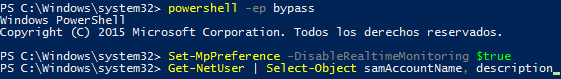
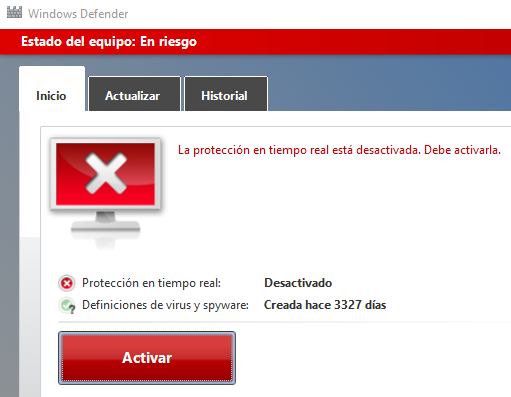
PC-16



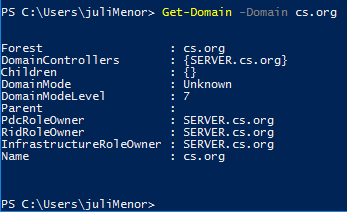
Con estos comandos desactivamos el Windows defender





Llamando al ejecutable PowerView.ps1, nos permitirá ejecutar comandos para sacar información del dominio.

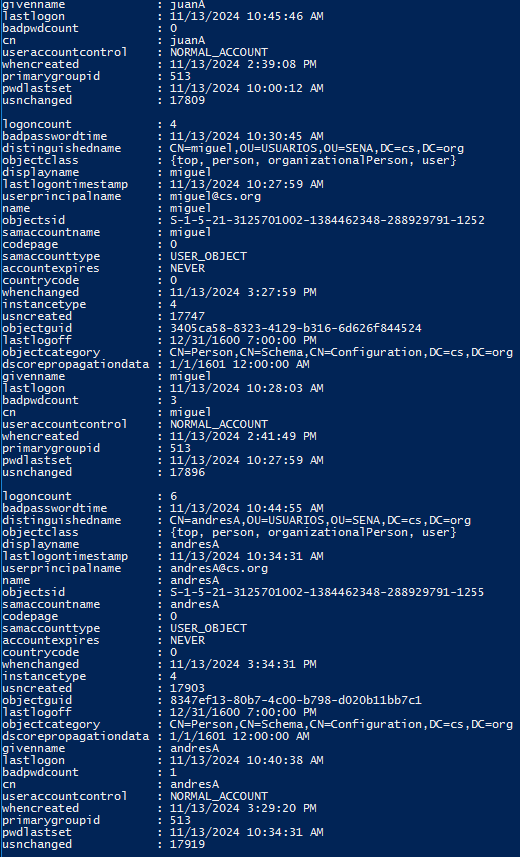
* Acá también vemos a que dominio estamos unidos, es diferente el comando y nos va arrojar la misma información.



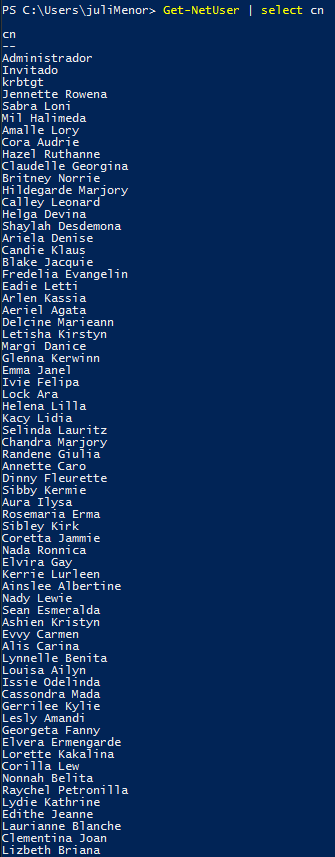
* El **SID** es un identificador único utilizado por Windows para representar objetos de seguridad, como usuarios, grupos y dominios.
* Cada dominio en Active Directory tiene su propio SID que se utiliza para identificarlo en la red.



* Procedemos hacer la enumeración de cuentas de usuario de Active Directory con el comando **Get-NetUser.**
* Este nos va a listar todos los usuarios que tiene el dominio y nos va a decir más información sobre ellos.

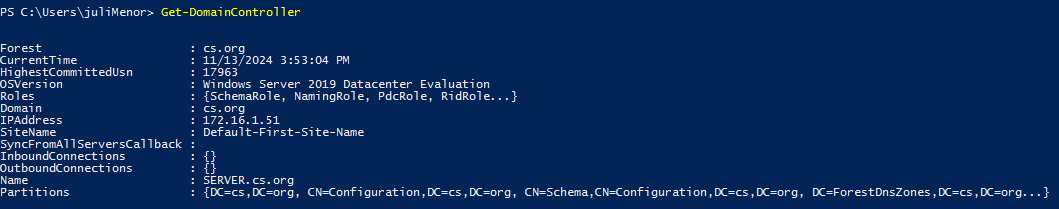


* Acá vamos a volver a listar los usuarios del AD pero solo nos va arrojar los nombres, no nos va a mostrar tanta información de los usuarios como en el paso anterior. Acá vamos a ver la información más específica.



