🧰 Understanding Active Directory (AD)

Intro

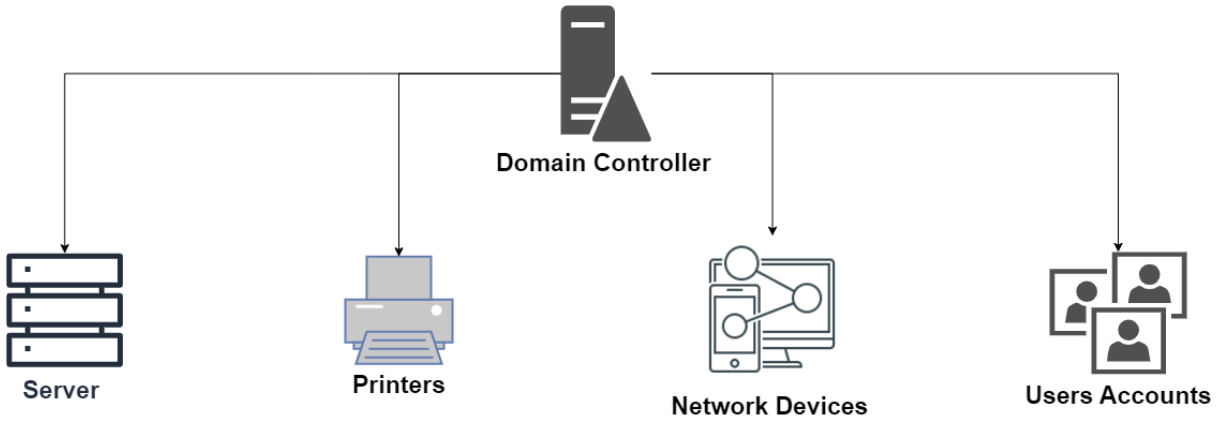
AD it is an information store of all the resources on a network.

When we are in a big organization, for example hundreds or thousands of employees, we will have a lot of resources in the network like users, many equipment connected on that network, printers, servers… many things that have to be managed and organized in some way. Going equipment by equipment making configurations is not a good option, especially in large organizations.

And for make easier the management of all this elements exist **Active Directory** 🪟

Active Directory 🪟 make it easier for a organization to search and manage all these elements for common user and administrators. Uses a structured and hierarchical data warehouse as base for that information. This data warehouse is called **directory** that includes:

- Servers
- Printers
- Users Accounts
- Network Equipments



This is the general concept that people have of **AD** 🪟**,** but **AD** is it's much more than just a hierarchical data warehouse.

In fact the real name is **Active Directory Domain Services (AD DS). AD** has a set of very important services that let us interact in different ways with the stored information and control different operations in a IT environment Like:

- **Authentication:** Ensures that each entity is who it says it is
- **Authorization:** Ensure that each entity has access to the data and services that are allowed.
- **Name Resolutions :** Allow de communications between the network elements through a name. To use DNS protocols service in a internal network
- **Centralized Management:** Allow the applications of groups policies

🧱 🧰 Active Directory Structure

As we said, **AD** provides us a hierarchical structure that creates different logical groups with which we can organize all the elements in a network.

The **tree** Logical groups that AD are structure are 🌲**forest,** 👑 **Domains and** 👥**Organizational Units (OU)**

🌲Forests

Is the highest and biggest organization level in Active Directory. Each Forest1 shares a unique directory and represents a security limit, that means , that by default, all that is stored in the forest, like users, won't be accessible for other forests.

- A forest can contains one or more **Domains**
- **Domains** can contains one or more **Organizational units**
- **Domain** and **organizational unit** information is stored on a **domain controller** for a specific domain. This warehouse is called **“Data Store”.**
- This information is stored in the form of 🎒**objects.** To understand better what an object is , **a user** is an object**, network equipment** is an object, **a printer** is an object. All of that is stored in **Active directory**, more specifically, in **“Data Store”**
- All objects will have a series of attributes, for example a **User** will have a **Name** and a **Password**, and all these attributes are defined by a **echeme,** who will define what attribute a Object will have.

