

SPRING 19

UNIDAD 2

EJERCICIOS 1 Y 2

*MÉTODOS“KERBEROASTING Y PASS THE TICKET”*

En el presente documento, se van a realizar dos ejercicios relacionados con la unidad 2 de este spring 19, para el cual, se ha montando el presente laboratorio. El orden de prelación para activar cada una de las máquinas en la aplicación *“Virtual Box”* debe ser:

- Kali

- Windows DC

- Windows User

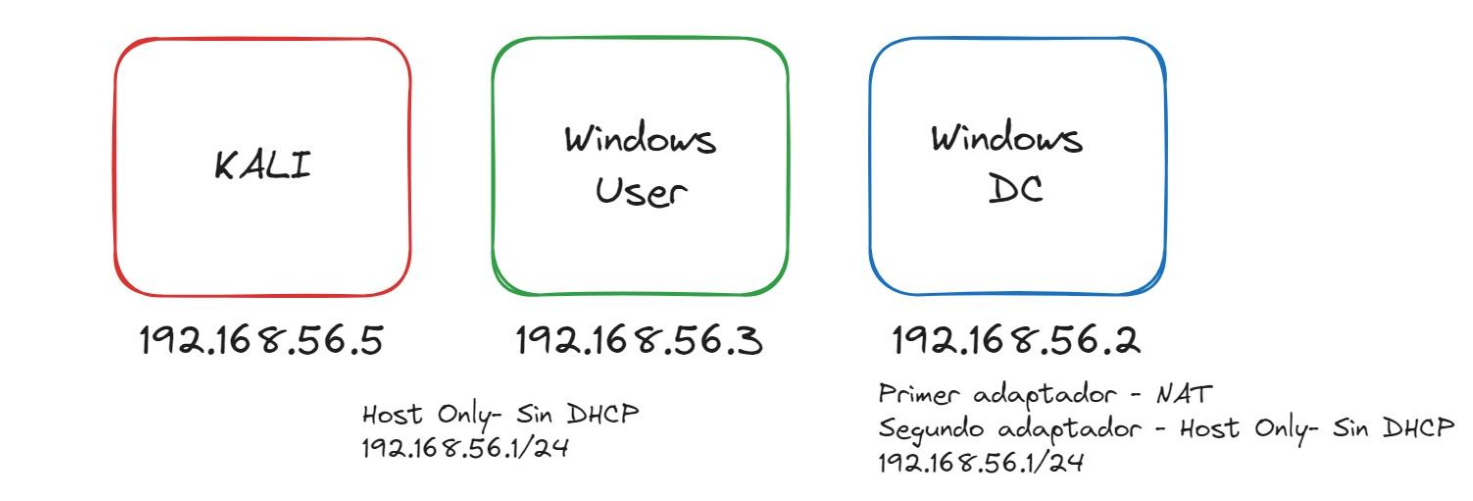


Imagen 1.- estructura del laboratorio

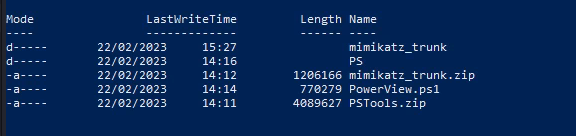
**-- EJERCICIO\_1.**- En este primer ejercicio debes ser capaz de ***generar un “Silver Ticket”*** pudiendo acceder al Disco Duro del controlador de domino desde ***un usuario sin privilegios***; para ello deberás utilizar las credenciales:

*”jane.doe:HeyH0Password”*

Para la realización de este ejercicio , se han realizado las siguientes gestiones:

- **INTRODUCCIÓN.-** Un Silver Ticket es un tipo de *ticket de autenticación* en el protocolo *“Kerberos”,* que se usa para acceder a servicios específicos dentro de una red (SQL, servicios web, etc), sin necesidad de autenticarse primero en el controlador de dominio. En términos de ataques, un ***“Silver Ticket Attack”*** implica que un atacante crea un ticket de autenticación falsificado dentro de “Kerberos”, al obtener la clave hash del servicio deseado, permitiéndole acceder directamente a ese servicio sin pasar por el controlador de dominio, lo que dificulta su detección.

Las herramientas usadas para la resolución del ejercicio, en un entorno real deberían ser transportadas desde la maquina atacante a la atacada para su uso, pero en este laboratorio de pruebas , ya se encuentran presentes en el escritorio del sistema atacado en el directorio: C:\Users\jane.doe\Desktop\Tools.



