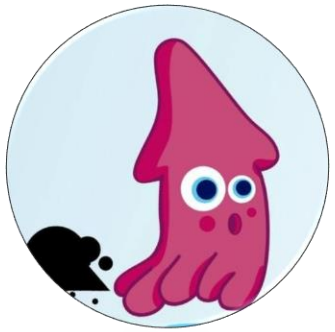
El compendio definitivo de ataques en Directorio Activo

> whoami

- Mi nombre es Jorge Escabias.
- Responsable del equipo de seguridad ofensiva en Zerolynx.
- Me gustan los Directorios Activos, Windows y BloodHound.
- Graduado en Ciencias Matemáticas. Nunca he sabido sumar.
- Tengo un NUC y monto entornos.
- Twitter: @MrSquid25
- LinkedIn: @jorgesca



Objetivo

Disponer de un esquema de los fallos y abusos más comunes que se pueden encontrar en un Directorio Activo a alto nivel y disponer de una serie de correcciones para su remediación o mitigación.

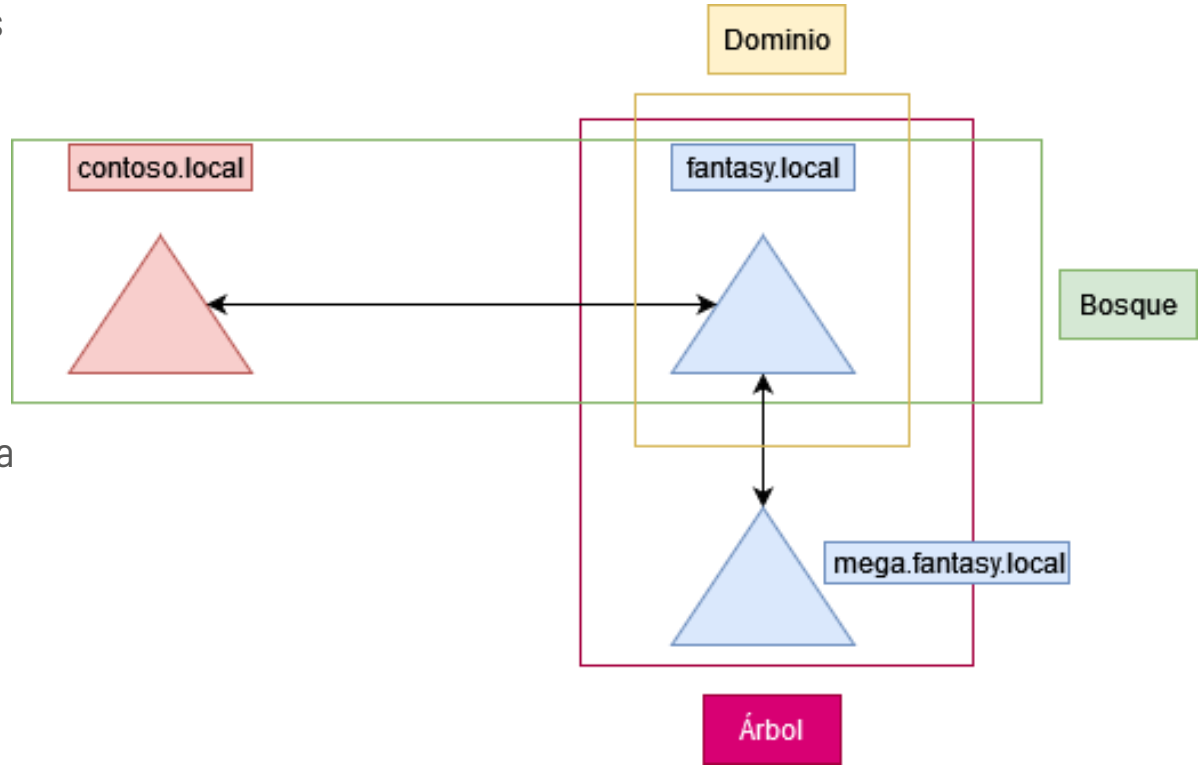
Spoiler: no tocaremos todo ni por asomo.

Agenda

1
Directorio Activo de un vistazo

Estructura de un Directorio Activo

- Introducido por primera vez en Windows 2000
- Es una estructura jerárquica que almacena información sobre los distintos elementos que conforman una red.
- Dentro de un AD podemos encontrar varios tipos de objetos:
  - Usuarios y equipos
  - Grupos
  - Unidades Organizativas
  - ...
- La forma de agrupación de los elementos de un Directorio se basa en:
  - Dominios (Rama)
  - Árboles
  - Bosques

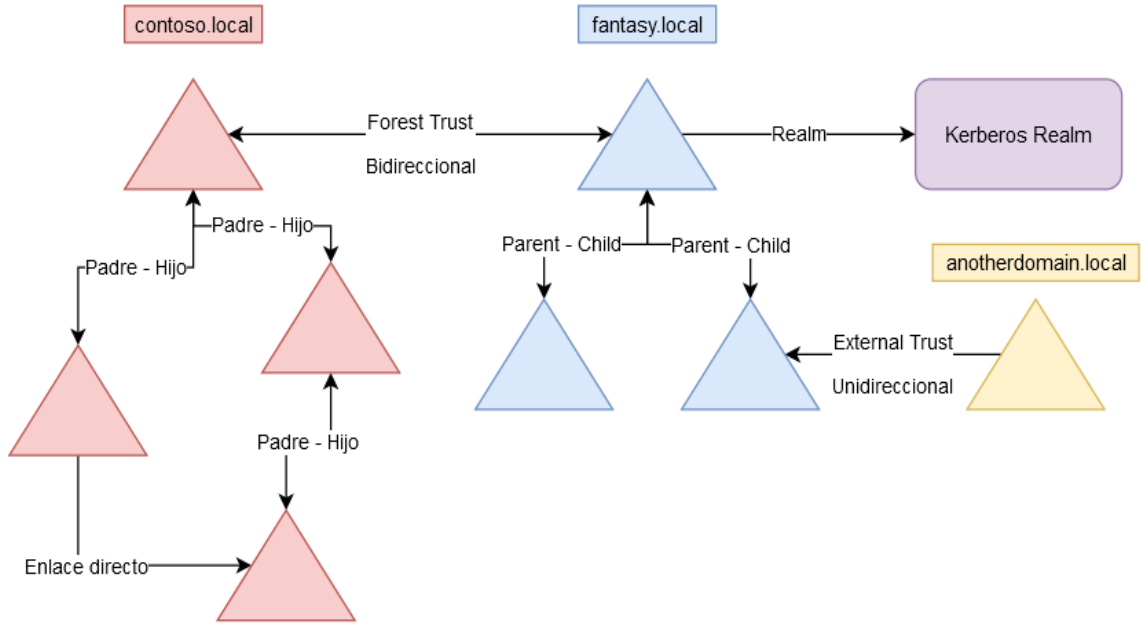


Confianzas en un Directorio Activo

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.

Los tipos de confianza existentes son:

- Forest Trust
- External Trust
- Realm Trust
- Enlace directo

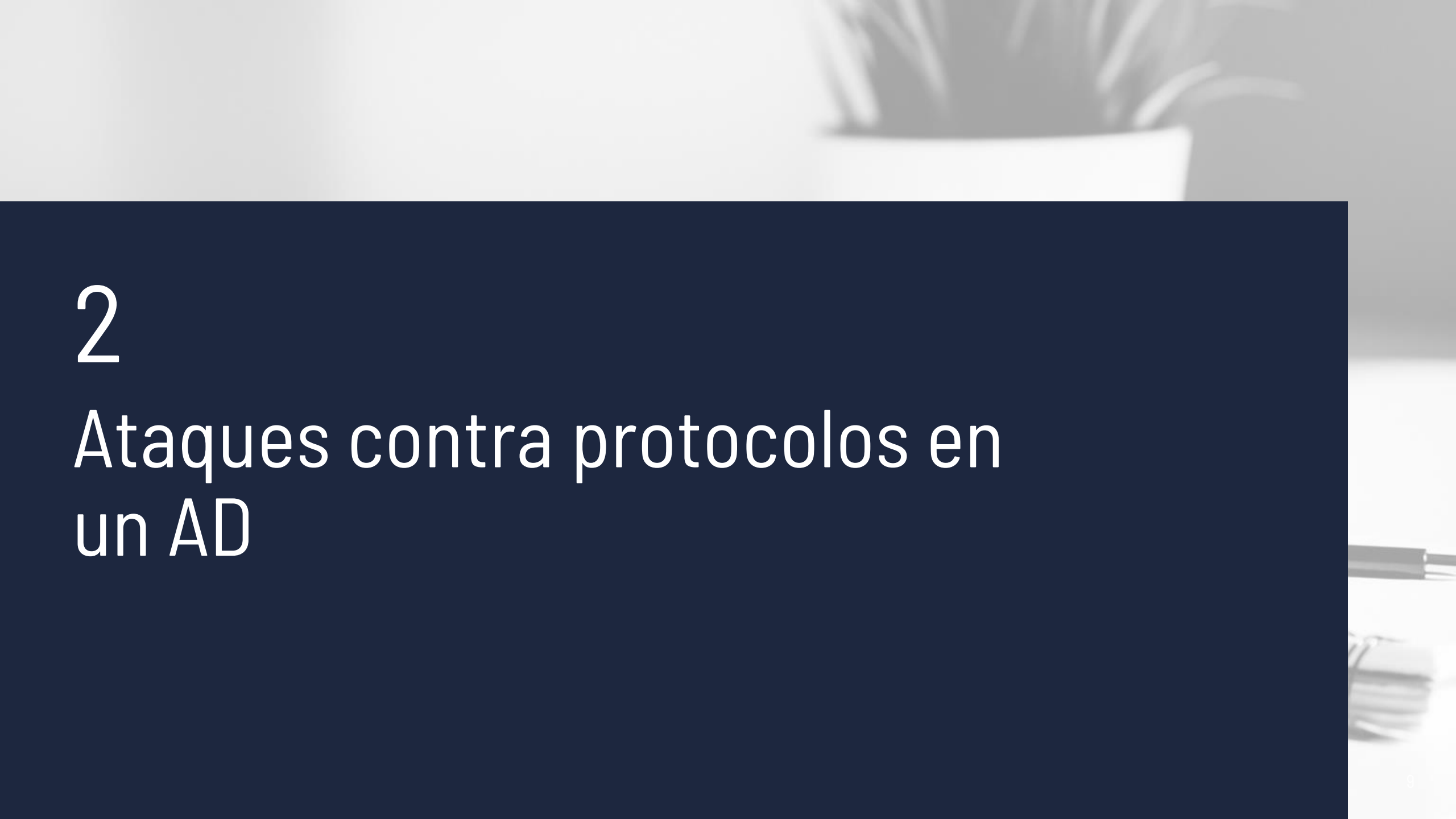


Protocolos en un Directorio Activo

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.

