Active Directory - Introduction

0xstarlight.github.io/posts/Active-Directory-Introduction

Bhaskar Pal March 29, 2022

Introduction

Welcome to my first article in the Red Teaming Series (Active Directory Introduction). I hope to provide you all with information for an initial foundation and motivation about Active Directory, so let's move forward to learn other exciting aspects of the directory service developed by Microsoft to manage windows domain networks.

This guide aims to explain the complete basics of Active Directory and those terms that every pentester/red-teamer should control to understand the attacks performed in an Active Directory network.

I will cover the following topics under this guide:

1. Domain, Domain Controllers
2. Trees, Forests
3. Group Policy Object
4. Access Control List
5. Users + Groups
6. Trusts
7. Policies

> Throughout the article I will use PowerView which is based on Powershell to show how to retrieve information of Active Directory. This article has been created with references from a few other articles. All used references for completing this article will be listed below. —

What is Active Directory?

In a short description, an Active Directory is a system that allows the collection of machines and servers connected inside the same network from a central server(known as a Domain) that are a collective part of a bigger server(known as a forest) that make up the Active Directory network.

It stores information related to objects, such as Computers, Users, Printers, etc. You can think about it as a phone book for Windows. One of its main purposes is for authentication using Kerberos tickets. Non-windows devices, such as Linux machines, firewalls, etc., can also authenticate to Active Directory via RADIUS or LDAP protocols.

Active Directory contains many functioning bits and pieces, a majority of which we will be covering in the upcoming tasks.

Why use Active Directory?

The majority of large companies use Active Directory because it allows for controlling and monitoring their user's computers through a single domain controller. It will enable a single user to sign in to any computer on the active directory network and have access to their stored files and folders in the server and the local storage on that machine. This allows any user in the company to use any machine that the company owns without setting up multiple users on a machine. Active Directory does it all for you.

If this is still unclear, let me give you an example.

Let's take the example of Microsoft. It's a worldwide company with millions of employees. Let's focus on one building of Microsoft, which has about a thousand plus employees. Each of these employees is working on their workstations (Windows/Linux). This building might contain different departments like Market Research, Product Decisions, HR, IT, etc. Now imagine if one of the departments required a software update, or if one of the employees forgot their password, or one of the employees needed higher privileges to access view some content.

It would be extremely tedious if the IT department tried to fix all the issues. But this issue can resolve if they have all the computers connected in an Active Directory network to perform all these operations under one hood.

Domain Controllers

First of all, I have been reffering an Active Directory network as a Domain. In brief, a domain is a set of connected computers that shares an Active Directory database, which is managed by the central servers of a domain, that are called 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. Outlineing some of the tasks of a domain controller below:

1. Holds the AD DS data store
2. Handles authentication and authorization services
3. Replicate updates from other domain controllers in the forest
4. Allows admin access to manage domain resources

PowerView Enumeration

We can gather additional information about our target using PowerView

1. Get current domain

```
PS C:\Tools> Get-NetUser
user-dc.it.starlight.local
user-
mssql.it.starlight.local
user-
adminsrv.it.starlight.local
```

2. Enumerate Domain Admins

```
Get-NetDomain
# See Attributes of the Domain Admins Group
Get-NetGroup -GroupName "Domain Admins" -
FullData
# Get Members of the Domain Admins group
Get-NetGroupMember -GroupName "Domain
Admins"
```

Active Directory 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:

1. 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
2. Stored by default in `%SystemRoot%\NTDS`
3. Accessible only by the domain controller

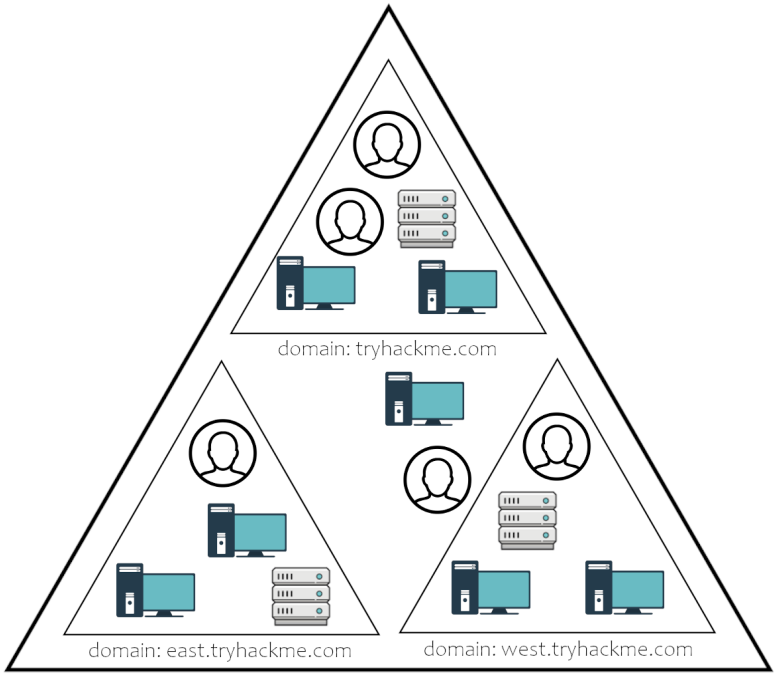
Trees

A hierarchy of domains in Active Directory Domain Services are known as Trees.

