Seguridad de los Sistemas Informáticos

PARTE 1 – Seguridad en Windows.

Práctica 2: Directorio Activo. Preparación del entorno.

Escuela de Ingeniería Informática
Universidad de Oviedo

Objetivo General del tema

Comprender los distintos sistemas relacionados con la Seguridad que integran los sistemas operativos Windows, y **ser capaces** de configurarlos y usarlos dentro de la política de seguridad que la Empresa haya establecido.

Objetivos específicos del tema

1. **Conocer y ser capaz de configurar y utilizar** de manera adecuada el sistema de ficheros NTFS para garantizar la **seguridad de la información** almacenada en el sistema.

2. **Conocer y ser capaz de configurar y utilizar** de manera adecuada el **Sistema de Ficheros Encriptado (EFS)**, para asegurar la confidencialidad de la información.

3. **Conocer y ser capaz de configurar y utilizar** de manera adecuada el **Directorio Activo** para gestionar de la mejor manera posible los activos del sistema.

4. **Conocer y ser capaz de configurar y utilizar** de manera adecuada las **políticas de grupo** para gestionar de la mejor manera posible la seguridad de los activos del sistema

Active Directory

- ***Active Directory*** es un *directorio*: una correspondencia entre **nombres** y **valores** (objetos).
- En Windows 2003 (y posteriores) sirve para **gestionar** los **objetos** que pueden definirse para configurar la **infraestructura** informática de la empresa.
- Se organiza de manera **jerárquica** con una gran **flexibilidad**, de manera que puede **reflejar** la estructura **funcional-organizativa-geográfica** de cualquier tipo de empresa.
- **Centraliza** la **gestión** de los objetos implicados en la informática de la empresa (usuarios, grupos y equipos, básicamente).
- Permite aplicar, de manera centralizada, ***políticas de grupo*** (configuraciones, entre otras de seguridad, a aplicar a un grupo de equipos/usuarios/…).

Active Directory

- Los **objetos** que gestiona Active Directory pueden ser de tres tipos:
  - **Recursos** (ordenadores, impresoras, …)
  - **Servicios** (correo electrónico, …).
  - **Usuarios** (cuentas individuales, grupos de usuarios, …)
- Cada objeto representa una **entidad** y sus **atributos**. Algunos pueden contener otros objetos.
- El conjunto de atributos de cada objeto depende del mismo; está determinado por la existencia de un **esquema** asociado al mismo.
- Dentro de los atributos, habrá algunos relativos a **seguridad**.
- El número de atributos asociados a un objeto puede ser gigantesco: desde restricciones en el uso de ciertos programas hasta establecer el tiempo de espera del protector de pantalla. Esto se logra mediante ***Group Policy Objects*** o políticas de grupo.

Active Directory

- Active Directory necesita que haya al menos una máquina que sea el **controlador de dominio**. Contendrá la base de datos en sí y proveerá el servicio de directorio a los clientes (entre otros, el de **autenticación**).
- Los servidores que no son controladores de dominio (por ejemplo, servidores web, de ficheros, …) se suelen denominar ***servidores miembro*** *(member servers).* No proveen servicios de autenticación.
- Suele recomendarse que haya al menos **dos máquinas** que sean controladores de dominio, por si una de ellas falla. En grandes instalaciones puede ser aconsejable un mayor número de controladores de dominio.
- Todos los controladores de dominio se **sincronizan automáticamente**, de manera que todos **los cambios se replican** independientemente de la máquina en que se hagan.

Active Directory: Componentes estructurales

Para organizar los objetos de la empresa, Active Directory crea una estructura jerárquica basada en los siguientes componentes:

- **Bosque**. Es la colección de todos los objetos, atributos y reglas asociadas que pertenecen al directorio activo.
- El bosque contiene 1 ó varios **árboles**. Si hay varios, pueden establecerse *relaciones de confianza transitiva* entre ellos.
- Un árbol puede contener 1 ó varios **dominios** (identificados por un nombre DNS único). También pueden establecerse relaciones de confianza entre los dominios. Pueden dividirse en subdominios.
- Dentro de un dominio pueden crearse *contenedores* de objetos, denominados **Unidades Organizativas**. Estas pueden contener más UO anidadas. Son la base para crear la estructura de la empresa.

