

SPRING 17

UNIDAD 1

**EJERICIO UNO**

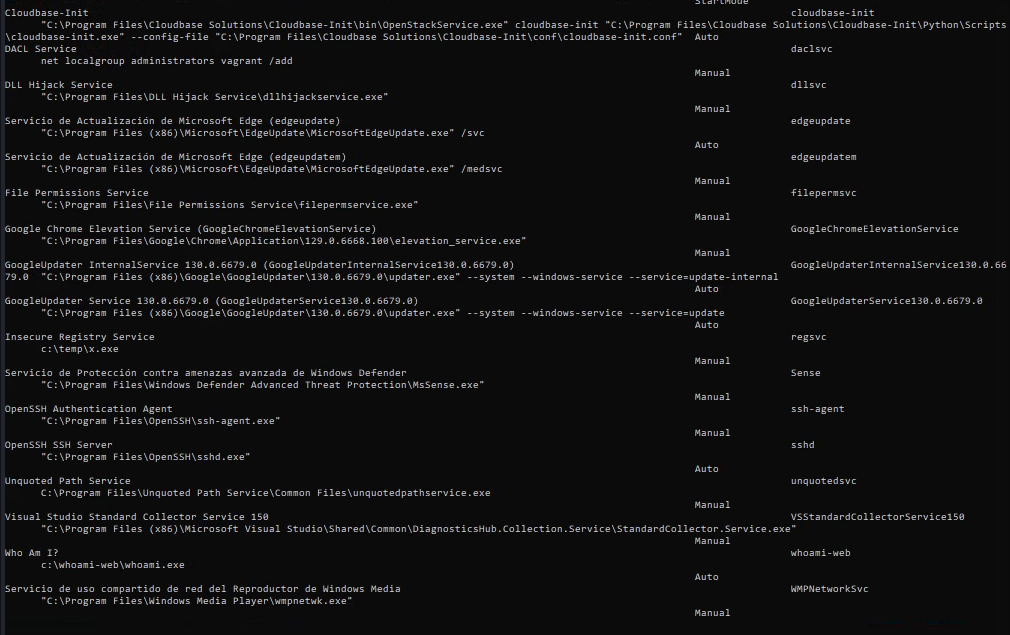
**MÉTODO “FILES PERMISSIONS SERVICES”**

En el presente ejercicio se expondrá la elevación de privilegios en Windows , utilizando el método ***“Files Permissions Services”***, utilizando nuestra maquina Kali como atacante y la máquina “Elv.priv.windows” como objetivo.

Se ha realizado las siguientes gestiones:

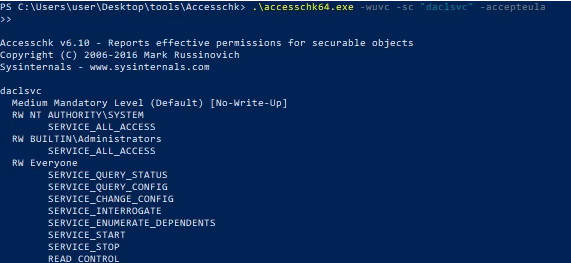
1. Esta técnica se basa en la búsqueda de servicios o archivos mal configurados y con permisos débiles en el sistema, por lo que se procede a enumerar los servicios que tengan ejecutables en rutas no estándar, por si alguno fuera explotable:





1 búsqueda de todos los servicios del sistema menos los que afecten a C:\Windows\

1. Observando los resultados no podemos conocer si esta técnica es aplicable o no, por lo que habrá que usar alguna herramienta o aplicación que nos aporte información de los permisos y los servicios de cada usuario, usando para ello la aplicación *“accesschk”:*



2.- Resultado de ejecutar la aplicación al servicio “DACL Service”

Se ejecuta en el servicio *“DACL Service”* la aplicación indicada, con los parámetros *“w”(* solo con acceso a escritura), *“u”* (sin errores), “*v”*( verbosidad), *“c”* ( nombre del servicio consultado) acompañado de “*sc”*( consulta los permisos de control de servicio para la aplicación consultada) sobre el servicio indicado, encontrando que tiene permisos de escritura y lectura para todos, en múltiples servicios.

1. Ahora vamos a profundizar sobre los servicios a los que tenemos acceso para ver cual es vulnerable al método *“File Permissions Services”:*

* SERVICE\_QUERY\_STATUS.- Este servicio permite conocer el estado actual del servicio.

Este permiso por sí solo **no tiene un alto riesgo de explotación**, ya que solo permite leer el estado del servicio, pero si para recopilación de información, con la finalidad de conocer detalles sobre los servicios en ejecución y planificar un ataque más amplio.

* SERVICE\_QUERY\_CONFIG.- Este servicio permite a los usuarios **consultar** la configuración del servicio ***(****tipo de inicio, la ruta al archivo ejecutable, las dependencias y la cuenta con la que se ejecuta*).

