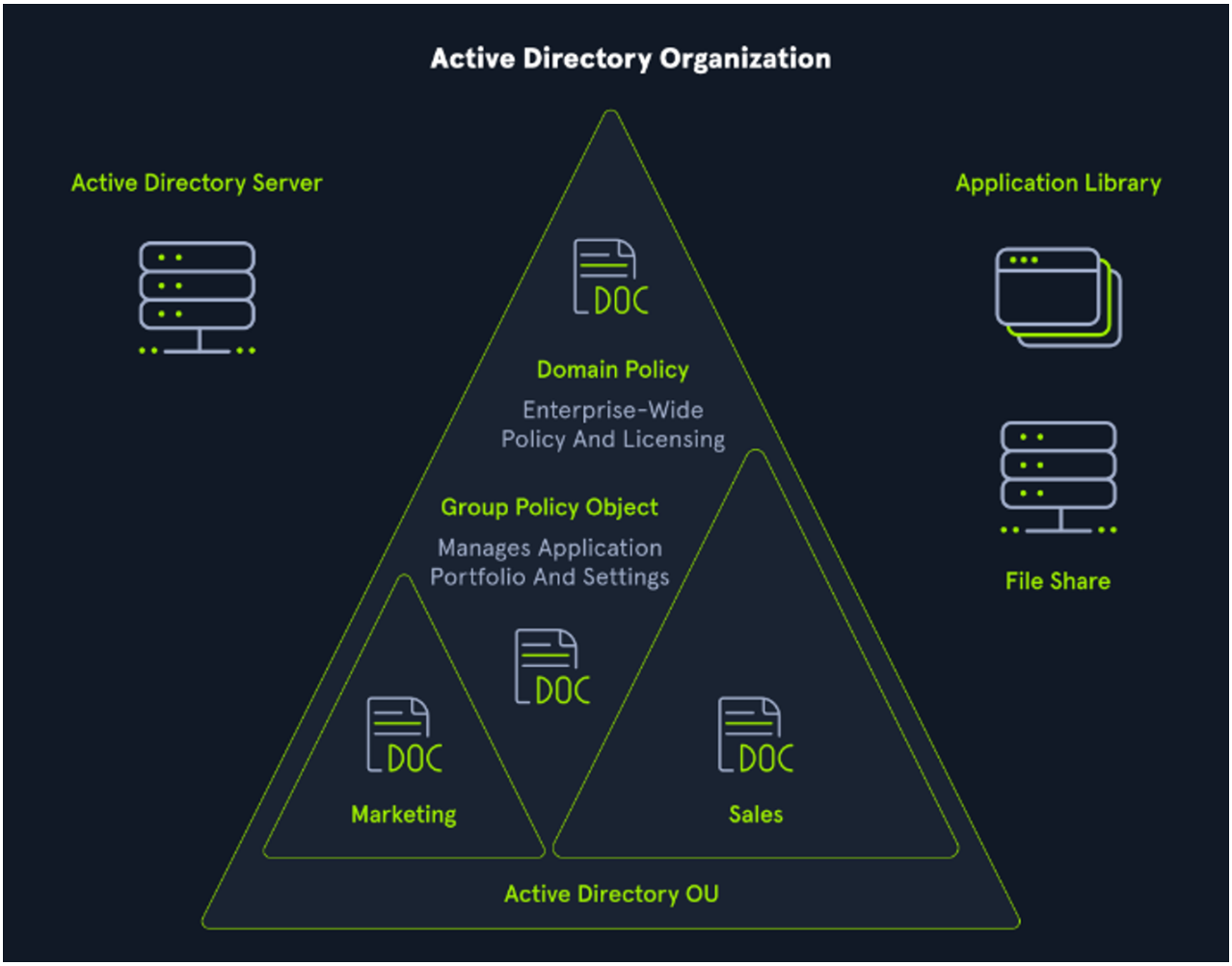
Pentesting Active Directory - Part 1 | Trees, Forest and Trust Relations

hacklido.com/blog/862-pentesting-active-directory-part-1-trees-forest-and-trust-relations

- 24 days ago



Let me introduce you to Active directory and familiarize with it's components like trees, forest and trust relations

Introduction

Active Directory (AD) is a directory service for Windows-based network environments and is crucial for the centralized management of an organization's resources such as users, computers, groups, network devices, file shares, group policies, devices, and trusts. The hierarchical and distributed structure of AD makes it a highly scalable solution, capable of supporting millions of objects per domain and allowing the creation of additional domains as the organization grows.

