



# Shortcuts to Domain Admin

Active Directory Attacks

# net user PlainText

- ❑ Julio Ureña
- ❑ Cristiano / Esposo / Padre / Amigo
- ❑ Certificaciones: OSCP, CRTO, PACES, etc.
- ❑ Líder de la Comunidad RedTeamRD
- ❑ HackTheBox Ambassador
- ❑ Microsoft Technical Specialist Security & Compliance
- ❑ Twitter: @JulioUrena
- ❑ Blog: <https://plaintext.do>
- ❑ YouTube: <https://www.youtube.com/c/JulioUreña>





Microsoft

Active Directory

# Active Directoy

- **Active Directory:** De forma sencilla se puede decir que es un servicio establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también la administración de políticas en toda la red.
- **Azure Active Directory:** es un servicio de administración de identidades y acceso basado en la nube de Microsoft que ayuda a los empleados a iniciar sesión y acceder a recursos en:
  - Recursos externos, como Microsoft 365, Azure Portal y miles de otras aplicaciones SaaS.
  - Recursos internos, como las aplicaciones de la red corporativa y la intranet, junto con todas las aplicaciones en la nube desarrolladas por su propia organización.



Azure Active Directory

# Empecemos con las formas fáciles (Vulnerabilidades)

- Vulnerability exists within the Remote Desktop Protocol (RDP) BlueKeep (CVE-2019-0708)
- Microsoft Windows DNS Server RCE Vulnerability (CVE-2020-1350)
- Zerologon (CVE-2020-1472)





Buscar con Google

Me siento con suerte

Ofrecido por Google en: [English](#)

# Diferentes formas de Obtener Cuentas

- Fuerza Bruta
- Password Spray
- Kerberoasting
- ASREPRoasting
- Otras interesantes son ataques a nivel de red como envenenamiento de solicitudes con Responder.

