Windows / AD

- [Énumération] AD
- [Énumération] Enum4linux
- [Énumération] Windows
- [Reconnaissance] NBTscan
- [Énumération] RpcClient
- [Énumération] Samba
- [Énumération] LDAP

[Énumération] AD

Introduction

L'énumération d'un envrionnement Active Directory est primordial pour trouver ses faibles.

Énumération distante

Scan réseau

Si vous avez un accès sur un sous-réseau et que vous cherchez les contrôleurs de domaine disponibles ou les serveurs Windows en général, vous allez pouvoir les identifier rapidement grâce à **CrackMapExec** :

```
cme smb <NET_IP/MASK>
```

> Vous allez récupérer les versions de Windows ainsi que les noms des domaines associés à ces serveurs.

Scan d'un contrôleur de domaine

Vous pouvez récupérer quelques informations utiles avec **CrackMapExec** :

```
cme smb <DC_IP|DC_FQDN>
```

Énumération des utilisateurs du domaine

Il est parfois possible de récupérer la liste des utilisateurs du domaine notamment avec **enum4linux** :

```
enum4linux -U <DC_IP>
```

Ou avec **kerbrute** :

```
kerbrute userenum --dc <DC_IP> -d <DOMAIN_FQDN> <USERLIST>
```

Énumération de la base de registre

```
reg.py <DOMAIN>/<USER>:<PASSWORD>@<IP> query -keyName "<REGISTRY_FOLDER>"
```

Voici un exemple pour lister les logiciels présent sur le poste :

```
reg.py <DOMAIN>/<USER>:<PASSWORD>@<IP> query -keyName "HKLM\\SOFTWARE"
```

Énumération des services

```
services.py <DOMAIN>/<USER>:<PASSWORD>@<IP> list
```

Récupérer les SID des utilisateurs

```
lookupsid.py <DOMAIN>/<USER>:<PASSWORD>@<IP>
```

Récupérer les comptes de service

```
GetUserSPNs.py <DOMAIN>/<USER>:<PASSWORD>
```

> On peut récupérer les TGS avec l'option **-request** à placer à la fin de la commande.

Récupérer des jetons TGT

Permet de récupérer les jetons TGT des comptes utilisateurs qui ont la pré-authentification Kerberos désactivée :

```
GetNPUsers.py <DOMAIN>/<USER>:<PASSWORD> -request
```

Récupérer des hashs de mots de passe

Permet d'interroger le serveur pour récupérer les hashs de mots de passe qui pourraient se trouver dans le **ntds.dit**, ou autre :

```
secretsdump.py <DOMAIN>/<USER>:<PASSWORD>@<IP>
```

Énumération locale

Ce petit mémo regroupe toutes les commandes pour énumérer des informations sur un domaine si vous avez un premier accès sur un poste du domaine.

Trouver le nom du domaine

```
systeminfo | findstr Domain
```

Lister les utilisateurs du domaine

```
Get-ADUser  -Filter *
```

Vous pouvez aussi ajouter un filtre pour lister tous les éléments d'un OU spécifique (ici **Users**) :

```
Get-ADUser -Filter * -SearchBase "CN=Users,DC=<DC_DN>,DC=<DC_TLD>"
```

On peut aussi récupérer les utilisateurs à privilèges élevés :

```
Get-ADUser -Filter * | select SamAccountName
```

Lister les logiciels anti-virus

```
wmic /namespace:\\root\securitycenter2 path antivirusproduct
```

Afficher l'état de Windows Defender

```
Get-Service WinDefend
```

Et pour afficher l'état des différents services de Windows Defender :

```
Get-MpComputerStatus
```

Afficher l'état du pare-feu

```
Get-NetFirewallProfile | Format-Table Name, Enabled
```

Afficher les règles du pare-feu

```
Get-NetFirewallRule | select DisplayName, Enabled, Description
```

Désactiver le pare-feu

```
Set-NetFirewallProfile -Profile Domain, Public, Private -Enabled False
```

> Nécessite les droits administrateurs !

