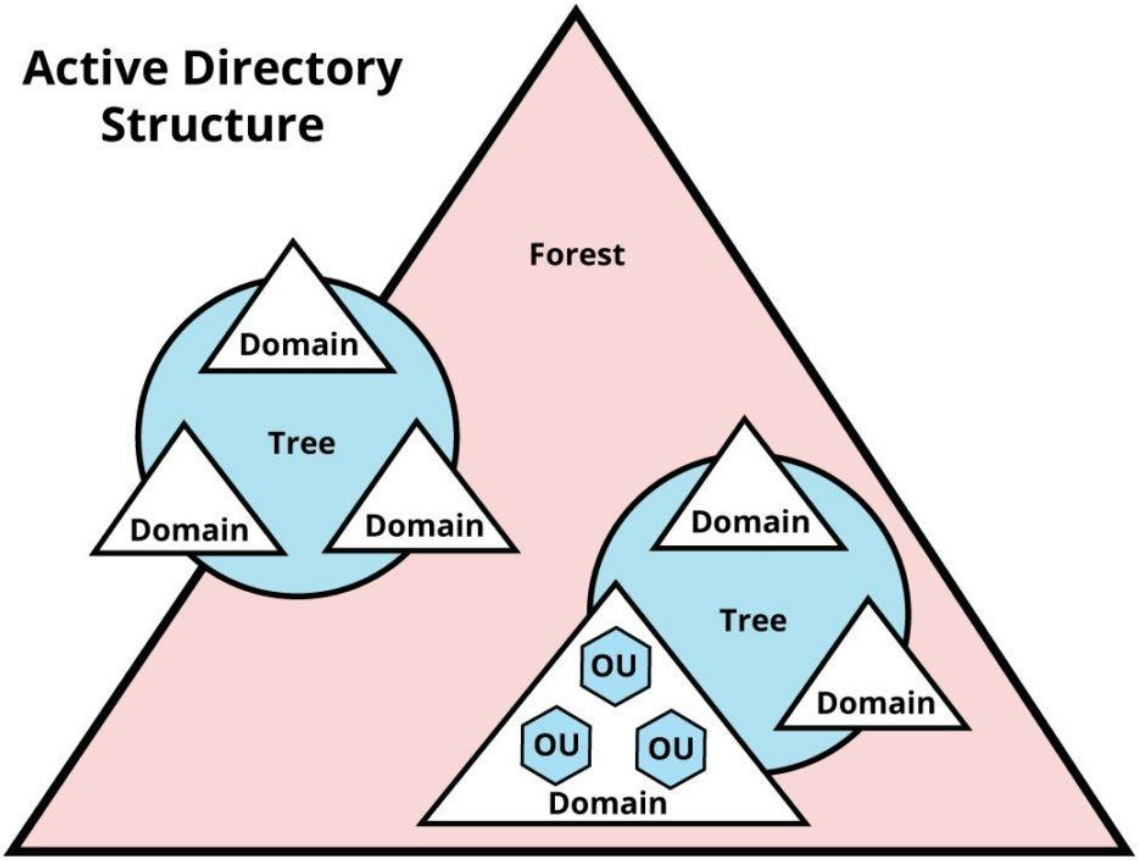
Active Directory and its Enumeration

What is AD?
The simplest representation of Active Directory can be done by a phone-book. Just like a phone-book has a hierarchical structure, an AD also has a hierarchical structure. An Active Directory Domain Service (AD DS) provides ways to store data and make it accessible on a network for other users and administrators.



Building Up On Basics:

- **Domain Controller:** A Domain Controller is nothing but a Windows Server, with the AD DS (Domain Services) role installed on it and has been specifically promoted to that role to host that directory storage. It also provides authentication and authorization services and administrator access to manage other user accounts and network resources.

- **AD Data Store:** The AD DS contains the database files and processes that store and manage directory information for users, services and other applications. It contains the NDTS.dit file which not only stores information about user objects, groups and group memberships but it also stores the password hashes for all the users present in that particular domain.

- **AS DS Schema:** As the name states, this contains the structural definition or the blueprint of any object which can be stored in the directory and enforces the rules regarding object creation and configuration.

- **Tree**: A tree in an AD can be defined as a hierarchy of domains. It is made up of several domains, sharing a common schema and configuration to form a contiguous namespace. It can have additional child domains and also create two way transitive trust with other domains.

- **Forest**: When multiple trees come together, they form a forest. Forests share a common schema, share common configuration partition, enable trusts between all domains in the forest and share enterprise admins and schema admin groups.

- **Trusts**: Security is offered in a forest on the basis of trust. A trust can be described as a mechanism for users to gain access to a resource in another domain. Before authenticating, Windows checks if the domain being requested has a trust relationship with the domain of the requesting account.

Challenge

Before enumerating the data from other domains we need to understand the trust between the current domain(where the current laptop is assigned) and other domains. We need to analyze which kind of trust and connectivity should be established to enumerate data from other domains.

