

Exploitation des tokens Windows

Introduction au pentest Active Directory et aux Internals Windows

whoami /all



Éditer le profil

Aurélien Chalot
@Defte_

Hacker, sysadmin and security researcher @OrangeCyberdef 🖥️
Calisthenic enthusiast 💪
100 Hide&Sec 100
[Traduire la biographie](#)



📍 The grid 🔗 blog.whiteflag.io 📅 A rejoint Twitter en novembre 2017









399 abonnements **224** abonnés

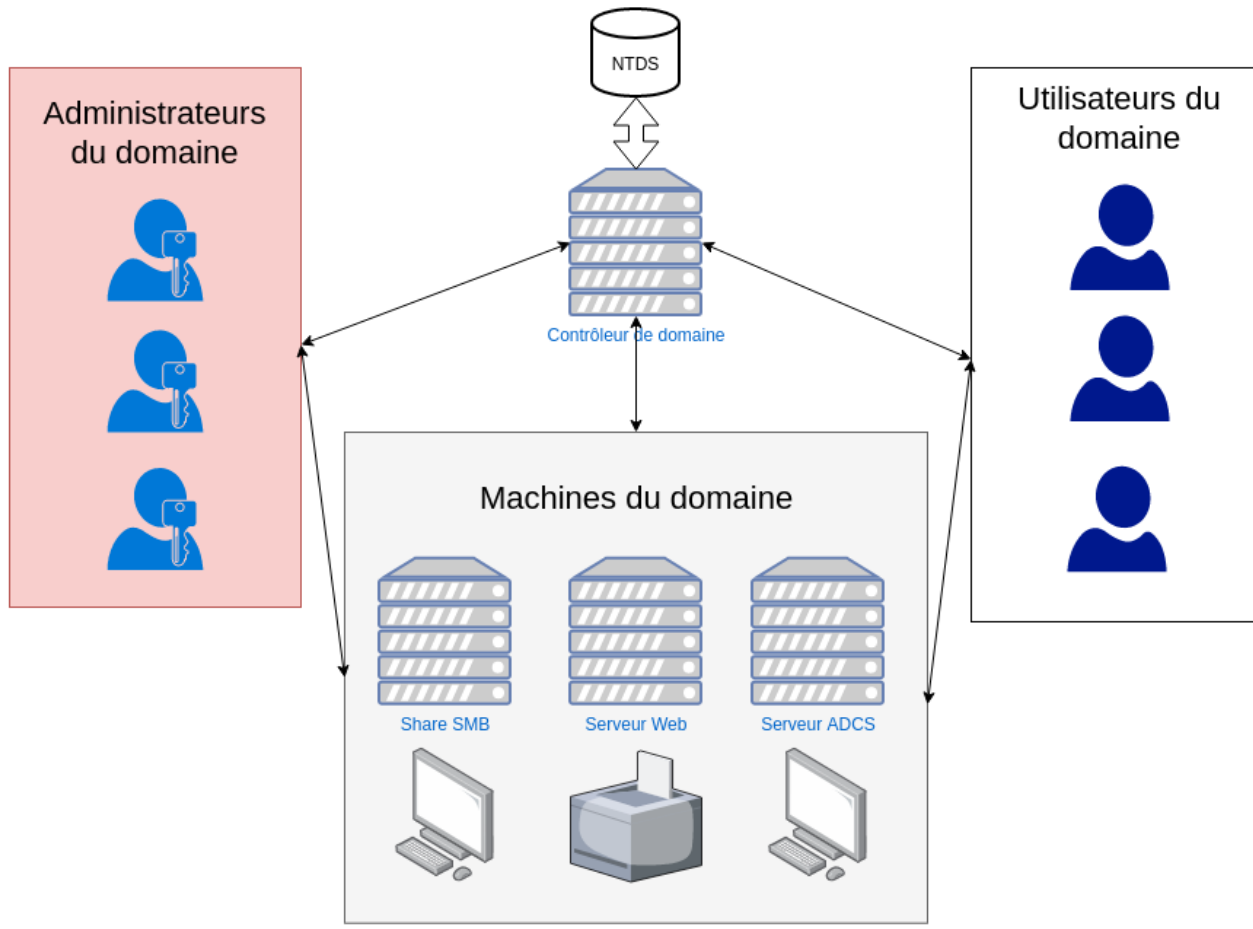
Vous avez dit Active Directory ?

