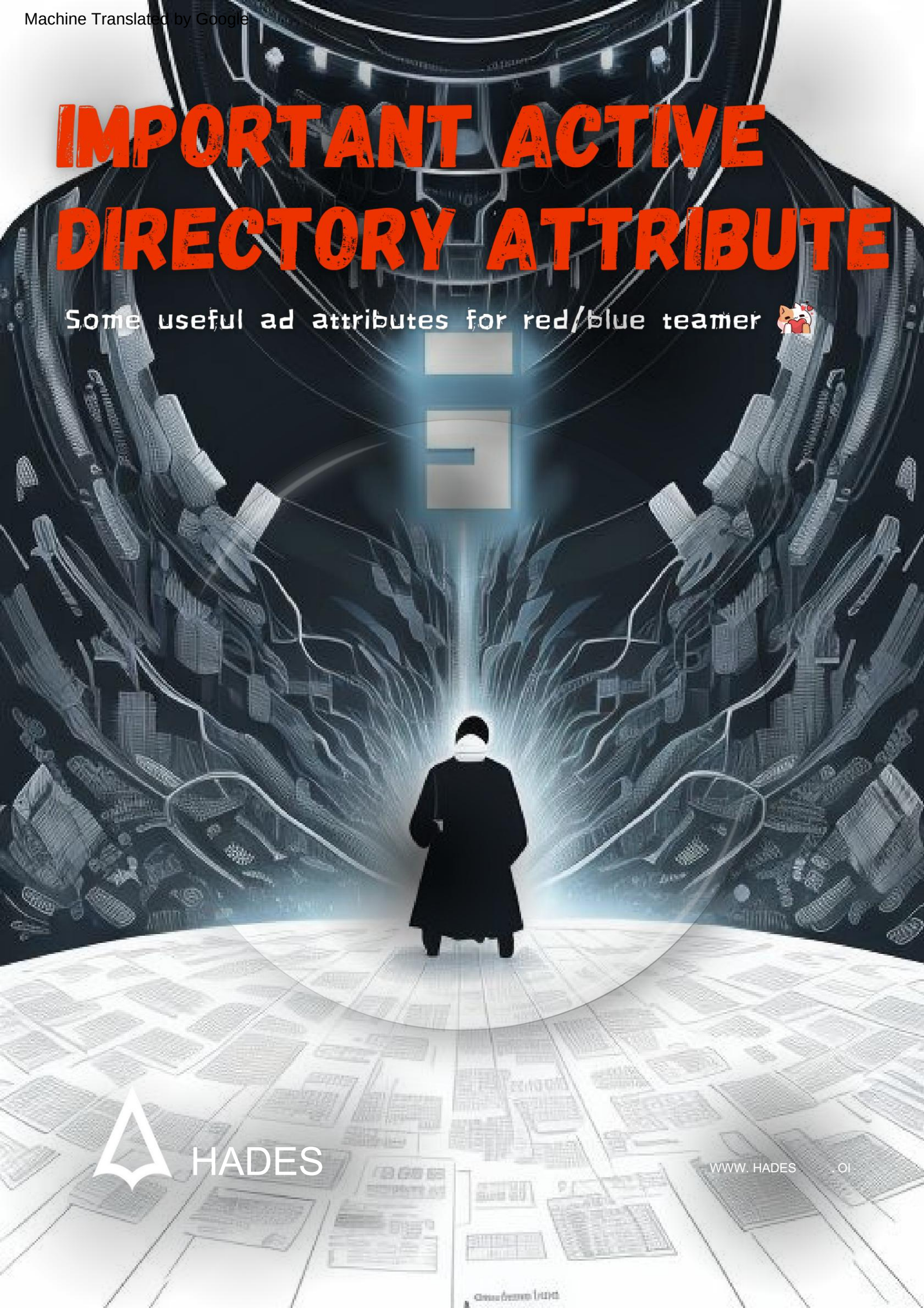
IMPORTANT ACTIVE DIRECTORY ATTRIBUTE

Some useful ad attributes for red/blue teamer



HADES

Atributo importante de Active Directory

Los atributos de Active Directory desempeñan un papel crucial en la gestión de cuentas de usuario y membresías de grupos dentro de Windows.
ambientes. Atributos como SAMACCOUNTNAME y USERPRINCIPALNAME suelen estar destinados a
enumeración de nombres de usuario y ataques de phishing. El atributo MEMBEROF proporciona información sobre la pertenencia a grupos,
que los adversarios explotan para el movimiento lateral y la escalada de privilegios. Los campos DESCRIPCIÓN ofrecen valiosas
información para esfuerzos de reconocimiento e ingeniería social. Las direcciones de CORREO ELECTRÓNICO almacenadas en el atributo CORREO son
objetivos principales para campañas de phishing y reconocimiento. Las rutas de HOMEDIRECTORY pueden exponer el acceso al sistema de archivos
puntos, convirtiéndolos en objetivos potenciales para la exfiltración o manipulación de datos. Comprender estos atributos y sus
Los vectores de ataque asociados son esenciales para proteger los entornos de Active Directory.

——	Atributo	Descripción	Vector de ataque
1	PRIVILEGIO SEIMPERSONATE Capacidad de	hacerse pasar por un cliente después de la autenticación	Impacket, atexec.py, Invoke-TokenManipulación
2	SELOADDRIVERPRIVILEGE Capacidad de cargar y	descargar controladores de dispositivos	Metasploit, explotación/windows/local/service_permissions
3	PRIVILEGIO DE COPIA DE SEGURIDAD	Evite ciertas restricciones de seguridad para operaciones de copia de seguridad y restauración	Pacto, manipulación de tokens de invocación
4	FORCECHANGEPASSWORD Obligar al usuario a	cambiar la contraseña en el próximo inicio de sesión	PowerSploit, Invoke-UserHunter, Set-ADCuentaContraseña
5	ESCRITURA GENÉRICA	Escribe en cualquier atributo del objeto objetivo, evitando la seguridad	SharpHound, Invocar-BloodHound, Set-Objeto AD
6	Privilegio SeTakeOwnership	Otorga la capacidad de tomar posesión de archivos y directorios.	PowerSploit, Invocar-TakeOwn
7	Privilegio SeDebug	Permite depurar procesos y acceder a su memoria.	Metasploit, explotación/windows/local/bypassuac_eventvwr
8	SeAssignPrimaryTokenPrivilege Asigna tokens primarios a los procesos.		Pacto, manipulación de tokens de invocación
