Mindmap by Olik3n

Active Directory

Microsoft Active Directory

Servicio de Microsoft que proporciona autenticación y autorización de forma centralizada a un **conjunto de dispositivos vinculados a una red/dominio** (Bases de datos-equipos-usuarios-contraseñas-archivos-políticas.)

¿Red/Dominios?

Las **unidades Organizativas (OUs)** digamos que son contenedores lógicos utilizados para **organizar y administrar objetos dentro de un dominio** (Dentro de una OU puede haber otras)

```
Domain: empresa.com
|
+-- NuevaYork
|   +-- Ventas
|   +-- RecursosHumanos
|   +-- TI
|
+-- Madrid
|   +-- Ventas
|   +-- TI
|
+-- Tokio
    +-- RecursosHumanos
```

-Cada ubicacion es una OU
- Dentro de cada ubicacion es una sub-OU
- Puedes aplicar disintintas políticas de forma individual a cada OU y sub-OU

La forma en la que se realizan las autenticaciones de estas **confianzas** suelen someterse a diferentes protocolos que pueden variar como **Kerberos,NTLM y etc,** Pero de igual forma los **DC generan una clave** a la hora de generar una confianza y a esta clave se les llama Trust

Los usuarios pueden acceder a otros dominios en el mismo bosque y a este tipo de conexión o vinculo se les llama **Confianza(Trusts)**

```
        ~ redteamrd.local
          *  v   v  *
   ,-----*  |   |  *-----,
   |  ,-----*   *-----,  |
   |  |  v         v  |  |
   v  v                v  v
it.redteamrd.local hr.redteamrd.local
   *  v
   |  |
   *  v
web.it.redteamrd.local
```

No es que simplemente podamos acceder a otro dominio porque si tambien existen configuraciones de confianza donde se dividen dos **tipos de confianza**:

-**Interna (Intra-forest)**:Automática y bidireccional entre dominios dentro de un mismo bosque.
-**Externa (Inter-forest)**:
Manual, conecta dominios de diferentes bosques. Suele ser unidireccional.
-**De atajo (Shortcut)**:
Acelera la comunicación entre dominios de un bosque grande.
-**De bosque (Forest Trust)**:
Conecta dos bosques completos.
-**Realm**:
Permite confianza entre AD y otros sistemas como Kerberos en Linux/UNIX.
-**De autenticación**:
Controla qué recursos son accesibles entre dominios o bosques.

```
PS C:\Users\Olik3n> nltest /domain_trusts
```

Enumerar las confianzas de tu dominio

Con el nombre DNS, podemos crear subdominios de forma jerárquica y a este orden de dominios/subdominio se les llama **Bosque**

```
redteamrd.local
|
|-------------------------
|                         |
it.redteamrd.local        hr.redteamrd.local
|
|
web.it.redteamrd.local
```

```
PS C:\Users\Olik3n> Get-AFForest

ApplicationPartitions : {DC=DomainDnsZones,DC=redteamrd,DC=local,
                        DC=ForestDnsZones,DC=redteamrd,DC=local}
CrossForestReferences : {}
DomainNamingMaster    : dc01.redteamrd.local
Domains               : {redteamrd.local}
ForestMode            : Windows2016Forest
GlobalCatalogs        : {dc01.redteamrd.local, dc02.redteamrd.local}
Name                  : redteamrd.local
PartitionsContainer   : CN=Partitions,CN=Configuration,DC=redteamrd,DC=local
RootDomain            : redteamrd.local
SchemaMaster          : dc01.redteamrd.local
Sites                 : {Default-First-Site-Name}
SPNSuffixes           : {}
UPNSuffixes           : {}
```

Enumeración a nivel Forestal

Los dominios/bosques también pueden tener su propia version

```
PS C:\Users\Administrator\Downloads> (Get-ADForest).ForestMode
Windows2016Forest
PS C:\Users\Administrator\Downloads> (Get-ADDomain).DomainMode
Windows2016Domain
```

Los protocolos de autenticaciones fundamentales de AD son ***Kerberos*** y ***LDAP***