- Un Active Directory c'est un annuaire qui contient les informations relatives aux ressources d'une entreprise:

- Ordinateurs / serveurs
- Imprimantes
- Dossiers partagés (share SMB)
- Utilisateurs

Nom	
 SERVEUR	
 WIN-7US6VSMRGR6	

Nom	Type	Description
 Administrateur	Utilisateur	Compte d'utilisateur d'a...
 Administrateurs clés	Groupe de sécurité - Global	Les membres de ce grou...
 Administrateurs clés Entreprise	Groupe de sécurité - Universel	Les membres de ce grou...
 Administrateurs de l'entreprise	Groupe de sécurité - Universel	Administrateurs désigné...
 Administrateurs du schéma	Groupe de sécurité - Universel	Administrateurs désigné...
 Admins du domaine	Groupe de sécurité - Global	Administrateurs désigné...
 Contrôleurs de domaine	Groupe de sécurité - Global	Tous les contrôleurs de ...
 Contrôleurs de domaine clonab...	Groupe de sécurité - Global	Les membres de ce grou...
 Contrôleurs de domaine d'entr...	Groupe de sécurité - Universel	Les membres de ce grou...



Le contrôleur de domaine (DC) est la pièce centrale qui permet de manager l'ensemble du réseau Active Directory

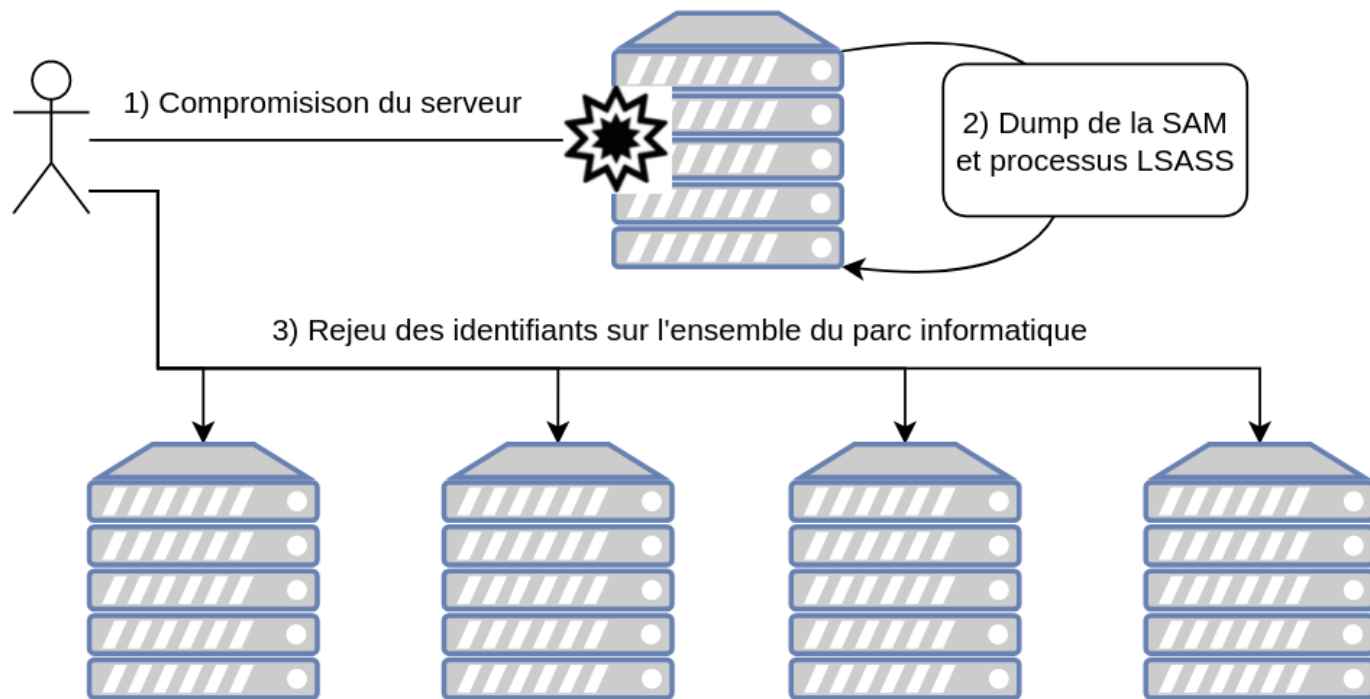
Test d'intrusion interne

Compromettre l'Active Directory -> être administrateur du domaine

Pour cela il existe plusieurs techniques:

