:Zone.Identifier
│   │   ├── Microsoft-Windows-User Profile Service%4Operational.evtx
```

```
|   |   ├── Microsoft-Windows-User Profile Service%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-VolumeSnapshot-Driver%4Operational.evtx
|   |   ├── Microsoft-Windows-VolumeSnapshot-Driver%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-VPN%4Operational.evtx
|   |   ├── Microsoft-Windows-VPN%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Wcmsvc%4Operational.evtx
|   |   ├── Microsoft-Windows-Wcmsvc%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-WFP%4Operational.evtx
|   |   ├── Microsoft-Windows-WFP%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Windows Defender%4Operational.evtx
|   |   ├── Microsoft-Windows-Windows Defender%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Windows Defender%4WHC.evtx
|   |   ├── Microsoft-Windows-Windows Defender%4WHC.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Windows Firewall With Advanced Security%4ConnectionSecurity.evtx
|   |   ├── Microsoft-Windows-Windows Firewall With Advanced
Security%4ConnectionSecurity.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx
|   |   ├── Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-WindowsUpdateClient%4Operational.evtx
|   |   ├── Microsoft-Windows-WindowsUpdateClient%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-WinINet-Config%4ProxyConfigChanged.evtx
|   |   ├── Microsoft-Windows-WinINet-Config%4ProxyConfigChanged.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-Winlogon%4Operational.evtx
|   |   ├── Microsoft-Windows-Winlogon%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-WinRM%4Operational.evtx
|   |   ├── Microsoft-Windows-WinRM%4Operational.evtx:Zone.Identifier
|   |   ├── Microsoft-Windows-WMI-Activity%4Operational.evtx
|   |   ├── Microsoft-Windows-WMI-Activity%4Operational.evtx:Zone.Identifier
|   |   ├── Security.evtx
|   |   ├── Security.evtx:Zone.Identifier
|   |   ├── Setup.evtx
|   |   ├── Setup.evtx:Zone.Identifier
|   |   ├── System.evtx
|   |   ├── System.evtx:Zone.Identifier
|   |   ├── Windows PowerShell.evtx
|   |   └── Windows PowerShell.evtx:Zone.Identifier
|   ├── firefox
|   ├── forecopy_handy.log
|   ├── forecopy_handy.log:Zone.Identifier
|   ├── hosts
|   |   ├── hosts
|   |   └── hosts:Zone.Identifier
|   ├── ie
|   ├── logfile
|   |   ├── $LogFile
|   |   └── $LogFile:Zone.Identifier
|   ├── mft
|   |   ├── $MFT
|   |   └── $MFT:Zone.Identifier
|   ├── prefetch
|   ├── registry
|   |   ├── Administrador_NTUSER.DAT
|   |   ├── Administrador_NTUSER.DAT:Zone.Identifier
|   |   ├── COMPONENTS
|   |   ├── COMPONENTS:Zone.Identifier
|   |   ├── DEFAULT
|   |   ├── Default_NTUSER.DAT
|   |   ├── Default_NTUSER.DAT:Zone.Identifier
|   |   ├── Default User_NTUSER.DAT
|   |   ├── Default User_NTUSER.DAT:Zone.Identifier
|   |   ├── DEFAULT:Zone.Identifier
|   |   ├── SAM
|   |   ├── SAM:Zone.Identifier
|   |   ├── SECURITY
|   |   ├── SECURITY:Zone.Identifier
```

```
│   │   ├── SOFTWARE
│   │   ├── SOFTWARE:Zone.Identifier
│   │   ├── SYSTEM
│   │   └── SYSTEM:Zone.Identifier
│   ├── SRUMDB
│   └── usnjrnl
│       ├── $UsnJrnl_$J.bin
│       └── $UsnJrnl_$J.bin:Zone.Identifier
├── NetworkInfo
│   ├── cports.html
│   ├── cports.html:Zone.Identifier
│   ├── nbtstat.txt
│   ├── nbtstat.txt:Zone.Identifier
│   ├── NetBIOS_sessions.txt
│   ├── NetBIOS_sessions.txt:Zone.Identifier
│   ├── netstat_anb_results.txt
│   ├── netstat_anb_results.txt:Zone.Identifier
│   ├── TCPView.txt
│   └── TCPView.txt:Zone.Identifier
├── PersistenceMechanisms
│   ├── autorunsc.csv
│   ├── autorunsc.csv:Zone.Identifier
│   ├── autorunsc.txt
│   ├── autorunsc.txt:Zone.Identifier
│   ├── Driver_group_load_order_wmic.txt
│   ├── Driver_group_load_order_wmic.txt:Zone.Identifier
│   ├── Loaded_dlls.txt
│   ├── Loaded_dlls.txt:Zone.Identifier
│   ├── scheduled_tasks.txt
│   ├── scheduled_tasks.txt:Zone.Identifier
│   ├── services_aw_processes.txt
│   ├── services_aw_processes.txt:Zone.Identifier
│   ├── Startup_wmic.txt
│   └── Startup_wmic.txt:Zone.Identifier
└── UserInfo
    ├── All_logons_wmic.txt
    ├── All_logons_wmic.txt:Zone.Identifier
    ├── whoami.txt
    └── whoami.txt:Zone.Identifier

