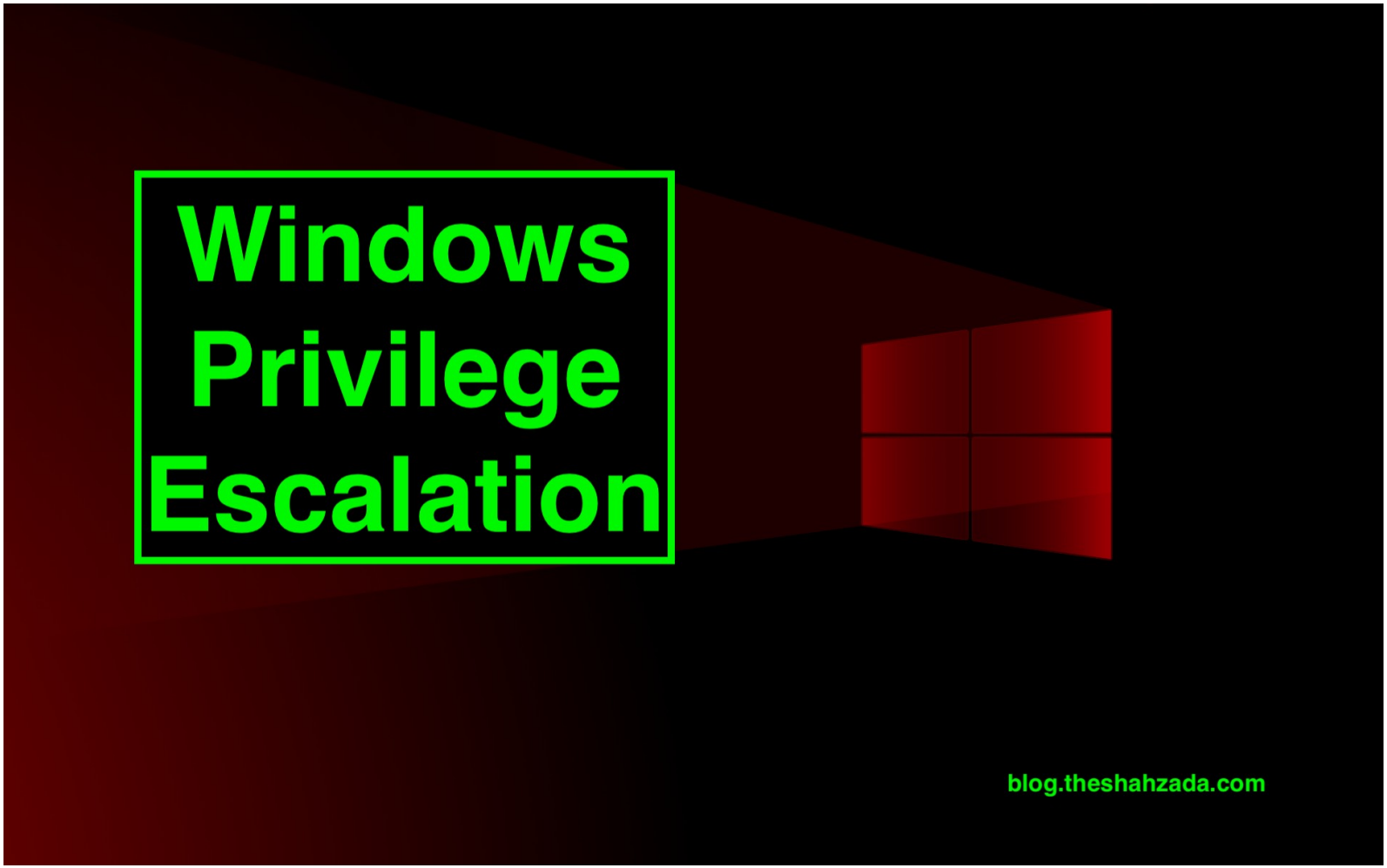
Escalada de Privilegios – Windows



Índice de contenido

Introducción

- ✓ Durante una prueba de intrusión, a menudo obtenemos una entrada a un sistema como un usuario estándar o no privilegiado.
- ✓ En estos casos, generalmente buscamos obtener derechos de acceso adicionales antes de poder demostrar el impacto total del compromiso.
- ✓ Este proceso se conoce como escalada de privilegios y es una habilidad necesaria ya que los exploits “direct-to-root” son raros o nulos en los entornos modernos.

