5

Active Directory is the directory service for Windows Domain Networks. It is used by many of today's top companies and is a vital skill to comprehend when attacking Windows.
It is recommended to have knowledge of basic network services, Windows, networking, and Powershell.
The detail of specific uses and objects will be limited as this is only a general overview of Active Directory. For more information on a specific topic look for the corresponding room or do your own research on the topic.
What is Active Directory
Active Directory is a collection of machines and servers connected inside of domains, that are a collective part of a bigger forest of domains, that make up the Active Directory network. Active Directory contains many functioning bits and pieces, a majority of which we will be covering in the upcoming tasks. To outline what we'll be covering take a look over this list of Active Directory components and become familiar with the various pieces of Active Directory:

- Domain Controllers
- Forests, Trees, Domains
- Users + Groups
- Trusts
- Policies
- Domain Services

All of these parts of Active Directory come together to make a big network of machines and servers.
Now that we know what Active Directory is, let's talk about the why.
Domain Controllers -
A domain controller is a Windows server that has Active Directory Domain Services (AD DS) installed and has been promoted to a domain controller in the forest. Domain controllers are the center of Active Directory -- they control the rest of the domain. I will outline the tasks of a domain controller below:
◇ holds the AD DS data store
◇ handles authentication and authorization services
◇ replicate updates from other domain controllers in the forest
◇ Allows admin access to manage domain resources

AD DS Data Store -
The Active Directory Data Store holds the databases and processes needed to store and manage directory information such as users, groups, and services. Below is an outline of some of the contents and characteristics of the AD DS Data Store:
◇ Contains the NTDS.dit - a database that contains all of the information of an Active Directory domain controller as well as password hashes for domain users
◇ Stored by default in %SystemRoot%\NTDS
◇ accessible only by the domain controller

That is everything that you need to know in terms of physical and on-premise Active Directory. Now move on to learn about the software and infrastructure behind the network.

Forest Overview -

A forest is a collection of one or more domain trees inside of an Active Directory network. It is what categorizes the parts of the network as a whole.

The Forest consists of these parts which we will go into farther detail with later:

◇ Trees - A hierarchy of domains in Active Directory Domain Services

◇ Domains - Used to group and manage objects

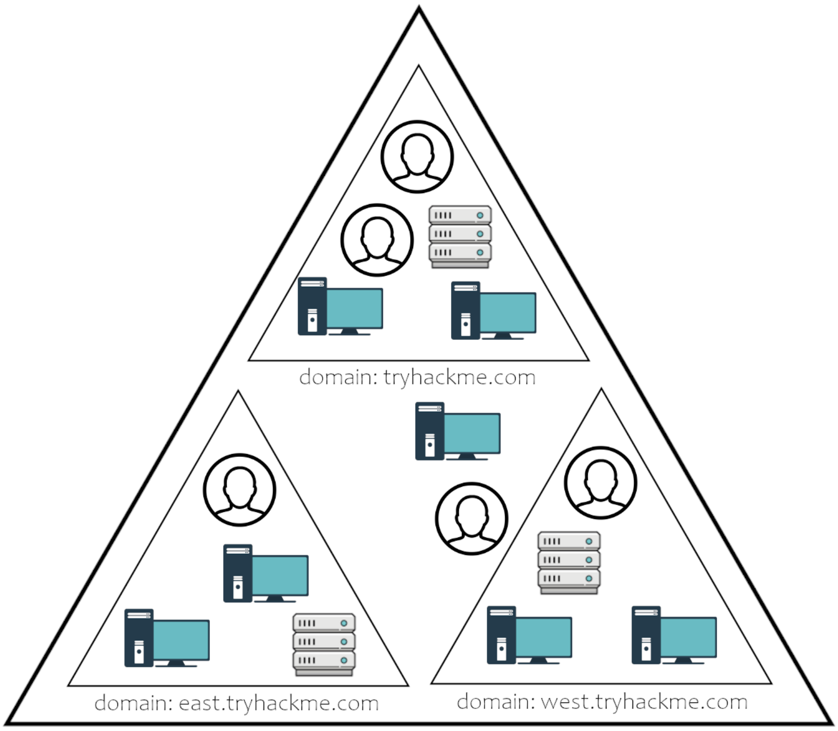
◇ Organizational Units (OUs) - Containers for groups, computers, users, printers and other OUs