9	SeAumentarCuotaPrivilegio	Ajusta las cuotas de memoria para procesos	Cobalt Strike, privilegio::depuración
10	SeCambiarNotificarPrivilegio	Recibe notificaciones de cambios en archivos o directorios	Imperio, elevate_privileges
11	Ver privilegios de hora del sistema	Permite ajustar la hora del sistema.	Mimikatz, sekurlsa::pth /dominio:destino / usuario:nombre de usuario /ntlm:hash /ejecutar:powershell.exe

——	Atributo	Descripción	Vector de ataque
12	SeShutdownPrivilegio	Otorga la capacidad de apagar el sistema.	CrackMapExec, apagado /r /t 0
13	Privilegio SeCreateToken	Permite crear tokens de acceso.	SharpSploit, CrearProcesoComoUsuario
14 NOMBRE DE CUENTA SAMA		nombre de cuenta SAM para un usuario o grupo	Enumeración de nombres de usuario, ataques de fuerza bruta
15 NOMBRE PRINCIPAL DE USUARIO		Nombre principal de usuario (UPN) para una cuenta de usuario	Ataques de phishing, ataques basados en Kerberos
16 MIEMBRO DE		Lista de grupos a los que pertenece el usuario o grupo	Movimiento lateral, escalada de privilegios.
17 DESCRIPCIÓN		Descripción textual o información adicional sobre un objeto.	Reconocimiento, ingeniería social.
18	CORREO	Dirección de correo electrónico asociada a una cuenta de usuario	Ataques de phishing, reconocimiento
19 DIRECTORIO DE INICIO		Ruta de red al directorio de inicio del usuario	Acceso al sistema de archivos, exfiltración de datos.
20 CUENTA BLOQUEADA		Indica si el usuario la cuenta está bloqueada afuera	Enumeración de cuentas, ataques de fuerza bruta
21 TIEMPO DE CONTRASEÑA MAL		tiempo de la ultima intento de contraseña no válida para una cuenta de usuario	Fuerza bruta de contraseñas, detección de ataques de fuerza bruta
22 ÚLTIMA MARCA DE TIEMPO DE INICIO DE INICIO		La última vez que un usuario iniciado sesión en el dominio	Identificar cuentas privilegiadas inactivas o poco utilizadas
23 TOKEN DE GRUPO PRIMARIO		Token de grupo principal para un usuario, determina el grupo principal	Escalada de privilegios, persistencia
24 ADMINISTRADOR		Identificador de seguridad (SID) del usuario o grupo considerado administrador	Escalada de privilegios, movimiento lateral
25 HORAS DE INGRESO		Horarios durante los cuales un usuario puede iniciar sesión en el dominio	Identificar oportunidades potenciales de acceso no autorizado
26 ESTACIONES DE TRABAJO DE USUARIO		Estaciones de trabajo de cual es un usuario	Compromiso de la estación de trabajo, movimiento lateral