Active Directory: Componentes estructurales

- Se recomienda utilizar el **menor número de dominios posible** y utilizar las **Unidades Organizativas** para establecer la estructura del Directorio Activo.
- Una última agrupación que puede hacerse es la de **sitio**. Un objeto *sitio* de DA representa un **conjunto de subredes IP**. Pueden usarse para agrupar recursos físicamente o para optimizar el replicado de la información entre controladores de dominio creando enlaces entre los sitios.
- Un sitio puede contener uno o varios dominios; un dominio puede contener uno o varios sitios.

Active Directory: Componentes estructurales

- El establecimiento de una estructura adecuada del Active Directory de la empresa u organización es una decisión crucial para facilitar la gestión de manera eficiente de la infraestructura informática.

Dominios: Aspectos de Seguridad

- El primer paso para establecer la seguridad en el sistema es **configurar la seguridad de dominio** (Inicio – Herramientas Administrativas – Directiva de seguridad de dominio o Administración de directivas de grupo, dependiendo de la versión). Afecta a todos los objetos del dominio.
- Aquí se pueden configurar, entre otras cosas:
  - **Directivas de cuentas**: Contraseñas, bloqueo de cuentas, autenticación.
    - Estas políticas no se heredan de dominios “padre”.
    - Tampoco se gestionan desde las Unidades Organizativas.
  - **Directivas locales**: Permite controlar la seguridad de los ordenadores del dominio.
    - No se propagan automáticamente a otros dominios.
    - Lo trataremos posteriormente.

Unidades Organizativas: Aspectos de Seguridad

- Las unidades organizativas sirven para crear la jerarquía dentro de un dominio. Pueden pertenecer a un dominio o a otra UO, pero no a varios.
- Aspectos importantes:
  - **Anidamiento**: Puede haber UO dentro de otras UO tantas veces como sea necesario para estructurar el sistema.
  - **Delegación**: Se puede delegar la administración de una UO a grupos o usuarios distintos del administrador.
  - **Políticas de grupo**: Pueden vincularse a una UO; así, se aplicarán a todos los objetos pertenecientes a ella (lo veremos).

Gestión de grupos

- Además de utilizar las UO para establecer la estructura jerárquica del dominio, pueden **agruparse** elementos (básicamente usuarios) en distintos tipos de grupos:
  - **De seguridad**. Tienen un SID, por lo que se les puede usar para asignarles permisos.
  - **De distribución**. No tienen SID, por lo que su funcionalidad es más limitada (por ejemplo, envío de e-mail).
- En función del ámbito del grupo, pueden ser:
  - Grupos de dominio local (DL).
  - Grupos globales (G).
  - Grupos Universales (U)
  - Grupos Locales (L). (no son del DA)

Dominios: Consejos de seguridad

- Establecer una **estructura** de AD adecuada.
- Trabajar con **grupos adecuados** y no con usuarios individuales.
- Cuentas:
  - Eliminar cuentas no usadas (deshabilitadas y *abandonadas;* se puede saber creando consultas en Usuarios y equipos de AD).
  - Forzar contraseñas suficientemente complejas.
  - Establecer una política adecuada de caducidad de contraseñas, de bloqueo de cuentas, etc.
- Las cuentas de usuario destinadas a ejecutar servicios (tareas administrativas como *backup*, por ejemplo) deben ser tratadas con cuidado, dado que, al tener acceso a muchos equipos con elevados privilegios es un claro riesgo.
  - Una forma de prevenir problemas es restringir las máquinas desde las que se puede acceder a ellas.