However, the centralization of information also makes AD a prime target for attackers, who are increasingly using it as a key component of their attack paths. It is estimated that around 95% of Fortune 500 companies rely on Active Directory, making it a critical focus

for attackers looking to penetrate a network. A successful phish can grant an attacker access to the AD environment as a standard domain user, which provides enough access to begin mapping the domain and looking for weaknesses.

One of the reasons AD has become a prime target for attackers is that it provides both authentication and authorization functions within a Windows domain environment. While AD is designed to be backward-compatible, many of its features are not considered secure by default, making it vulnerable to misconfiguration and exploitation. In addition, a basic AD user account can enumerate most objects within AD, making it extremely important to properly secure the AD environment.

In recent years, AD has come under increasing attack, and ransomware operators have specifically targeted it as a critical part of their attack paths. For example, the Conti Ransomware has been used in over 400 attacks worldwide and leverages recent critical Active Directory flaws such as PrintNightmare (CVE-2021-34527) and Zerologon (CVE-2020-1472) to escalate privileges and move laterally in target networks.

Trees and Forests / Components

Domain Controller

A Domain Controller is typically considered the overseer of the Active Directory, responsible for setting up the directory and its functionality. The main purpose of a Domain Controller is to grant access to network resources and user accounts by supplying Authentication and Authorization services to users and services. The Domain Controller is positioned at the highest level of priority within the Active Directory, possessing the greatest degree of control and administrative power. Essentially, a Domain Controller serves as the administrator of the Active Directory.

Active Directory Data Store

The Active Directory Data Store is a collection of database files and processes that maintain and store information about users, services, and applications. It holds the crucial “NTDS.DIT” file, which is located in the “%SystemRoot%\NTDS” folder on all domain controllers. This file is only accessible through the Domain Controller processes and protocols and is considered the most important component of the entire Active Directory.

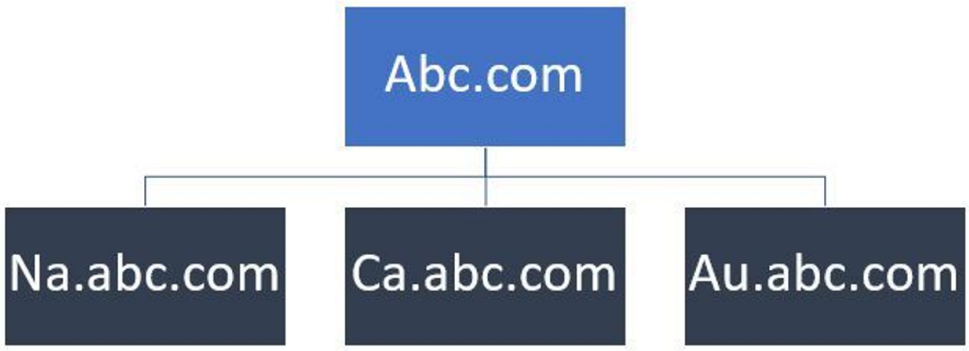
Logical Active Directory Components

The Logical Active Directory Components consist of various elements that exist within the Active Directory Data Store and establish the regulations for creating an object within an Active Directory environment. These components are integral components of the Active Directory and work together to ensure the smooth functioning of the AD.

Domain

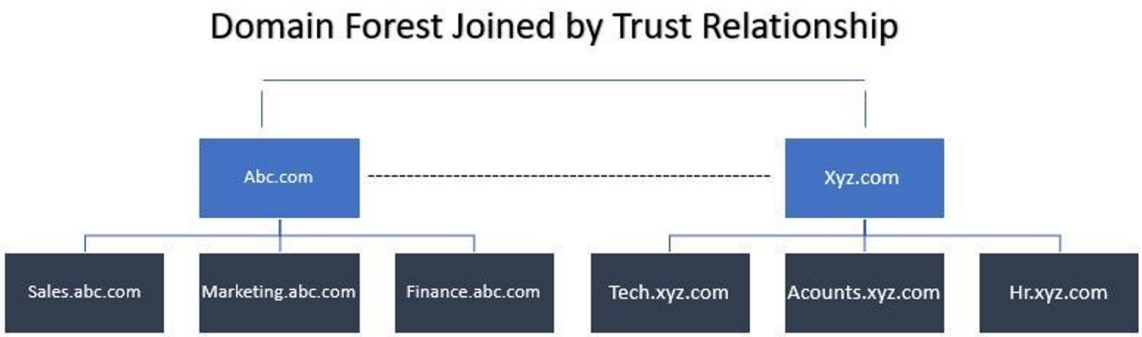
A Domain serves as an organizational unit that groups objects and enables management of these objects. The Domain creates a boundary for Authentication and Authorization, allowing control over access to the resources within that specific domain. For example, think of **http://abc.com** as a domain.

