Active Directory

El active directory es un servicio de directorio de Microsoft que facilita la gestión y organización de recursos en una organización. Funciona como un repositorio centralizado de información sobre usuarios, grupos, computadoras y otros objetos, permitiendo su administración de forma eficiente.

- Permite centralizar la administración de usuarios y recursos de una organización
  - Simplifica tareas de autenticación, autorización y administración de políticas de seguridad
  - Facilita la implementación de plíticas de acceso
  - Proporciona marco para la administración de servicios.

Aspectos vulnerables en Active Directory

- Contraseñas débiles
- Falta de parches
- Permisos inadecuados
- Ataques de fuerza bruta
- Phising/Ingeniería inversa

elementos dentro de Active Directory

- Controlador de Dominio: Servidor que ejecuta el servicio de Active Directory y almacena info sobre usuarios, grupos, equipos y otros objetos en un dominio.
- Dominio: Unidad lógica de organización en un entorno de Active Directory.
- Objetos: Representan entidades
- Atributos: Información adicional sobre un objeto
- Esquema: Define la estructura y tipos de objeto y atributo que puede almacenar el active directory.
- Global Catalog: Server que almacena info parcial de todos los objetos en el bosque del active directory.
- Grupos: Conjunto de objetos a los que se les puede asignar permisos y derechos.
- Políticas de grupo: Conjunto de configuraciones que se aplican a usuarios y computadoras en un dominio.

Árboles y Bosques

- Arbol: Colección de dominios que dependen de una raiz común y se encuentran organizados jerárquicamente.
- Bosque: Contenedor lógico más grande dentro de active directory, abarca todos los dominios dentro de un ámbito. Los dominios de un bosque confían los unos en los otras y pueden compartir recursos.

Tickets

- Key Distribution center: Servidor de kerberos encargado de distribuir los tickets a los users.
- TGT (Ticket Granting Ticket): Emitido por el servidor de autorización después de la autenticación. Permite solicitar otros tickets de servicio sin volver a autenticarse
- TGS (Ticket de Servicio): Emitido por el server de autorización en respuesta a una solicitud con un TGT.
- Diferencias y casos de uso de TGT y TGS:
    - TGT: utilizado para solicitar TGS y autenticarse en el dominio
    - TGS: Utilizado para acceder a servicios específicos.

Tipos de autenticación

- NTLM (NT LAN Manager): Protocolo de autenticación que utiliza hashes de contraseña para autenticar a los users.
- LM (LAN Manager): Protocolo más antiguo utilizado por widnows. Almacena contraseñas en un formato vulnerable a fuerza bruta