All the domains in the tree :

1. Can share a contiguous namespace with the parent domain
2. Can have additional child domains
3. By default create a two-way transitive trust with other child domains

Forests



Active-Directory-Basics-THM-Room

The forest is what defines everything; it is the container that holds all of the other bits and pieces of the network together – without the forest all of the other trees and domains would not be able to interact. The one thing to note when thinking of the forest is to not think of it too literally – it is a physical thing just as much as it is a figurative thing. When we say “forest”, it is only a way of describing the connection created between these trees and domains by 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

Group Policy Object

Group Policy provides the ability to manage configuration and changes easily and centrally in AD.

Allows configuration of :

- Security settings
- Registry-based policy settings
- Group policy preferences like startup/shutdown/log-on/logoff scripts settings
- Software installation

GPO can be abused for various attacks like privesc, backdoors, persistence etc.

PowerView Enumeration

We can gather additional information about our target using PowerView

1. Get list of GPO in current domain.

```
Get-NetGPO
Get-NetGPO -ComputerName <computer-name>
Get-GPO -All (GroupPolicy module)
Get-GPResultantSetOfPolicy -ReportType Html -Path
C:\Users\Administrator\report.html (Provides RSoP)
gpresult /R /V (GroupPolicy Results of current machine)
```

2. Get GPO(s) which use Restricted Groups or groups.xml for interesting users

```
Get-
NetGPOGroup
```

3. Get users which are in a local group of a machine using GPO

```
Find-GPOComputerAdmin -ComputerName <computer-
name>
```

4. Get machines where the given user is member of a specific group

```
Find-GPOLocation -Username student1 -
Verbose
```

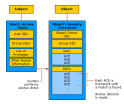
5. Get OUs in a domain

```
Get-NetOU -
FullData
```

6. Get GPO applied on an OU. Read GPOname from gplink attribute from Get-NetOU

```
Get-NetGPO -GPOname "{AB306569-220D-43FF-BO3B-83E8F4EF8081}"
Get-GPO -Guid AB306569-220D-43FF-B03B-83E8F4EF8081 (GroupPolicy
module)
```

Access Control List



The **Access Control Model** enables control on the ability of a process to access objects and other resources in active directory based on:

- Access Tokens (security context of a process — identity and privs of user)
- Security Descriptors (SID of the owner, Discretionary ACL (DACL) and System ACL (SACL))
- It is a list of Access Control Entries (ACE) — ACE corresponds to individual permission or audits access. Who has permission and what can be done on an object?
- Two types:
  - DACL : Defines the permissions trustees (a user or group) have on an object.
  - SACL : Logs success and failure audit messages when an object is accessed.
- ACLs are vital to security architecture of AD.

PowerView Enumeration

We can gather additional information about our target using PowerView

1. Get the ACLs associated with the specified object

```
Get-ObjectAcl -SamAccountName student1 -
ResolveGUIDs
```

2. Get the ACLs associated with the specified prefix to be used for search

```
Get-ObjectAcl -ADSprefix 'CN=Administrator,CN=Users' -
Verbose
```

3. We can also enumerate ACLs using ActiveDirectory module but without resolving GUIDs

```
(Get-Acl "AD:\CN=Administrator, CN=<name>, DC=<name>, DC=
<name>,DC=local").Access
```

4. Get the ACLs associated with the specified LDAP path to be used for search

```
Get-ObjectAcl -ADSpath "LDAP://CN=Domain Admins,CN=Users,DC=<name>,DC=
<name>,DC=local" -ResolveGUIDs -Verbose
```

5. Search for interesting ACEs

```
Invoke-ACLScanner -
ResolveGUIDs
```

6. Get the ACLs associated with the specified path

```
Get-PathAcl -Path "\\<computer-
name>\sysvol"
```

Users + Groups

The users and groups that are inside of an Active Directory are up to you; when you create a domain controller it comes with default groups and two default users: Administrator and guest. It is up to you to create new users and create new groups to add users to.

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.