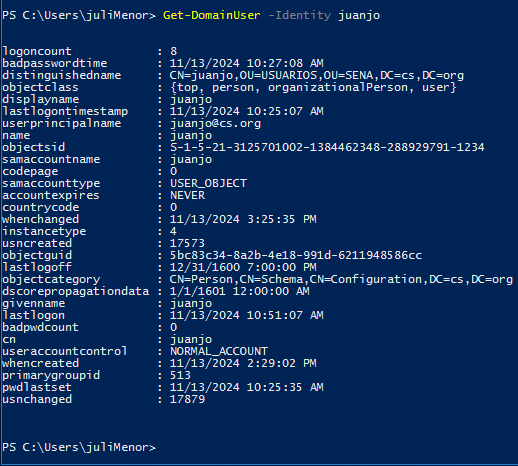
* Procedemos a listar y ver los detalles específicos del controlador de dominio.

Utilizamos el comando **Get-DomainController**



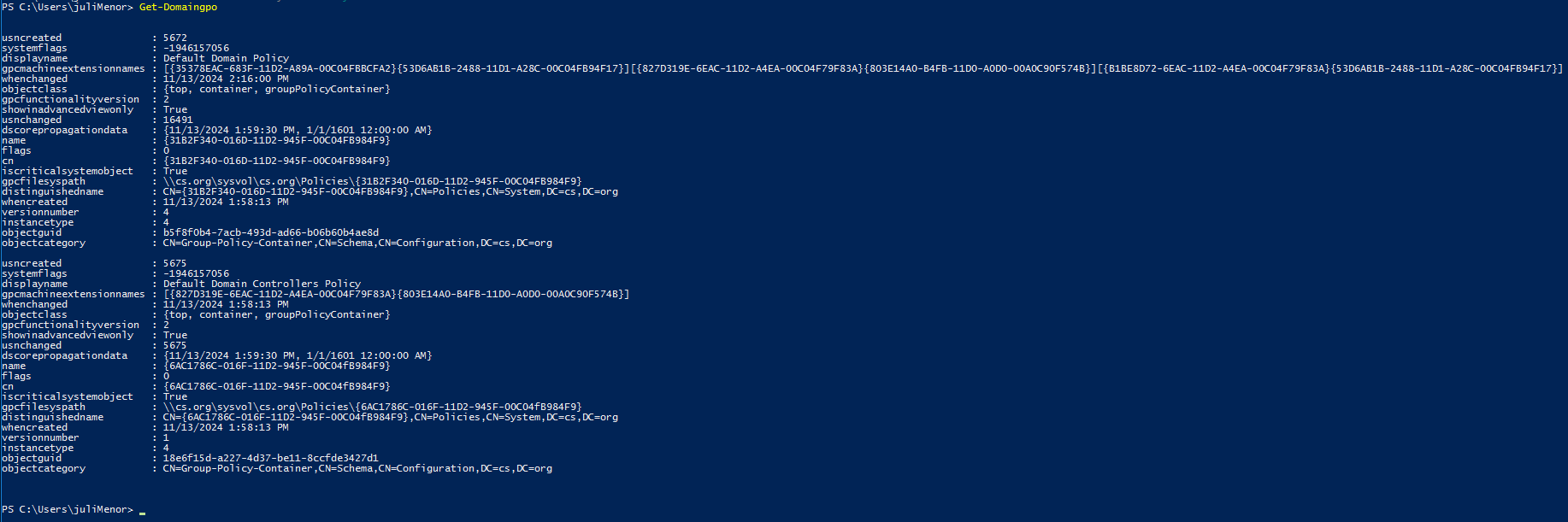
* Vemos información detallada sobre un usuario específico de Active Directory.

Utilizamos el comando **Get-DomainUser -Identity “nombre de usuario”.**



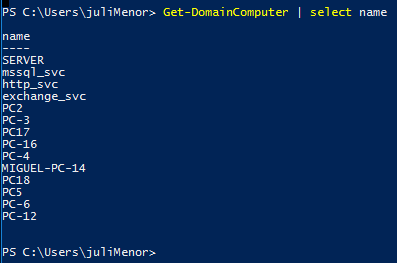
* Acá vamos a ver información sobre las Políticas de Grupo configuradas en el dominio.

Utilizamos el comando **Get-Domaingpo**



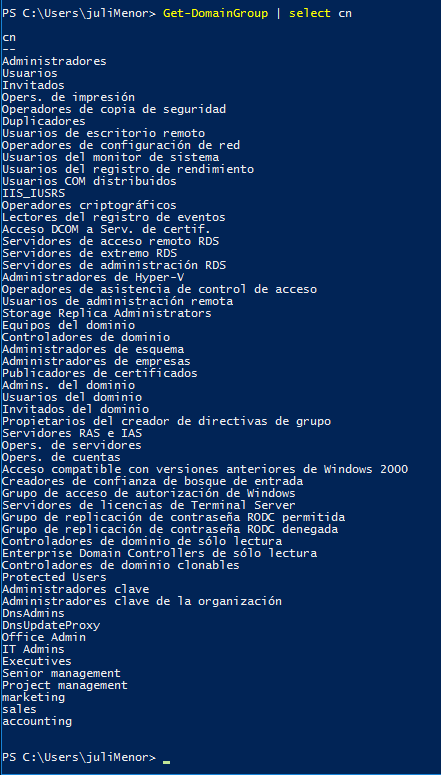
* Vamos a enumerar todos los equipos que forman parte de un dominio de Active Directory.