Los más importantes son:

- DHCP (Dynamic Host Configuración Protocol)
- DNS (Domain Name System)
- NTP (Network Time Protocol)
- LDAP (Lightweight Directorio Access Protocol)
- Kerberos
- NTLM



2
Ataques contra protocolos en un AD

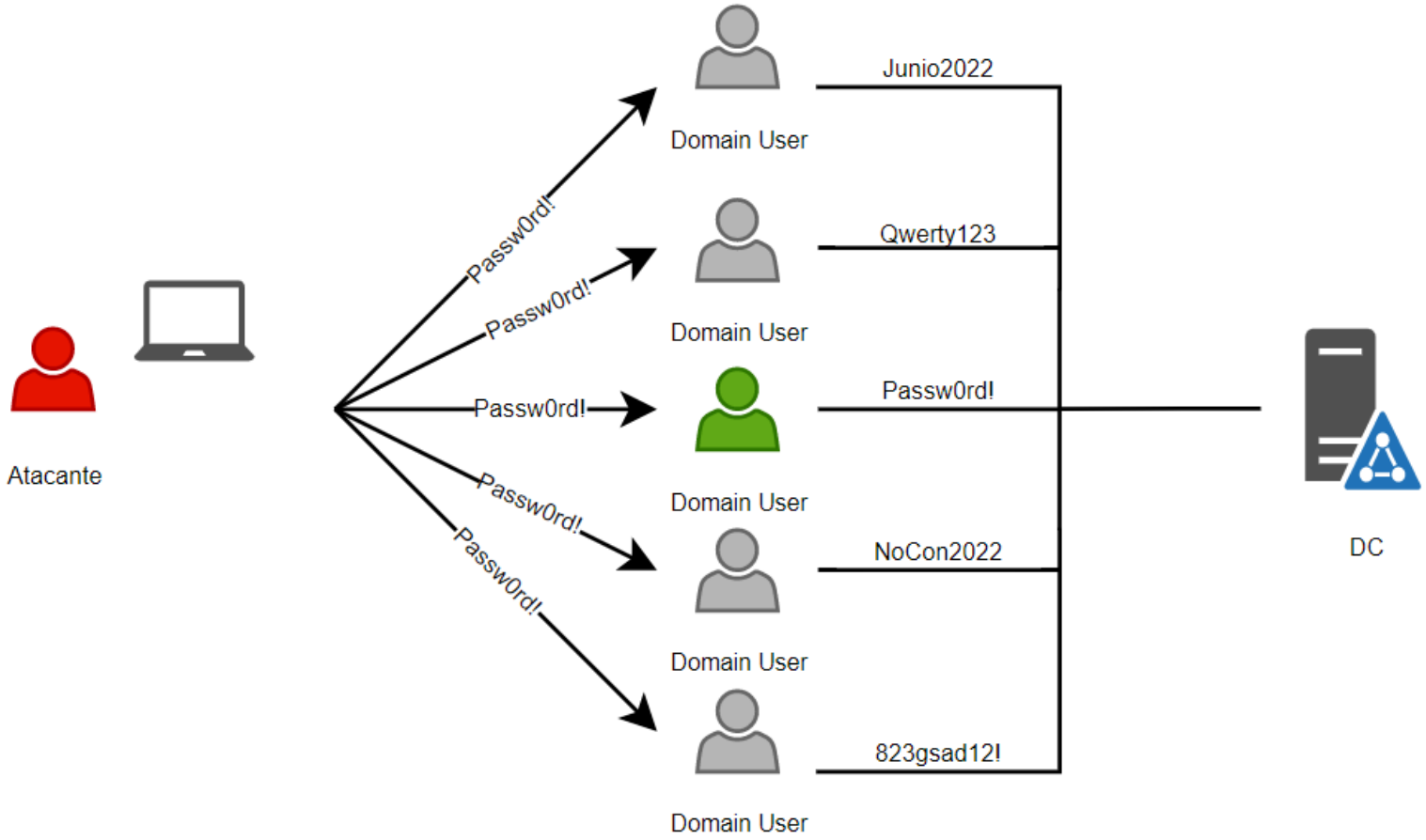
Password Spraying (LDAP)

Consideraciones

- Es posible aprovechar la presencia de LDAP para identificar credenciales válidas dentro de un dominio
- El ataque consiste en probar una misma contraseña contra múltiples usuarios del dominio sin llegar al límite de intentos fallidos permitidos para no bloquear las cuentas.

Recomendaciones

- Establecer una política de contraseñas robusta.
- Desplegar una política de bloqueo de cuentas.
- Monitorizar este tipo de ataques.



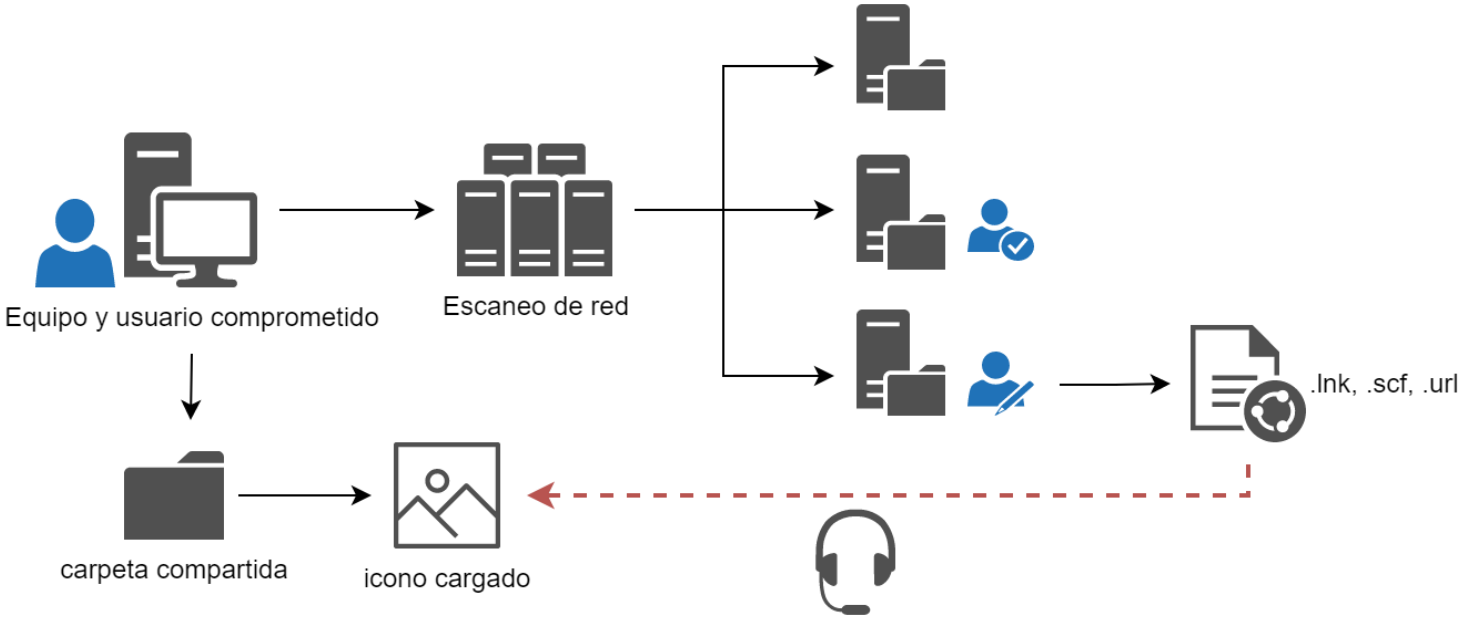
Autenticación forzada (SMB)

Consideraciones

- 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 corregido.
- Posibilidad de hacer relay.
- Posibilidad de crackear los hashes NetNTLM.

Recomendaciones

- Cerrar conexiones SMB hacia Internet.
- Habilitar el firmado de SMB.