Introducción

- La escalada de privilegios puede ser simple (kernel exploit / system exploit) o requerir mucha habilidad para el reconocimiento de otras vías de explotación en el sistema comprometido.

- La escalada de privilegios puede no solo depender de una sola configuración incorrecta, sino que puede requerir que piense o combine múltiples configuraciones incorrectas hasta lograr el objetivo.

- En su mayoría, la escalada de privilegios son ejemplos de violaciones de control de acceso.

https://www.hackingarticles.in/category/privilege-escalation/

Herramientas de escalada de privilegios

- El uso de herramientas nos sirve para automatizar el proceso de reconocimiento y poder identificar las brechas potenciales que nos ayudarán a escalar privilegios.
- Es importante conocer qué herramientas utilizar y qué estamos buscando para seleccionar la adecuada.
- Las herramientas no ofrecen una solución mágica y normalmente descubren las vías de escalada de privilegios más obvias o sencillas.

https://www.hackingarticles.in/window-privilege-escalation-automated-script/

Herramienta: WinPEAS

- **WinPEAS** es un script que busca posibles rutas para escalar privilegios en los hosts de Windows. Nos ayudará en el proceso de escalada de privilegios a encontrar las brechas abiertas de seguridad de forma automatizada.

- Está desarrollada por Carlos Polop y forma parte del conjunto de scripts PEAS (*Privilege Escalation Aweson Script*).

- La herramienta se encuentra en el siguiente link: https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/winPEAS

Herramienta: Windows-Exploit-Suggester

- ✓ Esta herramienta compara los niveles de parches de objetivos con la base de datos de vulnerabilidades de Microsoft para detectar posibles parches faltantes en el objetivo. También notifica al usuario si hay vulnerabilidades públicas y módulos Metasploit disponibles para los boletines faltantes.
- ✓ No recibe actualizaciones desde hace varios años.
- ✓ La herramienta puede descargarse del siguiente link:
  https://github.com/AonCyberLabs/Windows-Exploit-Suggester

Herramienta: Windows-Exploit-Suggester Next Generation

- **WES-ng** se basa en la salida de la herramienta *systeminfo* para ofrecer la lista de vulnerabilidades y exploits. Soporta todas las versiones de Windows desde Windows XP a Windows 11 (incluidas las versiones Server).

- La herramienta puede descargarse del siguiente link:
  https://github.com/bitsadmin/wesng

Herramienta: JAWS

- **JAWS** (*Just Another Windows -Enum- Script*) es un script de PowerShell diseñado para identificar posibles vectores de escalada de privilegios en sistemas Windows.

- Está escrito en PowerShell 2.0 por lo que se ejecuta en todas las versiones desde Windows 7.

- La herramienta puede descargarse del siguiente link: https://github.com/411Hall/JAWS

Herramienta: AccessChk

- **AccessChk** es una herramienta que sirve para verificar los derechos de control de acceso de los usuarios.
- Puede usarse para verificar si un usuario o grupo tiene acceso a archivos, directorios, servicios y claves de registro.
- La desventaja es que las versiones más recientes del programa generan una ventana emergente GUI "*accept EULA*". En versiones anteriores tiene la opción por línea de comandos */accepteula*.

https://docs.microsoft.com/es-es/sysinternals/downloads/accesschk

Escalada de privilegios con el Kernel

Explotación del Kernel de Windows

- El kernel es el encargado de que el software y el hardware de cualquier ordenador puedan trabajar juntos en un mismo sistema, para lo cual, administra la memoria de los programas y procesos ejecutados, el tiempo de procesador que utilizan los programas, o se encarga de permitir el acceso y el correcto funcionamiento de periféricos y otros elementos físicos del equipo.

- El kernel tiene control completo sobre el sistema operativo por lo que explotar una vulnerabilidad del kernel puede resultar en una escalada de privilegios a un usuario **SYSTEM**.