Utilizamos el comando **Get-DomainComputer | select name.**



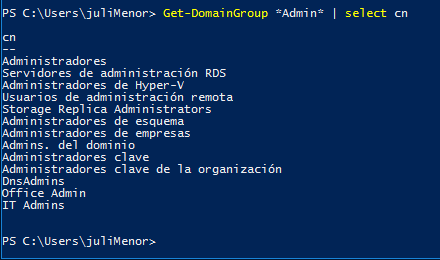
* Vamos a enumerar todos los grupos disponibles en un dominio de Active Directory.

Utilizamos este comando para ello  **Get-DomainGroup | select cn**



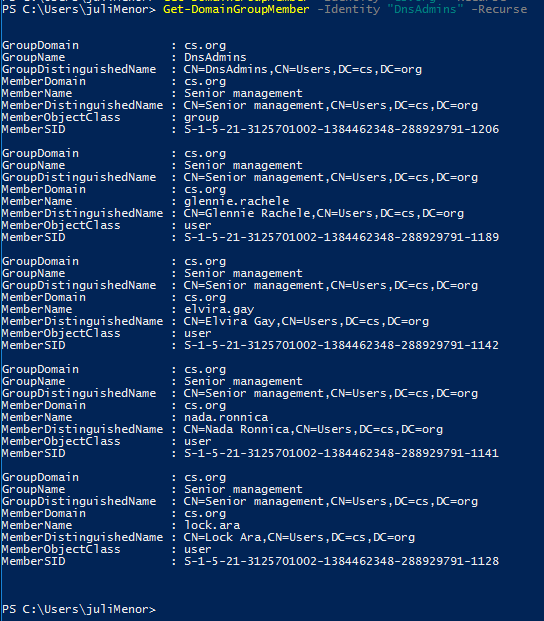
* Acá vamos a enumerar todos los grupos “Administradores” del Active Directory.

Se utiliza el siguiente comando  **Get-DomainGroup \*Admin\* | select cn.**

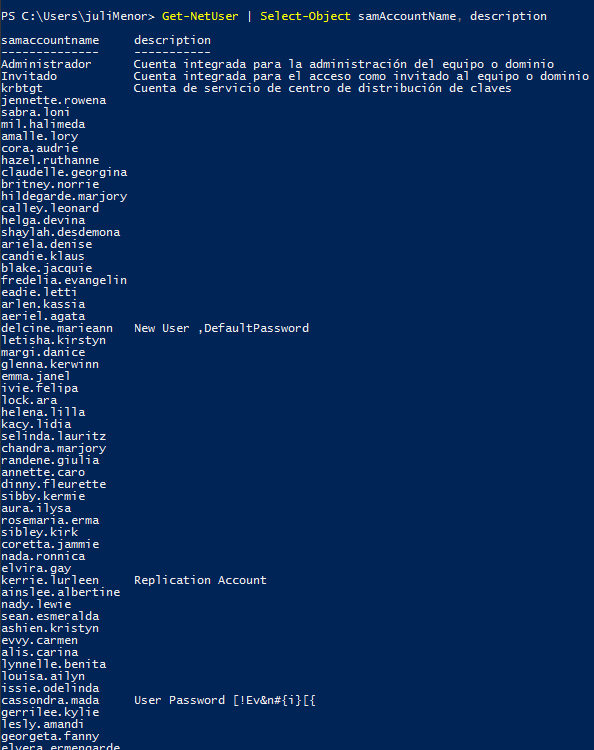


* Enumeramos todos los miembros de un grupo específico, en este caso, el grupo DNSAdmins, junto con los miembros indirectos (es decir, aquellos que pertenecen a grupos anidados