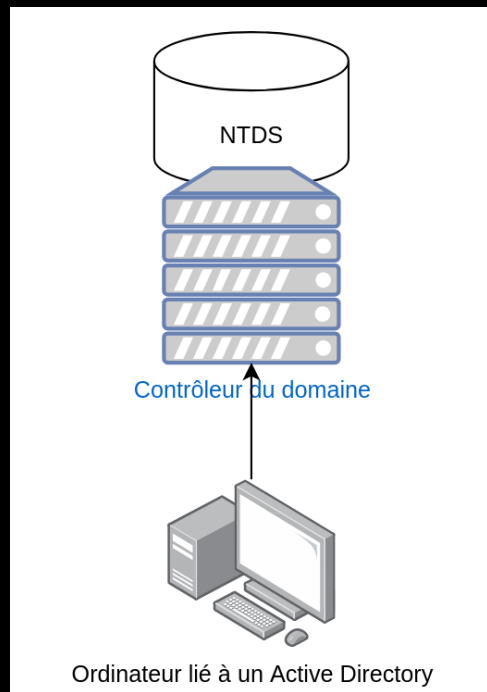
- Comptes utilisateurs avec des mots de passe faibles
- Exploitation de défauts de configuration Active Directory
- Exploitation de serveurs / services vulnérables et rebondir sur d'autres machines

Scénario classique



SAM, LSASS, NTDS, dafuk ?

NTDS (NT Directory Services): base de données des comptes sur un réseau Active Directory



Fichier présent sur les contrôleurs du domaine

System32

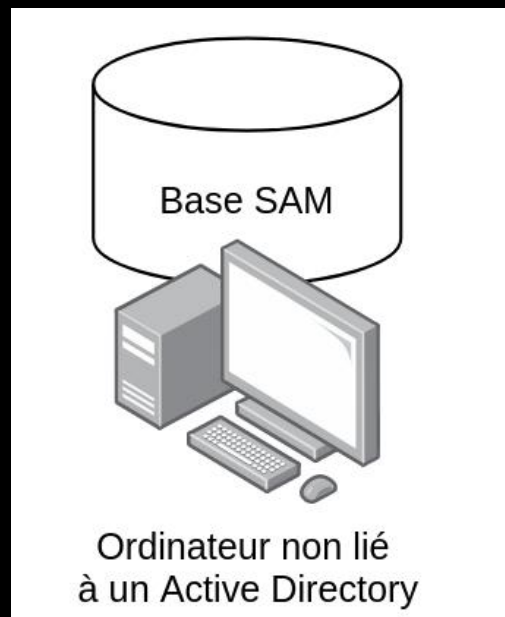
Fichier Accueil Partage Affichage

Ce PC > Disque local (C:) > Windows > System32

Nom	Modifié le	Type	Taille
nsisvc.dll	10/07/2010 13:10	extension de l'app...	50 Ko
nslookup	16/07/2016 15:18	Application	85 Ko
ntasn1.dll	16/07/2016 15:18	Extension de l'app...	232 Ko
ntdll.dll	02/02/2018 19:28	Extension de l'app...	1 844 Ko
ntds.dit	13/01/2022 11:44	Fichier DIT	12 288 Ko
ntdsutil.dll	13/01/2022 11:44	Extension de l'app...	94 Ko
ntdsai.dll	13/01/2022 11:44	Extension de l'app...	3 866 Ko

SAM, LSASS, NTDS, dafuk ?

SAM (Security Account Manager): base de données des comptes **locaux** sur un système Windows



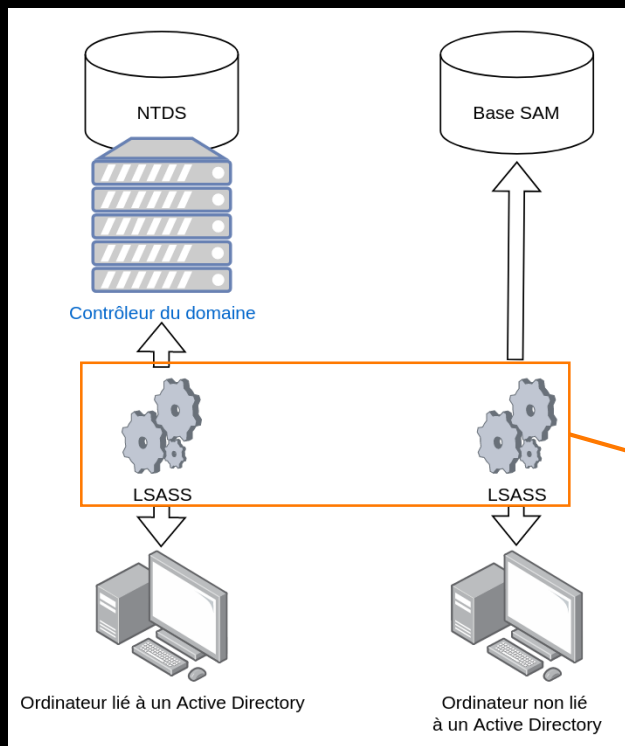
Clé de registre présente sur toutes les machines Windows