Un atacante con este permiso, podría ver detalles importantes como la ruta del archivo ejecutable el servicio, por lo que, si esa ruta está mal configurada o tiene permisos inseguros, podría llevar a un **ataque de Unquoted Service Path** (ruta sin comillas) pero no un ataque por el método del presente ejercicio.

* SERVICE\_CHANGE\_CONFIG.- Este servicio permite **cambiar** la configuración del servicio, incluyendo lo mismo que el servicio anterior, pero en este caso con la posibilidad de cambiarlos.

Este es un **permiso crítico y muy peligroso**, ya que un atacante que obtiene este permiso puede:

* + 1. Modificar la ruta del archivo ejecutable del servicio original y apuntarla a un archivo malicioso, como un script o binario que permita al atacante obtener una conexión remota.
    2. Cambiar el tipo de inicio para que el servicio se ejecute automáticamente con privilegios elevados.
    3. Escalada de privilegios: Al modificar el archivo ejecutable del servicio o cambiar su configuración, un atacante podría hacer que el servicio ejecute un binario malicioso con permisos de administrador o sistema.
* SERVICE\_INTERROGATE.- Este servicio permite que responda a una solicitud de estado o información que puede ser realizada por el sistema operativo o una aplicación al servicio, para que el mismo proporcione información sobre su estado actual (similar a Service\_Query\_Status).

Este permiso tiene un **riesgo bajo** por sí mismo, como ocurría con el Service\_Query\_Status, siendo útil para obtener información sobre el servicio y su estado.

* SERVICE\_ENUMERATE\_DEPENDENTS.- Este servicio sirve para enumerar los servicios dependientes de un servicio en particular, es decir, los servicios que dependen del servicio objetivo.

Este servicio junto a los ya nombrados Service\_Query\_Status y Service\_Interrogate, pueden permitir a un atacante obtener información para planificar ataques más amplios.

* SERVICE\_START.- Este **servicio crítico** inicia el servicio si se encuentra detenido.

Un atacante podría iniciar un servicio mal configurado o manipulado para ejecutar código malicioso, especialmente si ha logrado cambiar la configuración del servicio o el binario que ejecuta. Si un servicio se ejecuta con permisos elevados, como SYSTEM o Administrador, esto puede llevar a una escalada de privilegios.

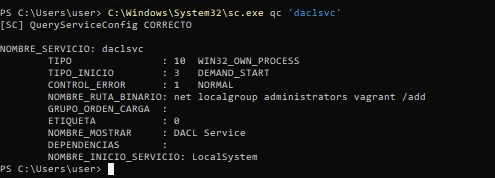
* SERVICE\_STOP.- Este **servicio crítico** permite detener el servicio si está en ejecución.

Detener servicios críticos podría afectar la disponibilidad de un sistema o aplicación (Windows Defender, antivirus, servicios de red) pudiendo dejar el sistema vulnerable a otros ataques.

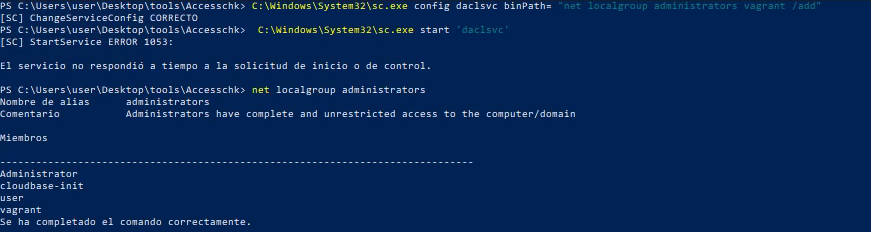
* READ\_CONTROL.- Este servicio permite leer los permisos ACL (Lista de Control de Accesos) del servicio, que son esenciales en el modelo de seguridad en un S.O Windows , debido a que definen los permisos que tienen los usuarios o grupos sobre un servicio específico, es decir, para ver quién tiene acceso al servicio y qué tipo de permisos tiene.

Este permiso ayuda a un atacante para auditar los permisos actuales del servicio y planificar ataques basados en los permisos que encuentran, por ejemplo, si al ejecutar este servicio observa que un usuario no privilegiado tiene permisos débiles en *“Service\_Change\_Config”,* puede aprovecharlo para manipular este servicio.

1. Vamos a proceder con el servicio SERVICE\_CHANGE\_CONFIG, para conocer la ruta del ejecutable del servicio, habida cuenta que tenemos permisos de escritura y lectura sobre él, con la finalidad de modificar ese ejecutable por un payload malicioso que nos aporte una conexión remota en nuestra Kali con permisos elevados:



3 ejecutamos la ruta absoluta del comando sc con el parámetro “qc” que muestra la configuración del servicio (query config)



4 En primer lugar, se ejecuta, y se inicia el cambio de configuración del servicio para agregar nuestro usuario “user” al grupo de administradores