23 directories, 373 files
```

Entre ellos se pueden descatar los siguientes:

- LastActivityView.html
- NTUSER.DAT
- Carpeta de eventos

d. Proceso de análisis forense.

Para realizar el análisis forense, en primer lugar, se ha realizado un estudio de las distintas evidencias aportadas para el caso. Se han estudiado en primer lugar, los logs de acceso al servidor, proporcionados por los eventos de Windows del sistema, donde se puede determinar quién accedió al servidor y la manera en la que accedió.

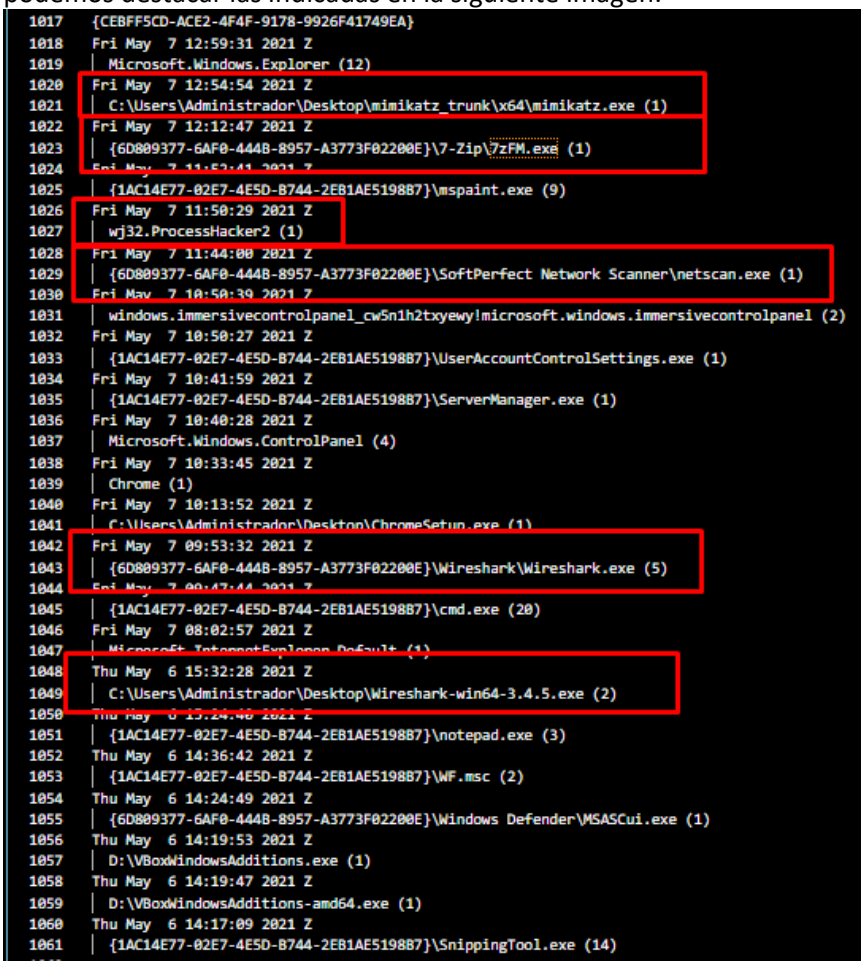
Para determinar las acciones realizadas por el usuario sospechoso, se ha realizado un análisis del LastEventView.html donde aparecen reportadas las distintas actividades de los usuarios. Para poder analizar de manera mas minuciosa los eventos del sistema, mediante la herramienta RegRipper, se ha procedido a ver el contenido de diversos archivos, entre ellos en NTUSER.DAT donde aparece información relativa a la ejecución de software en dicho servidor. Además de usar RegRipper, se han utilizado otras

herramientas:

- Hayabusa
- Autopsy
- DB-browser
- FullEventLogView
- NTFS data tracker
- WinPrefetch
- RegistryExplorer

e. Conclusiones.

Se ha realizado un acceso sospechoso al servidor por RDP desde la ip 129.205.96.3, previamente a dicho acceso se han llevado a cabo una serie de acciones entre las que podemos destacar las indicadas en la siguiente imagen:



El usuario sospechoso ha descargado varios programas externos para su posterior instalación. En las actividades de post-explotación ha utilizado el software Mimikatz para entre otras cosas obtener credenciales de los usuarios.

f. Recomendaciones.

- Limitar el acceso de red para no permitir accesos por la red pública, reforzando las medidas de segmentación de red
- Cambiar las credenciales de los usuarios locales.
- Centralizar los logs en un SIEM para detección temprana.