Explotación del Kernel de Windows

- La búsqueda de exploits de kernel suele seguir los siguientes pasos:
  1. Enumerar la versión del sistema y parches de seguridad (***systeminfo***).
  2. Buscar un exploit relacionado (ExploitDB, GitHub).
  3. Compilar el exploit y posteriormente ejecutarlo.

- Se debe tomar en cuenta que los exploits de kernel son inestables y solo nos funcionarán una vez antes de que el sistema reciba un crash y se reinicie.

https://www.hackingarticles.in/windows-kernel-exploit-privilege-escalation/

Escalada de privilegios en servicios

Explotación de servicios (cuentas de servicios)

- Se utilizan para la ejecución de algunos servicios del sistema. Estas cuentas tienen ciertas características, una de ellas es que no pueden utilizarse para iniciar sesión.

- La cuenta **SYSTEM** es una cuenta de servicio predeterminada que tiene los privilegios más altos de cualquier cuenta local en Windows.

- Existen otras cuentas creadas por defecto como son "**Network Service**" y "**Local Service**".

Explotación de servicios (grupos)

- ✓ Las cuentas de usuarios pueden pertenecer a múltiples grupos de usuarios.
- ✓ Los grupos permiten tener un acceso fácil a los recursos del sistema, entre los grupos predeterminados se encuentran “Administradores” y “Usuarios”.
- ✓ Existen usuarios que pueden estar asociados a diferentes grupos y una mala configuración nos podría ser útil para realizar una escalada de privilegios.

Explotación de servicios (grupos)

- En los sistemas operativos Windows existen múltiples tipos de recursos que también son nombrados como objetos.
  - Archivos / Directorios
  - Entradas de registro
  - Servicios

- Si un usuario o grupo tiene permiso para realizar una determinada acción en un recurso va a depender de la lista de control de acceso (ACL) de ese recurso.

Escalada de privilegios en servicios

- Un servicio de Windows es un programa que normalmente funciona en segundo plano y que se inicia cuando se carga el sistema operativo de Windows.
- Windows puede usar los servicios para controlar muchas cosas, como imprimir, compartir archivos, comunicarse con dispositivos Bluetooth, buscar actualizaciones de software, etc.
- Si el servicio se encuentra ejecutando con privilegios SYSTEM y posee malas configuraciones, explotarlo puede conducir a la ejecución de comandos con privilegios de SYSTEM.

Escalada de privilegios en servicios

- ✓ Trataremos los siguientes puntos con los cuales podremos realizar una escalada de privilegios basados en servicios:

1. Permisos inseguros en servicios.
2. DLL Hijacking.
3. Path de servicios sin comillas.
4. Permisos de registros débiles.
5. Servicios ejecutables inseguros.

1. Permisos inseguros en servicios

- ✓ Un servicio de Windows configurado incorrectamente puede tener una vulnerabilidad de escalada de privilegios.

- ✓ Un usuario no privilegiado podría **modificar o sobrescribir el ejecutable** con código arbitrario, que se ejecutaría la próxima vez que se inicie el servicio. Dependiendo del usuario con el que se ejecute el servicio, esto podría resultar en una escalada de privilegios.

https://www.hackingarticles.in/windows-privilege-escalation-weak-services-permission/