Tester l'état d'un port

Dans un premier shell, se mettre en écoute :

```
Test-NetConnection -ComputerName <IP> -Port <PORT>
```

Puis initiez une connexion :

```
(New-Object System.Net.Sockets.TcpClient("<IP>", "<PORT>")).Connected
```

Afficher les sources de logs

```
Get-EventLog -List
```

Afficher le processus Sysmon

S'il existe il sera affiché :

```
Get-Process | Where-Object { $_.ProcessName -eq "Sysmon" }
```

Lister les applications installées

```
wmic product get name,version
```

Afficher les dossiers et fichiers cachés

```
Get-ChildItem -Hidden -Path <DIR_PATH>
```

Afficher les services en cours d'exécution

```
net start
```

Afficher les informations d'un service

```
wmic service where "name like '<SERVICE>'" get Name,PathName
```

Afficher les informations sur un processus

```
Get-Process -Name <PROCESS>
```

Afficher les connexions en lien avec un processus

```
netstat -noa |findstr "LISTENING" |findstr "<PID>"
```

Afficher la politique de mot de passe du domaine

```
net accounts /domain
```

Afficher les informations d'un utilisateur du domaine

```
Get-ADUser -Identity <USER> -Server <DC_FQDN> -Properties *
```

Afficher les informations d'un groupe du domaine

```
Get-ADGroup -Identity <GROUP> -Server <FQDN_DC>
```

Afficher les membres d'un groupe du domaine

```
Get-ADGroupMember -Identity <GROUP> -Server <FQDN_DC>
```

Afficher des informations génériques sur le domaine

```
Get-ADDomain -Server <FQDN_DC>
```

Afficher les relations de confiance

```
nltest /domain_trusts
```

Bloodhound

Sharphound

Cet outil du framework va se charger de l'énumération du domaine.

Voici le lien du repos :

- https://github.com/BloodHoundAD/SharpHound

Il doit être lancé depuis un compte utilisateur du domaine.

Cependant, il est détecté par les antivirus et EDR, c'est pourquoi il est recommandé d'utiliser notre propre machine Windows et lancer Sharphound dessus avec les droits de l'utilisateur grâce à **runas**.

Cet outil prend soit la forme d'un exécutable, soit d'un script Powershell et peut être lancé de la manière suivante :

```
SharpHound.exe --CollectionMethods All --Domain <FQDN_DC> --ExcludeDCs
```

Normalement, une archive zip a été générée.

Nous pourrons la récupérer sur notre machine pour l'utiliser avec Bloodhound.

Bloodhound-python

Si vous n'avez pas de shell sur une machine du domaine, vous pouvez utiliser bloodhound-python ou rusthound pour remplacer le rôle de sharphound :

```
bloodhound-python -c DcOnly -u <USER> -p <PASSWORD> -d <DOMAIN_FQDN> -dc <DC_FQDN> -ns <DC_IP> --zip
```

Bloodhound GUI

Lancez la console neo4j (nécessaire au fonctionnement de l'outil) :

```
neo4j console
```

> Selon les distributions, vous devrez mettre ou non le mot **start** à la fin de la commande.

Puis dans un autre terminal, lancez bloodhound :

```
bloodhound --no-sandbox
```

> Les identifiants par défaut sont **neo4j:neo4j**.

[Énumération] Enum4linux

Introduction

L'outil **enum4linux** permet de collecter des informations sur un hôte windows ou un contrôleur de domaine.