LDAP (Lightweight Directory Access Protocol) se encarga de acceder y administrar las informaciones almacenadas del directorio por ejemplo el es como el intermediario de cuando solicitas un recurso como información de un usuario

- ***LDAP puerto 389***
- ***LDAPS puerto 636***

Las **claves Kerberos** se utilizan en el protocolo de autenticación Kerberos y estas hacen la función de **solicitar un vale/ticket de Kerberos** que represente al usuario

- ***Kerberos puerto 88***

Tipos de Cifrado que utiliza **Kerberos**:
- **Clave AES 256**
- **Clave AES 128**
- **Clave DES**

¿Que entendemos por autenticaciones del dominio?

Los DC básicamente es el servidor que se encarga de la **administración de los usuarios,grupos,políticas de seguridad,permisos y autenticaciones del dominio.**

El administrador de estos **Dominios** son los servidores centrales mejor conocido como **Controladores de Dominio (DC)**

- Dentro de un Active Directory podemos tener varios controladores de dominio (DC)
- Pueden existir mas de un dominio

Una red de AD (Active-Directory) se conoce generalmente como **Dominio** (Encapsula un conjunto de equipos que comparten una misma base de datos AD compartiendo el mismo Dominio)

Cada dominio tiene un nombre DNS como por ejemplo "**redteamrd.local**" en la mayoría de empresas el nombre del dominio suele ser el mismo de la empresa/web.

```
PS C:\Users\Olik3n> $env:USERDNSDOMAIN
redteamrd.local
PS C:\Users\Olik3n> (Get-ADDomain).DNSRoot
redteamrd.local
```

Identificación del dominio a nivel de usuario

```
PS C:\Users\Olik3n> (Get-WmiObject Win32_ComputerSystem).Domain
redteamrd.local
```

Identificación del dominio a nivel de equipo

```
PS C:\Users\Olik3n> Get-ADDomain | select DNSRoot,NetBIOSName,DomainSID

DNSRoot       NetBIOSName DomainSID
-------       ----------- ---------
redteamrd.local REDTEAMRD   S-1-5-21-1372086773-2238746523-2939299801
```

Enumerar a nivel de NetBIOS,DNS,SID del dominio.

Para administrar los **usuarios** de forma mas facil, se almacenan como **objetos** en la base de datos central

Para identificar a un usuario , generalmente se utiliza el **nombre de usuario** y además el **SID (Identificador de Seguridad)**

El nombre de usuario se guarda en los atributos **SamAccountName**

```
PS C:\Users\Olik3n> Get-ADUser Olik3n

DistinguishedName : CN=Anakin,CN=Users,DC=contoso,DC=local
Enabled           : True
GivenName         : Olik3n
Name              : Olik3n
ObjectClass       : user
ObjectGUID        : 58ab0812-9c96-4e97-bf53-019e86fd3ed7
SamAccountName    : Olik3n
SID               : S-1-5-21-1372086773-2238746523-2939299801-1103
Surname           :
UserPrincipalName : olik3n@redteamrd.local
```

Enumeracion nivel Usuario de dominio AD

El valor SID es un valor que muchas veces nos lo podremo topar a cambio del nombre de usuario como salida.

La **API LDAP** es un atributo que hace referencia a objetos tipo "atributo=valor" a través de la base de datos LDAP (muy común) entonces será muy probable que veas objetos a través de su archivo *"DistinguisheName"*

```
PS C:\Users\Olik3n> Get-ADUser -Filter * | select SamAccountName

SamAccountName
--------------
Administrator
Guest
krbtgt
anakin
han
POKEMON$
```

Enumerar usuarios Importantes (Cualquier Usuario puede enumerar a los demas usuarios sin necesidad de privilegios)

```
PS C:\> Get-ADObject -LDAPFilter "objectClass=User" -Properties SamAccountName |
select SamAccountName

SamAccountName
--------------
Administrator
Guest
DC01$
krbtgt
anakin
WS01-10$
WS02-7$
DC02$
han
POKEMON$
```

Enumerar cuentas por equipo

las cuentas de user se almacenan en instancias "User" mientras que las de equipo(Host) son una sub-clase de estas y estas se nombran con un signo de dolar $ al final

```
PS C:\> Get-ADUser  -LDAPFilter "(SamAccountName=*$)" | select SamAccountName

SamAccountName
--------------
POKEMON$
```

Enumerando cuentas fiduciarias

Las cuentas Fiduciarias son cuentas especiales que representan una relación de confianza entre dominios, Active Directory crea cuentas especiales terminadas en $ para representar esa relación.