2. DLL Hijacking

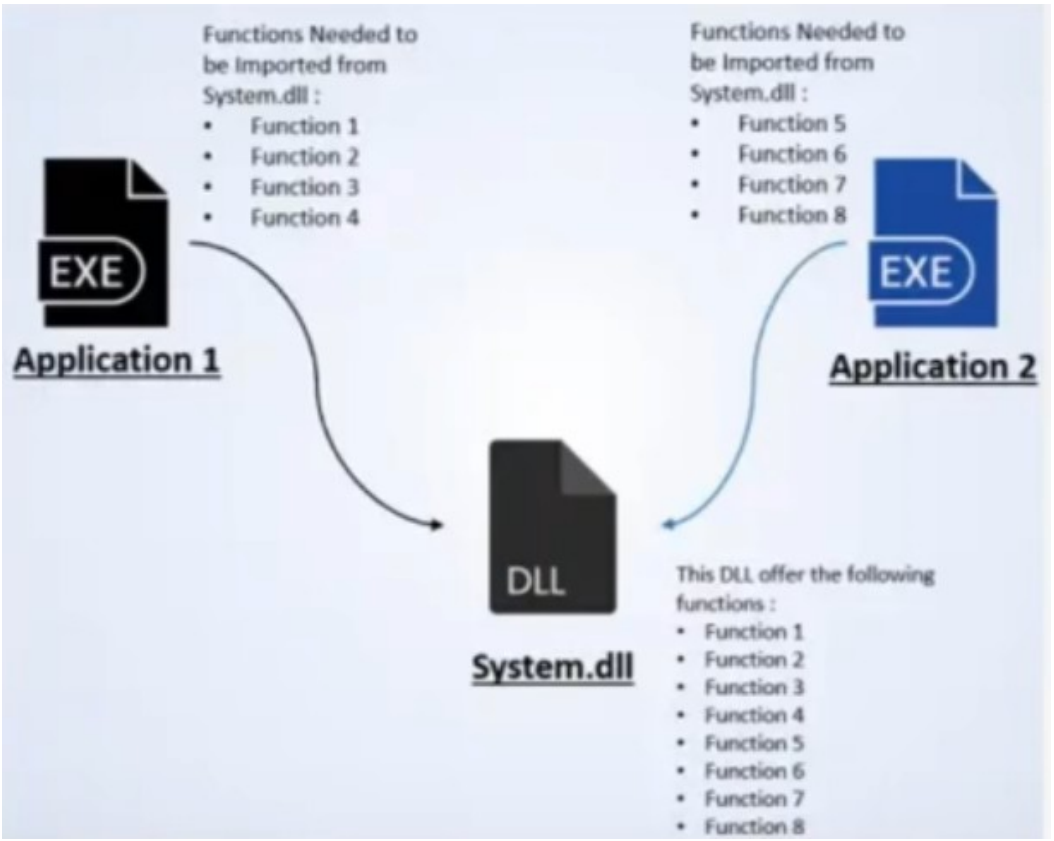
- DLL significa ***Dynamic Link Library***, es un archivo de biblioteca que contiene el código y los datos a los que se puede acceder y usar dinámicamente por más de una aplicación al mismo tiempo.

- Microsoft introdujo la DLL para implementar el concepto de biblioteca compartida que promueve la reutilización de código y el uso eficiente de la memoria.

- Cualquier funcionalidad que proporcione **la DLL se ejecutará con los mismos privilegios que el servicio que la llamó**.

2. DLL Hijacking

- ✓ En el siguiente ejemplo la aplicación 1 y la aplicación 2 intentan importar dinámicamente las funciones requeridas para ejecutar la aplicación desde system.dll



2. DLL Hijacking

- ✓ Una configuración incorrecta más común que se puede usar para escalar privilegios es si falta una DLL del sistema y nuestro usuario tiene acceso de escritura a un directorio dentro de la ruta en la que Windows busca las DLL.

- ✓ Desafortunadamente, la detección inicial de servicios vulnerables es difícil y a menudo todo el proceso es muy manual.

- ✓ Para buscar la posible vulnerabilidad de secuestro de DLL utilizaremos Procmon (*Process Monitor*).

https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/dll-hijacking

https://youtu.be/3eROsG_WNpE

3. Path de servicios sin comillas

- ***Unquoted Service Paths***. Podemos usar este ataque cuando tenemos permisos de escritura en el directorio principal y subdirectorios de un servicio, pero no podemos reemplazar los archivos dentro de ellos.

- Cuando se utilizan rutas de archivos o directorios que contienen espacios, siempre hay que asegurarse de que están entre comillas.

- Todo lo que viene después de cada carácter de espacio en blanco se tratará como un argumento u opción potencial para el ejecutable.

https://www.hackingarticles.in/windows-privilege-escalation-unquoted-service-path/

4. Permisos de registros débiles

- ✓ Es muy frecuente descubrir servicios que se ejecutan con privilegios SYSTEM y no tienen los permisos adecuados establecidos por el administrador.