◇ Trusts - Allows users to access resources in other domains

◇ Objects - users, groups, printers, computers, shares

◇ Domain Services - DNS Server, LLMNR, IPv6

◇ Domain Schema - Rules for object creation



Active Directory forest visualized

Users Overview -

Users are the core to Active Directory; without users why have Active Directory in the first place? There are four main types of users you'll find in an Active Directory network; however, there can be more depending on how a company manages the permissions of its users. The four types of users are:

◇ Domain Admins - This is the big boss: they control the domains and are the only ones with access to the domain controller.

◇ Service Accounts (Can be Domain Admins) - These are for the most part never used except for service maintenance, they are required by Windows for services such as SQL to pair a service with a service account

◇ Local Administrators - These users can make changes to local machines as an administrator and may even be able to control other normal users, but they cannot access the domain controller

◇ Domain Users - These are your everyday users. They can log in on the machines they have the authorization to access and may have local administrator rights to machines depending on the organization.

Domain Policies Overview -
Policies are a very big part of Active Directory, they dictate how the server operates and what rules it will and will not follow. You can think of domain policies like domain groups, except instead of permissions they contain rules, and instead of only applying to a group of users, the policies apply to a domain as a whole. They simply act as a rulebook for Active Directory that a domain admin can modify and alter as they deem necessary to keep the network running smoothly and securely. Along with the very long list of default domain policies, domain admins can choose to add in their own policies not already on the domain controller, for example: if you wanted to disable windows defender across all machines on the domain you could create a new group policy object to disable Windows Defender. The options for domain policies are almost endless and are a big factor for attackers when enumerating an Active Directory network. I'll outline just a few of the many policies that are default or you can create in an Active Directory environment:
◇ Disable Windows Defender - Disables windows defender across all machine on the domain
◇ Digitally Sign Communication (Always) - Can disable or enable SMB signing on the domain controller

Domain Services Overview -
Domain Services are exactly what they sound like. They are services that the domain controller provides to the rest of the domain or tree. There is a wide range of various services that can be added to a domain controller; however, in this room we'll only be going over the default services that come when you set up a Windows server as a domain controller. Outlined below are the default domain services:
◇ LDAP - Lightweight Directory Access Protocol; provides communication between applications and directory services
◇ Certificate Services - allows the domain controller to create, validate, and revoke public key certificates
◇ DNS, LLMNR, NBT-NS - Domain Name Services for identifying IP hostnames

Domain Authentication Overview -
The most important part of Active Directory -- as well as the most vulnerable part of Active Directory -- is the authentication protocols set in place. There are two main types of authentication in place for Active Directory: NTLM and Kerberos. Since these will be covered in more depth in later rooms we will not be covering past the very basics needed to understand how they apply to Active Directory as a whole. For more information on NTLM and Kerberos check out the Attacking Kerberos room - https://tryhackme.com/room/attackingkerberos.
◇ Kerberos - The default authentication service for Active Directory uses ticket-granting tickets and service tickets to authenticate users and give users access to other resources across the domain.
◇ NTLM - default Windows authentication protocol uses an encrypted challenge/response protocol

The Active Directory domain services are the main access point for attackers and contain some of the most vulnerable protocols for Active Directory, this will not be the last time you see them mentioned in

terms of Active Directory security.
Now that we understand the basics of active directory we can utilize this knowledge within the lab environment to get hands on practice with these concepts.

Answer the questions below

Read the above to get a basic understanding of Active Directory

Question Done