Active Directory

February 2023

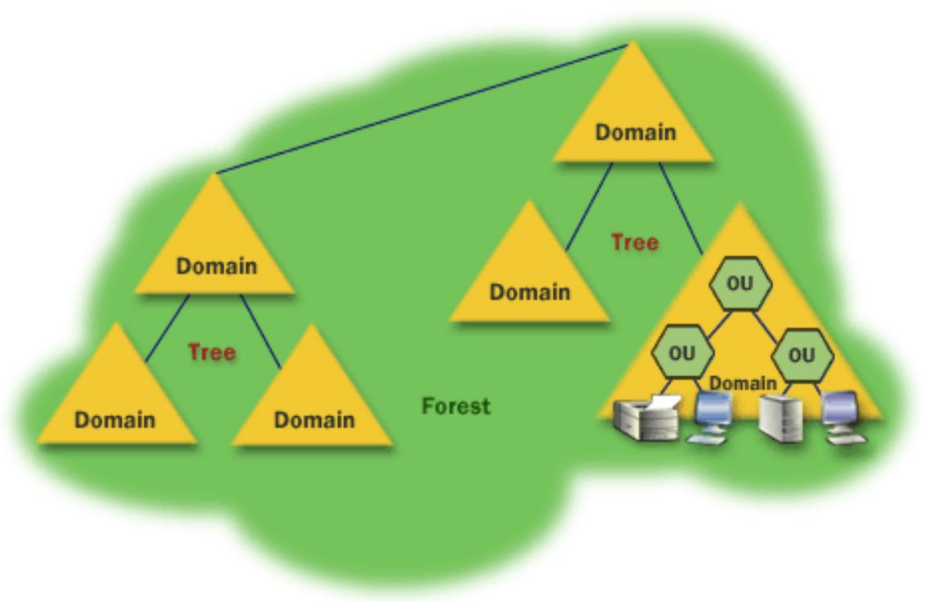
Overview

Central management of users and computers for Windows domains.

Domains can be hierarchically related in trees and forests.

Organizational Units - like a folder containing users, computers, and groups that policies can be applied to

Groups - a way to assign permissions to multiple users or computers



source: Logical Structure(Areas of Active Directory) (dispersednet.com)

Security

Security Groups

- Applied to Groups not Organizational Units
- Grant/assign permissions to resources - what can be accessed and what level of access (read only vs full control)

Group Policy Objects (GPOs)

- Applied to Organizational Units not Groups
- A collection of rules/policies that are settings restrictions or requirements (e.x. password policy)

Breaching Methods

NTLM Authentication Services

How it works:

1. Password is hashed locally
2. DC sends a random number logon challenge
3. Logon challenge is encrypted with password hash and sent back to DC
4. DC encrypts the logon challenge it sent with the password hash it has on record
5. The two encrypted values are compared by the DC

   Both client and DC use the same hashing and encryption methods

Issues:

- Hashes are not salted and algorithm is well known
- Bruteforce login
- Password spraying
- Rainbow tables
- Replay attacks

*NTLM has been replaced by Kerberos but is still supported

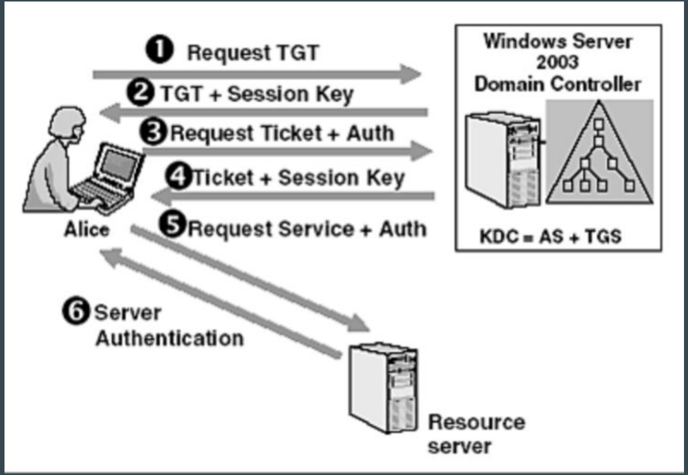
Kerberos

How it works:

1. Client sends ticket granting ticket (TGT) request to Kerberos KDC
2. Kerberos sends session key and TGT back to client
3. Client uses TGT to request an application session ticket from Kerberos KDC
4. Kerberos reuters a ticket and session key
5. Client connects to application server with the application session ticket

Kerbrute:

- bruteuser - bruteforce a single user
- passwordspray - test a single password against lots of usernames
- userenum - enumerate domain usernames with Kerberos



