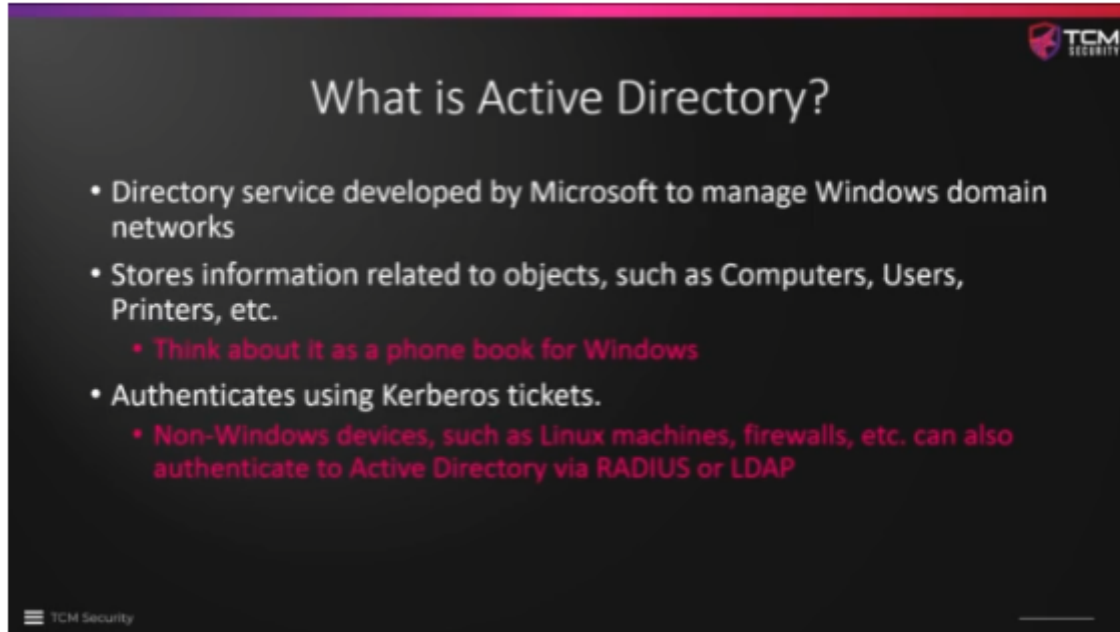


# Active Directory - Overview

---

Active Directory is most likely to be involve in internal penetration test assessments. It is like a phone book for windows.



**What is Active Directory?**

- Directory service developed by Microsoft to manage Windows domain networks
- Stores information related to objects, such as Computers, Users, Printers, etc.
  - Think about it as a phone book for Windows
- Authenticates using Kerberos tickets.
  - Non-Windows devices, such as Linux machines, firewalls, etc. can also authenticate to Active Directory via RADIUS or LDAP

TCM Security

It is a tool that is used to manage a network of computers that belongs and are connected to the Active Directory Domain. Although is a windows feature, Linux machines, firewalls, and other devices can also authenticate to AD via RADIUS or LDAP.



**Why Active Directory?**

- Active Directory is the **most commonly used** identity management service in the world
  - 95% of Fortune 1000 companies implement the service in their networks (<https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Success-with-Enterprise-Mobility-Identity/bap/248613>)
- Can be exploited **without ever attacking** patchable exploits.
  - Instead, we abuse features, trusts, components, and more.

TCM Security

# Physical Active Directory Components



## Active Directory Components

Active Directory is composed of both physical and logical components.

### • PHYSICAL

- Data store
- Domain controllers
- Global catalog server
- Read-Only Domain Controller (RODC)

### • LOGICAL

- Partitions
- Schema
- Domains
- Domain trees
- Forests
- Sites
- Organization units (OUs)



## Domain Controllers

A domain controller is a server with the AD DS server role installed that has specifically been promoted to a domain controller



### Domain controllers:

- Host a copy of the AD DS directory store
- Provide authentication and authorization services
- Replicate updates to other domain controllers in the domain and forest
- Allow administrative access to manage user accounts and network resources

Source: Microsoft Virtual Academy

# AD DS Data Store

The AD DS data store contains the database files and processes that store and manage directory information for users, services, and applications

## The AD DS data store:

- Consists of the Ntds.dit file
- Is stored by default in the %SystemRoot%\NTDS folder on all domain controllers
- Is accessible only through the domain controller processes and protocols