Enumeration Steps

1. **Trust Enumeration**

Powershell commands to enumerate domain trusts for the current & other domain

- PowerView
    - Get-NetDomainTrust
    - Get-NetDomainTrust -Domain <for other domains>
- ADModule
    - Get-ADTrust
    - Get-ADTrust -Identity <for other domains>

2. **Domain Enumeration**
    - Powershell commands to enumerate current domain information
        - Get-NetDomain (PowerView)
        - Get-ADDomain (ADModule)
    - Powershell commands to get information about object of another domain
        - Get-NetDomain -Domain <any other domain> (PowerView)
        - Get-ADDomain -Identity <any other domain> (ADModule)
3. **Forest Enumeration**
    - Get information about current forest
        - Get-NetForest (PowerView)
        - ADModule (Get-ADForest)
    - Get details about another forest
        - Get-NetForest -Forest <forest.local> (PowerView)
        - Get-ADForest -Identity <forest.local> (ADModule)

4. **Domain Controllers**
    - Get domain controller of current domain
        - Get-NetDomainController (PowerView)
        - Get-ADDomainController (ADModule)
    - Get domain controller of another domain
        - Get-NetDomainController -Domain <domain.local> (PowerView)
        - Get-ADDomainController -DomainName <domain.local> -Discover (ADModule)

Tools to enumerate Active Directory

1. **Local AD enumeration tools**

A. **Bloodhound**

Bloodhound(https://github.com/BloodHoundAD/BloodHound/releases) is an extremely useful tool, based on PowerView, that will help map out active directory relationships throughout the network.
In a pentest, this is critical because after the initial access(either User or Admin), it gives you insight on what to attack next. In a big infrastructure, having information about the domain/forest/trust relationships and infrastructure is critical for targeted exploitation.

Usage:

1. Once you have an initial foothold, download Bloodhound and extract it somewhere. Click on the .exe in the root directory of Bloodhound to run it. Open bolt://localhost:7687 in attacker machine browser and login with username and password.

2. Browse to somewhere\BloodHound\Ingestors and copy Sharphound.exe. Assuming you have Meterpreter or any other shell for the means of uploading Sharphound.exe on a target, you can then upload the .exe.

3. Execute Sharphound.exe on the target.

4. This will create a few CSV files. Majorly user/group memberships, local user/group memberships and session are enumerated.

5. Download the CSV files from the target machine onto the attacker machine.

6. Upload these CSV files to bloodhound and explore.

7. This can give a lot of juicy information about various infrastructure, trusts and memberships of the target system.

B. **Powersploit powerup**

PowerUp is to Windows which linenum is to linux and probably better at it as per my observations and experiences. PowerUp aims to be a clearinghouse of common Windows privilege escalation vectors that rely on misconfigurations. Clearly, PowerUp is something

useful in privilege escalation but it achieves this by checking for misconfigurations and missing security controls/patches.

Once you have a local remote execution, load up Powershell and execute below:

powershell.exe -nop -exec bypass

Then import the powerup module

Import-Module PowerUp.ps1

Now, you have access to all PowerUp cmdlets. To execute all the checks run:

Invoke-AllChecks | Out-File -Encoding ASCII checks.txt

2. **Remote AD enumeration tools**
    a. **Responder**
    Responder is a powerful tool to every Windows or Active Directory environment Pentester should have. If a Domain/Windows system cannot resolve a name via DNS it will fall back to name resolution via LLMNR (introduced in Windows Vista) and NetBIOS. With Responder running we can spoof the attacker's machine as the intended machine for all the LLMNR and NetBIOS requests.

    To execute responder, run:
    Responder -i <your IP> -wrf
    b. **Enum4linux**
    Enum4linux is a tool for enumerating information from Windows and Samba systems. Key features:
        - RID cycling (When RestrictAnonymous is set to 1 on Windows 2000).
        - User listing (When RestrictAnonymous is set to 0 on Windows 2000)
        - Listing of group membership information.

- Share enumeration
- Detecting if host is in a workgroup or a domain
- Identifying the remote operating system

Use below commands to execute enum4linux and analyze the result:

enum4linux -A target-ip # used for Null Sessions

enum4linux -u administrator -p password -A target-ip #used with known credentials

c. Smbmap

Smbmap is a very useful tool which is a subset of crackmapexec, which is going to be discussed shortly. With the right credentials, things which can be done with SMBmap like SMB share enumeration, recursive directory listing of all the smb shares, command execution, upload/download/delete, reverse shell.Most of the options for smbmap are compiled into below table:

Usage: python3 smbmap.py -H target_ip -u username -p password -d domain

d. CrackMapExec

CrackMapExec (a.k.a CME) is a post-exploitation tool that helps automate assessing the security of large Active Directory networks. Built with stealth in mind, CME abuses built-in Active Directory features/protocols to achieve it's functionality and allowing it to evade most endpoint protection/IDS/IPS solutions.

There are a lot of things that can be done in various pentest phases with CME and are mentioned below:

Cme <target(s)> #network enumeration

Cme smb <target(s)> -u username -p password –local-auth -x whoami #command execution

References

https://www.techtarget.com/searchwindowsserver/definition/Active-Directory#:~:text=Active%20Directory%20(AD)%20is%20Microsoft's,device%20such%20as%20a%20printer.

https://github.com/CiscoCXSecurity/enum4linux

https://www.kali.org/tools/smbmap/#:~:text=SMBMap%20allows%20users%20to%20enumerate,and%20even%20execute%20remote%20commands.

https://www.ivoidwarranties.tech/posts/pentesting-tuts/cme/crackmapexec/

https://infosecwriteups.com/automating-ad-enumeration-with-frameworks-f8c7449563be