Clé de registre présente sur toutes les machines Windows			
Nom	Type	Données	
ab (par défaut)	REG_SZ	(valeur non définie)	
C	REG_BINARY	08 00 01 00 00 00 00 00 d0 00 00 00 03 00 01 00 01 0...	
ServerDomainUpdates	REG_BINARY	fe ff 01	

Ordinateur	
HKEY_CLASSES_ROOT	
HKEY_CURRENT_USER	
HKEY_LOCAL_MACHINE	
BCD00000000	
HARDWARE	
SAM	
Domains	
Account	
Builtin	
LastSkuUpgrade	
RXACT	
SECURITY	
SOFTWARE	
SYSTEM	
HKEY_USERS	
HKEY_CURRENT_CONFIG	

SAM, NTDS, LSASS, dafuk ?

LSASS (Local Security Authority SubSystem): processus en charge de l'authentification sur un système Windows



Gestionnaire des tâches

Fichier Options Affichage

Processus Performance Utilisateurs Détails Services

Nom	7% Processeur	24% Mémoire
> Hôte de service : service local (8)	0%	5,9 Mo
> Hôte de service : service local (aucun réseau) (4)	0%	5,6 Mo
> Hôte de service : service local (réseau restreint)	0%	1,1 Mo
> Hôte de service : service local (réseau restreint) (4)	0%	9,4 Mo
> Hôte de service : service réseau (5)	0%	5,4 Mo
> Hôte de service : service réseau (réseau restreint)	0%	1,0 Mo
> Hôte de service : système local (14)	0%	16,6 Mo
> Hôte de service : système local (réseau restreint) (4)	0%	6,6 Mo
Interruptions système	0,8%	0 Mo
Local Security Authority Process (6)	0,5%	27,6 Mo
Processus d'exécution client-serveur	0%	1,1 Mo
Processus d'exécution client-serveur	0%	1,1 Mo

SAM, NTDS, LSASS, dafuk ?

Le processus LSASS stocke les secrets d'authentifications tels que:

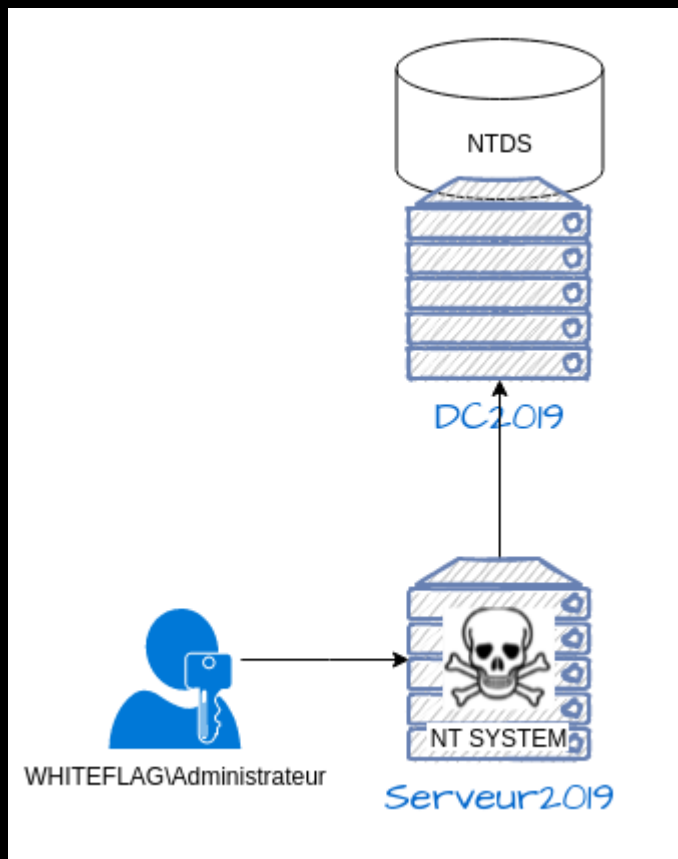
- Des mots de passe stockés en clair ou sous la forme d'un hash NTLM
- Des tickets Kerberos
- Pleins d'autres choses

Dumper le contenu du processus LSASS nous permet de récupérer ces informations.

On pourra ensuite les rejouer pour compromettre d'autres machines.