Groups Overview

Groups make it easier to give permissions to users and objects by organizing them into groups with specified permissions. There are two overarching types of Active Directory groups:

- Security Groups - These groups are used to specify permissions for a large number of users
- Distribution Groups - These groups are used to specify email distribution lists. As an attacker these groups are less beneficial to us but can still be beneficial in enumeration

Default Security Groups

There are a lot of default security groups so I won't be going into too much detail of each past a brief description of the permissions that they offer to the assigned group. Here is a brief outline of the security groups:

- Domain Controllers - All domain controllers in the domain
- Domain Guests - All domain guests
- Domain Users - All domain users

- Domain Computers - All workstations and servers joined to the domain
- Domain Admins - Designated administrators of the domain
- Enterprise Admins - Designated administrators of the enterprise
- Schema Admins - Designated administrators of the schema
- DNS Admins - DNS Administrators Group
- DNS Update Proxy - DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP servers).
- Allowed RODC Password Replication Group - Members in this group can have their passwords replicated to all read-only domain controllers in the domain
- Group Policy Creator Owners - Members in this group can modify group policy for the domain
- Denied RODC Password Replication Group - Members in this group cannot have their passwords replicated to any read-only domain controllers in the domain
- Protected Users - Members of this group are afforded additional protections against authentication security threats. See http://go.microsoft.com/fwlink/?LinkId=298939 for more information.
- Cert Publishers - Members of this group are permitted to publish certificates to the directory
- Read-Only Domain Controllers - Members of this group are Read-Only Domain Controllers in the domain
- Enterprise Read-Only Domain Controllers - Members of this group are Read-Only Domain Controllers in the enterprise
- Key Admins - Members of this group can perform administrative actions on key objects within the domain.
- Enterprise Key Admins - Members of this group can perform administrative actions on key objects within the forest.
- Cloneable Domain Controllers - Members of this group that are domain controllers may be cloned.
- RAS and IAS Servers - Servers in this group can access remote access properties of users

Trusts

- In an AD environment, trust is a relationship between two domains or forests which allows users of one domain or forest to access resources in the other domain or forest.
- Trust can be automatic (parent-child, same forest etc.) or established (forest, external).
- Trusted Domain Objects (TDOs) represent the trust relationships in a domain.

One-way trust

One-way trust — Unidirectional. Users in the trusted domain can access resources in the trusting domain but the reverse is not true. 

Two-way trusts

Two-way trust — Bi-directional. Users of both domains can access resources in the other domain. 

Trust Transitivity

- Transitive : Can be extended to establish trust relationships with other domains.
  All the default intra-forest trust relationships (Tree-root, Parent-Child) between domains within a same forest are transitive two-way trusts.
- Nontransitive — Cannot be extended to other domains in the forest. Can be two-way or one-way.
  This is the default trust (called external trust) between two domains in different forests when forests do not have a trust relationship. 

PowerView Enumeration

We can gather additional information about our target using PowerView

1. Get a list of all domain trusts for the current domain

```
Get-NetDomainTrust
Get-NetDomainTrust -Domain <domain-
name>
```

2. Get details about the current forest

```
Get-NetForest
Get-NetForest -Forest <forest-
name>
```

3. Get all domains in the current forest

```
Get-NetForestDomain
Get-NetForestDomain -Forest <forest-
name>
```

4. Get all global catalogs for the current forest

```
Get-NetForestCatalog
Get-NetForestCatalog -Forest <forest-
name>
```

5. Map trusts of a forest

```
Get-NetForestTrust
Get-NetForestTrust -Forest <forest-
name>
```

Hunting for users who have Local Admin access using Powerview

1. Find all machines on the current domain where the current user has local admin access

```
Find-LocalAdminAccess -
Verbose
```

This is very noise This function queries the DC of the current or provided domain for a list of computers `(Get-NetComputer)` and then use multi-threaded `Invoke-CheckLocalAdminAccess` on each machine. This can also be done with the help of remote administration tools like WMI and PowerShell remoting. Pretty useful in cases ports (RPC and SMB) used by Find-LocalAdminAccess are blocked. See `Find-WMILocalAdminAccess.ps1` This leaves a 4624 (log-on event) and 4634 (log-off event) on each and every object in the domain. Same for Blood-Hound.

2. Find computers where a domain admin (or specified user/group) has sessions

```
Invoke-UserHunter
Invoke-UserHunter -GroupName
"RDPUsers"
```

This function queries the DC of the current or provided domain for members of the given group (Domain Admins by default) using `Get-NetGroupMember`, gets a list of computers `(Get-NetComputer)` and list sessions and logged on users `(Get-NetSession/Get-NetLoggedon)` from each machine.

3. To confirm admin access

```
Invoke-UserHunter -
CheckAccess
```

4. Find computers where a domain admin is logged-in

```
Invoke-UserHunter -
Stealth
```

This option queries the DC of the current or provided domain for members of the given group (Domain Admins by default) using `Get-NetGroupMember`, gets a *list only* of high traffic servers (DC, File Servers and Distributed File servers) for less traffic generation and list sessions and logged on users `(Get-NetSession/Get-NetLoggedon)` from each machine.

Policies

The Active Directory domain services are the core functions of an Active Directory network; they allow for management of the domain, security certificates, LDAPs, and much more. This is how the domain controller decides what it wants to do and what services it wants to provide for the domain.

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.

- 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.

References

If you find my articles interesting, you can buy me a coffee