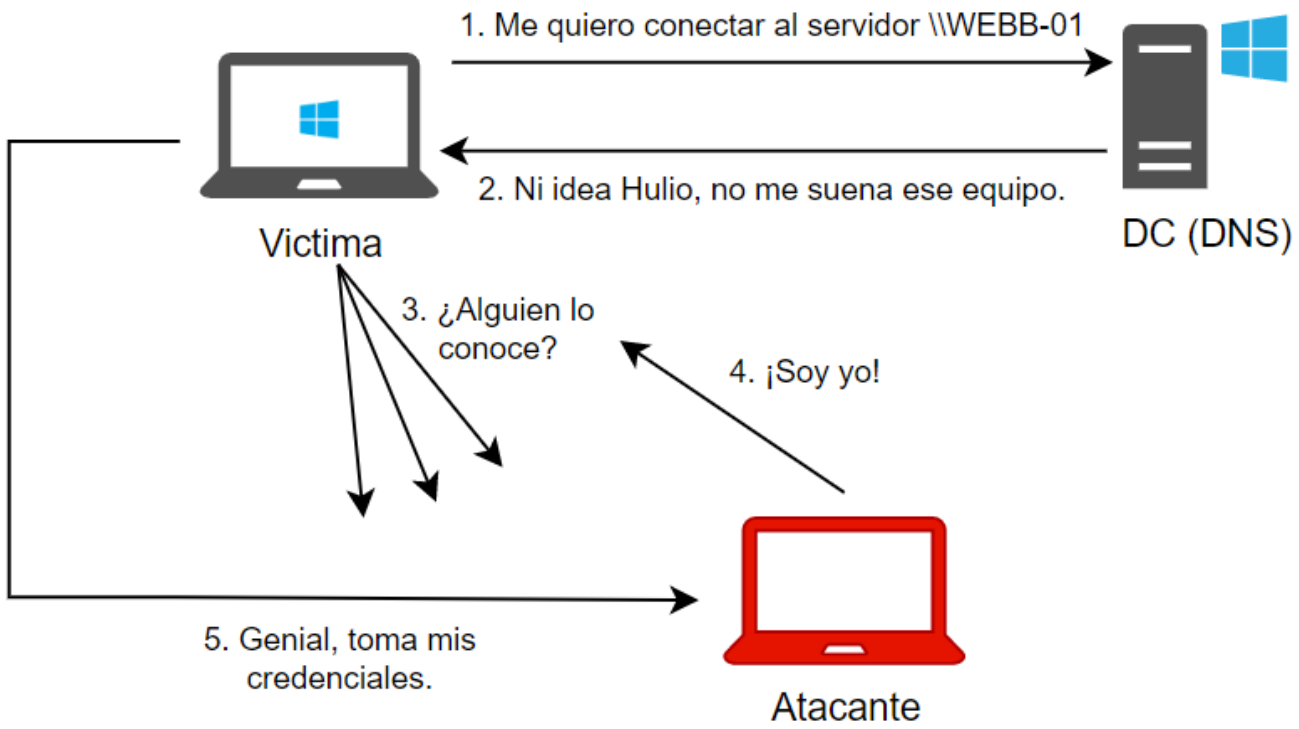
Envenenamiento LLMNR/NBT-NS

Consideraciones

- LLMNR y NBT-NS son los suplentes de DNS.
- Solo se puede abusar cuando un usuario solicita un recurso no existente en la red.
- Por defecto, ambos protocolos están activados.
- Posibilidad de hacer *relay*.
- Posibilidad de crackear los hashes NetNTLM.

Recomendaciones

- Desactivar LLMNR.
- Desactivar NBT-NS.
- Firmar SMB.



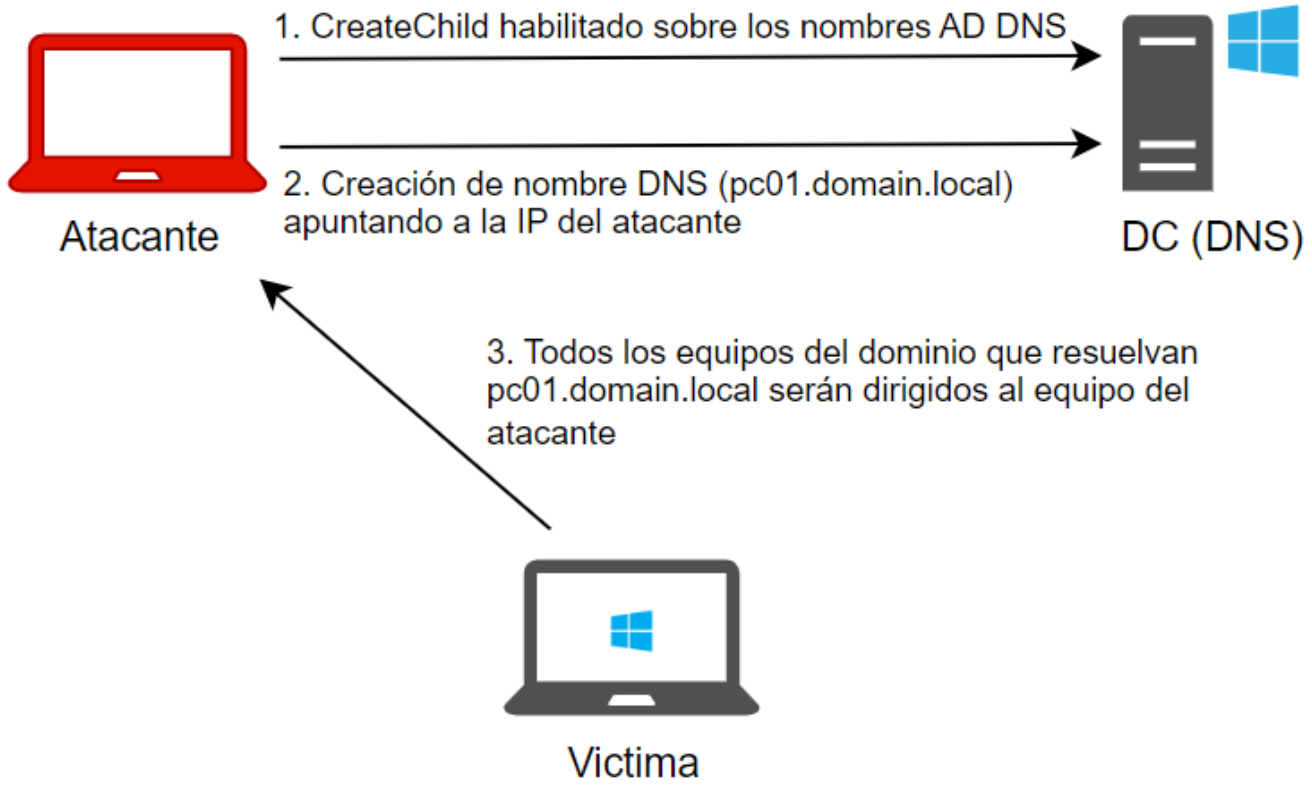
Alteración de zonas ADIDNS

Consideraciones

- Todo DC tiene almacenadas sus zonas DNS del dominio.
- Por defecto, cualquier usuario autenticado puede crear un registro DNS si no existe en una zona.
- Dicho registro será controlado en su totalidad por el usuario.
- Es viable crear registros DNS usando *wildcards*.
- Posibilidad de crackear los hashes NetNTLM.

Recomendaciones

- Eliminar el permiso *Create all child objects* de los usuarios autenticados sobre las zonas DNS.
- Crear una zona con *wildcard* para limitar dicha creación.
- Desactivar NBT-NS.
- Desactivar LLMNR.



3
Ataques contra Kerberos

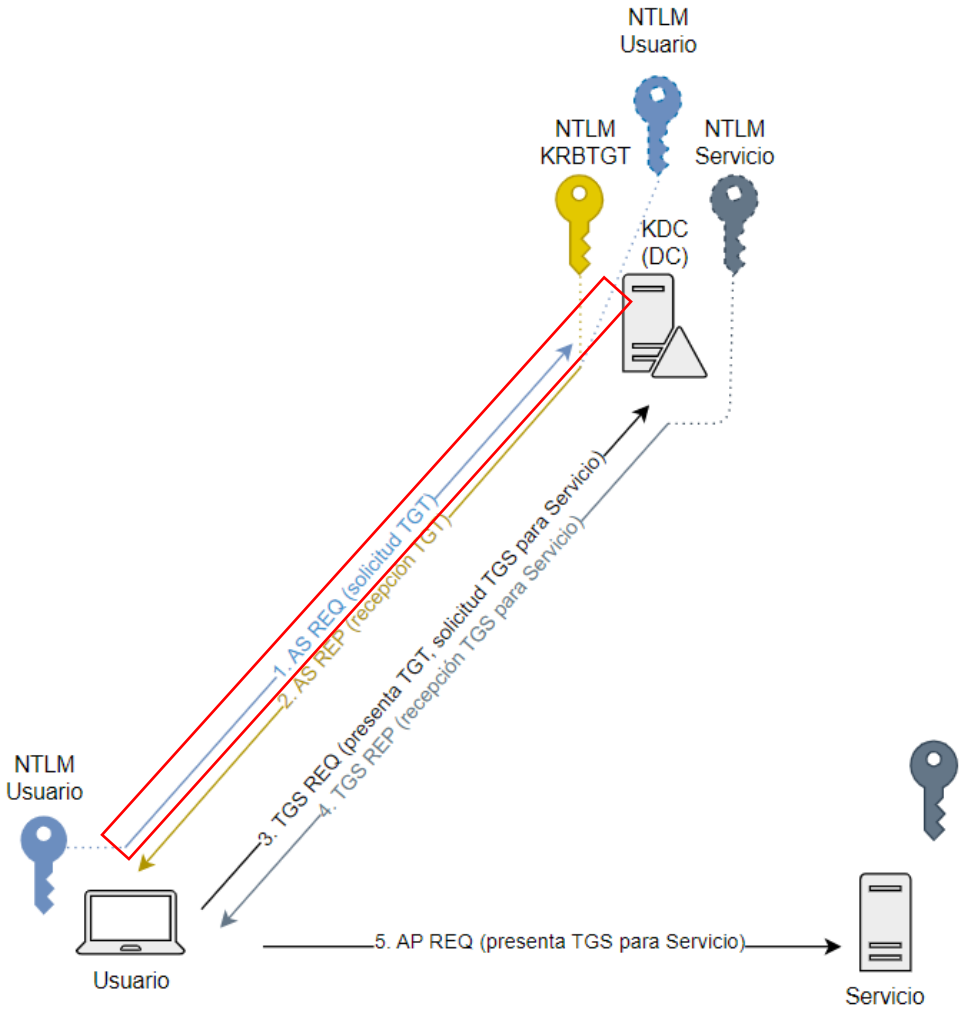
Asreproast

Consideraciones

- Cualquier cuenta de dominio necesita una preautenticación para obtener un TGT.
- Existe una opción para desactivar esa preautenticación.
- Dicha opción **NO** viene activada por defecto.
- Por defecto, Kerberos usa RC4.
- RC4 es lamentable y fácil de crackear.

Recomendaciones

- Revisar que dicha configuración no se encuentra activada en ninguna cuenta del dominio.
- Emplear contraseñas robustas para limitar la posibilidad de *crackeo*.
- Evitar activar configuraciones del AD sin saber las consecuencias.