——	Atributo	Descripción	Vector de ataque
		permitida para iniciar sesión en el dominio	
27 CONTADORES DE ADMINISTRACIÓN		Administrativo datos del contador, indica acciones administrativas	Escalada de privilegios, detección de actividad inusual

PRIVILEGIO SEIMPERSONAR

Descripción

Este atributo rige la capacidad de hacerse pasar por un cliente después de la autenticación. Usuarios o procesos con este privilegio puede actuar en nombre de otro usuario.

```
COINCIDIR p=(:Usuario)-[:MiembroDe*1..]->(:Grupo)-[:CanImpersonate]->()
VOLVER p
```

Código: SeImpersonatePrivilege

- Herramienta: Impacto
- Comando: atexec.py con bandera -k
- Comando: Invocar-TokenManipulation con el indicador -ImpersonateUser

PRIVILEGIO DE CARGA DEL CONDUCTOR

Descripción

Este privilegio permite a los usuarios o procesos cargar y descargar controladores de dispositivos en un sistema. A menudo es un privilegio sensible. restringido a administradores.

```
COINCIDIR p=(:Usuario)-[:MemberOf*1..]->(:Grupo)-[:CanLoadDriver]->()
VOLVER p
```

Código: SeLoadDriverPrivilege

- Herramienta: Metasploit
- Módulo: explotar/windows/local/service_permissions
- Comando: Invocar-WMIExec con el indicador -LoadDriver

PRIVILEGIO DE COPIA DE SEGURIDAD

Descripción

Los usuarios o procesos con este privilegio pueden eludir ciertas restricciones de seguridad para realizar copias de seguridad y restaurar. operaciones. Normalmente se concede a administradores o software de copia de seguridad.

```
COINCIDIR p=(:Usuario)-[:MiembroDe*1..]->(:Grupo)-[:CanBackup]->()
VOLVER p
```

Código: SeBackupPrivilege

- Herramienta: Pacto
- Comando: Invocar manipulación de tokens con SeBackupPrivilege

FORCECAMBIARCONTRASEÑA

Descripción

Este atributo controla si un usuario debe cambiar su contraseña en el siguiente inicio de sesión. Establecer esta bandera obliga a los usuarios a actualizar su contraseña inmediatamente.

```
COINCIDIR p=(:Usuario)-[:CanChangePassword]->()
VOLVER p
```

Código: El usuario debe cambiar la contraseña

- Herramienta: PowerSploit
- Comando: Invoke-UserHunter con el indicador -ForcePasswordReset
- - Comando: Establecer-ADAcontraseña de cuenta

ESCRITURA GENÉRICA

Descripción:

Este atributo permite que el usuario o grupo especificado escriba en cualquier atributo del objeto de destino en Active Directory, sin pasar por la seguridad a nivel de atributo.

```
COINCIDIR p=(:Usuario)-[:MemberOf*1..]->(:Grupo)-[:CanGenericWrite]->()
VOLVER p
```

Código: ADS_RIGHT_GENERIC_WRITE

- Herramienta: Sharphound
- Comando: Invocar-BloodHound con la opción -Find GenericWrite
- Comando: Establecer-ADObject con -Agregar o -Reemplazar bandera

Privilegio SeTakeOwnership

Descripción

Otorga la capacidad de tomar posesión de archivos y directorios.

```
COINCIDIR p=(:Usuario)-[:MiembroDe*1..]->(:Grupo)-[:CanTakeOwnership]->()
VOLVER p
```

Explotación

- Obtenga propiedad de archivos críticos para manipular permisos.
- Útil para escalada de privilegios.
- Herramienta: Comando
- PowerSploit : `Invoke-TakeOwn`

Mitigación

Limite este privilegio a administradores de confianza.