Utilizamos el comando **Get-DomainGroupMember –Identity “DNSAdmins” –Recurse**

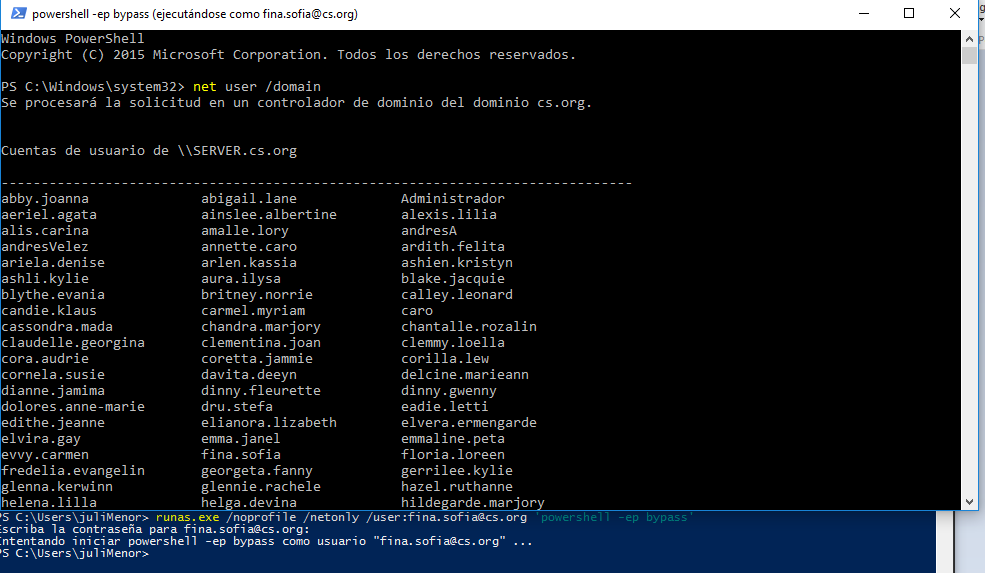


* Aca vamos a ver todos los usuarios de AD con descripciones.



Con esto podemos ver los usuarios del dominio

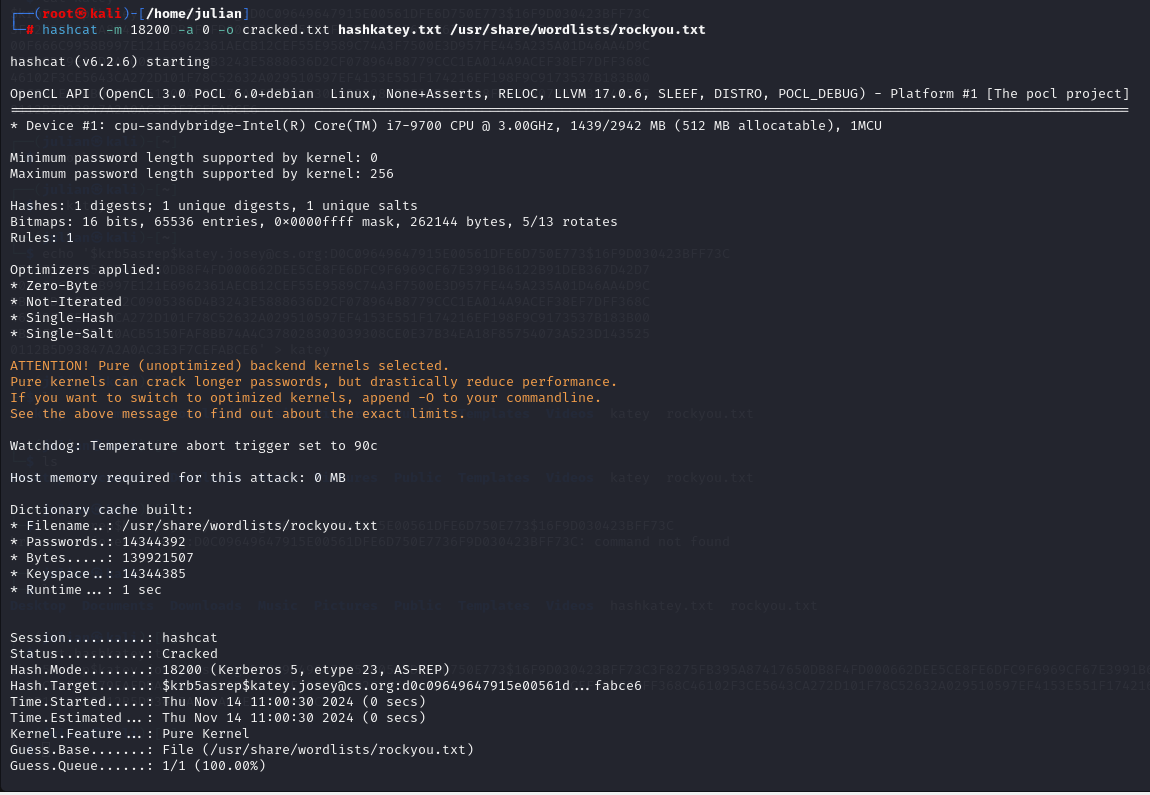




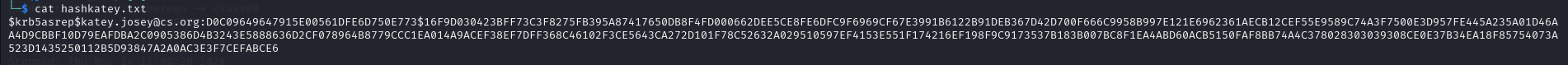
Con rubeus podremos sacar las contraseñas de los usuarios de candie, katey y maybelle