Trees



Trees are collections of domains in an Active Directory environment that share a contiguous namespace with the parent domain. They consist of the parent domain and any child domains that are associated with it. Trees establish transitive trust relationships between domains, meaning that the trust relationship between the domains in a tree are automatically extended to all the domains within that tree. In the context of Active Directory, a tree can be visualized as a hierarchy of domains, with the parent domain at the top and child domains branching off from it. An example of a tree structure would be a main domain, such as “abc.com”, with different geographic locations represented as child domains, such as “ca.abc.com” for Canada, “na.abc.com” for North America, and “au.abc.com” for Australia.

Forest



The Forest concept in Active Directory refers to a collection of Trees. All the Trees in the Forest are bound together by sharing a common schema. This means that the configuration remains uniform across all branches in the Forest. Trust between all domains is maintained within the Forest and it is typical for them to have a shared Enterprise Admin and Schema Admin. The image below provides a visual representation of the concept of Forest in Active Directory.

Organizational Units

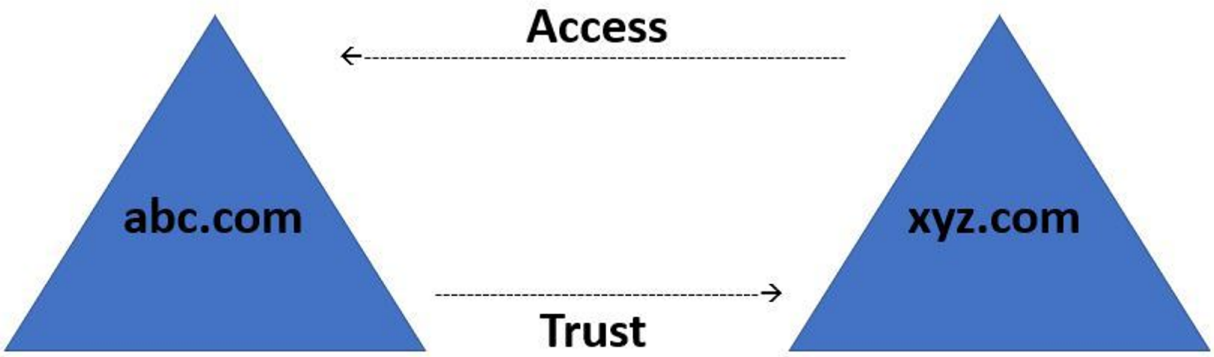
Organizational Units, also known as OUs, are containers within the Active Directory that are used to group and manage objects such as user groups, computers, and other OUs. They provide a hierarchical and logical structure for your organization and allow for efficient management of a collection of objects. Additionally, OUs allow for delegation of permissions to administrator groups and the application of policies and rules throughout the structure.