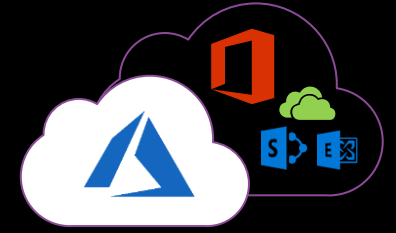


# Password Spray



Contraseña

**Compania2020!**



Microsoft Cloud



Cloud SaaS apps



On-premises  
& web apps

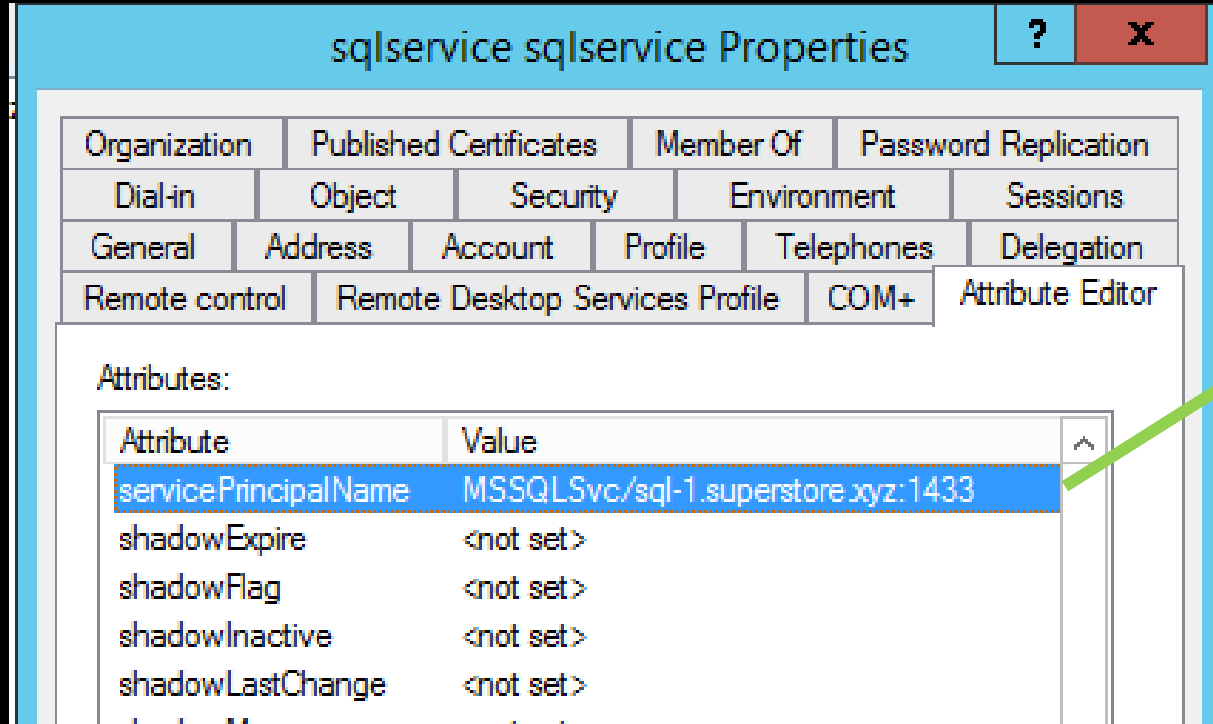
# Kerberoasting

- Los servicios corren en una maquina bajo el context de una cuenta de usuarios, esta cuenta puede ser Local o de Dominio.
- SPN (Service Principal Name) es un identificador único de la instancia de un servicio. SPNs son utilizados por Kerberos para asociar una instancia de un servicio con una cuenta.
- Parte del ticket (TGS) es encriptado con el password de la cuenta bajo la cual está corriendo el servicio.
- Kerberoasting es una técnica que nos permite hacer una solicitud de un TGS para poder hacer fuerza bruta sobre ese hash y obtener la contraseña.





# Kerberoasting



sqlservice sqlservice Properties

Organization Published Certificates Member Of Password Replication  
Dial-in Object Security Environment Sessions  
General Address Account Profile Telephones Delegation  
Remote control Remote Desktop Services Profile COM+ Attribute Editor

Attributes:

Attribute	Value
servicePrincipalName	MSSQLSvc/sql-1.superstore.xyz:1433
shadowExpire	<not set>
shadowFlag	<not set>
shadowInactive	<not set>
shadowLastChange	<not set>

Service Principal Name  
SPN