Configuration du laboratoire



- Un administrateur du domaine
- Un contrôleur du domaine (dc2019)
- Un serveur Windows 2019 (déjà compromis)

Demo time (Windows Defender désactivé)



Kernel

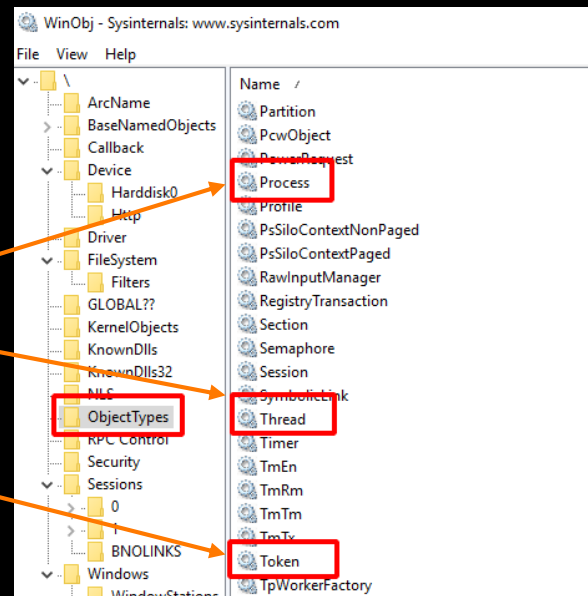
Le Kernel c'est le cœur du système d'exploitation Sa fonction est de:

- Gérer les ressources du système (mémoire RAM, processus etc.)
- Gérer les accès sécurisés à ces ressources
- Permettre la communication entre les logiciels et le hardware

Pour assurer cette fonction il dispose de plusieurs **objets**.

Par exemple:

- Un objet de type **Process** utilisé pour manager un processus
- Un objet de type **Thread** utilisé pour manager un Thread
- Ou encore un objet de type **Token**



Token

Token: objet Windows qui décrit le contexte de sécurité d'un processus ou d'un thread.

Au sein de ce token on trouve:

- L'identité de l'utilisateur qui détient ce token
- Les groupes dans lequel se trouve l'utilisateur
- L'ensemble des privilèges attribués à l'utilisateur sur le système

Propriétés de : powershell.exe (4356)

Memory	Environment	Handles	Job	.NET assemblies
.NET performance	GPU	Disk and Network	Comment	
General	Statistics	Performance	Threads	Token

User: WHITEFLAG\Administrateur

User SID: S-1-5-21-1254471023-1136857918-2392298254-500

Session: 1 Elevated: N/A Virtualized: Not allowed

App container SID: N/A

Name	Flags
AUTORITE NT\Cette organisation	Mandatory (de
AUTORITE NT\INTERACTIF	Mandatory (de
AUTORITE NT\Utilisateurs authentifiés	Mandatory (de
BUILTIN\Administrateurs	Mandatory (de
BUILTIN\Utilisateurs	Mandatory (de

Name	Status	Description
SeBackupPrivilege	Disabled	Sauvega...
SeChangeNotifyPrivilege	Default Enabled	Contour...
SeCreateGlobalPrivilege	Default Enabled	Créer de...
SeCreatePagefilePrivilege	Disabled	Créer un...
SeCreateSymbolicLinkPrivilege	Disabled	Créer de...
SeDebugPrivilege	Enabled	Débogu...
SeDelegateSessionUserImpersonatePrivilege	Disabled	Obtenir ...

To view capabilities, claims and other attributes, click Advanced.

Integrity Advanced

Privilèges Windows

Il existe 37 privilèges qui permettent à celui qui les détient d'effectuer différentes actions sur le système.

Par exemple:

- **SeLoadDriverPrivilege**: permet de charger un driver
- **SeShutdownPrivilege**: permet d'arrêter la machine
- **SeDebugPrivilege**: permet de déboguer n'importe quel processus du système

```
C:\Users\Administrateur>whoami /priv
```