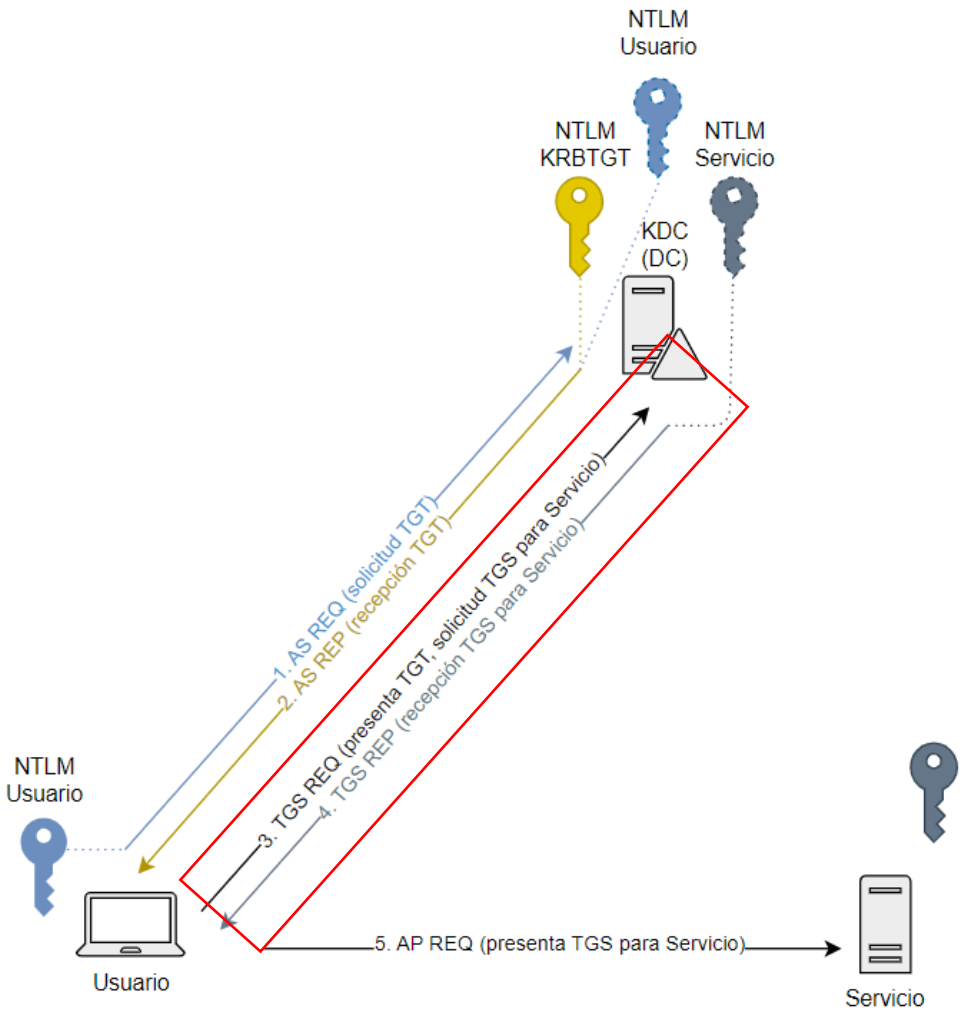
Kerberoast

Consideraciones

- Posibilidad de solicitar un **T**icket **G**ranting **S**ervice para cualquier **S**ervice **P**rincipal **N**ame por parte de cualquier usuario del dominio.
- Por defecto, Kerberos usa RC4.
- RC4 es lamentable y fácil de crackear.
- Suelen existir SPN asociados a cuentas de usuario.

Recomendaciones

- Limitar la presencia de cuentas de usuario con SPN asociado.
- Deshabilitar RC4 como algoritmo de cifrado válido.
- Establecer contraseñas robustas para estas cuentas.
- Limitar los privilegios de dichas cuentas *kerberostables*.
- ¿Crear cuentas gMSA?



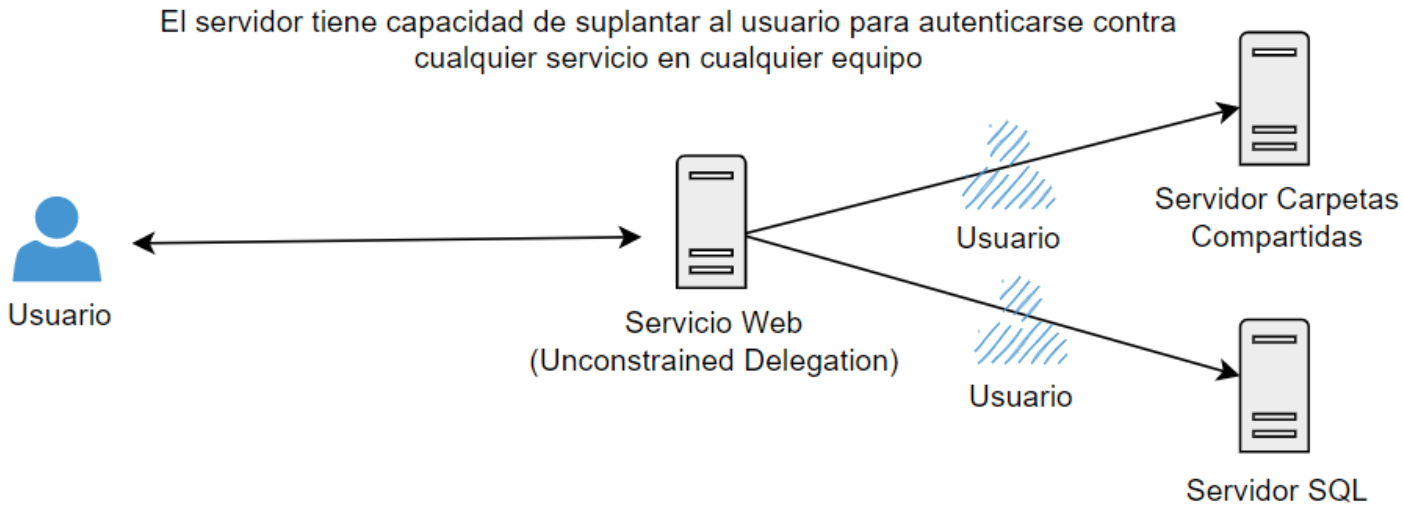
Unconstrained Delegation

Consideraciones

- Posibilidad de actuar en nombre de ese usuario para autenticarse contra cualquier servicio
- Puede asignarse a cualquier servidor existente dentro del dominio.
- Microsoft no recomienda su uso.
- Solo es viable mediante el uso de Kerberos.
- Provoca que el servidor cachee el TGT de los usuarios que hayan delegado en él.
- Posibilidad de robarlos y realizar un PTT.

Recomendaciones

- No habilitar la delegación no restringida.
- Impedir la delegación para cuentas administrativas.
- Incluir usuarios privilegiados en el grupo de *Protected Users*.



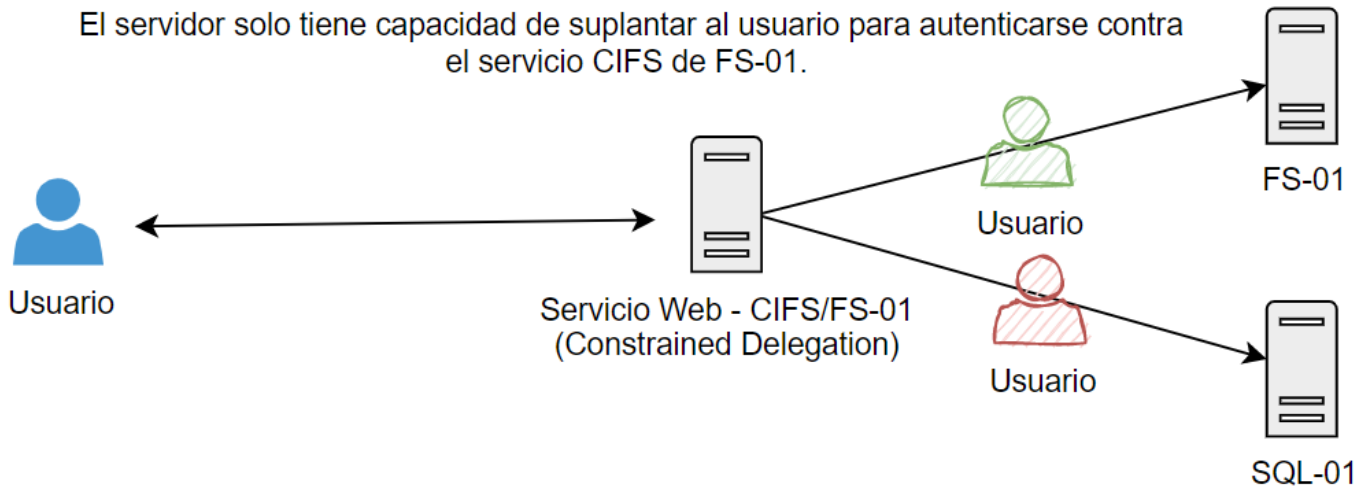
Constrained Delegation

Consideraciones

- Fue el primer intento de Microsoft de arreglar el fallo anterior. También es explotable.
- Restringe los servicios que puede solicitar un servidor para actuar en nombre de un usuario.
- Siendo SYSTEM sobre la máquina que delega, es posible solicitar TGS para cualquier servicio dado que no se validan.

Recomendaciones

- Impedir la delegación para cuentas administrativas.
- Incluir usuarios privilegiados en el grupo de *Protected Users*.
- Desplegar la delegación por roles (en caso de ser posible).