Source: Authentication Protocol Overview: OAuth2, SAML, LDAP, RADIUS, Kerberos (getkisi.com)

Lightweight Directory Access Protocol (LDAP) Bind Credentials

LDAP is used by directory clients to retrieve data from directory servers

- Simple bind - credentials passed in cleartext
    - Obviously bad
- Unsigned SASL bind - signing not required
    - Allow for MITM attack
- Signed SASL bind - signing required
    - Secure

Pass-back attack - gain access to a device with LDAP parameters and steal them by sending them to your rogue LDAP server

Bind to a domain controller with valid a AD credential pair and use search queries to enumerate

Configuration Files

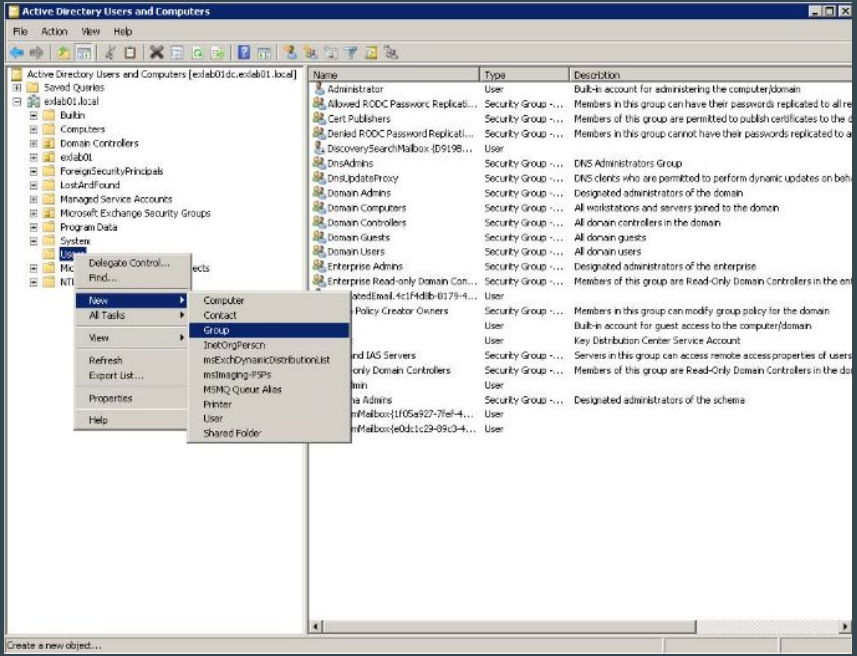
Steal credentials from a host on the target network from

- Web application config files
- Service config files
- Registry keys
- Centrally deployed applications

Then using those credentials access the Domain Controller.

