

SPRINT 16

UNIDAD 2

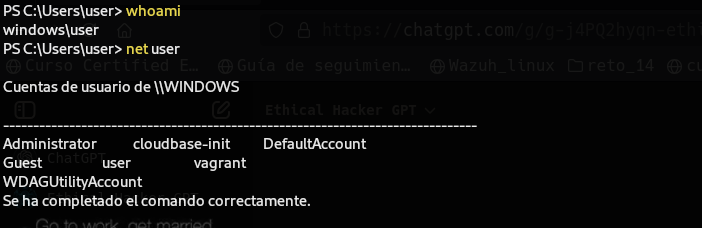
ELEVACION DE PRIVILEGIOS EN WINDOWS

**MÉTODO** “UNQUOTED PATH SERVICE”

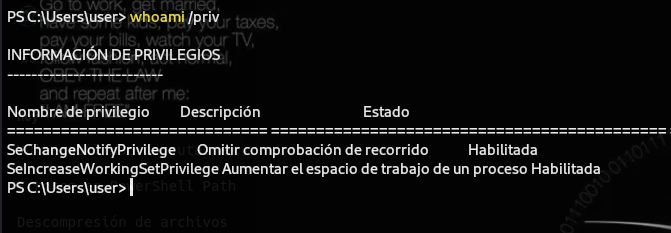
EXPLOTACIÓN MÁQUINA WINDOWS

MÉTODO *“UNQUORED PATH SERVICE”.*

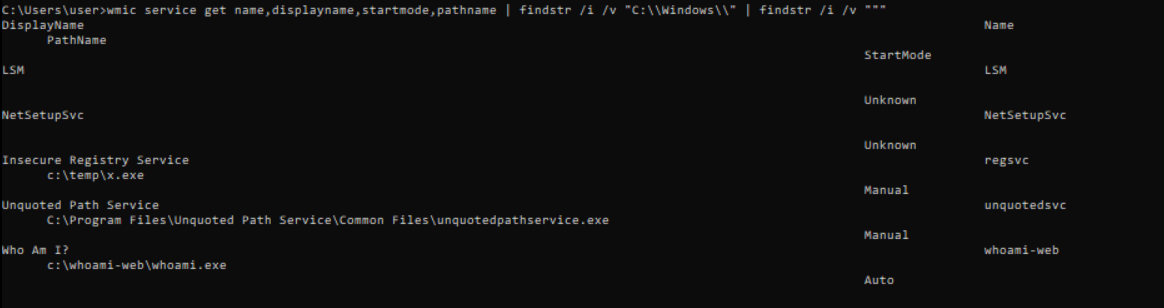
* Una vez instalada y conectada en el mismo rango de red que mi maquina Kali, procedemos a realizar un netdiscover para conocer la dirección IP del objetivo siendo esta 10.0.2.15.
* Ahora, dado que tenemos usuario y contraseña del usuario *“user”,* procedemos a conectarnos a la maquina Windows a través de SSH.
* Una vez que hemos accedido a la maquina objetivo, procedemos a realizar algunas comprobaciones, sobre nuestro usuario, asi como de otros usuarios del sistema y los servicios a los que podemos tener acceso



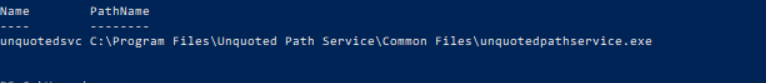
* Comprobamos los privilegios del usuario y como ya sabíamos son muy escasos



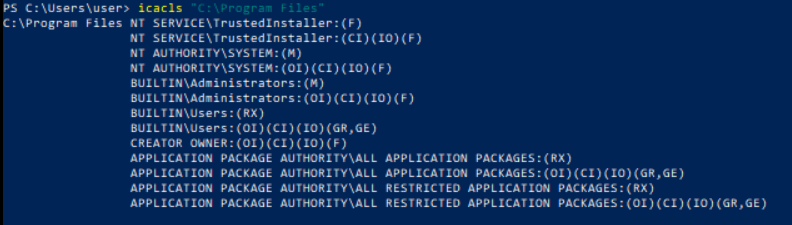
* Se procede a comprobar las rutas existentes sin comillas y/ espacios, pero a través de ssh no funciona, asi que probamos directamente en cmd de la maquina Windows:



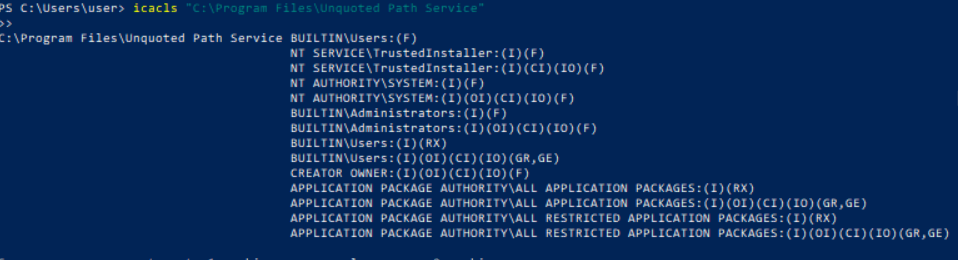
* Observamos que el único archivo que podría ser vulnerable a este método es:



* Ahora comenzaremos a verificar los permisos que tenemos en cada carpeta de la ruta vulnerable:
* C:\Program Files\ 🡪 permisos de lectura y ejecución(RX)

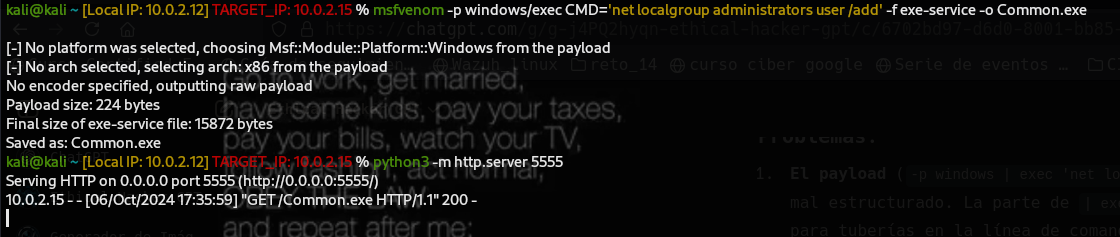


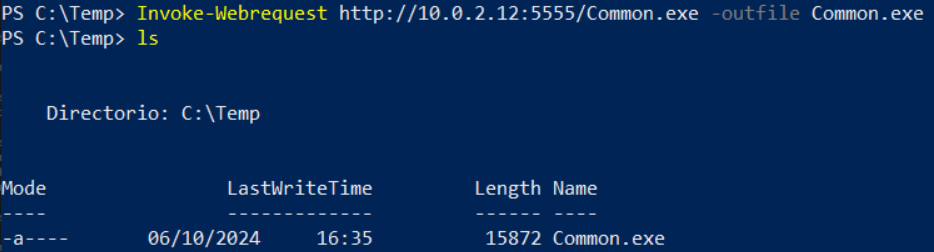
* C:\Program Files\Unquoted Path Service 🡪 plenos o totales permisos



* Windows en esta ruta comprometida y mal configurada, irá intentando ejecutar un ejecutable en cada espacio en blanco q vaya encontrando, como nosotros tenemos archivos totales en la carpeta *“Unquoted Path Service”,* el próximo ejecutable que realizará Windows sea en el próximo espacio, que será entre *“Common” y “Files”,* por lo que nuestro payload debe denominarse “*Common.exe”.*

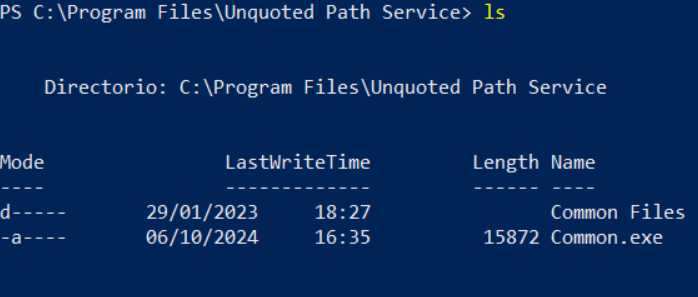
Para ello se procede a realizar el payload en nuestra maquina Kali para que nuestro “*users”*, tenga permiso de *“administrador”,* utilizando para ello la herramienta MSFvenom y siendo transferida a la máquina Windows con el sistema *“servidor python -wget”*

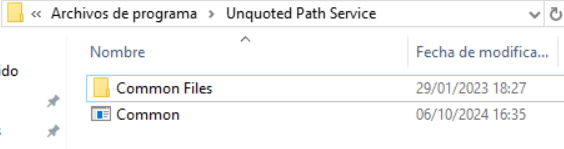


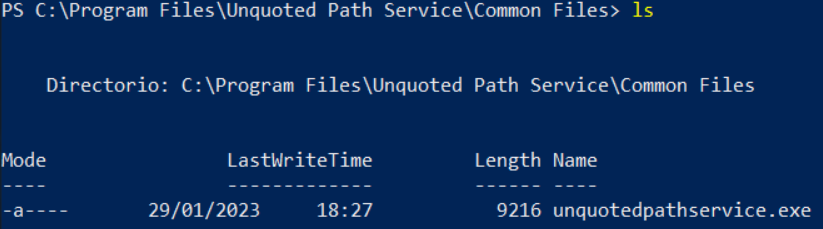


* Se coloca el payload en la carpeta *“Unquoted Path Service”*, justo donde está la carpeta del sistema *“Common Files”*, donde se ejecutará cuando Windows se encuentra el siguiente espacio en la ruta.









* Finalmente, se procede a parar y activar el servicio que hemos explotado, consiguiendo que nuestro usuario *“Users*” tenga privilegios del grupo administrador.