Podemos utilizar **Rubeus** o otros scripts en PowerShell para conseguir el ticket y hacer fuerza bruta sobre este para conseguir el password.



Administrator: Windows PowerShell

PS C:\Users\juurena\Desktop>



# ASREPROasting

- Cuando un usuarios no tiene pre-autenticación habilitada, AS-REP puede ser solicitado para ese usuario, esta solicitud contiene el password del usuario en forma de hash y es possible hacer fuerza bruta sobre el mismo para obtener la contraseña.
- Esta configuración se realiza en el objeto del usuario y es común en cuentas utilizadas en sistemas Linux.



# ASREPRoasting

Lisa Ewen Properties

Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
Remote Desktop Services Profile		COM+	Attribute Editor	
General	Address	Account	Profile	Telephones
Organization				

User logon name:

lewen @superstore.xyz

User logon name (pre-Windows 2000):

SUPERSTORE\ lewen

Logon Hours... Log On To...

☐ Unlock account

Account options:

- ☐ Use Kerberos DES encryption types for this account
- ☐ This account supports Kerberos AES 128 bit encryption.
- ☐ This account supports Kerberos AES 256 bit encryption.
- ☒ Do not require Kerberos preauthentication

Podemos utilizar **Rubeus** o otros scripts en PowerShell para conseguir el ticket y hacer fuerza bruta sobre este para conseguir el password.

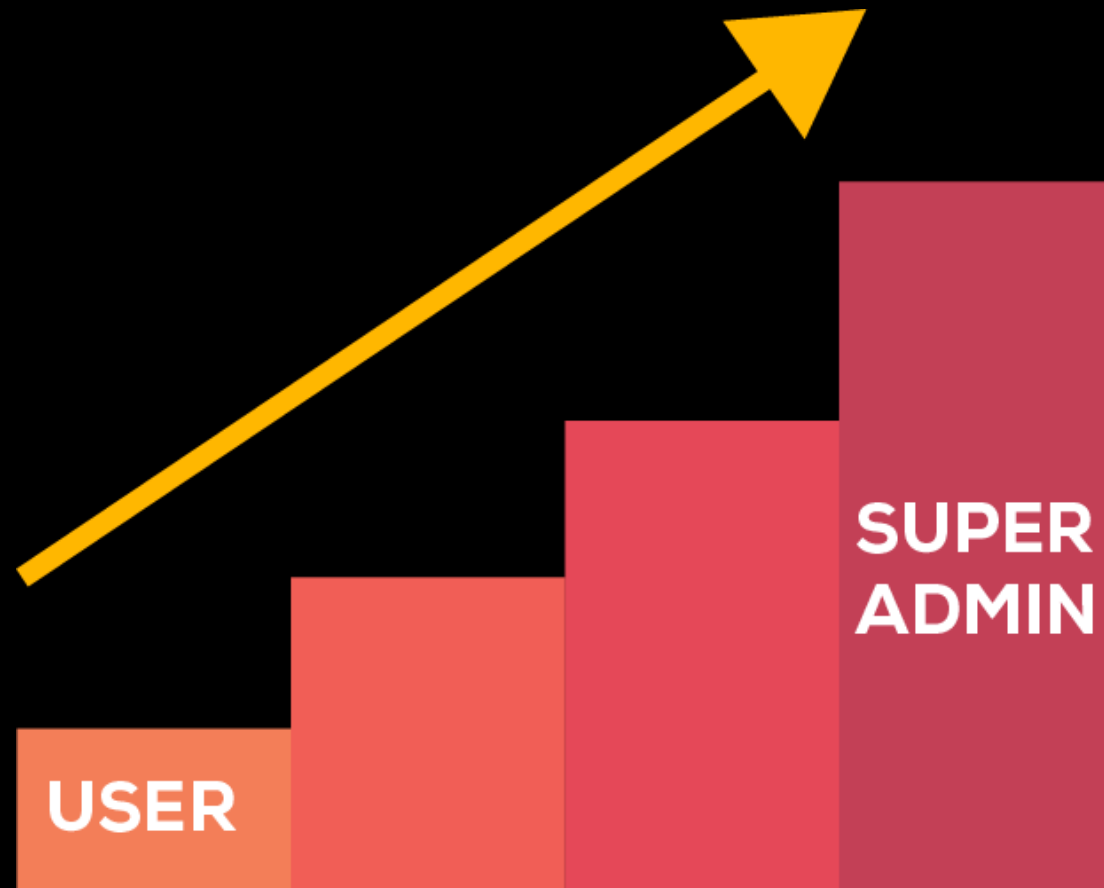
Comunmente utilizado para autenticación de equipos Linux



