Active Directory Overview

What is Active Directory?

→It is a service developed by Microsoft *to manage Windows Domain Networks*.
→ It stores information related to objects, such as Computers, Users, Printers, etc. (Example: Like a phonebook for windows)
→ Its Authenticates using Kerberos Tickets.
→ Even Non-Windows machines like Linux Machines , Firewalls can authenticate Active Directory Using LDAP (LightWeight Directory Protocol) , RADIUS (Remote Authentication Dial-In User Service)

Why Active Directory?

More than 95% of 1000 fortune companies use Active Directories. We don't need a exploit, to exploit it we can just exploit it as just how it works.(i.e By Abusing its features, trusts, components & more)

Physical Components of Active Directory

Domain Controller

→ Domain Controller hosts a copy of AD DS Directory Store(Active Directory Domain services)
→ It provides authorization and authentication services for the network
→ This allow administrative access to manage user accounts and network resources
Replicates updates to the other domain controllers in the domain or forest.

AD DS Data Store

→There is a file located at %SYSTEMROOT%\NTDS (Mostly C:\Windows\NTDS)
It contains NTDS.dit file which stores all system password hashes and also users and group info in it.

Logical Components of Active Directory

AD DS Schema

→ It's a rule book for Active Directory
→ It defines every type of object that can be stored in Directory
→ It enforces the rules regarding creating the object and even configuring it.

Domains

→ This is a administrative boundary to apply policies to groups of objects .
→A replication boundary for replicating data between domain controllers.
A Authentication and Authorization boundaries that provide a limit the scope of access to the available resources.

Trees

A Domain tree is the heirarchy of domains in AD DS
→ These share a contoguous name space with the parent domain
→Can have additional child domains
→ By default create a two-way transitive trust with other domains.

Forests

A forest is a collection of one or more domain trees
→ These share a common schema
→ These share a common configuration partitiomn
→ Shares a common catalogue to enable searching
→ Enables the trust between all the domains in the forests.
→ Share the Enterprise admins and Schema admin groups.

Organisational Units (OUs)

These are the Active Directory Containers which contains groups, users, computers and other OUs
→ These Represent your heirarchically and logically
→ Manage a collection of objects in a more consistent way
→ Delegate permissions to administer groups of objects
→ Apply policies

Trusts

1) Directional Trust

Here, The trust directions flow from trusting domain to the trusted domain.

2) Transitive Trust

The trust relation extends beyond a two domain to include other trusted domains
→ All domains in a forest trust all other domains in the forest
→ Trusts can extend outside the forest.

Objects

Objects

Object	Description
User	• Enables network resource access for a user
InetOrgPerson	• Similar to a user account • Used for compatibility with other directory services
Contacts	• Used primarily to assign e-mail addresses to external users • Does not enable network access
Groups	• Used to simplify the administration of access control
Computers	• Enables authentication and auditing of computer access to resources
Printers	• Used to simplify the process of locating and connecting to printers
Shared folders	• Enables users to search for shared folders based on properties

User

→ Enables Network resource access for a user

InetOrgPerson

→ Similar to user account
Usable for compatibibility with other directory services

Contacts

Used primarily to assign email address to external users
Doesn't enable network access

Groups

Used to simplify the administration of user control

Computers

Enables authentication and auditing of computer access to resources

Printers

Used to simplify the process of locating and connecting to the printers

Shared Folders

Enables the users to search the shared folders based on its properties.

`Cloud Security Overview -`

The best way to show you how the cloud takes security precautions past what is already provided with a physical network is to show you a comparison with a cloud Active Directory environment:

Windows Server AD	Azure AD
LDAP	Rest APIs
NTLM	OAuth/SAML
Kerberos	OpenID
OU Tree	Flat Structure
Domains and Forests	Tenants
Trusts	Guests