

SPRING 19

UNIDAD 1

EJERCICIO

*METODO “PASS THE HASH”*

**-- EJERCICIO\_1.-** Como actividad debes ser capaz de comprometer los hashes del Controlador de Domino y crakearlos. Para llevar a cabo el ejercicio se han realizado las siguientes gestiones y se han utilizado las siguientes credenciales:

*”jane.doe:HeyH0Password”*

1. Se ha procedido a realizar un escaneo de la red para buscar las maquinas que están conectadas:

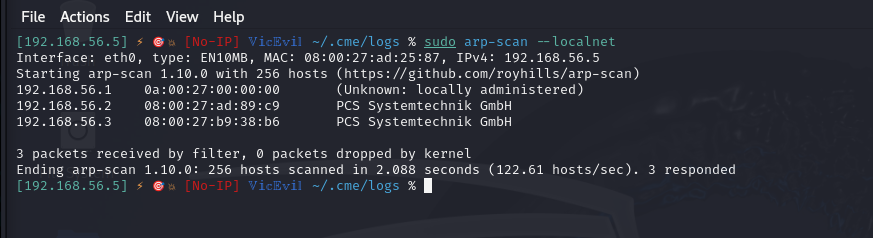


Imagen 1.- Uso de “arp-scan” consiguiendo las IPs de 2 máquinas, ya que una es la puerta de enlace de la red.

1. Se ha usado el comando ***nmblookup*** con la finalidad de conocer el nombre de dominio de la red, si lo hubiese. Este comando realiza una consulta NetBIOS en redes basadas en el protocolo SMB, e identifica nombres de dispositivos y sus recursos compartidos al que pertenecen, pudiendo ser usado en redes Windows y Linux. En este caso se ha utilizado con el ***flag -A***, el cual le indica que realice la consulta sobre una dirección IP especificada y devolverá la lista de nombres NetBIOS asociados, tipo de recurso y grupo o dominio de trabajo de la máquina en esa IP , entre otras.

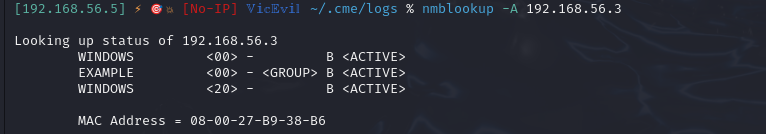


Imagen 2.- Como se puede observar que el **dominio/grupo es “EXAMPLE”.**

1. Se verifica a través de **crackmapexec** información de los ***hosts***, siendo una herramienta versátil para post-explotación y movimientos laterales en redes Windows, concretamente para entornos de directorios activos (active directory), trabajando con diferentes protocolos (SMB,RDP, etc) y realizando infinidad de tareas como: enumeración de usuarios, hosts, validación de credenciales, facilita los movimientos laterales, dumping de hashes,entre otros.



Imagen 3.- Se observa que los 2 hosts de la IP 192.168.56.3, son de Windows 10 server 2019

1. Con la información extraída con las consultas anteriores mas las credenciales de acceso facilitadas para el ejercicio, se ejecuta el comando ***crackmapexec*** consiguiendo verificar que las credenciales son correctas y ademas el usuario ***“jane.doe”*** tiene nivel de administrador en esa maquina.



Imagen 4.- Consulta para la maquina Windows User (192.168.1.3)

1. Se realiza la misma consulta pero añadiendo el **flag** **--ntds,** el cual, permite extraer los **hashes de contraseñas** (NTLM) de todos los usuarios almacenados en un **Controlador de Dominio** (DC) del “Active Directory”, obteniendo la información obrante en la base de datos **NTDS.dit** (*New Technology Directory Services*), permitiendo realizar ataques de *“Pass the Hash”* a cualquier equipo dentro del dominio. La ejecución del comando ha devuelto que no ha podido extraer ningún hash del tipo referenciado, por lo que se puede deducir que esta maquina funciona en local.

