Modelo de Protección Windows: Derechos y Permisos

20 de febrero de 2025

Objetivos de la Presentación

- Conocer el modelo de protección de Windows y sus dos conceptos fundamentales: derechos y permisos.
- Comprender la estructura y función del Security Access Token (SAT) y sus atributos.
- Analizar los derechos de usuario (logon rights y privilegios) y su influencia en el control del sistema.
- Revisar la protección de recursos en NTFS: el propietario, la DACL y la SACL.
- Estudiar los permisos estándar e individuales y las reglas de evaluación de acceso en Windows.
- Entender el mecanismo de herencia de permisos y la resolución de conflictos entre derechos y permisos.

Conceptos Básicos: Derechos vs. Permisos

- **Derechos (User Rights):** Son atributos asignados a usuarios o grupos que les permiten realizar acciones que afectan al sistema en su conjunto.
  - Ejemplos: Permiso para hacer copias de seguridad, tomar posesión de archivos, conectarse interactivamente.
- **Permisos (Permissions):** Son atributos asociados a recursos (archivos, carpetas, impresoras, etc.) que determinan el tipo de acceso (lectura, escritura, ejecución, borrado, etc.) para usuarios o grupos específicos.

El Security Access Token (SAT)

- Cuando un usuario inicia sesión en Windows, el sistema crea una acreditación denominada **Security Access Token** (SAT).
- El SAT contiene:
  - **SID:** Identificador único del usuario.
  - **SIDs de los grupos:** Lista de grupos a los que pertenece el usuario.
  - **Derechos:** Conjunto de derechos asignados al usuario, ya sea de forma individual o por pertenencia a grupos.
- Estos atributos se incluyen en cada proceso creado para el usuario y se utilizan para la verificación de acceso a recursos.

Derechos de Usuario: Concepto y Clasificación

- Un **derecho** es un atributo que confiere a un usuario o grupo la posibilidad de realizar acciones específicas que afectan al sistema en su conjunto.
- Windows distingue dos tipos de derechos:
  - **Derechos de conexión (Logon Rights):** Determinan las formas en que un usuario puede conectarse al sistema (por ejemplo, inicio de sesión interactivo o vía red).
  - **Privilegios:** Permiten realizar acciones específicas una vez conectado, como hacer copias de seguridad o tomar posesión de archivos.
- La lista de derechos se añade al SAT y está formada por los derechos asignados individualmente y a través de grupos.

Derechos de Conexión (Logon Rights)

- **Permitir inicio de sesión localmente:** Autoriza a un usuario a iniciar sesión físicamente en el equipo.
- **Permitir inicio de sesión a través de Servicios de Escritorio Remoto:** Facilita el acceso remoto mediante RDP.
- **Permitir inicio de sesión como trabajo por lotes:** Habilita la ejecución de tareas programadas o scripts sin interacción directa.
- **Permitir inicio de sesión como servicio:** Permite que procesos se ejecuten con credenciales de usuario, operando como servicios del sistema.
- **Permitir inicio de sesión a través de la red:** Autoriza el acceso remoto a recursos compartidos y servicios a través de la red.

Privilegios de Usuario (Privileges)

- Los privilegios son derechos asignados a un usuario o grupo que permiten realizar acciones que afectan a recursos globales.
- Se incorporan al SAT cuando el usuario inicia sesión y tienen prioridad sobre los permisos de objetos individuales.
- **Ejemplos de Privilegios:**
  - **Tomar posesión:** Permite al usuario asumir la propiedad de archivos o carpetas, incluso si no tiene permisos explícitos.
  - **Hacer copia de seguridad:** Permite realizar copias de archivos sin necesidad de tener permisos de lectura sobre ellos.
  - **Restaurar copias de seguridad:** Habilita al usuario para restaurar archivos y configuraciones del sistema.
  - **Cambiar la hora del sistema:** Autoriza al usuario a modificar la configuración horaria global.
  - **Forzar el cierre de sesión:** Permite terminar sesiones de otros usuarios cuando sea necesario.
- La asignación y gestión de privilegios se configura mediante la Política de Seguridad Local o mediante Directivas de Grupo (GPOs).

