NetNTLM: Su propósito principal es autenticar usuarios y dispositivos en una red cuando no es posible usar otros protocolos más modernos, como Kerberos.

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*

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

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 por cada servicio que debamos solicitar

Kerberos puerto 88

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

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:653b87a8db112a0fc3bf92528ac01f6:::
user:1001:aad3b435b51404eeaad3b435b51404ee:5d5d3ae6dd75902aa0bb3aea0fc79b:::
```

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 vacía.

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

¿Que entendemos por autenticaciones del dominio?

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?

```
Domain: empresa.com
|
|
|- NameWork
|   |- 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

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)

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)

Domain
thm.local

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

Los DC básicamente es el servidor que se encarga de la **administración de los usuarios,grupos,políticas de seguridad,permisos y autenticaciones 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=Olik3n,CN=Users,DC=contoso,DC=local
Enabled           : True
GivenName         : Olik3n
Name              : Olik3n
ObjectClass       : user
ObjectGUID        : 8bab0112-0c96-4e87-bf53-01be8ef43ef7
SamAccountName    : Olik3n
SID               : S-1-5-21-1372086773-2238706523-2939299801-1103
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 comun) entonces será muy probable que veas objetos a través de su archivo `'DistinguishedName'`

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

SamAccountName
--------------
Administrator
Guest
krbtgt
anakin
test
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
krbtgt
anakin
WS01-10$
WS02-10$
DC01$
test
POKEMON$
```

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

Enumerar cuentas por equipo

```
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.

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-1-5-21-1372086773-2238706523-2939299801
```

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

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

Tomamos como que cada subdominio es un árbol de un bosque y que el conjunto de este forman un Bosque

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

ApplicationPartitions : {DC=DomainDnsZones,DC=redteamrd,DC=local,
                        DC=ForestDnsZones,DC=redteamrd,DC=local}
CrossRefs             : {}
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
```

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 vínculo se les llama **Confianza(Trusts)**

```
- redteamrd.local
  |   |
  |   |
  |   |
```