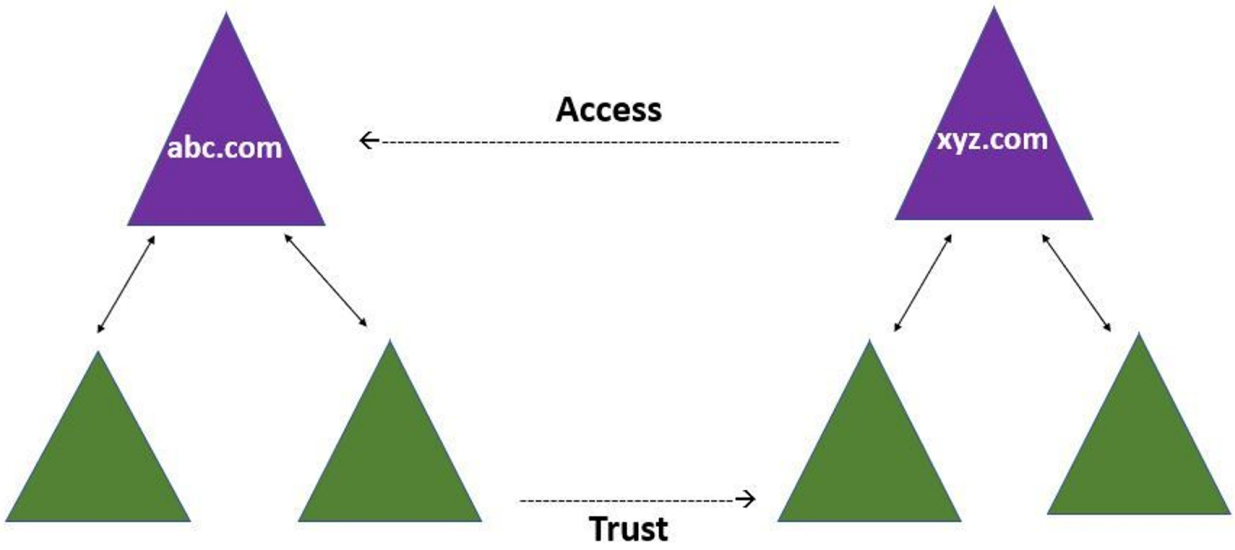
Trusts

In simple terms, Trusts in Active Directory are a means of establishing access between resources to gain permission to use resources in another domain. Trusts can be broadly categorized into two types: Directional Trust and Transitive Trust.

- Directional Trust: This type of trust is established in a one-way direction, where the Trusting domain grants access to the Trusted domain. A visual representation of this concept is shown in the diagram.
- Transitive Trust: This type of trust extends the relationship beyond a single domain trust to include other trusted domains. A diagram is provided for better understanding of this concept.

It’s important to note that Trusts are established to allow for secure access to resources across multiple domains, making them a crucial component of Active Directory security.





Enumerating AD with Bloodhound

Step 1: Download and Install BloodHound

1. Download the latest release of BloodHound from the GitHub repository: **https://github.com/BloodHoundAD/BloodHound/releases**
2. Extract the downloaded ZIP file to a folder on your system.
3. Install Neo4j Community Edition (required by BloodHound) from: **https://neo4j.com/download-center/#community**
4. After installing Neo4j, run it, and create a new graph database. Remember the database's password.

Step 2: Run BloodHound

1. Go to the folder where you extracted BloodHound and run the “BloodHound.exe” file.
2. Connect to the Neo4j database by entering the default username “neo4j” and the password you set for the graph database.
3. Once connected, BloodHound will display its main interface.

Step 3: Collect Active Directory Data using SharpHound

1. Download the latest release of SharpHound from the GitHub repository: **https://github.com/BloodHoundAD/SharpHound3/releases**
2. Extract the downloaded ZIP file to a folder on your system.
3. Run SharpHound on the target domain using a command prompt with administrative privileges. Navigate to the folder containing the “SharpHound.exe” file and execute the following command:

```
SharpHound.exe --CollectionMethod All
```

4. After SharpHound finishes collecting data, it will generate a ZIP file containing JSON files. This file is usually named “*BloodHound-yyyyMMddhhmmss.zip*”.

Step 4: Import Collected Data into BloodHound

1. In BloodHound, click the “Upload Data” button (cloud icon with an up arrow) in the top-right corner.
2. Browse to the location where the ZIP file generated by SharpHound is stored, and select it.
3. BloodHound will start importing the data, which may take a few minutes depending on the size of the data.

Step 5: Analyze the Results

1. Once the data is imported, you can use BloodHound to analyze the results and identify potential vulnerabilities and attack paths.
2. Use the search bar in the top-left corner to find specific users, computers, or groups.
3. Click on the nodes and view their properties, incoming, and outgoing relationships to analyze their connections and privileges.
4. Use the built-in queries in BloodHound to identify potential attack paths, such as “Shortest Paths to Domain Admins” or “Find All Domain Admins.”

By following these steps and using BloodHound, you can effectively analyze your Active Directory environment and identify potential vulnerabilities that attackers could exploit.

Home for infosec writers and readers.

Create your account today and explore more content on this platform. You can also start blogging and be inspiration for others 😎

11 days later

admiralarjun changed the title to **Pentesting Active Directory - Part 1 | Trees, Forest and Trust Relations** 13 days ago.