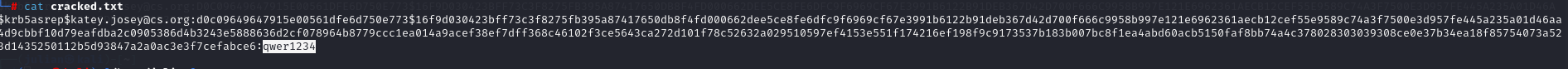


CS

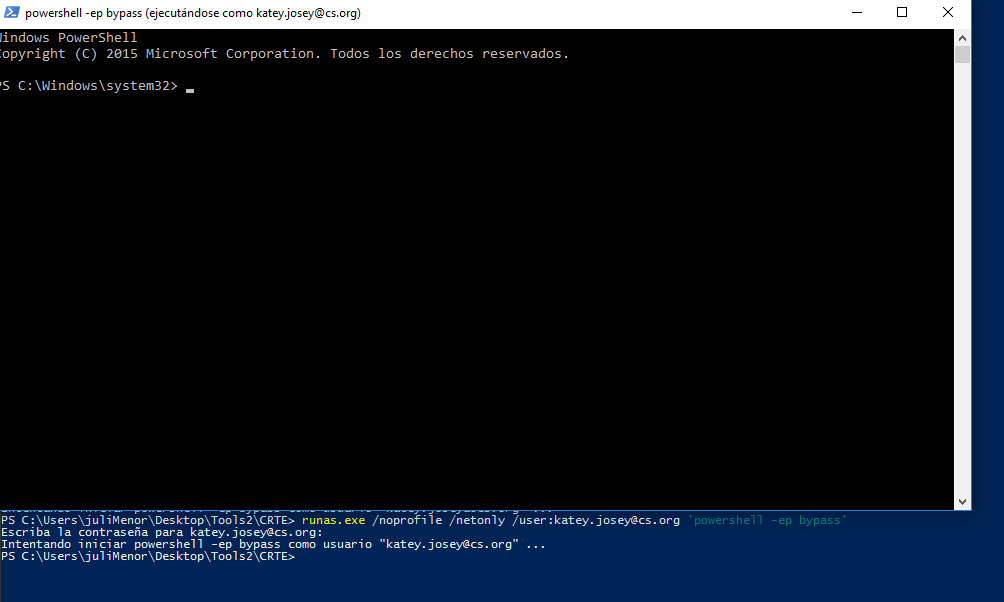


Desencriptamos con hashcat los .txt y uno de estos tiene usuario y contraseña

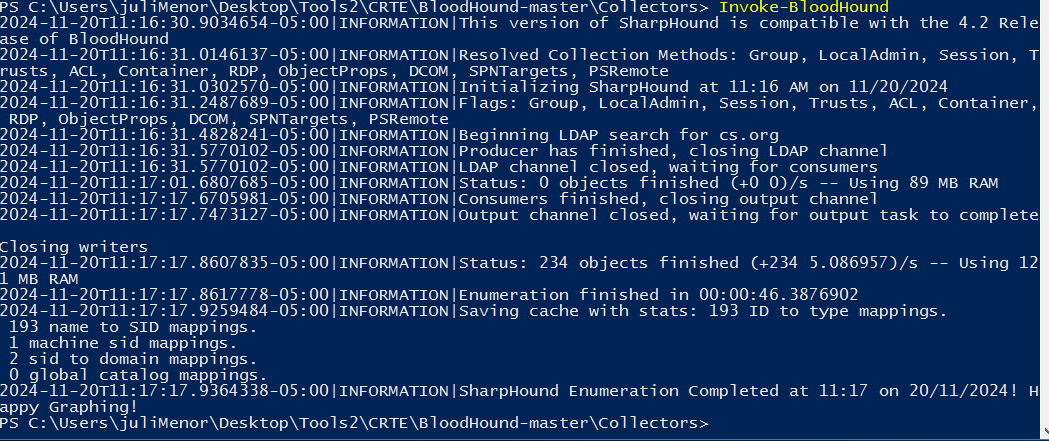




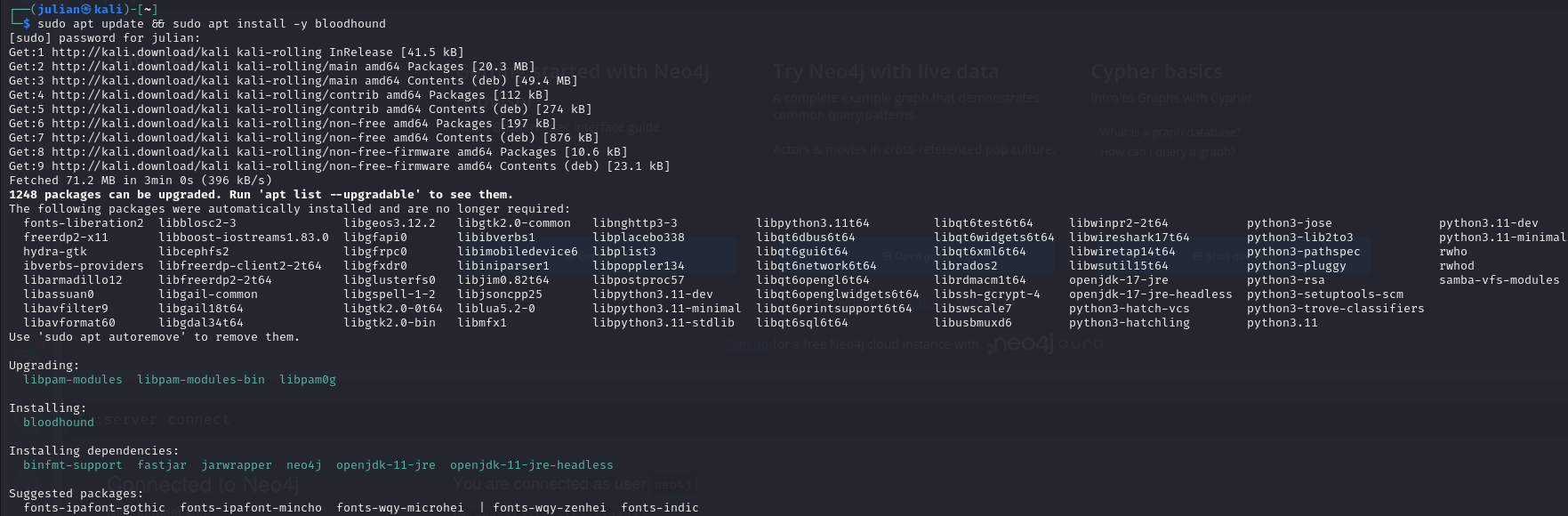


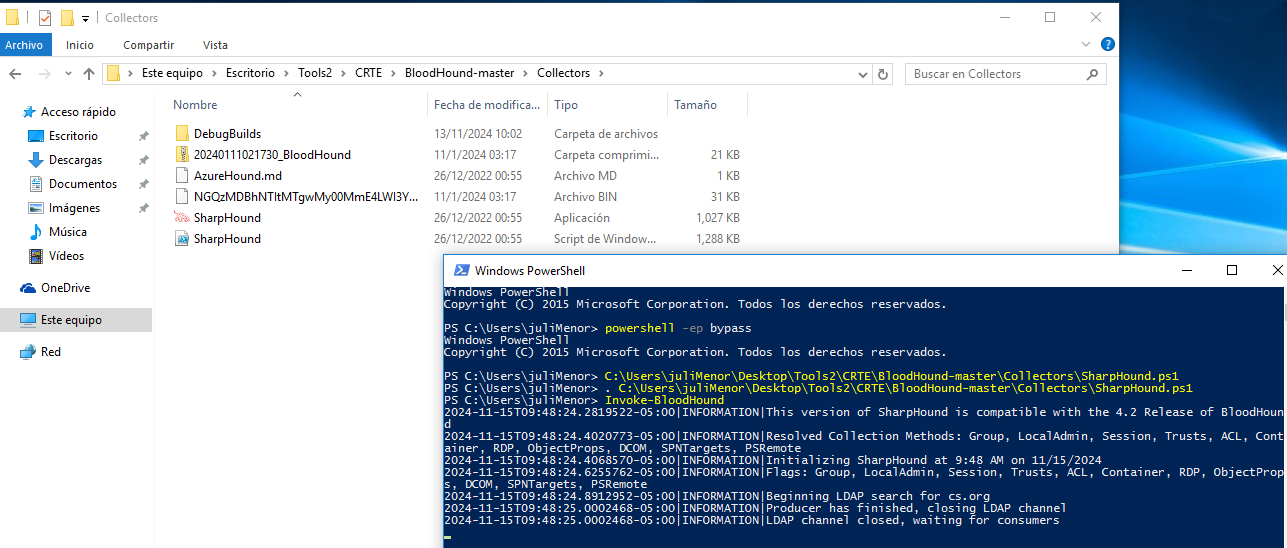


Con las credenciales podemos ver que podemos acceder como katey