Privilegio SeDebug

Descripción

Permite depurar procesos y acceder a su memoria.

```
COINCIDIR p=(:Usuario)-[:MiembroDe*1..]->(:Grupo)-[:CanDebug]->()
VOLVER p
```

Explotación

- La depuración puede conducir a la ejecución de código o a una escalada de privilegios.
- Herramienta: Metasploit
- Módulo: `explotar/windows/local/bypassuac_eventvwr`

Mitigación

Limite este privilegio a administradores de confianza.

VerSuplantarPrivilegio

Descripción

Permite hacerse pasar por otros usuarios.

```
COINCIDIR p=(:Usuario)-[:MiembroDe*1..]->(:Grupo)-[:CanImpersonate]->()
VOLVER p
```

Explotación

- Suplantar cuentas privilegiadas para acciones no autorizadas.
- Herramienta:
- Comando Impacket : `wmiexec.py` con el indicador `-k`

Mitigación

Restrinja este privilegio a las cuentas necesarias.

Privilegio SeAssignPrimaryToken

Descripción

Asigna tokens primarios a los procesos.

```
COINCIDIR p=(:Usuario)-[:MemberOf*1..]->(:Grupo)-[:CanAssignPrimaryToken]->()
VOLVER p
```

- Herramienta: Pacto
- Comando: Invocar manipulación de tokens

Explotación

- Manipule las asignaciones de tokens para escalar privilegios.

Mitigación

Limite este privilegio a procesos confiables.

SeAumentarCuotaPrivilegio

Descripción

Ajusta las cuotas de memoria para los procesos.

```
COINCIDIR p=(:Usuario)-[:MiembroDe*1..]->(:Grupo)-[:CanIncreaseQuota]->()
VOLVER p
```

Explotación

- Modifique las cuotas de memoria para evadir las restricciones.
- Herramienta: Golpe de cobalto
- Módulo: privilegio::depurar

Mitigación

Limite este privilegio a procesos confiables.

SeCambiarNotificarPrivilegio

Descripción

Recibe notificaciones de cambios en archivos o directorios.

```
COINCIDIR p=(:Usuario)-[:MiembroDe*1..]->(:Grupo)-[:CanChangeNotify]->()
VOLVER p
```

Explotación

- Supervise los cambios de archivos en busca de datos confidenciales.
- Herramienta:
- Comando Imperio : elevate_privileges

Mitigación

Limite este privilegio a las cuentas necesarias.

Ver privilegios de hora del sistema

Descripción

Permite ajustar la hora del sistema.

```
COINCIDIR p=(:Usuario)-[:MemberOf*1..]->(:Grupo)-[:CanChangeSystemTime]->()
VOLVER p
```

Explotación

- Manipular el tiempo del sistema para varios ataques.
- Herramienta: Mimikatz
- Comando: sekurlsa::pth /dominio:destino /usuario:nombre de usuario /ntlm:hash /ejecutar:powershell.exe

Mitigación

Limite este privilegio a administradores de confianza.

SeShutdownPrivilegio

Descripción

Otorga la capacidad de apagar el sistema.

```
COINCIDIR p=(:Usuario)-[:MiembroDe*1..]->(:Grupo)-[:CanShutdown]->()
VOLVER p
```

Explotación

- Apagado no autorizado del sistema.
- Herramienta: Comando
- CrackMapExec : cme smb <objetivo> -u <nombre de usuario> -p <contraseña> --exec-command "shutdown /r /t 0"

Mitigación

Limite este privilegio a administradores de confianza.

Privilegio SeCreateToken

Descripción

Permite crear tokens de acceso.

```
COINCIDIR p=(:Usuario)-[:MiembroDe*1..]->(:Grupo)-[:CanCreateToken]->()
VOLVER p
```

Explotación

- Cree tokens personalizados para escalar privilegios.
- Herramienta: SharpSploit
- Comando: `CrearProcesoComoUsuario`

Mitigación

Limite este privilegio a procesos confiables.