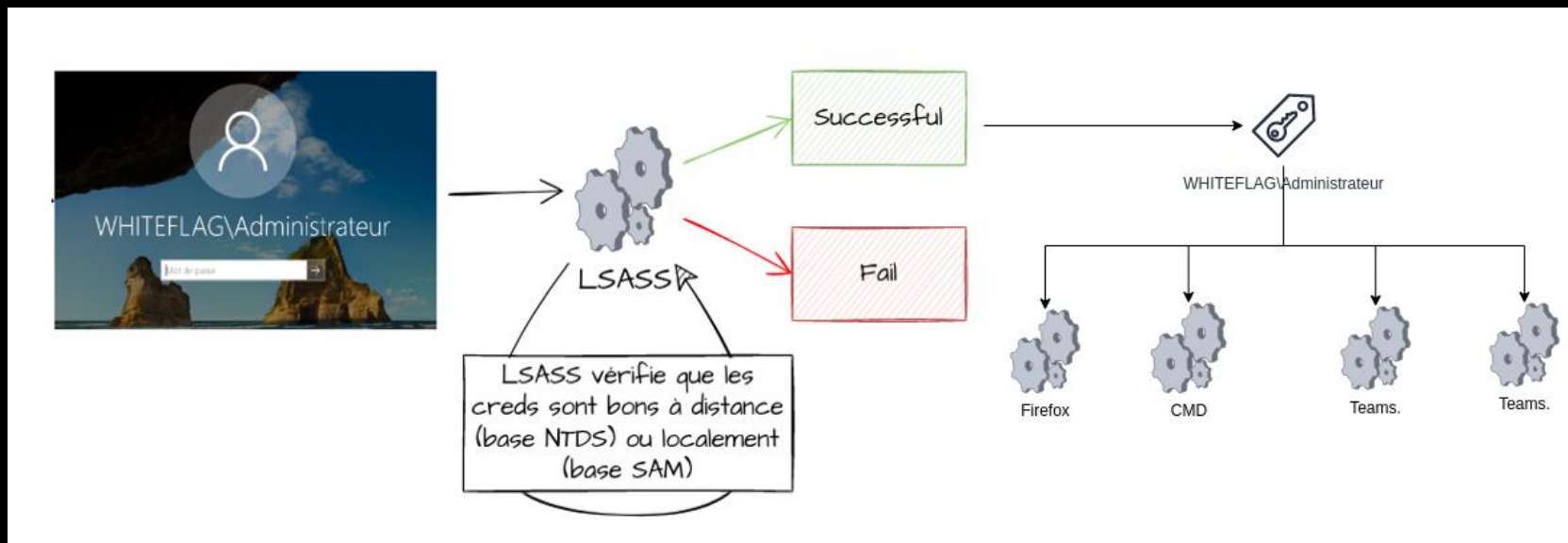
```
Informations de privilèges
```

```
-----
```

Nom de privilège	Description
SeIncreaseQuotaPrivilege	Ajuster les quotas de mémoire pour un processus
SeMachineAccountPrivilege	Ajouter des stations de travail au domaine
SeSecurityPrivilege	Gérer le journal d'audit et de sécurité
SeTakeOwnershipPrivilege	Prendre possession de fichiers ou d'autres objets
SeLoadDriverPrivilege	Charger et décharger les pilotes de périphériques
SeSystemProfilePrivilege	Performance système du profil
SeSystemtimePrivilege	Modifier l'heure système
SeProfileSingleProcessPrivilege	Processus unique du profil
SeIncreaseBasePriorityPrivilege	Augmenter la priorité de planification
SeCreatePagefilePrivilege	Créer un fichier d'échange
SeBackupPrivilege	Sauvegarder les fichiers et les répertoires
SeRestorePrivilege	Restaurer les fichiers et les répertoires
SeShutdownPrivilege	Arrêter le système
SeDebugPrivilege	Déboguer les programmes
SeSystemEnvironmentPrivilege	Modifier les valeurs de l'environnement du microproc

Deux types de token: primary token et impersonate token

Quand obtient-on un primary token?



Quand obtient-on un primary token?

Propriétés de : powershell.exe (4356)

Memory	Environment	Handles	Job	.NET assemblies	
.NET performance	GPU	Disk and Network		Comment	
General	Statistics	Performance	Threads	Token	Modules