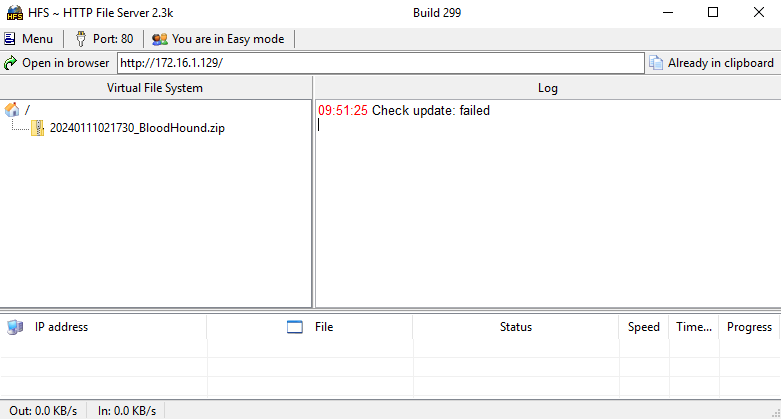


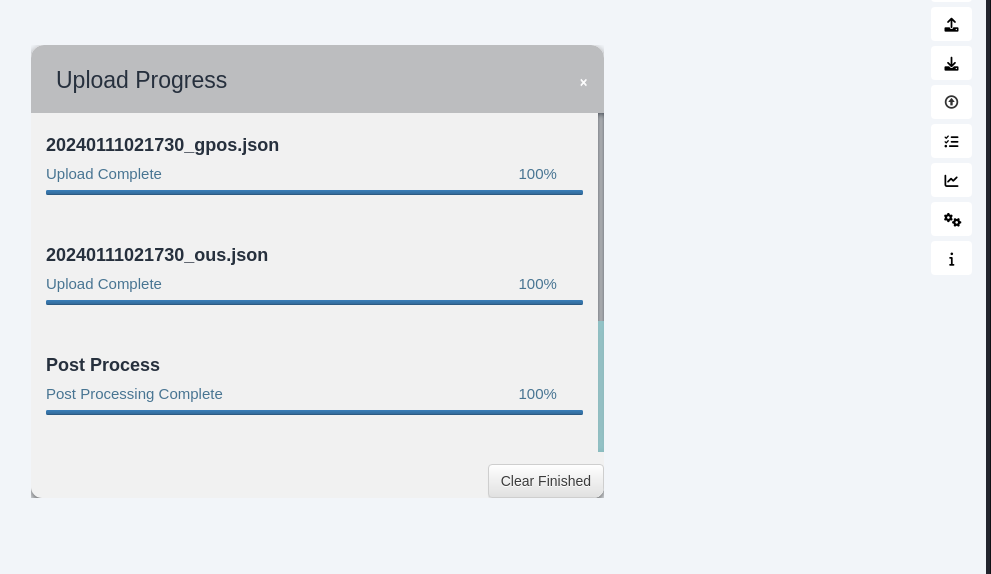
Instalación bloodhund

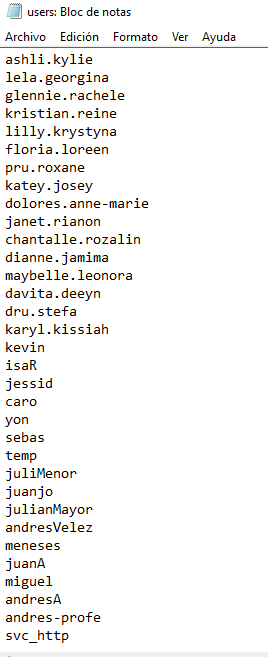


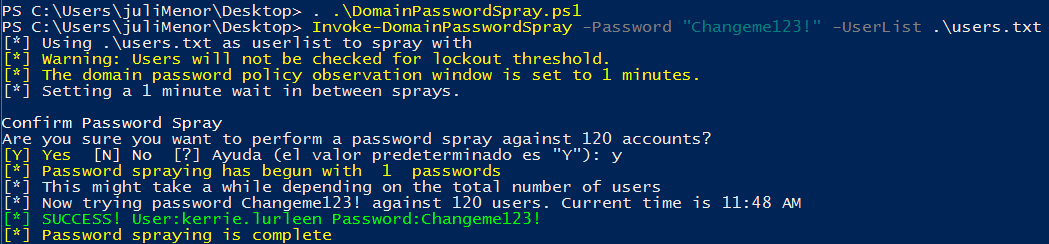


Generamos el bloodhound para analizarlo en kali

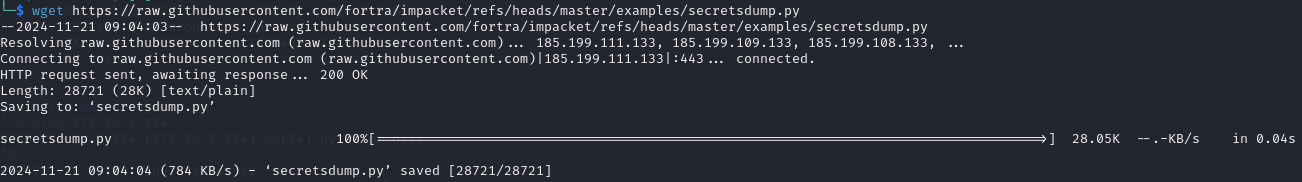


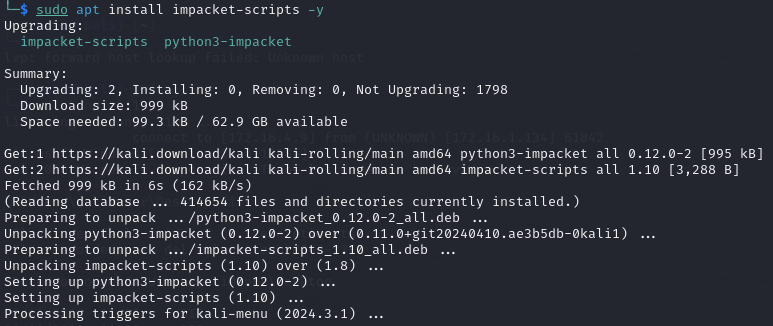






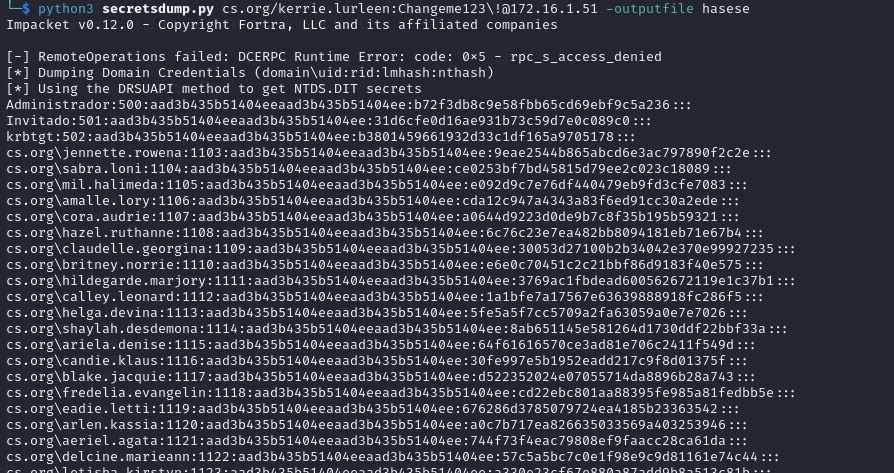