CUENTADESHABILITADA

- Comando: comando de PowerShell `Set-ADAccountControl`
- Descripción: este atributo determina si la cuenta de usuario está habilitada o deshabilitada. Cuando se establece en `TRUE` , la , el cuenta está deshabilitada y el usuario no puede iniciar sesión.
- Código: `ADS_UF_ACCOUNTDISABLE`
- Ejemplo:

```
Set-ADAccountControl -Identidad "nombre de usuario" -AccountDisabled $true
```

TIEMPO DE BLOQUEO

- Comando: comando de PowerShell `Get-ADUser`
- Descripción: este atributo indica el momento en que la cuenta de usuario se bloqueó debido a que se superó el umbral de bloqueo de la cuenta. Se representa como un valor entero grande.
- Código: `tiempo de bloqueo`
- Ejemplo:

```
Get-ADUser -Identidad "nombre de usuario" -Propiedades lockoutTime | Seleccionar-Objeto-ExpandirPropiedad
tiempo de bloqueo
```

ÚLTIMO INICIAR SESIÓN

- Comando: comando de PowerShell `Get-ADUser`
- Descripción: este atributo registra la marca de tiempo del último inicio de sesión exitoso del usuario en el dominio. Ayuda a los administradores a rastrear la actividad de los usuarios e identificar cuentas inactivas.

- Código: último inicio de sesión
- Ejemplo:

```
Get-ADUser -Identity "nombre de usuario" -Propiedades lastLogon | Seleccionar-Objeto -ExpandirPropiedad lastLogon
```

CONJUNTO DE CARGA DE PWD

- Comando: comando de PowerShell Get-ADUser
- Descripción: este atributo almacena la marca de tiempo de la última vez que se cambió la contraseña del usuario. Se utiliza para hacer cumplir las políticas de caducidad de contraseñas y determinar cuándo es necesario un cambio de contraseña.
- Código: pwdLastSet
- Ejemplo:

```
Get-ADUser -Identity "nombre de usuario" -Properties pwdLastSet | Seleccionar-Objeto -ExpandProperty pwdLastSet
```

MIEMBRO DE

- Comando: comando de PowerShell Get-ADUser o Get-ADGroup
- Descripción: este atributo enumera los grupos a los que pertenece el usuario u objeto de grupo. Ayuda a administrar los permisos de acceso y la membresía de grupos.
- Código: miembro de
- Ejemplo:

```
Get-ADUser -Identity "nombre de usuario" -Properties memberOf | Seleccionar-Objeto -ExpandirPropiedad miembroOf
```

SAMACUENTANOMBRE

- Comando: comando de PowerShell Get-ADUser o Get-ADGroup Descripción: este
- atributo representa el nombre de la cuenta SAM para un usuario o grupo, que es un identificador único utilizado en los protocolos de autenticación de Windows.
- Código: sAMAccountName
- Ejemplo:

```
Get-ADUser -Identity "nombre de usuario" | Seleccionar-Objeto -ExpandirPropiedad sAMAccountName
```

NOMBRE PRINCIPAL DE USUARIO

- Comando: comando de PowerShell Get-ADUser
- Descripción: este atributo representa el nombre principal de usuario (UPN) para una cuenta de usuario. UPN tiene el formato nombre de usuario@dominio.com y se utiliza para el inicio de sesión del usuario.
- Código: nombre principal de usuario
- Ejemplo:

```
Get-ADUser -Identity "nombre de usuario" | Seleccionar-Objeto -ExpandProperty userPrincipalName
```

DESCRIPCIÓN

- Comando: comando de PowerShell Get-ADUser o Get-ADGroup

- Descripción: este atributo proporciona una descripción textual o información adicional sobre un usuario u objeto de grupo dentro de Active Directory.
- Código: `descripción`
- Ejemplo:

```
Get-ADUser -Identity "nombre de usuario" | Seleccionar-Objeto -Expandir descripción de propiedad
```

CORREO

- Comando: comando de PowerShell `Get-ADUser`
- Descripción: este atributo almacena la dirección de correo electrónico asociada con una cuenta de usuario. Se utiliza comúnmente para la comunicación por correo electrónico y la integración de la libreta de direcciones.
- Código: `correo`
- Ejemplo:

```
Get-ADUser -Identity "nombre de usuario" | Seleccionar-Objeto -ExpandirPropiedad correo
```