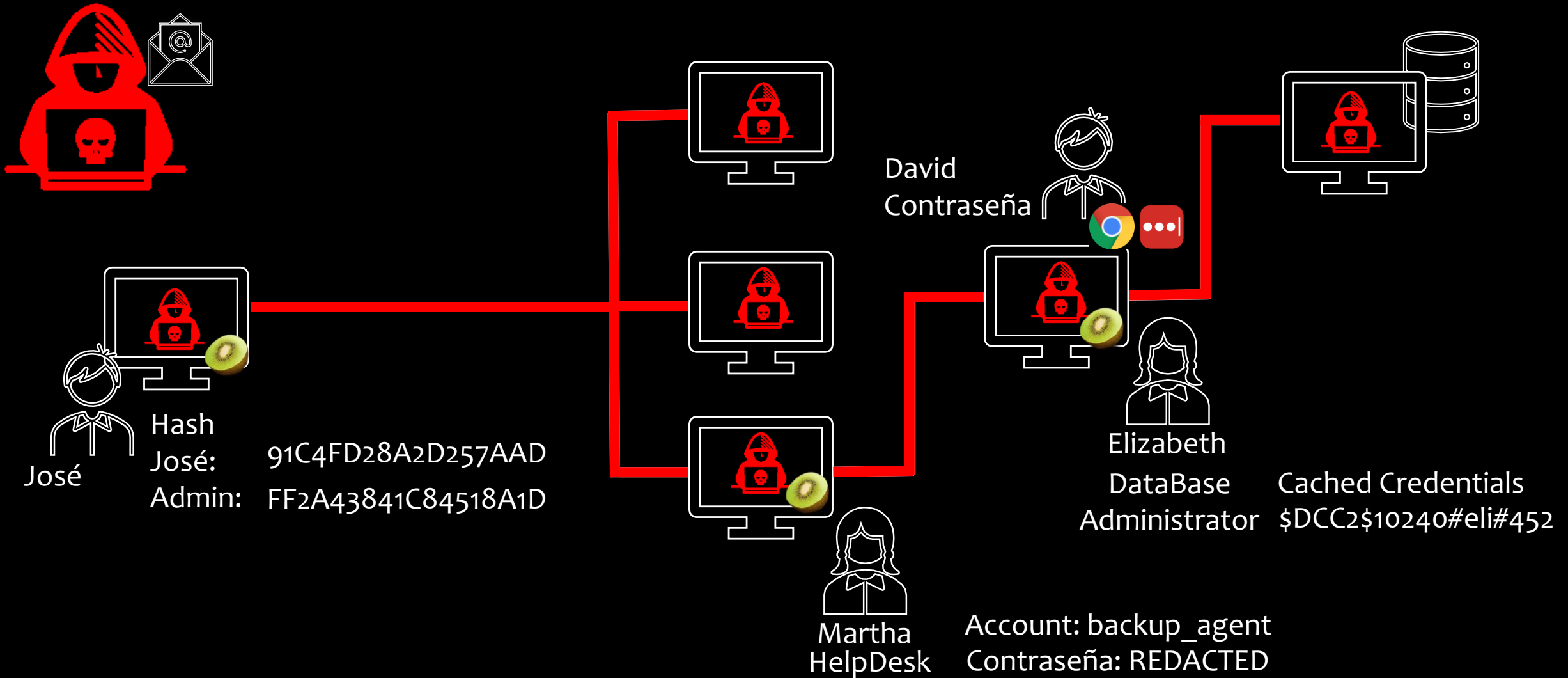
```
Administrator: Windows PowerShell
PS C:\Users\juurena\Desktop>
```