Con domainpasswordsplay sacaremos otras credenciales de la contraseña que anteriormente tenía.



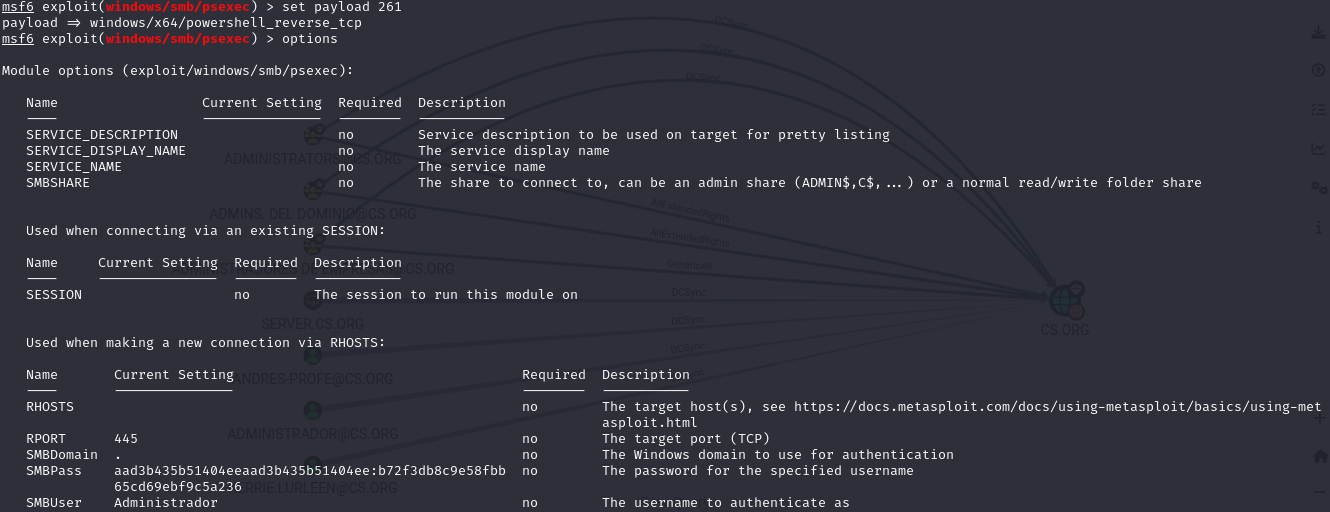


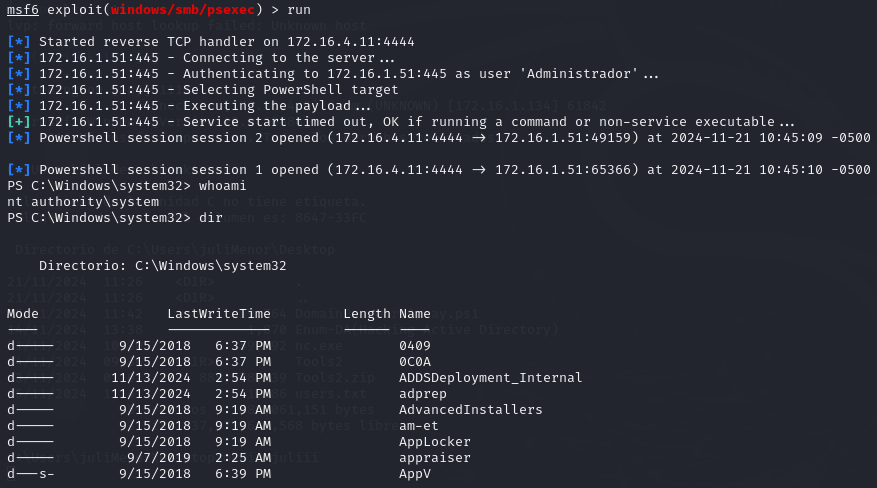
**Ejecuta el comando corregido:** Si el error se debe a un malentendido del argumento o formato, asegúrate de que el comando sea correcto. Por ejemplo:

python3 secretsdump.py -just-dc -outputfile hashes kerrie.lurleen:Changeme123\!@172.16.1.51



Ingresamos al exploit y le agregamos el lhost, el rhost, el payload y lo ejecutamos





Podremos ingresar a la powershell del Windows gracias al payload que le asignamos

Con este ejecutable podremos ingresar a la revershell

Ejecutamos el archivo nc desde la maquina victima mientras halla una terminal en Linux escuchando.