**- GESTIONES:**

1. Una vez conectado el laboratorio se comprueba que las maquinas están conectadas entre si con la configuración adecuada:

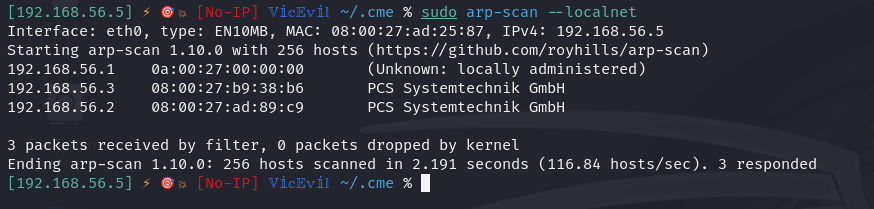


Imagen 2.- Consulta de los dispositivos conectados a la red

1. Se procede a la conexión a través de RDP con la maquina “Windows User” con IP 192.168.1.3, usando las credenciales facilitadas:

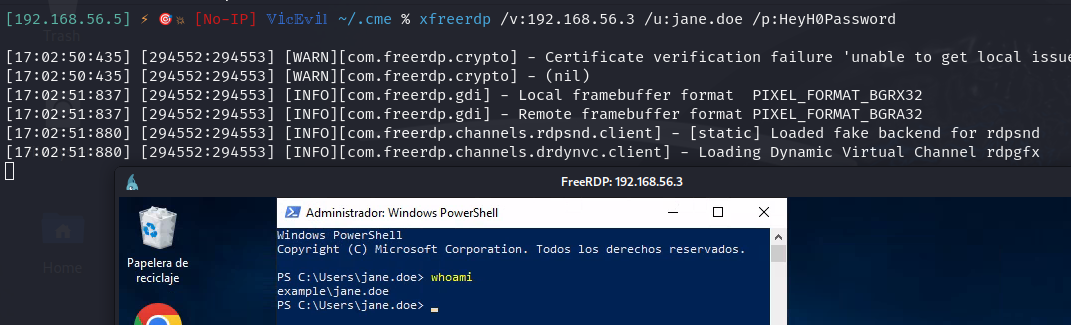
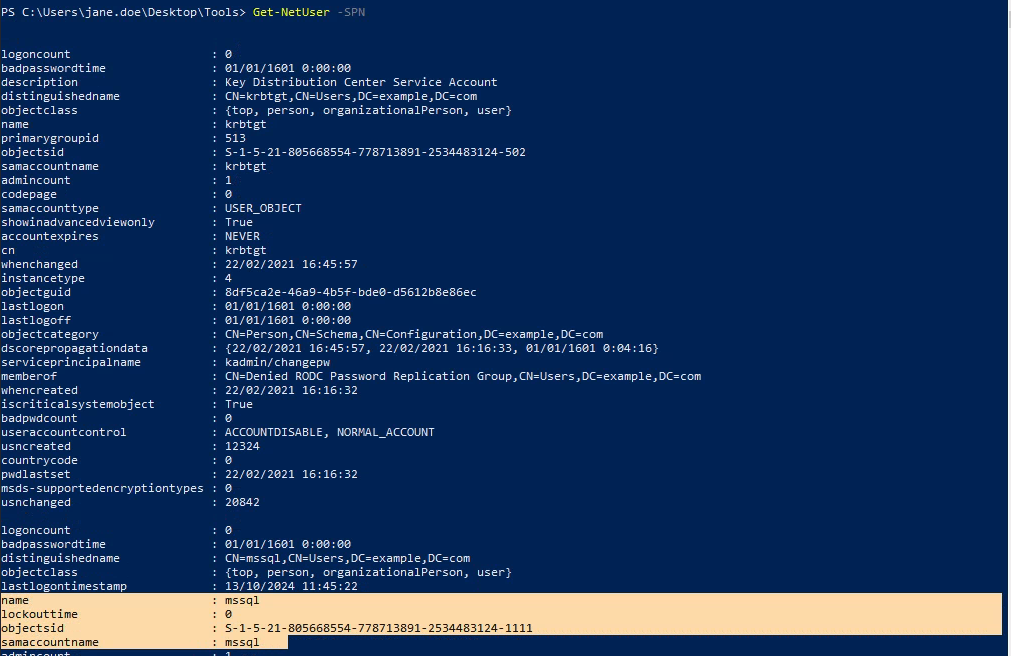
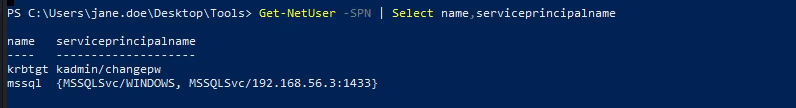