# Abuso de Privilegios en las Cuentas

- **Privilegios:**
  - Administradores Locales
  - Operadores de LAPS
  - Operadores de GPO
  - Operadores de Backups
- Unconstrained Delegation.
- Constrained Delegation.



# Todo empezó con un acceso...





tools

File Home Share View

This PC > Local Disk (C:) > tools

Search tools

Quick access

Desktop

Downloads

Documents

Pictures

Music

System32

Videos

OneDrive

This PC

New Volume (D:)

Network

Name	Date modified	Type	Size
mimidrv.sys	7/5/2020 8:59 PM	System file	37 KB
mimikatz	7/5/2020 8:59 PM	Application	1,235 KB
mimilib.dll	7/5/2020 8:59 PM	Application extens...	46 KB
procexp64	7/8/2020 10:15 PM	Application	1,456 KB
rdcman	7/8/2020 8:32 PM	Windows Installer ...	1,161 KB
SharpChromium	6/28/2020 4:54 PM	Application	571 KB

6 items

Windows Defender Security Center

Virus & threat protection settings

View and update Virus & threat protection settings for Windows Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

Cloud-delivered protection is off. Your device may be vulnerable.

Dismiss

Off

[Privacy statement](#)

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

Automatic sample submission is off. Your device may be vulnerable.

Dismiss



# Operadores: LAPS, GPO & Backups

Con ciertos privilegios es posible manipular componentes del sistema operativo para ganar acceso a otros usuarios y/o equipos.

**LAPS** – provee una forma automática de gestión de administradores locales en los computadores miembros de un Active Directory.

**LAPSToolKit** es una herramienta escrita en PowerShell que utiliza componentes de PowerView para identificar usuarios que tengan estos privilegios y mostrar las contraseñas de Administradores locales de esos equipos.

- <https://github.com/leoloobeek/LAPSToolkit>

**GPO's/Backups** – Tener acceso a cuentas con privilegios para modificar las GPO o para realizar backups comúnmente permitirá ganar acceso a otros equipos y recursos en la red.

# LAPS Enumeration

```
PS C:\> Find-LAPSDelegatedGroups
```

OrgUnit	Delegated Groups
OU=Computers,OU=Vikings,DC=loobeek,DC=net	LOOBEEK\Coaches

```
PS C:\> Get-NetGroupMember -GroupName "Coaches" | Select-Object -Property MemberName
```

MemberName
mzimmer

```
PS C:\> whoami
```

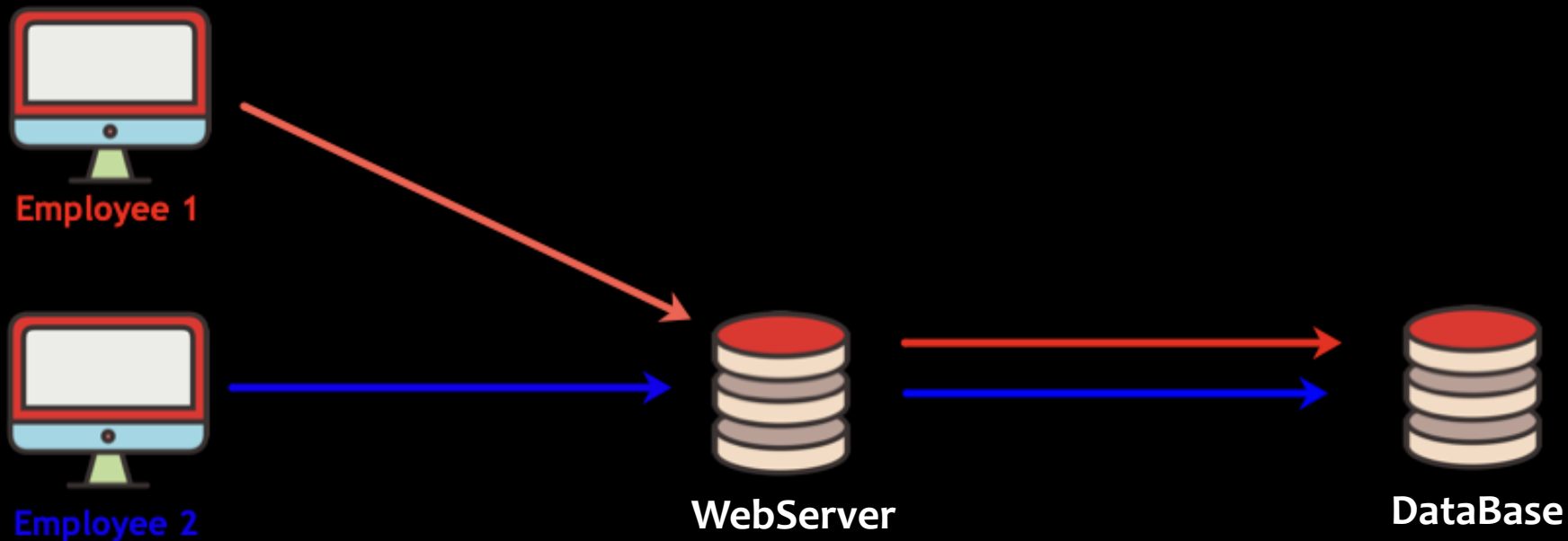
```
loobeek\tbridge
```

```
PS C:\> Get-LAPSComputers
```