Enumeration & Escalation

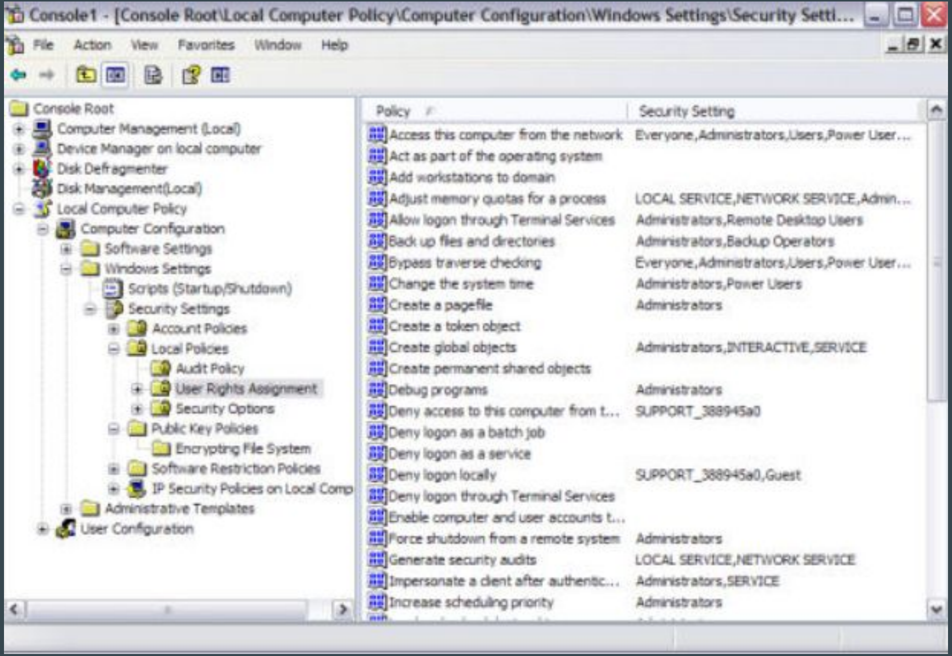
Microsoft Management Console



Name	Type	Description
Administrator	User	Built-in account for administering the computer/domain
Allowed RODC Password Replicati...	Security Group -...	Members in this group can have their passwords replicated to all re
Cert Publishers	Security Group -...	Members of this group are permitted to publish certificates to the d
Denied RODC Password Replicati...	Security Group -...	Members in this group cannot have their passwords replicated to a
DiscoverySearchMailbox {D9198...	User	
DnsAdmins	Security Group -...	DNS Administrators Group
DnsUpdateProxy	Security Group -...	DNS clients who are permitted to perform dynamic updates on beh
Domain Admins	Security Group -...	Designated administrators of the domain
Domain Computers	Security Group -...	All workstations and servers joined to the domain
Domain Controllers	Security Group -...	All domain controllers in the domain
Domain Guests	Security Group -...	All domain guests
Domain Users	Security Group -...	All domain users
Enterprise Admins	Security Group -...	Designated administrators of the enterprise
Enterprise Read-only Domain Con...	Security Group -...	Members of this group are Read-Only Domain Controllers in the ent
atedEmail.4c1f4d8b-8179-4...	User	
Policy Creator Owners	Security Group -...	Members in this group can modify group policy for the domain
	User	Built-in account for guest access to the computer/domain
	User	Key Distribution Center Service Account
nd IAS Servers	Security Group -...	Servers in this group can access remote access properties of users
only Domain Controllers	Security Group -...	Members of this group are Read-Only Domain Controllers in the do
lmin	User	
a Admins	Security Group -...	Designated administrators of the schema
mMailbox{1f05a927-7fef-4...	User	
mMailbox{e0dc1c29-89c3-4...	User	

Create a new object...

Users and Computers



Policy	Security Setting
Access this computer from the network	Everyone,Administrators,Users,Power User...
Act as part of the operating system	
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVICE,Admin...
Allow logon through Terminal Services	Administrators,Remote Desktop Users
Back up files and directories	Administrators,Backup Operators
Bypass traverse checking	Everyone,Administrators,Users,Power User...
Change the system time	Administrators,Power Users
Create a pagefile	Administrators
Create a token object	
Create global objects	Administrators,INTERACTIVE,SERVICE
Create permanent shared objects	
Debug programs	Administrators
Deny access to this computer from t...	SUPPORT_388945a0
Deny logon as a batch job	
Deny logon as a service	
Deny logon locally	SUPPORT_388945a0,Guest
Deny logon through Terminal Services	
Enable computer and user accounts t...	
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE,NETWORK SERVICE
Impersonate a client after authentic...	Administrators,SERVICE
Increase scheduling priority	Administrators

Configuration and Policies

Command Prompt

- net accounts
- net computer
- net config
- net user
- net group
- net localgroup

PowerShell

- Get-ADGroupMember
- Get-ADUser
- Get-ADComputer
- Get-ADObject
- Get-ADDomain
- Get-ADAuthenticationPolicy
- Get-ADOrganizationalUnit

Bloodhound

Find and visualize complex attack paths

Create a CSV of all AD permissions to import into Bloodhound:

```
Invoke-Bloodhound -CollectionMethod ACLs
```

Attack path options:

- Password Reset (ForceChangePassword)
- Group Membership (AddMember)
- Change an object’s permissions (WriteDacl)
- Combinations

Mimikatz

Extract passwords from memory

- *sekurlsa::logonpasswords -* extract user id and password for currently and recently logged in users

Extract Kerberos tickets

Extract certificates and their private keys

Runas

Run tools, programs, or applications with permissions other than the ones the current user is logged in with.

cmdkey /list - list stored credentials

Use runas with stored credentials to create a reverse shell.

Activity

THM room - Post-Exploitation Basics

[TryHackMe | Post-Exploitation Basics]()

Additional Resources

Understand and test the security of identity providers - Active Directory Video Tutorial | LinkedIn Learning, formerly Lynda.com

TryHackMe | Active Directory Basics

TryHackMe | Breaching Active Directory

TryHackMe | Enumerating Active Directory

TryHackMe | Attacktive Directory

ActiveDirectory Module | Microsoft Learn

GitHub - S1ckB0y1337/Active-Directory-Exploitation-Cheat-Sheet: A cheat sheet that contains common enumeration and attack methods for Windows Active Directory.