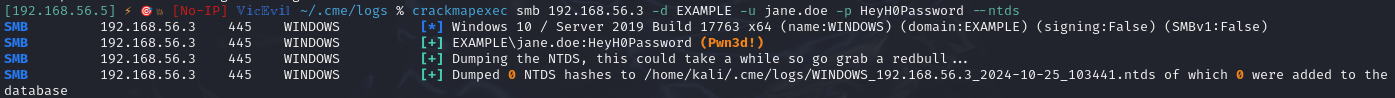


Imagen 5.- “Dumped 0 NTDS hashes”

1. Se verifica que la maquina 192.168.56.3 funciona en local, ya que con el flag **--sam**, ha podido **extraer los hashes locales** de los **usuarios** almacenados en la base da datos **SAM** (*Security Account Manager*)

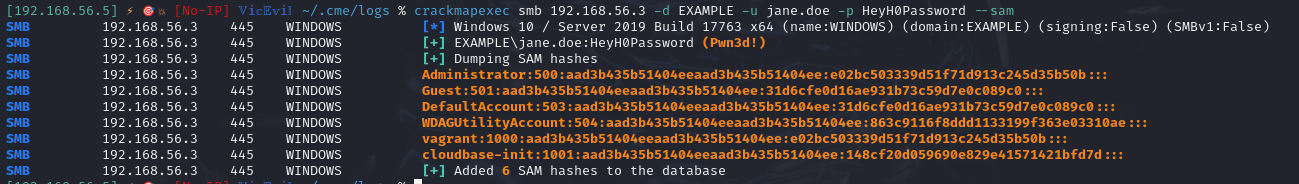


Imagen 6.- extracción de hashes locales nuevos NTLM de la base de datos SAM: cloudbase-init y vagrant

1. Ahora que sabemos 2 nuevos usuarios locales, vamos a probar si alguno de ellos pertenece al controlador de dominio del directorio activo. Para ello, usamos la herramienta crackmapexec, utilizando el nombre de usuario nuevo y con el **flag -H** el **hash NTLM de su contraseña**, siendo este el número comprendido entre el tercer símbolo *“:”* y el antepenúltimo símbolo *“:”*

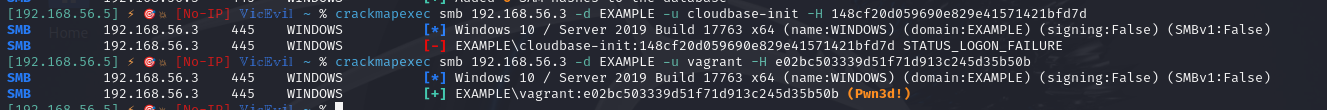


Imagen 7.- Se observa que el *“cloudbase-init”* no se ha podido validar su hash, sin embargo ***“vagrant”*** se ha validado y es **administrador** del sistema como *“jane.doe”* en la maquina Windows User

1. Se prueba ambos usuarios, por si alguno perteneciera también al equipo con IP 192.168.56.2 (Windows DC), ya que, en caso positivo, se podría presumir que alguno de los usuarios pertenece al controlador de dominio, resultando que, al realizar la consulta con el usuario **“vagrant”** , éste pertenece al mencionado equipo con un usuario de nivel de administrador del nuevo equipo Windows User, por lo que se procede a consultarlo con el **flag -ntds**, pudiendo extraer los **hashes de contraseña (NTLM)** de los usuarios del dominio obrantes en la **base de datos NTDS**

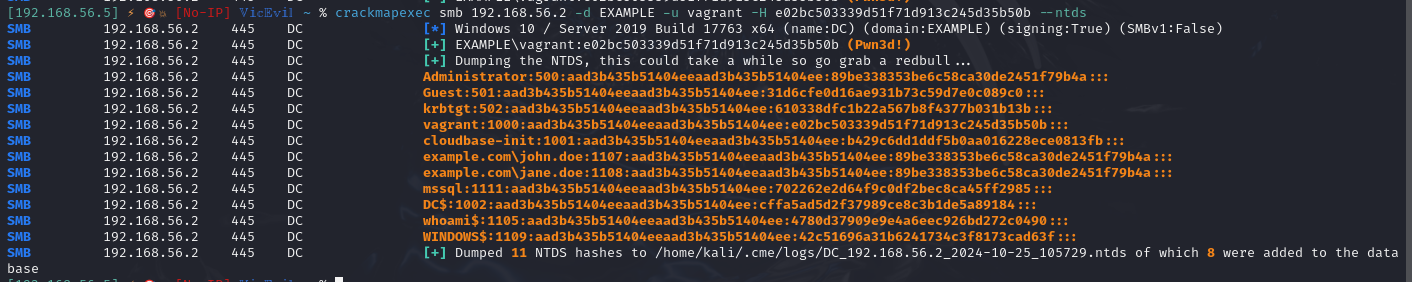


Imagen 8.- Extracción de hashes de usuarios del controlador de dominio, estando entre ellos el usuario vagrant

1. En este punto, se procede a usar fuerza bruta mediante la aplicación **hashcat,** para extraer de los hashes NTLM las contraseñas de los usuarios, almacenados en el directorio */home/kali/.cme/logs/DC\_192.168.56.2\_2024-10-25\_105729.ntds* , para intentar extraer las contraseñas de usuarios y poder acceder al equipo Windows DC.