Imagen 3.- Conexión mediante el comando “xfreerdp” a la maquina Windows User

1. Una vez conectados, procedemos a utilizar la herramienta ***“PowerView”***, la cual, forma parte de la suite “*PowerSploit*”[[1]](#footnote-0), diseñada para realizar reconocimiento en redes*, p*ermitiendo enumerar información crítica en un dominio, como usuarios, grupos, permisos, entre otros, siendo especialmente útil para identificar posibles objetivos y rutas de ataque dentro de un entorno de *“Active Directory”*. Una vez ejecutada la herramienta en la máquina atacada, mediante el comando: ***“. .\PowerView.ps1”,*** se enumerará la información necesaria para poder generar el ticket TGS para el servicio que queremos ejecutar( Silver Ticket), consultando los ***“Nombres del Servicios Principales” (SPNs).***

Los ***SPNs,*** son identificadores únicos que asociados a un servicio de red con una cuenta específica de algún usuario o servicio perteneciente al controlador del dominio(AD, en adelante), siendo esenciales para la autenticación en Kerberos, permitiendo que los servicios de la red identifiquen y autentiquen al usuario o servicio, sin necesidad de contraseñas.

Imagen 4.- Consulta de los atributos de la cuenta de servicio en Active Directory

1. Se amplia información del servicio *“mssql*” , para conocer el nombre completo del SPN y su host, enumerando el atributo concreto SPN para el servicio citado, obteniendo ***“MSSQLsvc/WINDOWS”,*** el cual es necesario para la petición del ticket TGS al KDC.

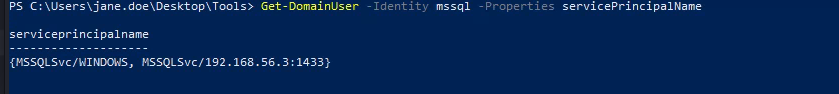


Imagen 5.- Comando consultando los atributos del SPN del servicio MSSQL

1. Ya que tenemos un usuario comprometido del CD del AD, se solicita, y con el SPN concreto y su host del servicio, se solicita el **hash del usuario** del *servicio de Microsoft-SQL con* ***SPN:***  ***"MSSQLSvc/WINDOWS"***

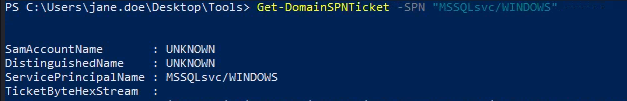




Imagen 6.- Hash del servicio que vamos a suplantar

1. Una vez obtenido el hash del servicio, procedemos a copiar en un documento .txt el hash Kerberos en nuestra Kali Virtual, donde se hacen varias pruebas con diferentes hashes obtenidos tras reinicios y restauración de las maquinas, incluso intentándolo con el usuario john.doe, usando hashcat con diferentes opciones para su descifrado, tanto con el diccionario habilitado en el ejercicio y con el rockyou, con resultado negativo, no descifrando el hash.

También lo he probado directamente en mi Kali-host con idénticos resultados. Se significa que en la tarde del día 30 de octubre, mientras visualizaba y realizaba los vídeos del workout, me ha descifrado la contraseña Admin.123, pero en estos momentos no, desconociendo el motivo.



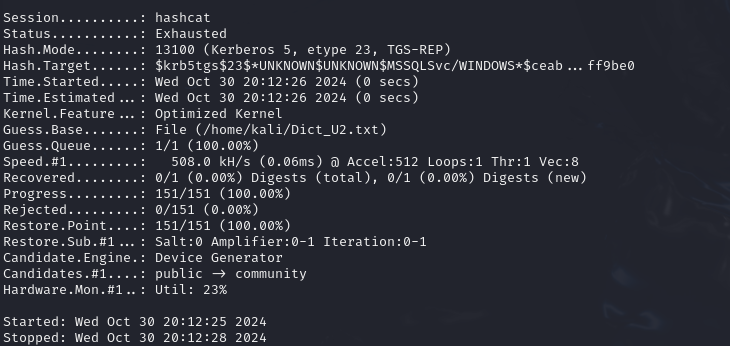


Imagen 7.- resultado infructuoso reiterado del descifrado del hash de Kerberos de jane.doe