Source: Microsoft Virtual Academy

# Logical Active Directory Components

## AD DS Schema

### The AD DS Schema:

- Defines every type of object that can be stored in the directory
- Enforces rules regarding object creation and configuration

Object Types	Function	Examples
Class Object	What objects can be created in the directory	<ul style="list-style-type: none"><li>• User</li><li>• Computer</li></ul>
Attribute Object	Information that can be attached to an object	<ul style="list-style-type: none"><li>• Display name</li></ul>

Source: Microsoft Virtual Academy

## Domains

Domains are used to group and manage objects in an organization



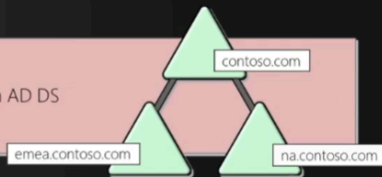
### Domains:

- An administrative boundary for applying policies to groups of objects
- A replication boundary for replicating data between domain controllers
- An authentication and authorization boundary that provides a way to limit the scope of access to resources

Source: Microsoft Virtual Academy

# Trees

A domain tree is a hierarchy of domains in AD DS



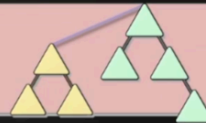
All domains in the tree:

- Share a contiguous namespace with the parent domain
- Can have additional child domains
- By default create a two-way transitive trust with other domains

Source: Microsoft Virtual Academy

# Forests

A forest is a collection of one or more domain trees



Forests:

- Share a common schema
- Share a common configuration partition
- Share a common global catalog to enable searching
- Enable trusts between all domains in the forest
- Share the Enterprise Admins and Schema Admins groups

Source: Microsoft Virtual Academy

# Organizational Units (OUs)

OUs are Active Directory containers that can contain users, groups, computers, and other OUs



OUs are used to:

- Represent your organization hierarchically and logically
- Manage a collection of objects in a consistent way
- Delegate permissions to administer groups of objects
- Apply policies

Source: Microsoft Virtual Academy

# Trusts

Trusts provide a mechanism for users to gain access to resources in another domain

Types of Trusts	Description	Diagram
Directional	The trust direction flows from trusting domain to the trusted domain	A diagram showing two green triangles representing domains. A solid red arrow points from the left domain to the right domain, labeled 'TRUST'. A dashed red arrow points from the right domain back to the left domain, labeled 'Access'.
Transitive	The trust relationship is extended beyond a two-domain trust to include other trusted domains	A diagram showing three green triangles representing domains. A solid red arrow points from the left domain to the middle domain, labeled 'Trust & Access'. A solid red arrow points from the middle domain to the right domain, labeled 'Trust & Access'. A dashed red arrow points from the left domain to the right domain, labeled 'Access'.

- All domains in a forest trust all other domains in the forest
- Trusts can extend outside the forest

Source: Microsoft Virtual Academy

Objects live inside OUs.

# Objects

Object	Description
User	<ul style="list-style-type: none"><li>Enables network resource access for a user</li></ul>
InetOrgPerson	<ul style="list-style-type: none"><li>Similar to a user account</li><li>Used for compatibility with other directory services</li></ul>
Contacts	<ul style="list-style-type: none"><li>Used primarily to assign e-mail addresses to external users</li><li>Does not enable network access</li></ul>
Groups	<ul style="list-style-type: none"><li>Used to simplify the administration of access control</li></ul>
Computers	<ul style="list-style-type: none"><li>Enables authentication and auditing of computer access to resources</li></ul>
Printers	<ul style="list-style-type: none"><li>Used to simplify the process of locating and connecting to printers</li></ul>
Shared folders	<ul style="list-style-type: none"><li>Enables users to search for shared folders based on properties</li></ul>

Source: Microsoft Virtual Academy

1 / 5

## How is Active Directory authentication handled?

Using session tokens

correct

Using Kerberos tickets



Using openID

Continue >

2 / 5

Active Directory can be exploited without using patchable exploits?

correct

True



False

◀ Back

Continue ▶

3 / 5

What is the roles are carried out by the Domain Controller? (multiple choice)

correct

Provide authentication and authorization



correct

Allow administrative access to manage user accounts



incorrect

Monitors the network for intrusions



◀ Back

Continue ▶



---

4 / 5

Trees are a...

correct

Group of Domains



A collection of Domain Controllers

A structure of user objects within a Domain

◀ Back

Continue ▶

---

5 / 5

Forests are a...

A collection of Domain Controllers

A structure of user objects within a Domain

correct

A collection of Domain Trees



◀ Back

Continue ▶

---