ComputerName	Password	Expiration
VICTIM1.loobeek.net	4Eg;c+z4C10BYZ	08/23/2016 21:25:43

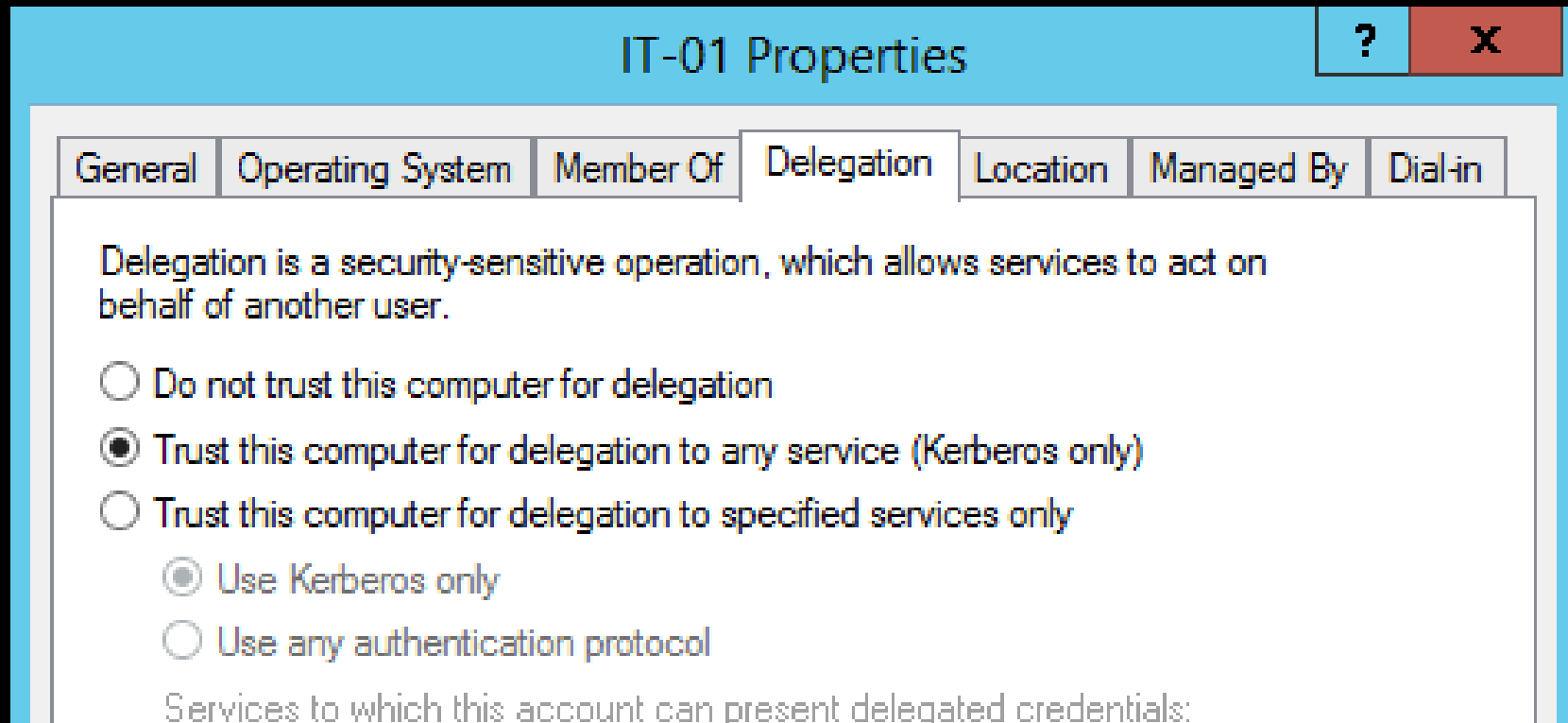
# Unconstrained Delegation

Permite a un usuarios o servicio actuar en nombre de otro usuario o servicio. Una comun implementación de esto sucede en las aplicaciones web, donde la aplicación web recibe la consulta y la pasa a otro servidor (Front-End / Back-End).