1. **Por intentar realizar el ejercicio**, vamos a usar el usuario vagrant, aunque no haya podido hashear la contraseña, ya que es conocida la misma por el alumno.
2. Una vez conseguida la contraseña *“vagrant”,* se procede a realizar el volcado de la base de datos del Controlador de Dominio, consultando, en primer lugar, la BBDD Sam del equipo “Windows User” y después con el **“hash NTLM**” del usuario vagrant : e02bc503339d51f71d913c245d35b50b, el volcado de la BBDD NTDS.dit del controlador de dominio del entorno Active Directory.

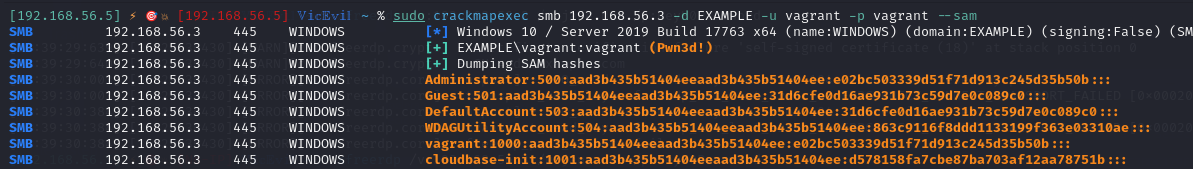


Imagen 8.- Volcado de la base de datos SAM del equipo “Windows User”

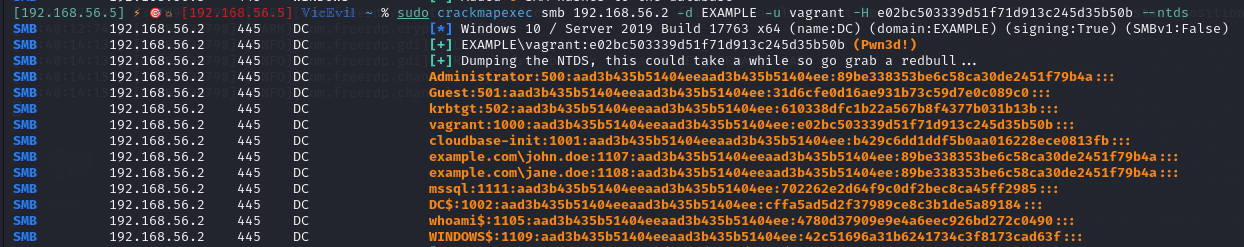


Imagen 9.- Volcado de la BBDD NTDS del Controlador de Dominio del Entorno AD

1. Ahora vamos a preparar el Silver Ticket, habiendo borrado previamente los tickets almacenados en la máquina Windows User (comandos klist y klist purge). Para ello, necesitamos:

- Nombre del Dominio: ***example.com***

- SID del Dominio.- Es un identificador único que representa a un dominio específico, siendo la base para generar objetos dentro del dominio (grupos, usuarios y equipos). En nuestro caso es: **S-1-5-21-805668554- 778713891-2534483124**



Imagen 10.- Identificador de seguridad del Dominio en el entorno Active Directory

- Nombre del equipo de conexión: ***DC***

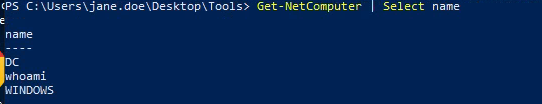


Imagen 11.- Consulta de los equipos conectados al CD, filtrado por su nombre

- Hash NTLM del usuario administrador del CD: **e02bc503339d51f71d913c245d35b50b**.

- Nombre del usuario atacado o suplantado: ***Administrator***

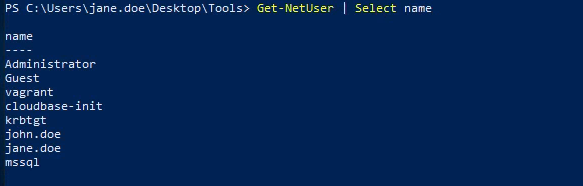
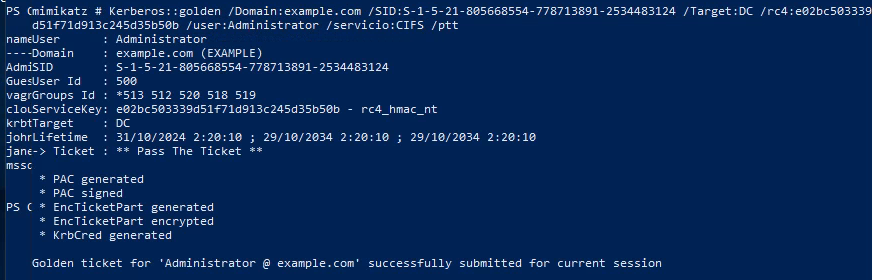


Imagen 12.- Consulta de los usuarios del controlador de dominio, filtrado por su nombre.