Atributos de Protección de Recursos en NTFS

- Cada archivo o carpeta en NTFS tiene asociados:
  - **SID del Propietario:** Inicialmente, el usuario que crea el objeto; puede ser modificado posteriormente.
  - **Lista de Control de Acceso Discrecional (DACL):** Define qué usuarios o grupos tienen permisos (positivos o negativos) sobre el objeto.
  - **Lista de Control de Acceso de Seguridad (SACL):** Especifica qué acciones sobre el objeto deben ser auditadas y registradas en el Visor de Sucesos.

La DACL y la Herencia de Permisos

- La DACL se compone de varias entradas (ACE: Access Control Entries), cada una asigna permisos a un SID.
- Los permisos en la DACL pueden ser:
  - **Explícitos:** Definidos directamente sobre el objeto.
  - **Heredados:** Provienen de la carpeta contenedora.
- La herencia es dinámica: los objetos nuevos (o copiados) pueden recibir la DACL del objeto padre, a menos que se desactive.
- El orden de evaluación en la DACL es como sigue:
  - Se evalúan primero las entradas negativas explícitas, luego las positivas explícitas, seguidas por las negativas heredadas y finalmente las positivas heredadas.

Permisos Estándar e Individuales

- **Permisos Estándar:** Son combinaciones predefinidas que agrupan varios permisos individuales para facilitar su asignación.
  - Ejemplo: Control Total, Modificar, Lectura y Ejecución, Solo Lectura, etc.
- **Permisos Individuales:** Controlan acciones sobre un objeto:
  - **Atravesar carpeta / Ejecutar archivo:** Permite acceder a subcarpetas o ejecutar un fichero.
  - **Leer datos:** Permite ver el contenido de un archivo o listar el contenido de una carpeta.
  - **Leer atributos:** Permite ver propiedades como "oculto" o "sólo lectura".
  - **Crear ficheros / Escribir datos:** Permite crear nuevos archivos o modificar los existentes.
  - **Crear carpetas / Anexar datos:** Permite generar nuevas subcarpetas o añadir datos a un archivo.
  - **Borrar:** Permite eliminar un archivo o carpeta.
  - **Cambiar permisos y Tomar posesión:** Permite modificar la DACL o asumir la propiedad de un objeto.

Evaluación de Permisos en Windows

- Para cada acción, Windows verifica de forma acumulativa los permisos otorgados a todos los SIDs del SAT.
- Si algún permiso requerido está denegado explícitamente, la acción se rechaza.
- Si todas las entradas necesarias están concedidas, se permite la acción.
- En caso de conflicto, los permisos negativos tienen prioridad sobre los positivos y las entradas explícitas sobre las heredadas.

Ejemplo de Conflicto de Permisos

- Los miembros del grupo `Operadores de Copia` pueden realizar copias de seguridad de todos los archivos, incluso si no tienen permisos explícitos en algunos objetos.
- El administrador puede tomar posesión de cualquier archivo, incluso si la DACL deniega ciertos accesos.
- **Conclusión:** Los derechos y privilegios (atributos del SAT) prevalecen sobre los permisos establecidos en la DACL en caso de conflicto.

Herencia de Permisos en NTFS

- Al crear un nuevo objeto, Windows asigna permisos heredados de la carpeta contenedora, a menos que se desactive la herencia.
- Al copiar un archivo o carpeta a otra ubicación en el mismo volumen, se mantienen los permisos explícitos; si se copia a otro volumen, se aplican los permisos de la carpeta de destino.
- Los administradores pueden controlar la herencia mediante las propiedades avanzadas de seguridad.

Configuración y Administración de Permisos

- Las herramientas gráficas de Windows permiten visualizar y modificar la DACL y la SACL de cada objeto.
- Es posible asignar permisos positivos (concedidos) o negativos (denegados) de forma individual o mediante grupos.

Conclusiones

- El modelo de protección de Windows se basa en dos conceptos complementarios: derechos (privilegios a nivel de sistema) y permisos (acceso a recursos individuales).
- El Security Access Token (SAT) agrupa la identidad del usuario, sus grupos y sus derechos, siendo la base para la verificación de acceso.
- La protección de recursos en NTFS se gestiona mediante listas de control de acceso (DACL y SACL), que pueden ser explícitas o heredadas.
- Los permisos estándar e individuales permiten un control detallado sobre las operaciones permitidas en archivos y carpetas.
- En la evaluación de acceso, los permisos negativos y explícitos tienen prioridad.