DIRECTORIO DE INICIO

- Comando: comando de PowerShell `Get-ADUser`
- Descripción: este atributo especifica la ruta de red al directorio de inicio del usuario. Se utiliza para mapear automáticamente unidades de red y proporcionar almacenamiento específico del usuario.
- Código: `directorio de inicio`
- Ejemplo:

```
Get-ADUser -Identity "nombre de usuario" | Seleccionar-Objeto -ExpandirPropiedad directorio de inicio
```

CUENTABLOQUEADA

- Comando: comando de PowerShell `Get-ADUser`
- Descripción: este atributo indica si la cuenta de usuario está actualmente bloqueada. Es un atributo booleano donde `VERDADERO` significa que la cuenta está bloqueada.
- Código: `IsAccountLockedOut`
- Ejemplo:

```
(Get-ADUser -Identidad "nombre de usuario").IsAccountLockedOut
```

TIEMPO DE CONTRASEÑA MALA

- Comando: comando de PowerShell `Get-ADUser`
- Descripción: este atributo registra la hora del último intento de contraseña no válida para una cuenta de usuario. Ayuda a detectar posibles ataques de fuerza bruta.
- Código: `badPasswordTime`
- Ejemplo:

```
Get-ADUser -Identidad "nombre de usuario" -Propiedades badPasswordTime | Seleccionar-Objeto-ExpandirPropiedad malacontraseñahora
```

cuentaadmin

- Comando: comando de PowerShell Get-ADUser o Get-ADGroup Descripción: este
- atributo indica si el usuario o grupo ha sido marcado como si tuviera privilegios elevados, normalmente por ser miembro de un grupo administrativo integrado. Los evaluadores de penetración a menudo buscan objetos con ADMINCOUNT configurado para identificar objetivos potenciales para la escalada de privilegios.
- Código: adminCount
- Ejemplo:

```
Get-ADUser -Identity "nombre de usuario" -Properties adminCount |
```

ÚLTIMO CIERRE DE SESIÓN

Descripción

Este atributo indica la última vez que un usuario cerró sesión en el dominio. Los evaluadores de penetración pueden usar este atributo junto con otros datos para identificar posibles momentos de baja actividad para realizar operaciones sigilosas.

Detección

```
Get-ADUser -Identity "nombre de usuario" -Properties lastLogoff | Seleccionar-objeto -Expandir propiedad último cerrar sesión
```

AUDITFLAG

Descripción

Este atributo especifica la configuración de auditoría para un objeto de Active Directory, incluido si la auditoría está habilitada y qué eventos se están auditando. Los evaluadores de penetración pueden identificar configuraciones de auditoría mal configuradas para una posible seguridad debilidades.

Detección

```
Get-ADObject -Identidad "DN del objeto" -Propiedades auditFlag | Seleccionar-Objeto-ExpandirPropiedad
auditoríaBandera
```

ESPACIO DE NOMBRES DE POLÍTICA DE GRUPO

Descripción

Este atributo especifica el espacio de nombres de un objeto de política de grupo (GPO), que define el alcance y la configuración aplicados por el GPO. Los evaluadores de penetración pueden analizar los espacios de nombres de GPO en busca de configuraciones erróneas que podrían generar privilegios. escalada o ejecución.

Detección

```
Get-ADGroupPolicy -Identidad "GPOName" -Properties gPCNameSpace | Seleccionar-Objeto-ExpandirPropiedad
gPCNombreEspacio
```

ENLACES DE POLÍTICA DE GRUPO

Descripción

Este atributo especifica los objetos de política de grupo (GPO) vinculados a una unidad organizativa (OU) o a todo el dominio.
Los evaluadores de penetración pueden analizar los enlaces GPO en busca de configuraciones erróneas o vulnerabilidades que podrían explotarse.

Detección

```
Get-ADOrganizationalUnit -Identidad "OUName" -Propiedades gPLink | Seleccionar-Objeto -ExpandirPropiedad gPLink
```

CUOTA DE CUENTA DE MÁQUINA

Descripción

Este atributo especifica el número máximo de cuentas de máquina (por ejemplo, objetos de computadora) que se pueden crear en el dominio. Los probadores de penetración pueden aprovechar configuraciones erróneas en las cuotas de cuentas de máquinas para ataques de agotamiento de recursos o acceso no autorizado.

