[INT] Active Directory

Las principales vulnerabilidades son:

- Contraseñas débiles
- Falta de parches
- permisos inadecuados
- Ataques de fuerza bruta
- Phising e ingeniería social

Elementos dentro de AD

- Controlador de dominio
- Dominio
- Esquema
- Catalogo global
- Grupos
- Políticas de Grupo

Concepto de tickets

- Key distribution center: Distribuye tickets a los usuarios
- Ticket Grating Ticket (TGT): Emitido por el servidor de autorización tras la autenticación. Permite al usuario solicitar otros tickets de servicio sin tener que volver a autenticarse
- Ticket de Servicio (TGS): Emitido por el servidor de autorización en respuesta a una petición de usuario TGT
- Diferencias y casos de uso de TGT y TGS

Tipos de autenticación

- MTLM (NT LAN Manager): Protocolo de autenticación que usa hashes de contraseñas para autenticar usuarios en entornos windows
- LM (LAN Manager): Protocolo antiguo de autenticación

Enumeración: Se deben buscar los siguientes puertos:

- SMB
- Kerberos
- LDAP

Tras eso podemos hacer ataques en 4 casos:

- conseguimos usuario y password hasheada de user de dominio
    - Se intenta obtener info con Null Session
- Obtenemos usuario y contraseña en claro
- No tenemos contraseña, pero tenemos un Hash: se hace ataque de fuerza bruta

Kerberoasting

Se identifican distintos tipos de tickets y a través de dichos tickets nos colamos en las máquinas. Una vez se obtiene el TGT, se generan TGS.

Pass-The-Ticket (PtT)