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:6535b87abdb112a8fc3bf92528ac01f6:::
user:1001:aad3b435b51404eeaad3b435b51404ee:57d583aa46d571502aa04bb7aea0f%70:::
```

Volcado de Hashes

Formato: `<username>:<rid>:<LM>:<NT>::aad3b435b51404eeaad3b435b51404ee:`

los hashes LM y NT, y por lo general devuelven un salida con varias líneas, una por usuario, con el formato . En caso de que LM no se utilice, el hash LM de una cadena vacia.

Los hashes NT y LM se almacenan tanto en la SAM local de Windows como en la base de datos active directory NTDS

El hash NT es el mas comun actual debido a su seguridad

Las contraseñas de usuarios no se guardan en texto plano por lo que deriva a los cifrados:

-Hash NT (Hash LM para cuentas mas antiguas)
-Claves Kerberos

Ni siquiera los equipos del dominio pueden acceder a ellos, sino que dejan la autenticación a el controlador de dominio.

Los grupos se almacenan en la base de datos del dominio y se pueden identificar igual que los usuarios es decir a nivel SID y atributo

```
PS C:\Users\Anakin> Get-ADGroup -Filter * | select SamAccountName

SamAccountName
--------------
Administrators
Users
Guests
<-- stripped output -->
Domain Computers
Domain Controllers
Schema Admins
Enterprise Admins
Cert Publishers
Domain Admins
Domain Users
<-- stripped output -->
Protected Users
Key Admins
Enterprise Key Admins
DnsAdmins
DnsUpdateProxy
DHCP Users
DHCP Administrators
```

ACCOUNTDISABLE -> cuenta está deshabilitada y no se puede usar.
DONT_REQUIRE_PREAUTH -> La cuenta no requiere Kerberos autenticación previa.
NOT_DELEGATED -> Esta cuenta no se puede delegar a través de Kerberos delegación.
TRUSTED_FOR_DELEGATION -> la delegación sin restricciones de Kerberos está habilitada para esta cuenta y sus servicios.
SeEnableDelegationPrivilege necesario para modificar eso.
TRUSTED_TO_AUTH_FOR_DELEGATION -> La extensión Kerberos S4U2Self está habilitada para esta cuenta y sus servicios.
SeEnableDelegationPrivilege necesario para modificar eso.

UserAccountControl (UAC) es un atributo en los objetos que almacena una serie de configuraciones relacionadas con el comportamiento y las propiedades de la cuenta de usuario super relevantes a nivel de seguridad .

en AD existen grupos predeterminados ya definidos por lo tanto uno de los mas importantes seria como el "Domain Admins"

```
PS C:\Users\Anakin> Get-ADGroup "Domain Admins" -Properties members,memberof


DistinguishedName : CN=Domain Admins,CN=Users,DC=contoso,DC=local
GroupCategory     : Security
GroupScope        : Global
MemberOf          : {CN=Denied RODC Password Replication Group,CN=Users,DC=contoso,DC=local,
                    CN=Administrators,CN=Builtin,DC=contoso,DC=local}
Members           : {CN=Administrator,CN=Users,DC=contoso,DC=local}
Name              : Domain Admins
ObjectClass       : group
ObjectGUID        : ac1ac095-1ea0-4922-8130-efa99ba99afa
SamAccountName    : Domain Admins
SID               : S-1-5-21-1372086773-2238746523-2939299801-512
```

El administrador de estos **Dominios** son los servidores centrales mejor conocido como **Controladores de Dominio (DC)**

- Dentro de un Active Directory podemos tener varios controladores de dominio (DC)
- Pueden existir mas de un dominio