- ✓ El registro de Windows almacena entradas para cada servicio. Dado que las entradas del registro pueden tener ACL, si la ACL está mal configurada, es posible modificar la configuración de un servicio.

- ✓ Esto significa que el usuario tiene permisos sobre el servicio o sobre la carpeta donde está almacenado el archivo binario del servicio.

https://www.hackingarticles.in/windows-privilege-escalation-weak-registry-permission/

5. Servicios ejecutables inseguros

- ✓ Esta vulnerabilidad se da cuando un ejecutable es modificable por el usuario, para comprometerlo únicamente debemos de reemplazar el archivo original por nuestra Shell reversa.

- ✓ Es recomendable crear una copia del ejecutable original o renombrarlo si la vulnerabilidad se está dando en un ambiente real.

Escalada de privilegios con registros

Explotación de registros (registros AUTORUN)

- ✓ En Windows podemos configurar aplicaciones que se ejecuten de forma automática durante el inicio del sistema, estas aplicaciones poseen privilegios elevados.
- ✓ Las ejecuciones automáticas se encuentran configuradas en los registros de Windows.
- ✓ Si un usuario posee privilegios para poder escribir el registro de ejecución automática podrá ser capaz de escalar privilegios utilizando este método.

https://www.hackingarticles.in/windows-privilege-escalation-logon-autostart-execution-registry-run-keys/

Explotación de registros (AlwaysInstallElevated)

- ***AlwaysInstallElevated*** es una funcionalidad que ofrece a todos los usuarios la ejecución de archivos MSI con privilegios elevados. MSI es un formato de archivo de paquete de instalador basado en Microsoft.

- Esta opción es equivalente a otorgar derechos administrativos completos, por lo que Microsoft desaconseja el uso de esta configuración.

https://www.hackingarticles.in/windows-privilege-escalation-alwaysinstallelevated/

Escalada de privilegios con contraseñas

Contraseñas en registros

- ✓ Algunos administradores almacenan sus contraseñas en formatos o ubicaciones legibles a simple vista.
- ✓ Windows puede almacenar las contraseñas de algunos programas en los registros del sistema.
- ✓ Es importante poder verificar en el sistema el uso de contraseñas que se encuentren en los registros.

Contraseñas almacenadas

- ✓ Windows tiene el comando "***runas***" que permite a los usuarios ejecutar comandos con los privilegios de otros usuarios.

- ✓ Requiere el conocimiento de la contraseña del otro usuario. Sin embargo, Windows también permite a los usuarios guardar sus credenciales en el sistema y estas credenciales se pueden usar para omitir este requisito.

https://www.hackingarticles.in/windows-privilege-escalation-stored-credentials-runas/

Contraseñas en archivos

- ✓ Existen algunos comandos nativos en Windows para poder hacer la búsqueda de contraseñas en archivos, buscando palabras claves.

  C:\> dir /s *pass* == *.config

- ✓ También podemos hacer búsquedas recursivas de palabras en algunos formatos de extensiones.

  C:\> findstr /si password *.xml *.ini *.txt

Contraseñas en SAM y SYSTEM

- ***Security Account Managet*** (SAM) es un archivo de base de datos en Windows que almacena las contraseñas de los usuarios.

- SAM utiliza medidas criptográficas para evitar que usuarios no autenticados accedan al sistema.

- Los hashes están encriptados con una clave que se puede encontrar en un archivo llamado SYSTEM. Si tenemos la capacidad de leer los archivos SAM y SYSTEM podemos extraer los hashes.

Security Account Manager (SAM)

- Las contraseñas de los usuarios se almacenan en formato hash en una sección del registro como hash LM o como hash NTLM.
- Este archivo se puede encontrar en C:\Windows\System32\config\SAM y está montado en HKLM/SAM. Estos archivos están bloqueados mientras se ejecuta Windows.
- Las copias de seguridad de los archivos pueden existir en los directorios:

  C:\Windows\Repair

  C:\Windows\System32\config\RegBack

Pass the hash

- ✓ Windows acepta hashes en lugar de contraseñas para autenticar a una serie de servicios.
- ✓ Podemos usar una versión modificada de winexe, pth-winexe para generar un símbolo del sistema utilizando el hash del usuario administrador.
- ✓ Descifrar hashes puede llevar mucho tiempo, pero podemos emplear la técnica Pass-the-Hash que permite que un atacante se autentique en un objetivo remoto mediante el uso de una combinación válida de nombre de usuario y hash NTLM/LM en lugar de una contraseña de texto sin cifrar.