1. Se procede a la realización del Silver Ticket, con el cual, acceder al controlador de dominio del entorno AD, para lo cual usaremos **Mimikatz**, siendo una herramienta de seguridad para Windows, que permite realizar tareas de post-explotación en entornos Windows, principalmente ***extraer credenciales*** en texto claro de la ***memoria***, ***hashes de contraseñas***, ***tickets Kerberos***, entre otras.



1. Se ejecuta el comando en esta herramienta, para conseguir generar el Silver Ticket, siendo generado satisfactoriamente e inyectado en la sesión actual del sistema:



En el comando que ha generado el ticket TGS, se compone de:

- ***Kerberos::golden***: Indica, en este caso, que se va a crear un Silver Ticket de Kerberos válido que da acceso al servicio CIFS del dominio, aunque si fuera Golden Ticket empezaría de la misma forma.

- ***/Domain:example.com:*** Especifica el nombre del dominio atacado del Active Directory .

- ***/SID:S-1-5-21-805668554-778713891-2534483124:*** Es un identificador único representa el dominio en el cual se está generando el ticket, siendo necesario para la validación del mismo.

- ***/Target:DC***: Nombre del controlador de dominio (DC) que será objetivo del ticket y que autenticará el mismo.

- **/rc4:e02bc503339d51f71d913c245d35b50b:** Es el hash NTLM de la cuenta “krbtgt”, necesaria para firmar el ticket y que sea aceptado como legítimo por el sistema.

- ***/user:Administrator:*** Nombre del usuario que sera suplantado, para el cual se genera el ticket.

- ***/service:CIFS****:* Especifica el servicio para el que se genera el ticket, siendo en este caso, CIFS (*Common Internet File System)* siendo un servicio esencial en entornos corporativos para la gestión de recursos compartidos, siendo el protocolo de red en Windows que permite acceso compartido a impresoras, archivos y otros recursos de la red.

- ***/ptt:*** Activa el modo "Pass-the-Ticket", lo que significa que el ticket se inyectará directamente en la sesión del atacante, permitiéndole usarlo inmediatamente sin necesidad de guardarlo.

·

1. Se ejecuta el comando “klist” fuera de la herramienta Mimikatz, con el usuario jane.doe, verificando que se ha generado de manera correcta en el sistema:

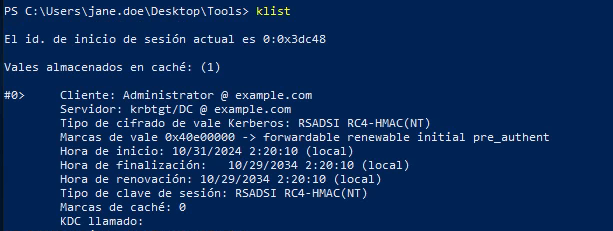
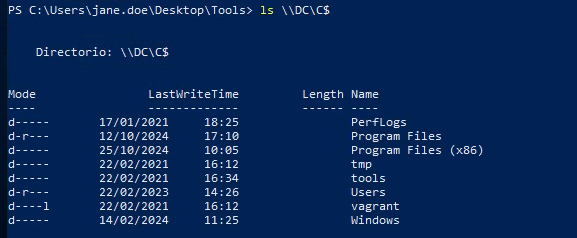


Imagen 13.- Silver Ticket generado para suplantar al usuario Administrator

1. Se procede a ejecutar con el usuario jane.doe un comando para listar el disco duro del controlador de dominio para lo cual hay que tener permiso de administrador, siendo positivo:



**-- EJERCICIO\_2.**- Para este ejercicio debes ser capaz de ***generar un Golden Ticket*** pudiendo abrir así una ***PowerShell remota*** conectada al Controlador de Dominio (Windows DC). Todo esto debes realizarlo partiendo de las credenciales:

*jane.doe // HeyH0Password*

Para la realización de este ejercicio , se han realizado las siguientes gestiones:

- **INTRODUCCIÓN.-** Un **Golden Ticket** es un tipo de ticket del protocolo Kerberos, que permite a un atacante obtener acceso completo y persistente en un dominio de “*Active Directory”,*  utilizando, para ello, el hash de la cuenta KRBTGT (la cuenta de servicio Kerberos en el dominio), permitiéndole crear tickets de autenticación válidos para cualquier usuario o servicio del controlador dominio, sin necesidad de contraseñas.