Detección

```
Obtener-ADDominio | Seleccionar-Objeto -ExpandProperty ms-DS-MachineAccountQuota
```

CONTROL DE CUENTAS DEL USUARIO

Descripción

Este atributo controla varias opciones de cuenta para una cuenta de usuario, incluido si la cuenta está habilitada, deshabilitada, bloqueada o requiere un cambio de contraseña. Los evaluadores de penetración pueden manipular estas configuraciones para escalar o ejecutar privilegios.

Detección

```
Get-ADUser -Identidad "nombre de usuario" -Propiedades userAccountControl | Seleccionar-Objeto-ExpandirPropiedad
control de cuentas del usuario
```

PERMITIDO ACTUAR EN NOMBRE DE OTRAS IDENTIDADES

Descripción

Este atributo determina si el usuario puede hacerse pasar por otras identidades con fines de delegación. Los operadores del equipo rojo pueden abusar de este privilegio para movimientos laterales o escalada de privilegios.

Detección

```
(Get-ADUser -Identidad "nombre de usuario" -Propiedades msDS-AllowedToActOnBehalfOfOtherIdentity).msDS-
AllowedToActOnBehalfOfOtherIdentity
```

GROUPPOLICYNAMESPACE (repetido)

Descripción

Este atributo especifica el espacio de nombres de un objeto de política de grupo (GPO), que define el alcance y la configuración aplicados por el GPO. Los operadores del equipo rojo pueden analizar los espacios de nombres de GPO en busca de configuraciones erróneas que podrían generar privilegios

escalada o ejecución.

Detección

```
Get-ADGroupPolicy -Identidad "GPOName" -Properties gPCNNameSpace | Seleccionar objeto -ExpandProperty gPCNNameSpace
```

ENLACES DE POLÍTICA DE GRUPO (repetidos)

Descripción

Este atributo especifica los objetos de política de grupo (GPO) vinculados a una unidad organizativa (OU) o a todo el dominio.
Los operadores del equipo rojo pueden analizar los enlaces GPO en busca de configuraciones erróneas o vulnerabilidades que podrían explotarse.

Detección

```
Get-ADOrganizationalUnit -Identidad "OUName" -Propiedades gPLink | Seleccionar-Objeto -ExpandirPropiedad gPLink
```

NOMBRE PRINCIPAL DE USUARIO

Descripción

Este atributo representa el nombre principal de usuario (UPN) de una cuenta de usuario. Los operadores del equipo rojo pueden abusar de los UPN para realizar ataques de phishing dirigidos o ataques basados en Kerberos.

Detección

```
Get-ADUser -Identity "nombre de usuario" | Seleccionar-Objeto -ExpandProperty userPrincipalName
```

SIDHISTORIA

Descripción

Este atributo almacena identificadores de seguridad (SID) de dominios confiables de los que el usuario o grupo ha sido miembro anteriormente. Los operadores del equipo rojo pueden explotar el historial de SID para obtener acceso a recursos en dominios confiables.

Detección

```
Get-ADUser -Identidad "nombre de usuario" -Propiedades sIDHistory | Seleccionar-Objeto -ExpandirPropiedad sIDHistory
```

CREDENCIALES SUPLEMENTARIAS

Descripción

Este atributo almacena información de credenciales adicional para un usuario, como credenciales almacenadas en caché. Los operadores del equipo rojo pueden apuntar a este atributo por robo de credenciales o movimiento lateral.

Detección

```
Get-ADUser -Identidad "nombre de usuario" -Propiedades suplementalesCredenciales | Seleccionar objeto -
ExpandirPropiedad suplementariaCredenciales
```

MEMBRESÍA DE GRUPO

Descripción

Este atributo enumera los grupos a los que pertenece el usuario. Los operadores del equipo rojo pueden analizar la membresía del grupo en busca de objetivos potenciales para escalada de privilegios o movimiento lateral.

Detección

```
Get-ADUser -Identity "nombre de usuario" -Properties memberOf | Seleccionar-Objeto -ExpandirPropiedad miembroOf
```

PWDHISTORYLONGITUD

Descripción

Este atributo especifica la cantidad de contraseñas anteriores almacenadas en el historial de contraseñas. Los operadores del equipo rojo pueden analizar esta configuración para determinar la política de reutilización de contraseñas e identificar vías potenciales para la reutilización de credenciales. ataques.

Detección

```
Obtener-ADDominio | Seleccionar-Objeto -ExpandProperty msDS-PSOAppliesTo
```