User: WHITEFLAG\Administrateur

User SID: S-1-5-21-1254471023-1136857918-2392298254-500

Session: 1 Elevated: N/A Virtualized: Not allowed

App container SID: N/A

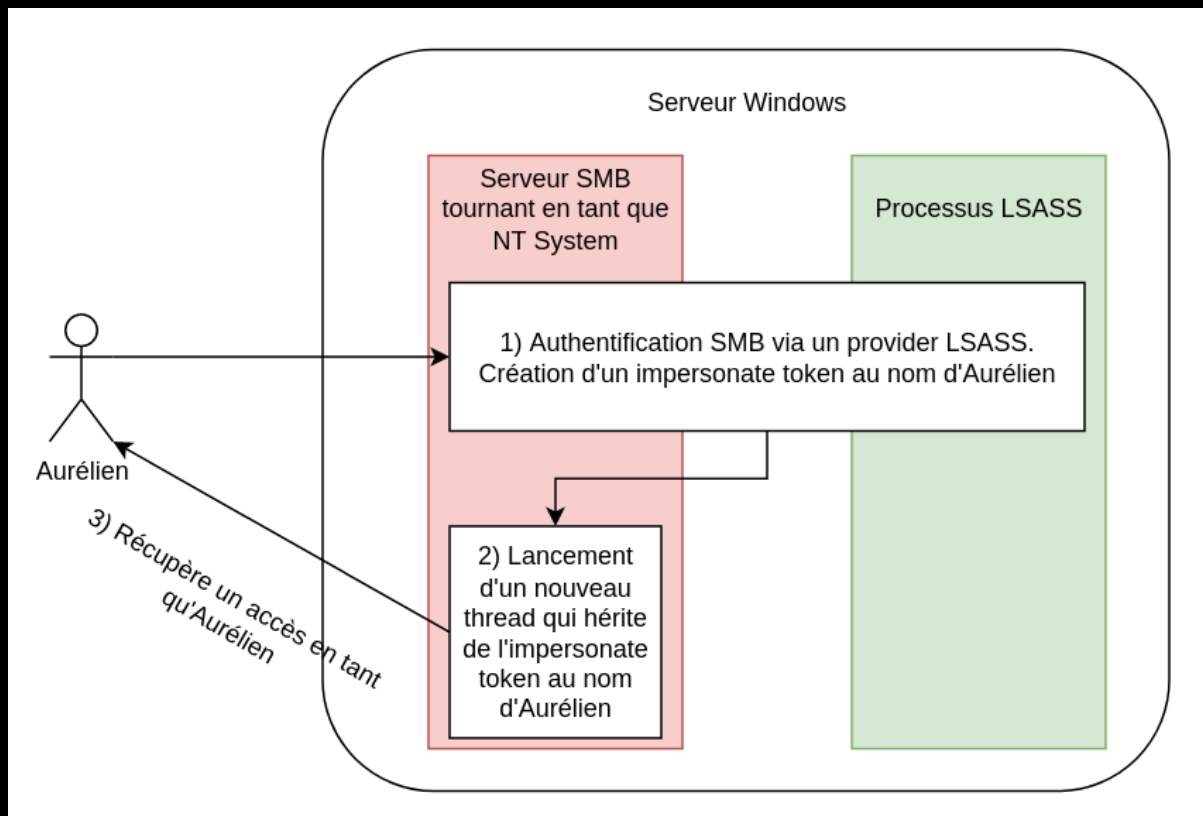
Name	Flags
AUTORITE NT\Cette organisation	Mandatory (de
AUTORITE NT\INTERACTIF	Mandatory (de
AUTORITE NT\Utilisateurs authentifiés	Mandatory (de
BUILTIN\Administrateurs	Mandatory (de
BUILTIN\Utilisateurs	Mandatory (de

Name	Status	Description
SeBackupPrivilege	Disabled	Sauvega...
SeChangeNotifyPrivilege	Default Enabled	Contour...
SeCreateGlobalPrivilege	Default Enabled	Créer de...
SeCreatePagefilePrivilege	Disabled	Créer un...
SeCreateSymbolicLinkPrivilege	Disabled	Créer de...
SeDebugPrivilege	Enabled	Débogu...
SeDelegateSessionUserImpersonatePrivilege	Disabled	Obtenir ...

To view capabilities, claims and other attributes, click Advanced.

Integrity Advanced

Quand obtient-on un impersonate token ?



Primary token vs Impersonate token

	Primary token	Impersonate token
Est attribué à:	Un processus	Un thread
Est obtenu suite à:	Une authentification interactive	Principalement via une authentification réseau
Des identifiants de connexion sont stockés dans LSASS?	Oui	Non

Where is this going ?

Les tokens sont des objets Windows qui représentent **un utilisateur mais aussi et surtout les privilèges associés à cet utilisateur sur le système**. Ce sont aussi des objets qu'il est **possible de manipuler** à condition de disposer des privilèges suffisants.