👑Domains

Is a **logical object partition in a** 🌲**Forest** that shares common configurations of administrators, security and replication. All the information that is part of the domain, all the 🎒**objects** that are part of the domain will be stored in the **Domain Controller**. In the function are;

- **Guarantees the identity** of a user in the whole network
- Provides **authentication** services
- Provides **authorization** services
- Allow **replicates the information** between different Domain Controllers (DC) and manage them as a single unit. Is it possible that in a big organization it takes the decision to create one or more Domain Controllers with all the information replicated so as not to lose it in case of a failure or an attack. And even they can manage all of them like a unique domain controller.

👥Organizational Units (OU)

Is an object container that allows organizing other 🎒**objects** in a domain. **OU** has three principal functions:

1) Allows an **organized display** of Domain objects, thinking that in organization there are hundreds or thousand 🎒**objects** in a domain

2) Groups different 🎒**objects** to which it is applied **Group Policy**

3) Group different 🎒**objects** so that **management permissions can be delegated** to other users and groups in a domain.

🗺️ 🧰 Active Directory Schema

All Stored in **AD** is stored in the form of ***"🎒objects"***. The **schema** defines the attributes to each kind of object. Example, a **User Object** has a Name, could has a last name, could has a Password, and those attributes are defined by **schema** for that **User Object**

It will defined a schema by 🌲**forest** .Thats means that all 👑**domains** created in the same 🌲**forest** will have the same schema.

A copy of the schema resides in the in every domain controller in the 🌲**forest.** So the definition of the 🎒**objects** is the same.

The **"Data Store"** uses the **schema** to force information integrity.This means that if an attribute is not in the **schema,** Data Store will make sure that you cannot introduce that object into the database.

As a result, all 🎒**objects** are created uniformly, regardless of whether the **Domain Controller** create new 🎒**objects** or modify them.

🗄️ 🧰 Active Directory Data Store

Data Store, normally called as directory, **store information about the** 🌲**forest** (users, groups, domains,..) Data stores is the interface **between** the **users and database.**

The Directory is stored on **Domain Controllers** and it can be accessible by applications and network services. This is an important thing to keep in mind, because it is the origin of some security issues. If any network user has access to this directory and finds all resource in the infrastructure **going to be a big problem.**

If there is more than one Domain Controller, each Domain Controller will have a copy of the directory with whole 👑**domain** information.

⚙️🗄️ Data Store Components

Interfaces (LDAP, REPL, MAPI, SAM): The interfaces give a way to communicate with the database. ⚠️In a pentesting scenario we are going to show special interest on **LDAP**, **that is a protocol that will allow us *gain access to the database***, and will help us to collects information about a networks infrastructure⚠️ 👀

DSA: Allows access to the directory. Keep the **schema**, guarantees the 🎒**objects** identity, Force data types

Database Layer: Is an API which serves as an interface between the applications and the directory. regardless the applications can not interact directly with the Database

ESE: Communicates directly with individual records stored in the directory

Database files: The directory information is stored in a unique database file. Additionally, use log files for transactions that do not end properly.

About all of this, for us, the most important thing, and what we have to pay more attentions is **LDAP**

The Conclusion

🧰 **Active Directory** is a technology that allows us to manage in a centralized manner all the resources in a network infrastructure, users, equipment, servers printers, groups, security policy.

To do that use a hierarchy structure in which they exist 🌲**Forest** as principal logical structure, then we have 👑**Domains**, in the 🌲**Forest**, in the 👑**Domains** we have 👥**Organizational Units** and in the 👥**Organizational Units** we have the 🎒 **objects**

All Information that is hierarchy structure must be in some places and this place is the **DOMAIN CONTROLLER.** That is a server that will contain different pieces and modules like 📊 **schema** that guarantees that all information stored meets all specific criteria.

Has a determined attributes, the 🎒 **objects** exist a has been previously defined

Has the 🗄️ **Data Store** which will ensure that the scheme is complied with, will provide interfaces to access to the database

And 📁**Database file** which is a unique file where all the informations is stored and other logs files where possible errors are stored that has been produce by accessing that information.