Escalada de privilegios con aplicaciones no estándar

Aplicaciones no estándares

- En algunas ocasiones escalar privilegios es el resultado de desbordamientos de búfer, por lo que saber cómo identificar las aplicaciones instaladas y las vulnerabilidades conocidas sigue siendo importante.

- Algunas herramientas o métodos para detectar las aplicaciones y sus brechas de seguridad pueden ser:
  - Enumeración manual de programas en ejecución:

    C:\> tasklist /v
  - Utilizar la herramienta "***Seatbelt***" para buscar procesos:

    C:\> seatblet.exe NonstandardProcesses

Aplicaciones no estándares

- ✓ Una vez que se encuentre un proceso interesante hay que identificar su versión y verificar sus archivos de configuración y ficheros de texto dentro del directorio de la aplicación.
- ✓ Utilizar Exploit-DB para buscar un exploit correspondiente a la aplicación en caso de que exista.
- ✓ Es buena práctica buscar información relevante de la explotación de la aplicación.

Escalada de privilegios con tareas programadas

Tareas programadas

- Los atacantes suelen aprovechar las tareas programadas en los ataques de escalada de privilegios.
- Los sistemas que actúan como servidores a menudo ejecutan periódicamente tareas automatizadas y programadas.
- Cuando estos sistemas están mal configurados, o los archivos creados por el usuario quedan con permisos inseguros, podemos modificar estos archivos que serán ejecutados por el sistema de forma recurrente en un nivel de privilegio alto como SYSTEM.

Tareas programadas

- Las tareas generalmente se ejecutan con los privilegios del usuario que las creó, sin embargo, los administradores pueden configurar tareas para que se ejecuten como otros usuarios, incluido SYSTEM.

- Podemos crear y ver tareas programadas en Windows con el comando ***schtasks*** o utilizar PowerShell.

  C:\ schtasks /query /fo LIST /v

- El resultado del comando incluye información como: la tarea a ejecutar, la próxima vez que se debe de ejecutar, la última vez que se ejecutó, etc.

https://www.hackingarticles.in/windows-privilege-escalation-scheduled-task-job-t1573-005/

Escalada de privilegios con aplicaciones de inicio

Aplicaciones de inicio

- Los programas de inicio son similares a los servicios con la diferencia de que los servicios son administrados por el administrador de servicios.
- Cada usuario puede definir aplicaciones que comienzan cuando se inicia sesión, colocando accesos directos a ellas en un directorio específico.
- Windows posee un directorio de inicio de aplicaciones que afectan a todos los usuarios del sistema.

  C:\ProgramData\Microsoft\Windows\Menú Inicio\Programas\Inicio
- Si tenemos permisos para crear archivos en este directorio podremos usar nuestra Shell reversa y escalar privilegios cuando un administrador inicia sesión.

https://www.hackingarticles.in/windows-privilege-escalation-boot-logon-autostart-execution-startup-folder/

Escalada de privilegios con cuentas de servicio

Cuentas de servicio

- Las cuentas de servicio pueden recibir privilegios especiales para que puedan ejecutar sus servicios, no sirven para iniciar sesión directamente.
- El comando ***whoami*** con el parámetro ***/priv*** se puede usar para enumerar los privilegios de nuestros usuarios.

  C:\ whoami /priv

- El privilegio ***SeImpersonatePrivilege*** otorga la capacidad de suplantar cualquier token de acceso que pueda obtener.
- Si se puede obtener un token de acceso de un proceso SYSTEM, podremos generar un nuevo proceso usando ese token.

https://www.hackingarticles.in/windows-privilege-escalation-seimpersonateprivilege/

Escalada de Privilegios – Windows

Fin