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 Actiev 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.