# Unconstrained Delegation

Configuración en Active Directory



The screenshot shows the 'IT-01 Properties' dialog box with the 'Delegation' tab selected. The dialog has a title bar with a question mark and a close button. The tabs are: General, Operating System, Member Of, Delegation (selected), Location, Managed By, and Dial-in. The text inside the dialog reads: 'Delegation is a security-sensitive operation, which allows services to act on behalf of another user.' Below this, there are three radio button options: 'Do not trust this computer for delegation', 'Trust this computer for delegation to any service (Kerberos only)' (which is selected), and 'Trust this computer for delegation to specified services only'. Under the third option, there are two sub-options: 'Use Kerberos only' (selected) and 'Use any authentication protocol'. At the bottom, there is a text field labeled 'Services to which this account can present delegated credentials:'.

IT-01 Properties

General Operating System Member Of **Delegation** Location Managed By Dial-in

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

☐ Do not trust this computer for delegation

☒ Trust this computer for delegation to any service (Kerberos only)

☐ Trust this computer for delegation to specified services only

☒ Use Kerberos only

☐ Use any authentication protocol

Services to which this account can present delegated credentials:



Recycle Bin



Microsoft  
Edge



Roblox



PowerView



Firefox



SharpHound



Neo4j



tools

Administrator: Windows PowerShell

PS C:\Users\juurena\Desktop>

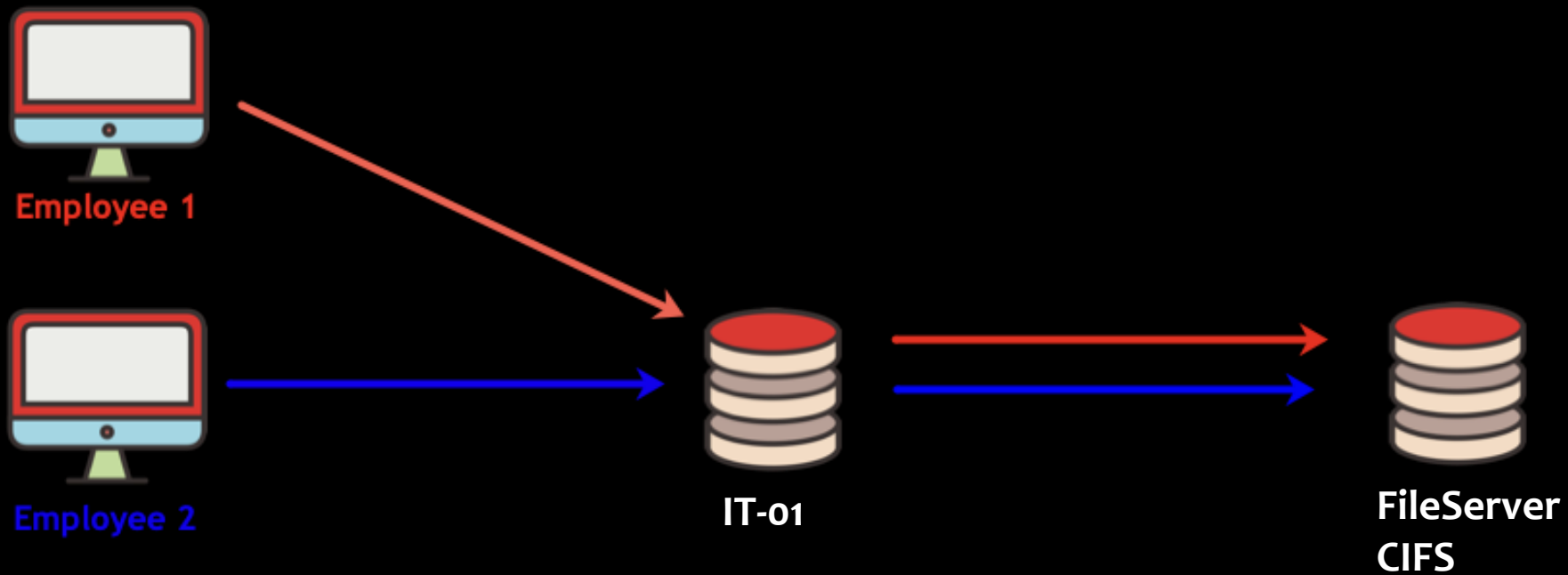
Type here to search



11:48 AM  
2/6/2021

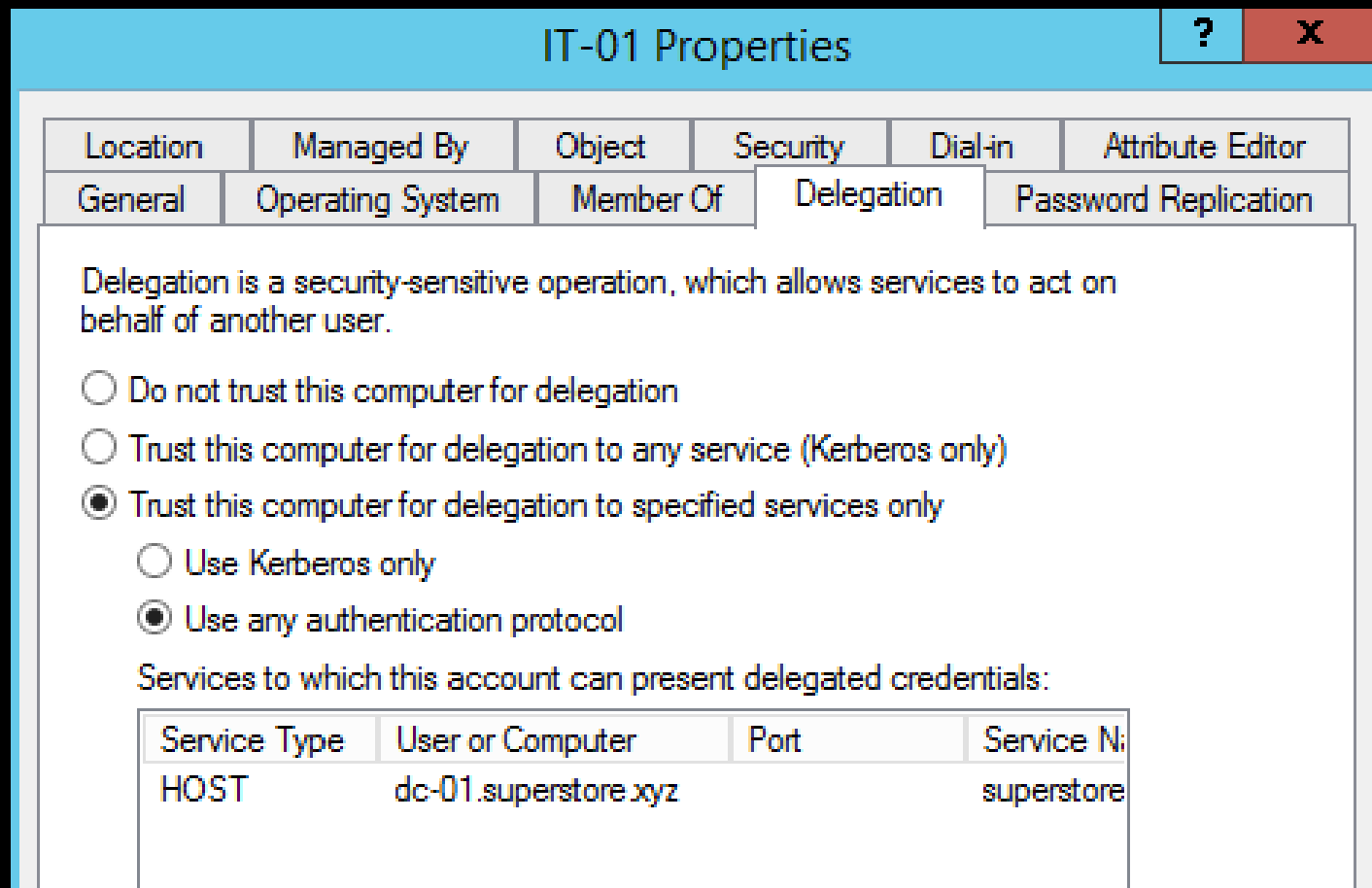
# Constrained Delegation

Constrained Delegation fue lanzado como un mecanismo seguro para hacer la delegación de Kerberos. Su función es restringir el servicio al cual el servidor puede actuar a nombre del usuario.