Un peu de code et quelques structures Windows

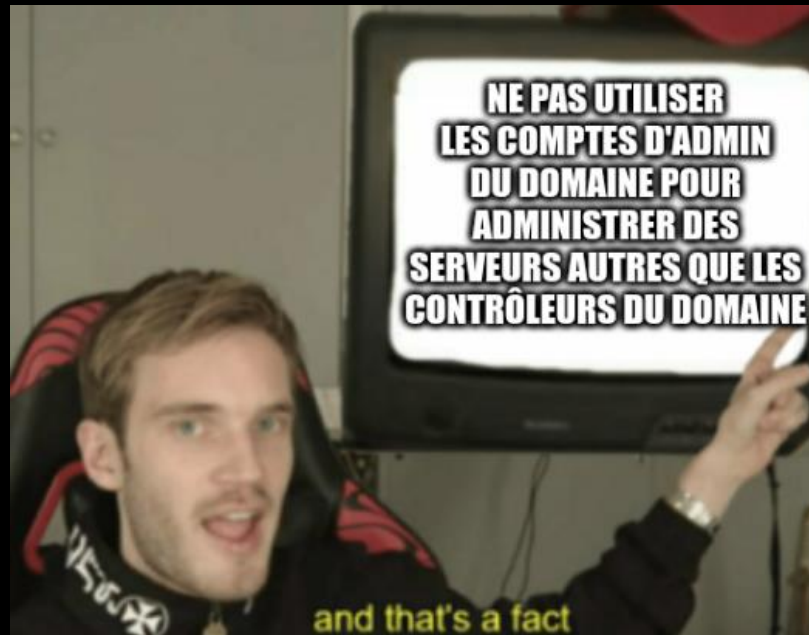
Demo time (avec Windows Defender activé)

Test d'intrusion réel

```
[*] Listing available tokens
[ID: 0][TokenPrimary][ ] Owner:
[ID: 1][TokenImpersonation][S
[ID: 2][TokenImpersonation][S
[ID: 3][TokenPrimary][Securit
[ID: 4][TokenImpersonation][S
[ID: 5][TokenImpersonation][S
[ID: 6][TokenImpersonation][S
[ID: 7][TokenImpersonation][S
[ID: 8][TokenImpersonation][S
[ID: 9][TokenImpersonation][S
[ID: 10][TokenImpersonation][
[ID: 11][TokenImpersonation][
[ID: 12][TokenImpersonation][
[ID: 13][TokenImpersonation][
[ID: 14][TokenPrimary][Securi
[ID: 15][TokenPrimary][Securi
[ID: 16][TokenImpersonation][
[ID: 17][TokenPrimary][Securi
[ID: 18][TokenImpersonation][
[ID: 19][TokenPrimary][Securi
[ID: 20][TokenPrimary][Securi
[ID: 21][TokenPrimary][Securi
[ID: 22][TokenImpersonation][
[ID: 23][TokenImpersonation][
[ID: 24][TokenImpersonation][
[ID: 25][TokenImpersonation][
[ID: 26][TokenImpersonation][
[ID: 27][TokenPrimary][Securi
[ID: 28][TokenPrimary][Securi
[ID: 29][TokenPrimary][Securi
[ID: 30][TokenPrimary][Securi
[ ] Impersonating [ ] Administrateur and launching command [cmd.exe /c net group 'Domain Admins' [ ] /Add /doma
La demande sera traitée sur contrôleur de domaine du domaine [ ]
C:\Users\Administrateur>
```

Comment s'en protéger ?

- Analyser statiquement les exécutables pour voir quelles fonctions ils utilisent (AV)
- Analyser dynamiquement le comportement de l'exécutable (EDR /XDR)
- Mais surtout:



En résumé

L'authentification Windows est réalisée par le processus LSASS:

- Localement via la base SAM
- A distance en contactant le contrôleur du domaine (base NTDS.dit)

Une fois l'authentification validée, un token est créé au nom de l'utilisateur. Ce token contient:

- Le nom de l'utilisateur
- Les groupes dans lequel il est présent
- Les privilèges associés à l'utilisateur

Les tokens sont des objets Windows que l'on peut manipuler si on dispose des bons privilèges.

En dupliquant le token d'un utilisateur, on peut usurper son identité et donc ses privilèges. Dans le cadre d'un test d'intrusion interne, dupliquer le token d'un administrateur du domaine revient à compromettre son compte et donc l'Active Directory. Comme c'est un mécanisme interne de Windows, il est très compliqué pour les solutions de sécurité de détecter l'attaque.

Une bonne connaissance des Internals Windows permet de contourner les solutions de sécurité type AV / EDR en exploitant des comportements légitimes de Windows.

- Rejoignez nous sur nos différents workshops:
- Attaques RFID samedi à 21h
 - Exploitation de l'autorité de certification ADCS samedi à 23h
 - Attaques USB sur des claviers dimanche à 1H

Des questions ?

Mail: aurelien.chalot@orange.com

Twitter: <https://twitter.com/Defte>

Mon blog: <https://blog.whiteflag.io>

Projet github du tool: <https://github.com/Dfte/Impersonate>