**- GESTIONES.-** Las gestiones para la obtención de un Golden Ticket son iguales al de un Silver Ticket, no teniendo que usar el nombre de un servicio, ya que este ticket te permite ejecutar cualquier servicio para cualquier usuario del dominio, ni *“target”* por similares motivos, pero incluyendo además:

- ***/rc4:*** El hash NTLM usado será el del ***usuario “KRBTGT”,*** siendo una cuenta de servicio altamente privilegiada , utilizada por el protocolo Kerberos para firmar y emitir tickets TGT (Ticket Granting Tickets) , que luego permiten solicitar acceso a servicios y su ***hash de contraseña*** es usado para ***generar Golden Tickets***, que pueden otorgar acceso completo al dominio del entorno Active Directory.

- **/ID:** Número único asignado a cada cuenta o grupo dentro de un dominio, formando parte del SID, siendo usado para identificar de manera única a los objetos dentro de ese dominio de Active Directory.

* Por todo lo cual, se procede a ejecutar en Mimikatz el comando para generar el Golden Ticket, siendo satisfactorio el proceso:

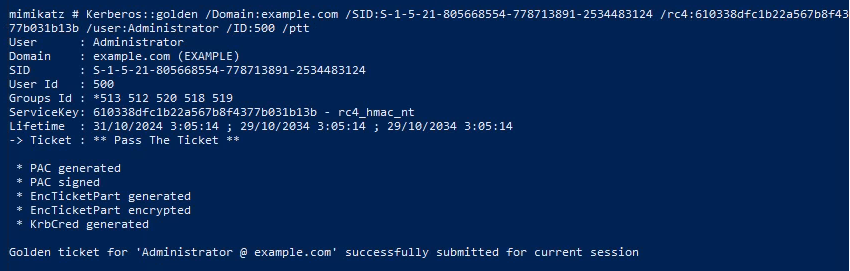


Imagen 14.- Comando para crear el Golden Tickets en la herramienta “Mimikatz”

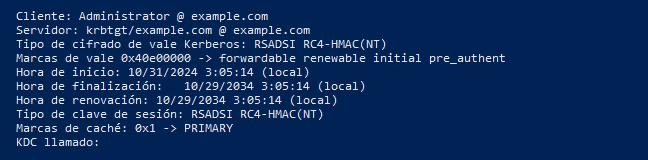


Imagen 15.- Ticket emitido en el sistema para ejecutar cualquier servicio por cualquier usuario

* Se procede a ejecutar una PowerShell remota dentro del controlador de dominio, con resultado positivo como se puede ver en la imagen, donde través del comando ***“Enter-PSSession -ComputerName DC”*** , nos hemos conectado al usuario DC de la maquina Windows DC con IP 192.168.56.2, siendo nuestro usuario no jane.doe sino Administrator.

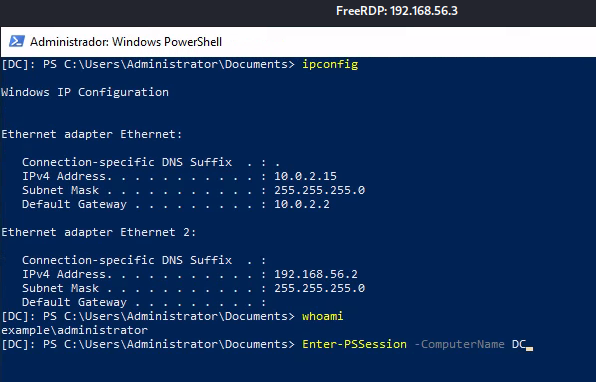


Imagen 16.- Ejecución de PowerShell remota conectando con el usuario Administrador de la maquina Windows DC a través de la Windows User.

1. Colección de scripts en***PowerShell***diseñada para realizar pruebas de penetración y post-explotación en entornos Windows, de manera automatizada. [↑](#footnote-ref-0)