# Constrained Delegation

Configuración en Active Directory



IT-01 Properties

Location Managed By Object Security Dial-in Attribute Editor

General Operating System Member Of Delegation Password Replication

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

☐ Do not trust this computer for delegation

☐ Trust this computer for delegation to any service (Kerberos only)

☒ Trust this computer for delegation to specified services only

☐ Use Kerberos only

☒ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service Name
HOST	dc-01.superstore.xyz		superstore

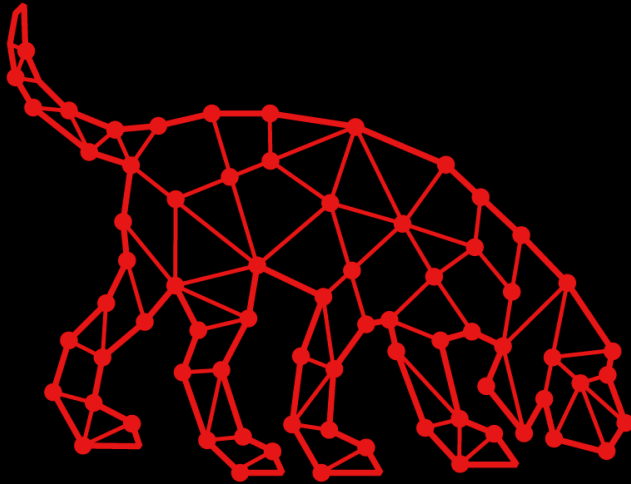


```
Administrator: Windows PowerShell
PS C:\Users\juurena\Desktop>
```



# Todo es más fácil con BloodHound

Todos los ataques anteriormente demostrados pueden ser complicados de mantener en mente, con BloodHound Podemos automatizar la recolección de información del Active Directory y los posibles ataques que podamos realizar.



BLOODHOUND



SPECTEROPS



Recycle Bin



MEMORY...



Microsoft  
Edge



Roblox



PowerView



Firefox



SharpHound



Neofj



tools



Mimikatz



2021020512...

Windows PowerShell

PS C:\Users\juurena\Desktop>



Type here to search



12:50 PM  
2/6/2021



# Extras

Más elementos interesantes de Active Directory

# De la nube a las premisas.

- BloodHound 4.0
- <https://posts.specterops.io/introducing-bloodhound-4-0-the-azure-update-9b2b26c5e350>
- Otros privilegios interesantes de la nube:
  - Intune Administrator
  - Password Administrator
  - Security Administrator
  - Custom Roles
- AD Connect



Recomendaciones

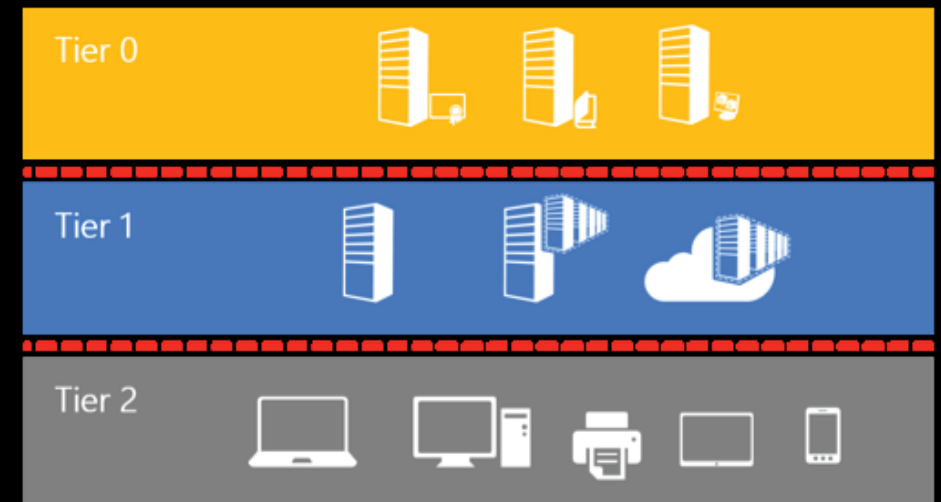
# De lo “simple” a lo complejo.

- ❑ Actualizar los controladores de Dominio.
- ❑ LAPS (Local Administrator Password Solution)
- ❑ Asignar contraseñas complejas en las cuentas de servicio.
- ❑ Revisan los privilegios/roles asignados a las cuentas.
- ❑ Comprender la superficie de Ataque de su organización.
- ❑ Uso de Tier Model



## Cuentas:

- julio\_da
- julio\_adm
- julio



# ¿Dónde puedo aprender más?

## ❑ Publicaciones de expertos

❑ <https://posts.specterops.io/>

❑ <https://adsecurity.org/>

❑ <https://dirkjanm.io/>

## ❑ Laboratorios:

❑ HackThebox

## ❑ Cursos:

❑ Pentester Academy

## ❑ Certificaciones:

❑ Red Team Ops ZeroPoint Security

❑ <https://www.zeropointsecurity.co.uk/red-team-ops>

# ¿Preguntas?