Dominios: Consejos de seguridad

- Usar cuentas distintas para distintos servicios.
- Las cuentas de administración son muy peligrosas y “golosas” para posibles atacantes:
  - Usar una única cuenta de administrador, en lugar de varias pertenecientes a “Administradores del Dominio”.
  - Revelar su clave al menor número posible de personas.
  - No usarla como cuenta para un servicio.
  - Renombrarla y cambiar su descripción; dejar una cuenta de Administrador falsa sin privilegios.
  - Usar una clave larga y compleja, obligando a cambiarla frecuentemente.
  - Usarla sólo para tareas administrativas. Los administradores deben tener una cuenta normal para otras tareas.

Dominios: Consejos de seguridad

- Hay que proteger especialmente los controladores de dominio:
  - Sólo los administradores deben poder iniciar sesión localmente.
  - No se debe poder acceder remotamente, salvo en horarios, lugares y situaciones autorizadas expresamente.
  - No permitir la traducción SID/nombre, para evitar que se sepa cuál es la cuenta de administración si se obtiene una lista de nombres del dominio.
  - No permitir a usuarios anónimos obtener una enumeración de los recursos compartidos o de los usuarios.
  - No incluir a usuarios anónimos en el grupo Todos.
- Todas esas opciones (y más) se controlan a través de la Directiva de Seguridad del controlador del dominio.

Contraseñas: Consejos de seguridad

- La base de cualquier sistema de seguridad son las contraseñas. Se deben seguir una serie de normas para que este sistema sea bueno:
  - No usar nunca cifrado reversible. Es más fácil su ataque.
  - En cifrado de una dirección se usan ataques de fuerza bruta. Para evitarlos, puede definirse la “Directiva de Bloqueo de cuenta”.
  - Usar contraseñas “seguras”:
    - Que sean largas (mín.8; recomendable >15)
    - Que tenga mezcla de símbolos: mayúsculas, minúsculas, números, otros símbolos.
    - Cambiarlas de manera regular o ante cualquier sospecha.
    - No usar datos personales.
    - No compartirlas.
    - No anotarlas-> Deben ser fáciles de recordar

Contraseñas: Consejos de creación

- El que sean largas, crípticas y fáciles de recordar hacen que sea complicado encontrarlas. Algunos consejos pueden ser:
  - Uso del “lenguaje leet-1337”.
  - Uso de lenguaje de móvil.
  - Uso de frases enteras, con signos de puntuación. No usar citas famosas.
  - En lugar de las frases, se pueden usar las iniciales de las palabras de la misma, si esta es suficientemente larga.
  - Mezclar varios de los consejos anteriores.
- En cualquier caso, debe ser fácil de recordar.

Gestión remota del Servidor de Dominio

- Para gestionar el servidor de dominio lo más habitual es que el administrador (y sólo él) trabaje directamente sobre el controlador de dominio (bien presencialmente o bien mediante acceso remoto).
- Sin embargo, hay situaciones en que no es lo más conveniente. Por ejemplo, si se delega la administración de una parte del sistema a otro usuario.
- Por seguridad, se recomienda que sólo el administrador pueda iniciar sesión en el controlador de dominio (puede cambiarse modificando la directiva Permitir el inicio de sesión local en Configuración de seguridad predeterminada de controlador de dominio – Directivas locales – Asignación de derechos de usuario).

Gestión remota del Servidor de Dominio

- En cualquier caso, Microsoft ha ido desarrollando distintas utilidades para ayudar en la gestión de sus sistemas. En concreto para este caso ha desarrollado el Windows Server 2003 Administration Tools Pack (válido para clientes XP). También lo hay parar la versión 2008 (no válido para clientes XP)
- Puede descargarse de http://www.microsoft.com/en-us/download/details.aspx?id=16770 (para Windows 7+ y que permite trabajar con versiones 2008+ http://www.microsoft.com/es-es/download/details.aspx?id=7887)
- Una vez instalada en una máquina Windows Cliente, el administrador tendrá a su disposición en [Inicio – Todos los programas – Herramientas administrativas] un nuevo conjunto de utilidades para gestionar el Directorio Activo desde la estación de trabajo.
- Otros usuarios deben acceder a ellas desde el [Panel de Control – Herramientas administrativas]