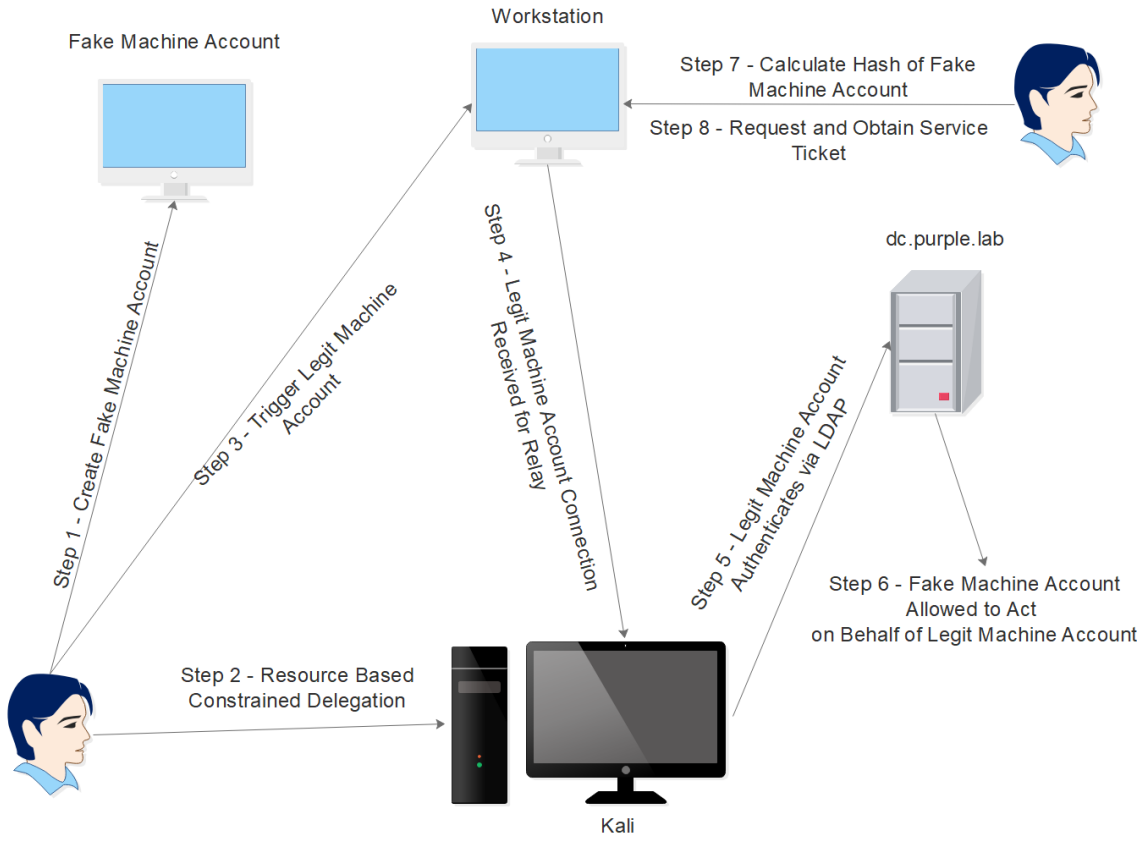
Resource-Based Constrained Delegation

Consideraciones

- Fue el segundo intento de Microsoft de arreglar el fallo anterior. También es explotable.
- Se añade una capa más. El recurso solicitado decide si dicha cuenta tiene acceso o no.
- Es posible alterar este parámetro si se tienen permisos de escritura sobre dicho objeto.

Recomendaciones

- Revisar los permisos de escritura sobre equipos del dominio con delegación restringida activada.
- Impedir la delegación para cuentas administrativas.
- Incluir usuarios privilegiados en el grupo de *Protected Users*.
- Limitar la creación de cuentas de máquina en el dominio.



Fuente: https://pentestlab.blog/2021/10/18/resource-based-constrained-delegation/

4
Aprovechando la herencia

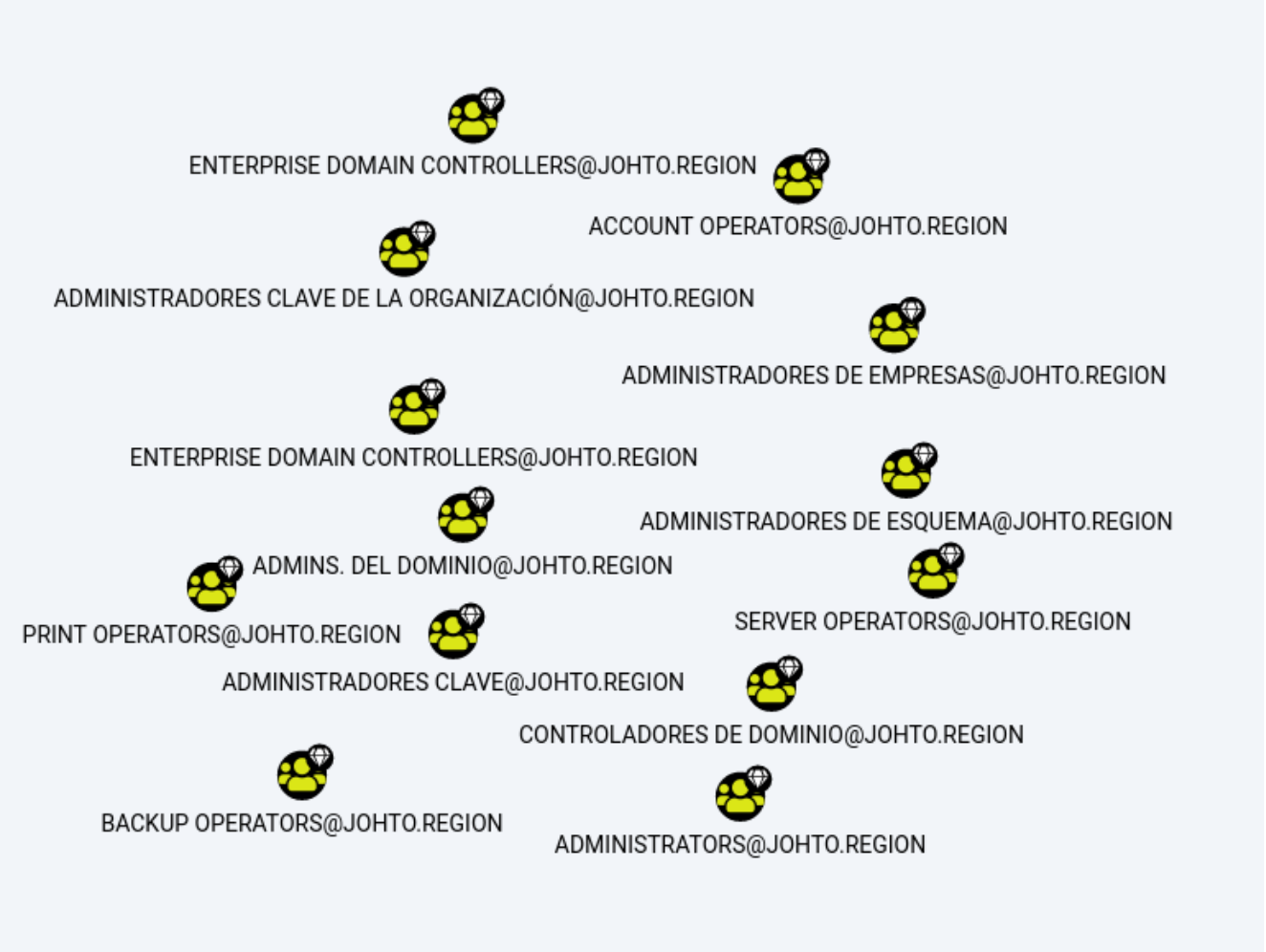
Abuso de grupos privilegiados

Consideraciones

- Existen gran cantidad de grupos con privilegios dentro de un AD.
- La pertenencia a dichos grupos puede suponer el compromiso total del mismo.
- Muchos grupos no son necesarios a día de hoy.
- Print Operators, Administrators, Domain Admins, Backup Operators, Server Operators, Account Operators...

Recomendaciones

- Revisar la pertenencia de objetos del AD a dichos grupos.
- Establecer mecanismos de seguridad para proteger dichas cuentas en caso de necesidad de pertenencia.
- Revisar las ACLs que aplican a dichos grupos.



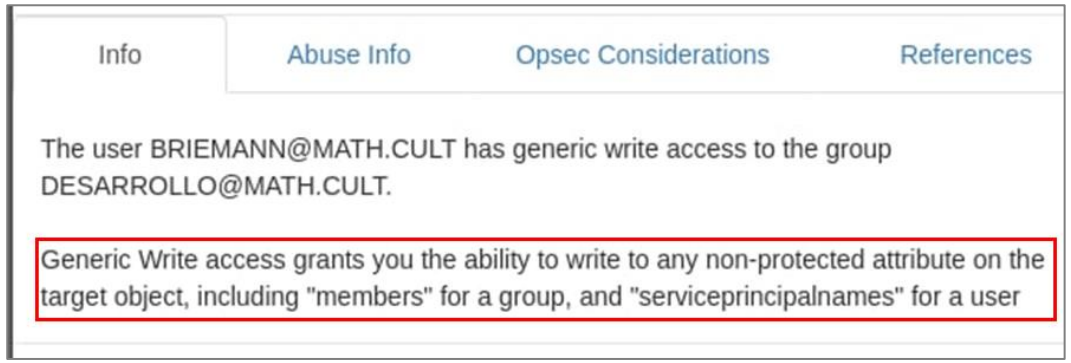
Abuso de ACLs

Consideraciones

- Las ACLs dentro de un AD son las propiedades más difíciles de bastionar.
- Siguen el modelo de herencia.
- Una ACE mal asignada puede permitir cambiar la contraseña de un usuario, autoagregarse a un grupo del dominio o acceder a una carpeta de SharePoint como lectura.
- Las carpetas compartidas sufren el mismo problema.
- En SharePoint, los permisos se gestionan de la misma manera.

Recomendaciones

- Eliminar cualquier presencia de ACEs peligrosas (GenericAll, Generic Write, WriteOwner, AllExtendedRigths, ForceChangePassword, Self-Membership) del entorno mediante el uso de herramientas ofensivas como BloodHound o Invoke-ACLScanner



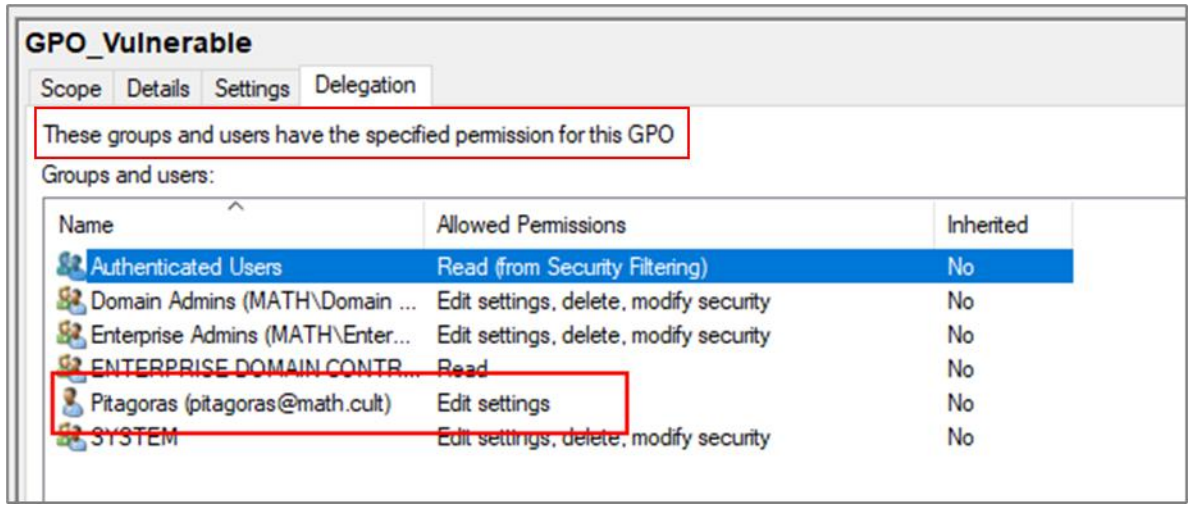
Abuso de GPOs

Consideraciones

- Son políticas que se aplican a OUs a lo largo del entorno.
- Por defecto, solo los Domain/Enterprise Admins tienen permisos para crear y editar GPOs.
- Normalmente, su gestión, suele estar delegada a grupos de administradores o usuarios con privilegios del dominio.
- Una mala gestión de estos permisos puede desembocar en usuarios con privilegios sobre ciertas (o todas) las GPOs de un entorno.