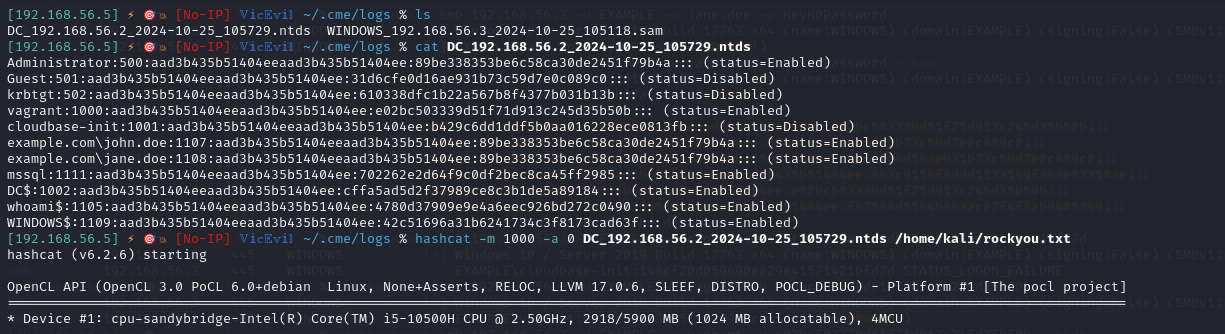


Imagen 9.- contenido del archivo del directorio /home/kali/.cme/logs/DC\_192.168.56.2\_2024-10-25\_105729.ntds

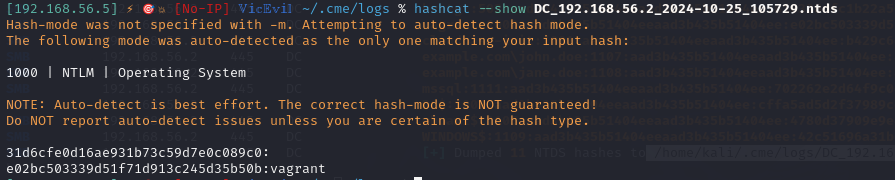
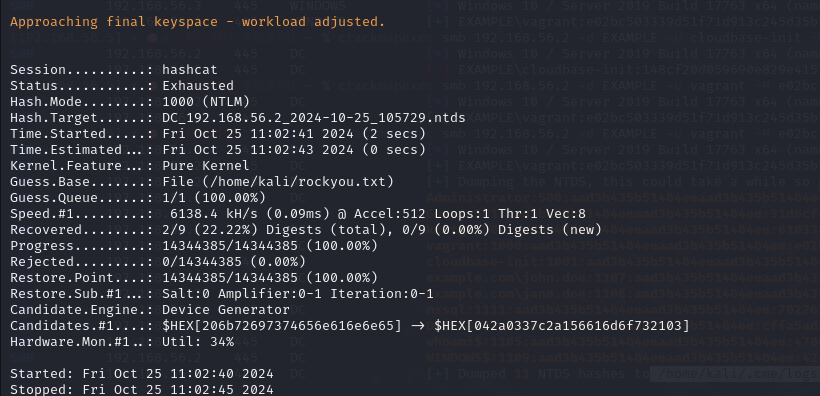


Imagen 10.- Resultado desencriptado del hash de contraseña NTLM del DC: **vagrant**

1. Finalmente, a través de protocolo RDP mediante linea de comandos desde Kali Linux, se ejecuta **xfreerdp** para conectarnos a la máquina **Windows DC** con IP **192.168.56.2**, el **usuario “vagrant”** y la **contraseña** extraída en el punto anterior **“vagrant”**, siendo la misma **positiva**, habiendo procedido a la realización de un movimiento lateral mediante la técnica “Pass The Hash”.