Manuel

Syntaxe globale

```
enum4linux [OPTIONS] <TARGET_IP>
```

Énumérer les utilisateurs

```
enum4linux -U <TARGET_IP>
```

Énumérer les groupes

```
enum4linux -G <TARGET_IP>
```

Lister les informations sur les groupes

```
enum4linux -M <TARGET_IP>
```

Énumérer les partages samba

```
enum4linux -S <TARGET_IP>
```

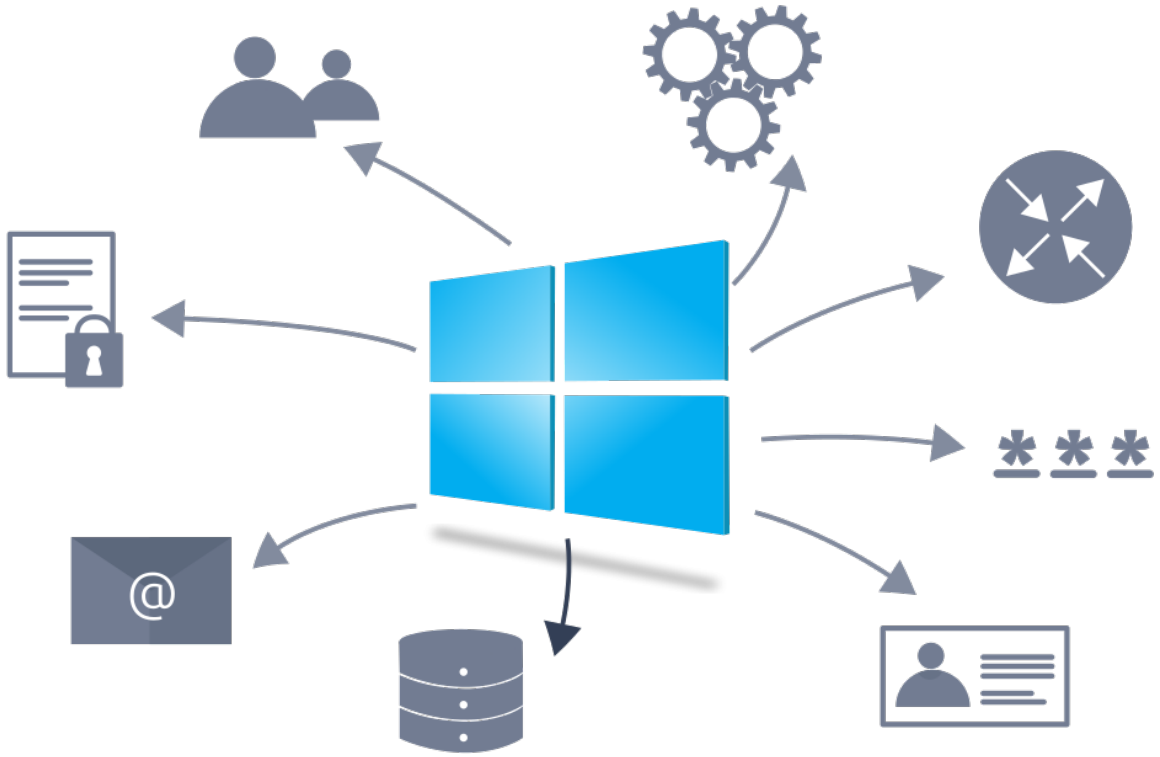
Lister les mots de passe

```
enum4linux -P <TARGET_IP>
```

[Énumération] Windows

Introduction

Cette page décrit les procédés pour énumérer un système Windows lorsque vous y avez accès.



Manuel

Afficher les informations systèmes

```
systeminfo
```

Afficher les mises à jour installées

```
wmic qfe get Caption,Description
```

Afficher les services installés et démarrés

```
net start
```

Afficher les applications installées

```
wmic product get name,version,vendor
```

Afficher les privilèges de l'utilisateur actif

```
whoami /priv
```

Afficher les groupes de l'utilisateur actif

```
whoami /groups
```

Afficher les utilisateurs du système

```
net user
```

Afficher le SID des utilisateurs du système

```
wmic useraccount get name,sid
```

> À noter que le dernier octet du SID représente le **RID** de l'utilisateur.

Afficher les groupes du système

```
net localgroup
```

Afficher les membre d'un groupe

```
net localgroup <GROUP>
```

Afficher les configurations locales

```
net accounts
```

Lister les tâches planifiées

```
schtasks
```

Et pour afficher le détail d'une tâche planifiée :

```
schtasks /query /tn <TASK_NAME> /fo list /v
```

[Reconnaissance] NBTscan

Introduction

L'outil **nbtscan** permet de scanner les hôtes windows présents sur un sous-réseau.

Ses utilisations sont variées et permettent de récupérer différentes informations utiles lors d'un pentest.

Codes NetBios

Codes	Descriptions
00	Workstation service
03	Messenger service
20	File Server service
1B	Domain Master Brower (contrôleur de domaine)
1C	Contrôleur de domaine
2B	Services d'annuaire

Manuel

Syntaxe globale

```
nbtscan <SUBNET_ID/CIDR_MASK>
```

Exemple :

```
nbtscan 192.168.1.0/24
```

Options

Options	Descriptions
-v	Mode verbeux.
-e	Affiche des informations d'extension (utilisateurs actifs etc).
-m	Affiche les informations MAC des machines.
-r <RANGE>	Scanner une plage d'IP spécifique.
-f <FILE>	Scanner les adresses IP du fichier spécifié.
-t <DELAY>	Définit un délai d'attente personnalisé.
-h	Affiche la page d'aide

[Énumération] RpcClient

Introduction

RpcClient est un outil en ligne de commande permettant d'interagir avec les services **RPC** (*Remote Procedure Call*) dans les systèmes basés sur Windows ou Samba.

Manuel

Syntaxe globale

```
rpcclient [OPTIONS] -U <USERNAME>%<PASSWORD> //<IP|HOSTNAME>
```

Exemples d'utilisation

- Connexion à un serveur :

```
rpcclient -U user%password //192.168.1.1
```

- Lister les partages accessibles :

```
rpcclient -U user%password -c "enumprinters" //192.168.1.1
```

- Exécuter des commandes spécifiques :

```
rpcclient -U user%password -c "querydispinfo" //192.168.1.1
```

Connexion anonyme :

```
rpcclient -N //192.168.1.1
```

Options courantes

Options	Descriptions
-U	Spécifie le nom d'utilisateur et le mot de passe pour l'authentification.
-c	Exécute une commande spécifique après la connexion.
-N	Spécifie un nom d'utilisateur mais n'effectue pas d'authentification (utilisé pour les connexions anonymes).
-W	Spécifie le domaine Windows à utiliser.
-I	Spécifie l'adresse IP du serveur DNS.