Recomendaciones

- Revisar los grupos con privilegios para gestionar las GPOs.
- Revisar la herencia de permisos de dichos grupos.
- Monitorizar intentos de alteración de GPOs existentes.
- Monitorizar intentos de creación de GPOs.



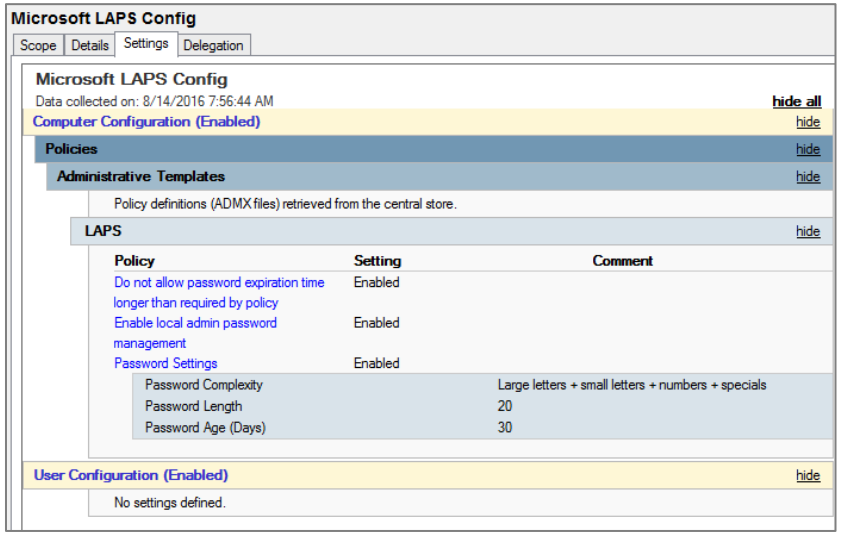
Abuso de LAPS

Consideraciones

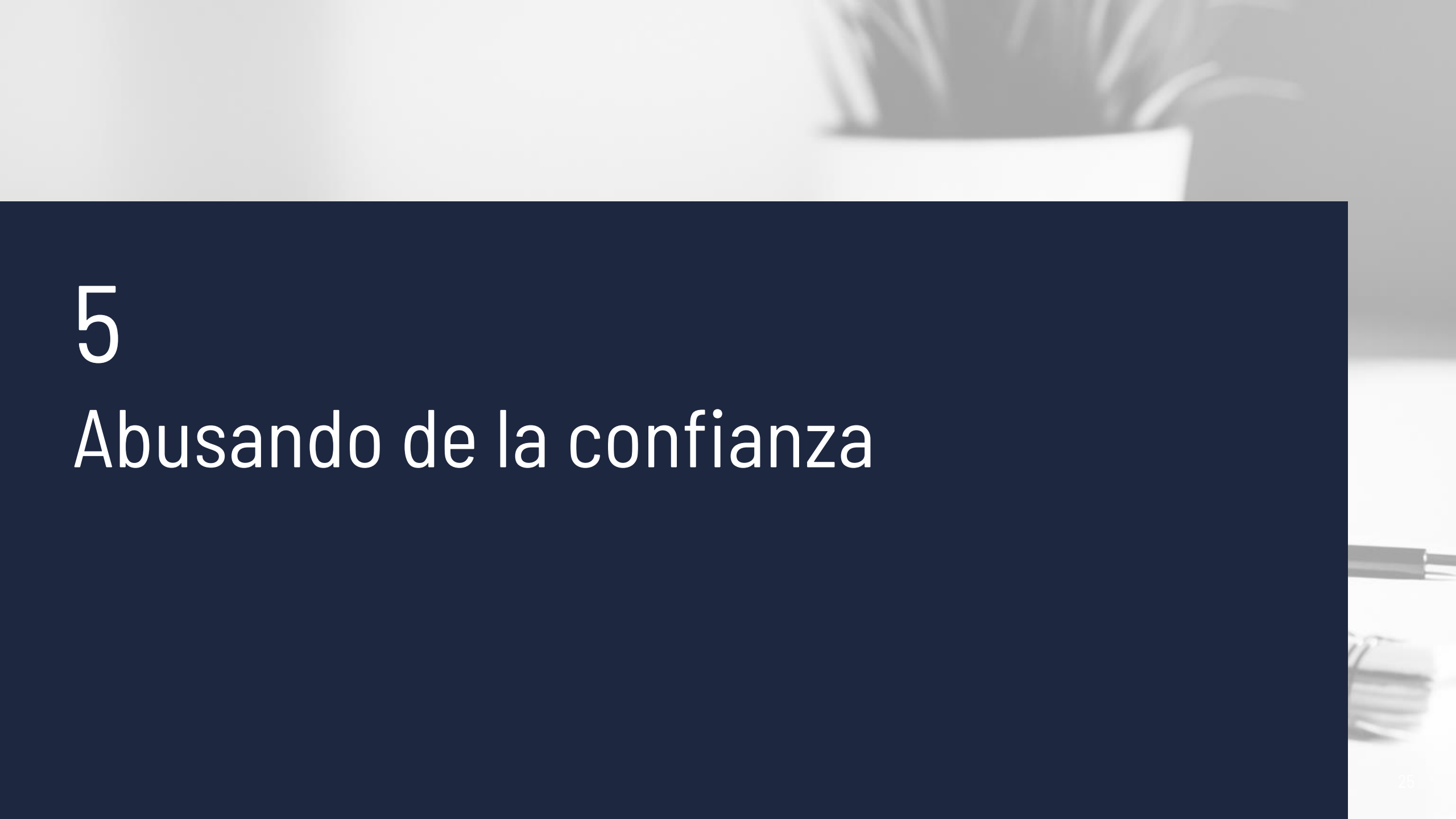
- LAPS permite gestionar de una manera única y centralizada los permisos locales de administrador de cualquier equipo de un Directorio Activo.
- Permite tener una contraseña compleja que rota cada cierto tiempo de manera automática.
- Dicha contraseña es accesible solo por los Domain Admins.
- Normalmente, la gestión de LAPS suele delegarse a otros grupos/usuarios del dominio. El compromiso de estos objetos compromete todos los equipos del dominio.

Recomendaciones

- Revisar qué grupos y qué usuarios tienen permisos para leer el atributo ms-Mcs-AdmPwd.
- Limitar la delegación de permisos críticos a la menor cantidad de usuarios/grupos de Directorio Activo.



Fuente: https://adsecurity.org/?p=3164/



5
Abusando de la confianza

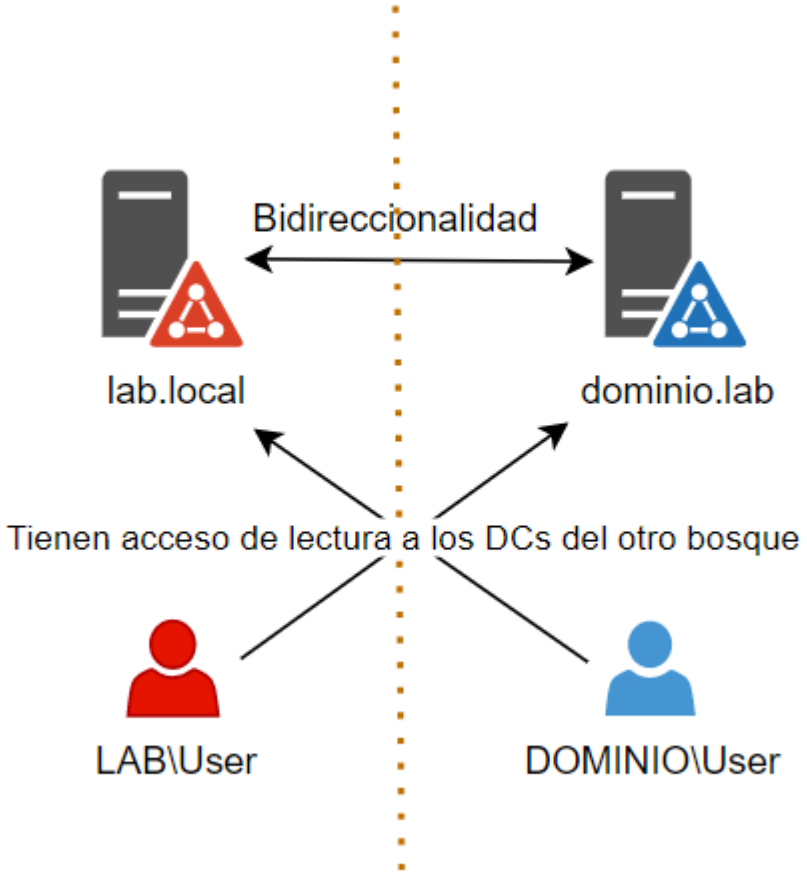
Saltos entre bosques

Consideraciones

- Una confianza bidireccional entre bosques permite acceder a los recursos de un bosque desde el otro.
- Esto implica que haya visibilidad entre ambos bosques.
- El compromiso de uno de los bosques puede permitir el acceso a los recursos del otro bosque.
- La presencia de recursos compartidos puede generar la aparición de mismos usuarios con misma contraseña en ambos bosques.
- Se podría solicitar un Inter-realm TGT para estas cuentas.

Recomendaciones

- Revisar la necesidad de tener confianza doble en este tipo de entornos.
- Evitar duplicidad de credenciales y usuarios entre bosques.
- Segmentar la red para limitar la visibilidad.



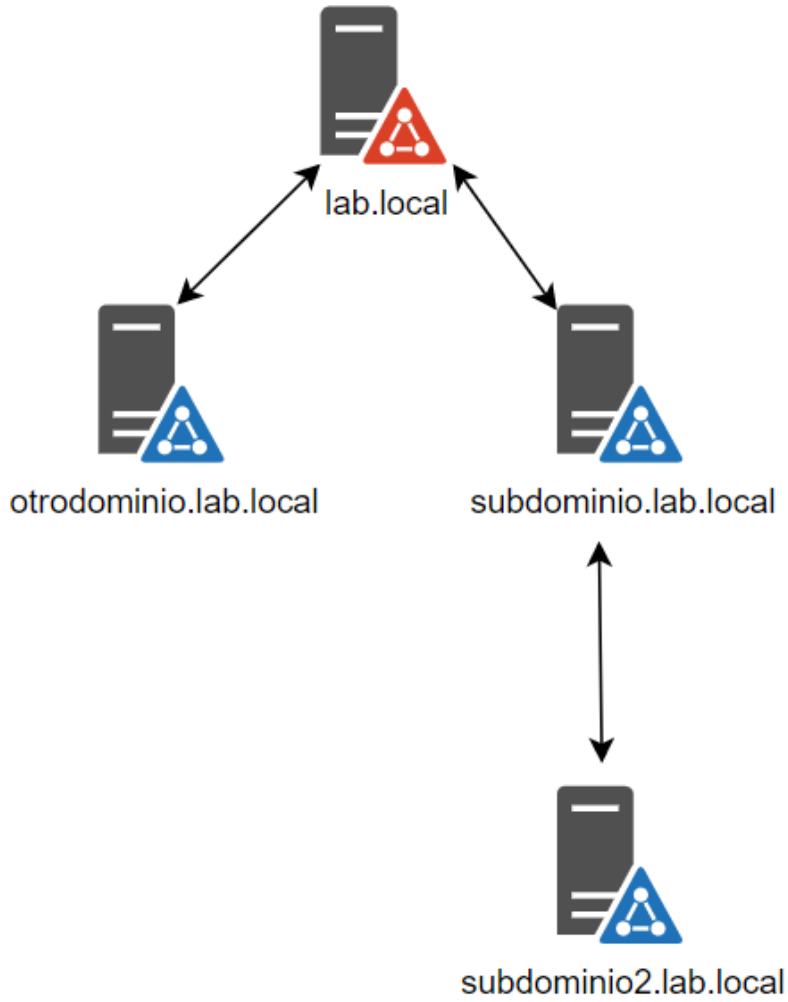
Saltos entre árboles y ramas

Consideraciones

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

Recomendaciones

- Evitar la presencia de usuarios "entre" ramas. Cada usuario debe limitarse a su dominio.
- Segmentar la red para limitar la visibilidad.
- Habilitar el SID Filtering para todos los dominios (¡pueden romperse cosas!).



Ataque SID History

Consideraciones

- Es un atributo creado para permitir los escenarios de migración.
- SID History permite clonar el acceso de una cuenta a otra y es muy útil para asegurarse de que los usuarios conservan el acceso cuando migran de un dominio a otro.
- Si dicho atributo no se elimina tras la migración, puede ser utilizado para escalar privilegios.

Recomendaciones

- Eliminar el atributo SID History una vez la migración haya sido completada.
- Aplicar el filtrado de SID entre confianzas.
- Realizar barridos en el AD para detectar estos atributos.

```
PS C:\temp\mimikatz> get-aduser bobafett -properties sidhistory,memberof


DistinguishedName : CN=BobaFett,CN=Users,DC=lab,DC=adsecurity,DC=org
Enabled           : True
GivenName         :
MemberOf          : {}
Name              : BobaFett
ObjectClass       : user
ObjectGUID        : d4d1e6c0-82a8-469f-b243-8602300e2dbe
SamAccountName    : BobaFett
SID               : S-1-5-21-1583770191-140008446-3268284411-3103
SIDHistory        : {S-1-5-21-1583770191-140008446-3268284411-500}
Surname           :
UserPrincipalName : BobaFett@lab.adsecurity.org
```

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

6
Servicios a tu servicio

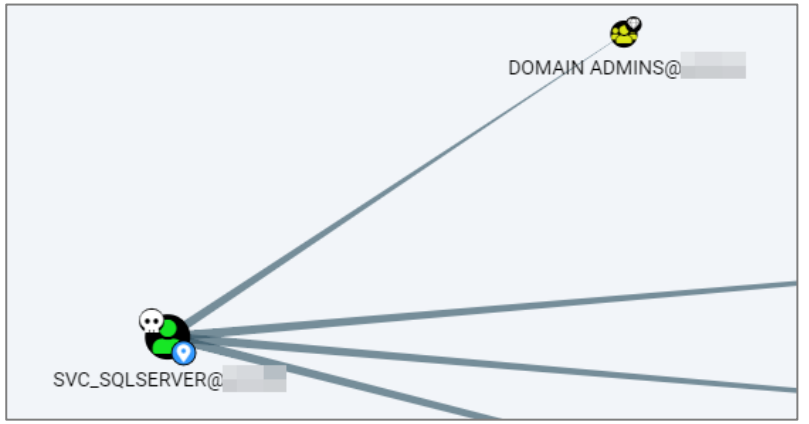
Microsoft SQL Servers

Consideraciones

- Son las gran olvidadas en un entorno de AD.
- Presentan integración con el Directorio Activo. Propensas a ataques de fuerza bruta.
- Suele estar interconectadas entre sí (Database Links) == máquina de salto entre dominios.
- Pueden configurarse como *trustworthy*, es decir, elemento confiable del AD para acceder a recursos como carpetas compartidas.
- Su cuenta de servicio suele tener exceso de privilegios por mala praxis.

Recomendaciones

- Revisar los permisos de las cuentas de servicio de la base de datos.
- Inhabilitar xp_cmdshell. Firmado de *stored procedures*.
- Revisar la presencia del privilegio *IMPERSONATE* en los usuarios sin privilegios.
- Revisar las bases de datos configuradas como *trustworthy*.



SQLQuery2.sql - SQ...H\sramanujan (51))* | SQLQuery1.sql - SQ...H\sramanujan

```
SELECT distinct b.name
FROM sys.server_permissions a
INNER JOIN sys.server_principals b
ON a.grantor_principal_id = b.principal_id
WHERE a.permission_name = 'IMPERSONATE'
-- Verify you are still running as the myuser1

SELECT SYSTEM_USER
SELECT IS_SRVROLEMEMBER('sysadmin')
--Impersonate the sa

EXECUTE AS LOGIN = 'sa'
-- Verify you are now running as the sa login
SELECT SYSTEM_USER
SELECT IS_SRVROLEMEMBER('sysadmin')
--Enable show options
EXEC sp_configure 'show advanced options',1
RECONFIGURE
--Enable xp_cmdshell
EXEC sp_configure 'xp_cmdshell',1
RECONFIGURE
--Quickly check what the service account is via xp_cmdshell
EXEC master..xp_cmdshell 'whoami'
```

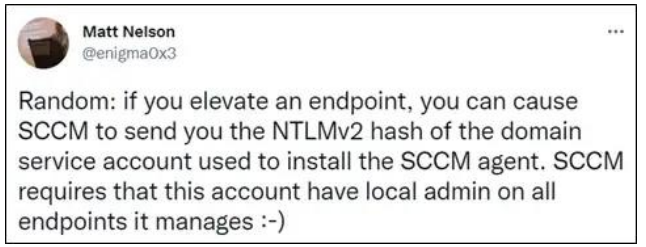
Microsoft Endpoint Configuration Manager

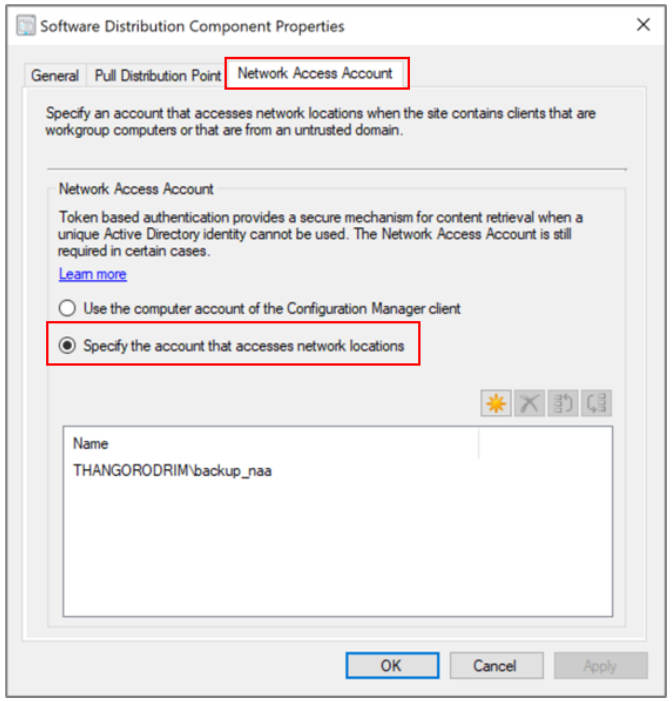
Consideraciones

- Es el nuevo nombre para SCCM (System Center Configuration Manager).
- Está desplegado en la red por medio de agentes ejecutándose como SYSTEM.
- El agente ejecuta las tareas enviadas por el servidor.
- El despliegue del agente requiere admin local para autenticarse contra la máquina e instalar el agente.
- Si se ha configurado una *NAA*, su credencial queda persistente en memoria.
- Por defecto, una instalación no es vulnerable a estos ataques.

Recomendaciones

- No utilizar *Network Access Accounts*.
- Revisar si la propiedad *Allow connection fallback to NTLM está activada*.
- No utilizar usuarios privilegiados para las instalaciones de clientes mediante push.
- Seguir la guía de instalación de SCCM de Microsoft.