[Énumération] Samba

Introduction

L'énumération des partages samba est cruciale pour les tests d'intrusions d'envrionnement Windows.

Script nmap

Énumération globale de l'OS utilisé

```
nmap --script smb-os-discovery <IP>
```

Énumération des utilisateurs samba

```
nmap --script smb-enum-users <IP>
```

> Cette technique ne marche que si la session "**null**" est activée sur le poste cible (rare).

Smbmap

Utilisation avec un compte

Si vous possédez un compte pour faire l'énumération :

```
smbmap -u <USER> -p <PASSWORD> -H <IP>
```

> Vous aurez un aperçu des droits de lecture et d'écriture que vous avez sur les partages.

Utilisation de la session null

```
smbmap -u '' -p '' -H <IP>
```

Options

Options	Descriptions
-R	Active la récursivité pour afficher le contenu des dossiers (si vous possédez les droits de lecture).

ShareEnum

Installation

Vous pouvez récupérer la dernière release sur le github et lancer l'installation du paquet sur votre système :

```
dpkg -i <PACKAGE>.deb
```

Utilisation standard

```
shareenum <IP>
```

> Si vous ne spécifiez pas d'utilisateur, la session **null** sera utilisée.

Options

Options	Descriptions
-o <FILE>	Spécifie un fichier de sortie de la commande.
-u <USER>	Spécifie un nom d'utilisateur.
-p <PASSWORD>	Spécifie un mot de passe.

SMBClient

On peut énumérer tous les fichiers d'un partage avec **smbclient** :

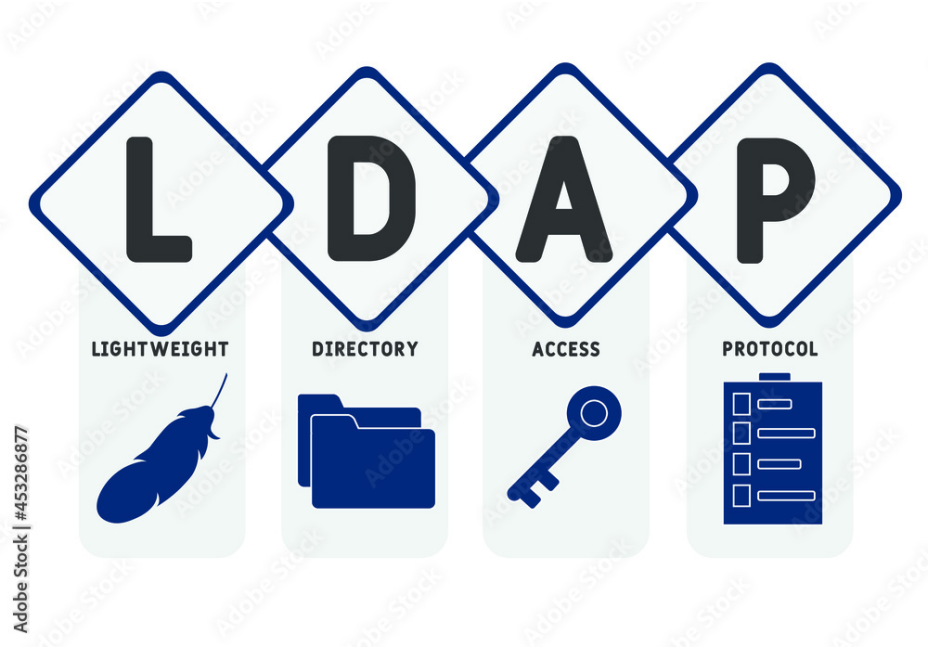
```
smbclient -N //<IP>/<SHARE>
```

[Énumération] LDAP

Introduction

LDAP pour Lightweight Directory Access Protocol, est un protocole d'annuire utilisé par des outils libres tels que **OpenLDAP**, mais aussi des solutions propriétaires comme **Active Directory**.

Quand il est utilisé au sein d'une organisation, il est une source d'information gigantesque pour un pirate qui arriverait à énumérer l'annuaire.



Nmap

Un script est présent au sein de l'outil pour scanner les annuaires LDAP.

Pour cela, exécutez la commande suivante :

```
nmap -p 389 --script=ldap-search <IP>
```