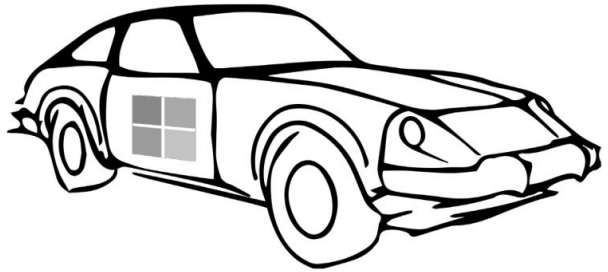


Fuente: https://posts.specterops.io/the-phantom-credentials-of-sccm-why-the-naa-wont-die-332ac7aa1ab9

Active Directory Certificate Services

Consideraciones

- Es la implementación de PKI para un Directorio Activo.
- No se instala por defecto en un entorno de AD.
- Debido a la estructura de la arquitectura, es propensa a varios ataques:
    - Robo de certificados (mediante DPAPI, robo de pfx con clave exportable o no y abuso de PKINIT).
    - Persistencia (solicitar un certificado en nombre de un usuario/máquina tras robar sus credenciales y modificar la duración de los mismos).
- Una mala configuración puede convertir la infraestructura de PKI en un camino directo hacia el compromiso del Dominio
    - Errores de configuración en plantillas de certificados (usuario a DA) – ESC1, ESC2, ESC3, ESC9 y ESC10
    - Abuso de ACE para convertir una plantilla en vulnerable o la propia CA – ESCS4, ESC5, ESC7
    - Abuso del atributo EDITF_ATTRIBUTESUBJECTALTNAME2 (usuario a DA) – ESC6
    - Abuso de la interfaz web de registro (NTLM Relay) – ESC8



Certified Pre-Owned

Abusing Active Directory Certificate Services

Fuente: White Paper Certified Pre-Owned - SpecterOps

Active Directory Certificate Services

Recomendaciones

- Monitorizar eventos clave.
- Tratar las CAs como Tier 0.
- Revisar las plantillas de certificados publicadas y bastionar los permisos de cada una.
- Proteger las claves privadas mediante hardware para evitar su robo abusando de DPAPI.
- Deshabilitar el uso de *Subject Alternative Name* (SAN) en caso de no estar siendo utilizado.
- Eliminar la presencia de AD CS HTTP endpoints.
- Leer la investigación realizada por Will Schroeder y Lee Christensen.
- Mantener los sistemas actualizados. Por primera vez en mucho tiempo, Microsoft se encuentra actualizando la arquitectura de ADCS para limitar las vulnerabilidades.

Servidores Exchange

Consideraciones

- A día de hoy, siguen existiendo servidores de Exchange *on premise*.
- Suelen ser servidores antiguos == vulnerables.
- Por defecto, los servidores Exchange tienen privilegios elevados si no se ha aplicado el parche de febrero de 2021 (manual). Suficiente para saltar a DA.
- El compromiso de este servidor compromete todo su contenido (emails) e, incluso, el AD.
- No suelen publicarse exploits públicos, pero…

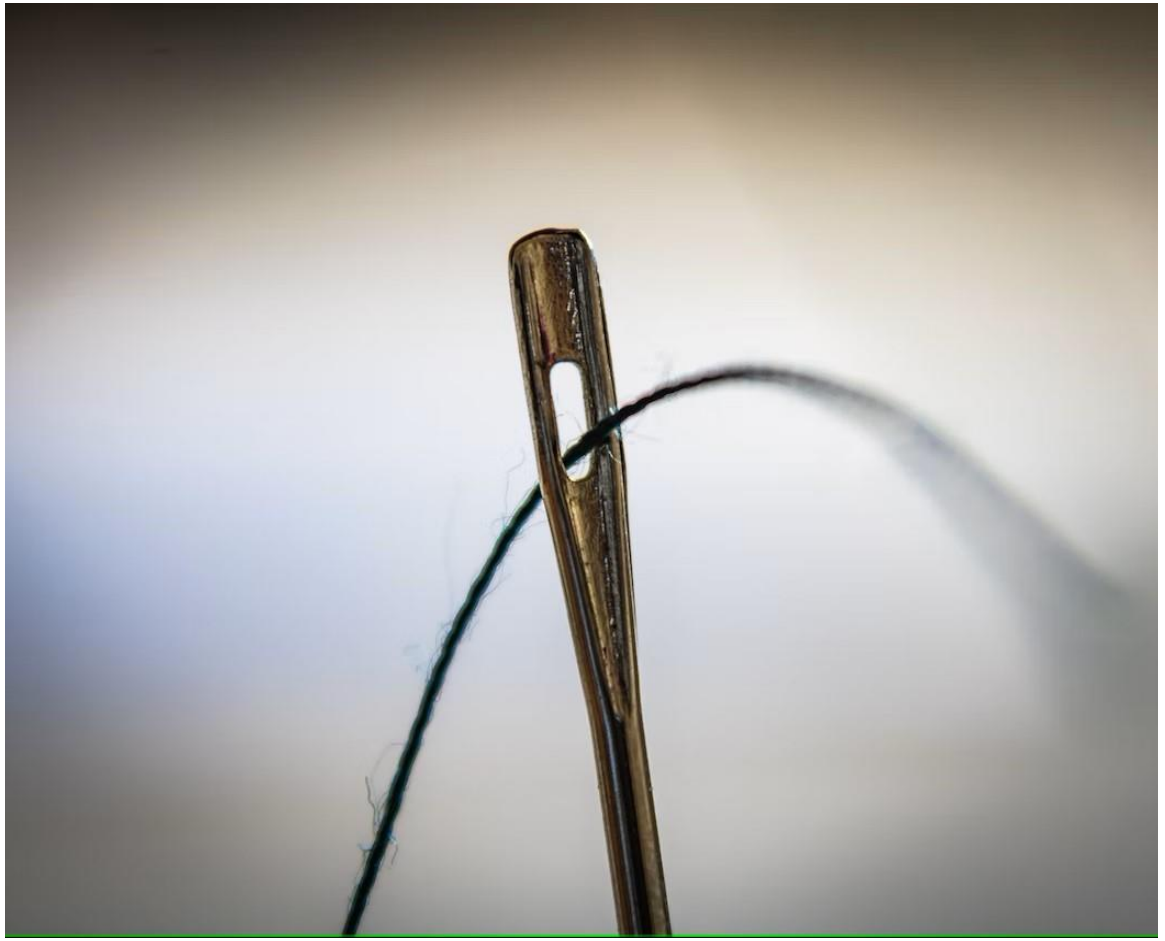
Recomendaciones

- Aplicar el parcheo manual de Exchange.
- Mantener actualizado el propio servidor.
- Migrar a Office 365 y evitar problemas.

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level
1	CVE-2022-41123				2022-11-09	2022-11-10	0.0	None
Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41080.								
2	CVE-2022-41082			Exec Code	2022-10-03	2022-11-07	0.0	None
Microsoft Exchange Server Remote Code Execution Vulnerability.								
3	CVE-2022-41080				2022-11-09	2022-11-10	0.0	None
Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-41123.								
4	CVE-2022-41079				2022-11-09	2022-11-10	0.0	None
Microsoft Exchange Server Spoofing Vulnerability. This CVE ID is unique from CVE-2022-41078.								
5	CVE-2022-41078				2022-11-09	2022-11-10	0.0	None
Microsoft Exchange Server Spoofing Vulnerability. This CVE ID is unique from CVE-2022-41079.								
6	CVE-2022-41040	269			2022-10-03	2022-11-07	0.0	None
Microsoft Exchange Server Elevation of Privilege Vulnerability.								
7	CVE-2022-34692				2022-08-09	2022-08-12	0.0	None
Microsoft Exchange Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-21979, CVE-2022-30134.								
8	CVE-2022-30134				2022-08-09	2022-09-22	0.0	None
Microsoft Exchange Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-21979, CVE-2022-34692.								
9	CVE-2022-24516				2022-08-09	2022-09-22	0.0	None
Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21980, CVE-2022-24477.								
10	CVE-2022-24477				2022-08-09	2022-09-22	0.0	None
Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-21980, CVE-2022-24516.								
11	CVE-2022-24463				2022-03-09	2022-03-14	4.0	None
Microsoft Exchange Server Spoofing Vulnerability.								
12	CVE-2022-23277			Exec Code	2022-03-09	2022-08-26	6.5	None
Microsoft Exchange Server Remote Code Execution Vulnerability.								
13	CVE-2022-21980				2022-08-09	2022-09-22	0.0	None
Microsoft Exchange Server Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-24477, CVE-2022-24516.								
14	CVE-2022-21979				2022-08-09	2022-09-22	0.0	None
Microsoft Exchange Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-30134, CVE-2022-34692.								

7
Conclusiones

En resumen:



Y eso que no lo hemos visto todo...

- Escalado de privilegios en Windows
- Persistencia (Golden Tickets, Silver Tickets, Diamond Tickets, Abuso de DSRM...)
- Pass the Hash
- Pass the Ticket
- Pass the Certificate
- Abuso del servicio de impresión (Printer Bug)
- Uso de exploits conocidos: PrintNightmare, Zerologon, SeriousSAM, SMBGhost, PetitPotam...
- Abuso de Tokens (RoguePotato, JuicyPotato, EFSPotato, RottenPotato, SweetPotato...)
- Abuso de DPAPI
- Abuso de Shadow Copies
- Abuso de Azure RBAC

8
Referencias

Referencias

- Password Spraying
- Autenticación forzada por SMB
- Envenenamiento LLMNR/NBT-NS
- Alteración de zonas de ADIDNS
- Asreproast
- Kerberoast
- Unconstrained and Constrained Delegation
- RBCD Delegation
- Abuso de Grupos Privilegiados
- Abuso de ACLs
- Abuso de ACLs II
- Abuso de GPOs
- Abuso de LAPS
- Saltos entre bosques, árboles y ramas
- SID History Attack
- Abuso de MSSQL I
- Abuso de MSSQL II
- Abuso de SCCM I
- Abuso de SCCM II
- Abuso de SCCM III
- Abuso de ADCS
- Abuso de Exchange

ZEROLYNX

No con Name

¡Gracias!