Investigation numérique sur l'annuaire Active Directory avec les métadonnées de réplication

https://github.com/ANSSI-FR/ADTimeline

Intervenant

C:\Windows\system32\cmd.exe

```
C:\>WHOAMI /USER /GROUPS

Informations sur l'utilisateur
------------------------------

Nom d'utilisateur               SID
=================               ============================================
leonard.savina@ssi.gouv.fr      S-1-5-21-2594175445-3465634044-2509762353-1006


Informations de groupe
----------------------

Nom du groupe                                 Type             SID
============================================= ================ ============
ANSSI                                         Groupe bien connu S-1-5-11
Sous_Direction_Operations                     Groupe           S-1-5-21-2594175445-3465634044-2509762353-1002
Division_Reponse                              Groupe           S-1-5-21-2594175445-3465634044-2509762353-1003
Bureau_Investigation_Numerique                Groupe           S-1-5-21-2594175445-3465634044-2509762353-1004
CERT-FR                                       Groupe           S-1-5-21-2594175445-3465634044-2509762353-1005

C:\>
```

Plan

- Active Directory et les métadonnées de réplication.
- Outil ADTimeline.

AD et la réplication – Présentation AD

Active Directory est l'annuaire d'entreprise Microsoft, installé sur des DCs (Contrôleurs de domaine). Rôles :

- Annuaire LDAP ;
- Service DNS ;
- Service NTP ;
- Service KDC (Kerberos) et Netlogon ;
- Gestion centralisée des clients : Stratégie de groupe (GPOs).

AD et la réplication – Réplication AD

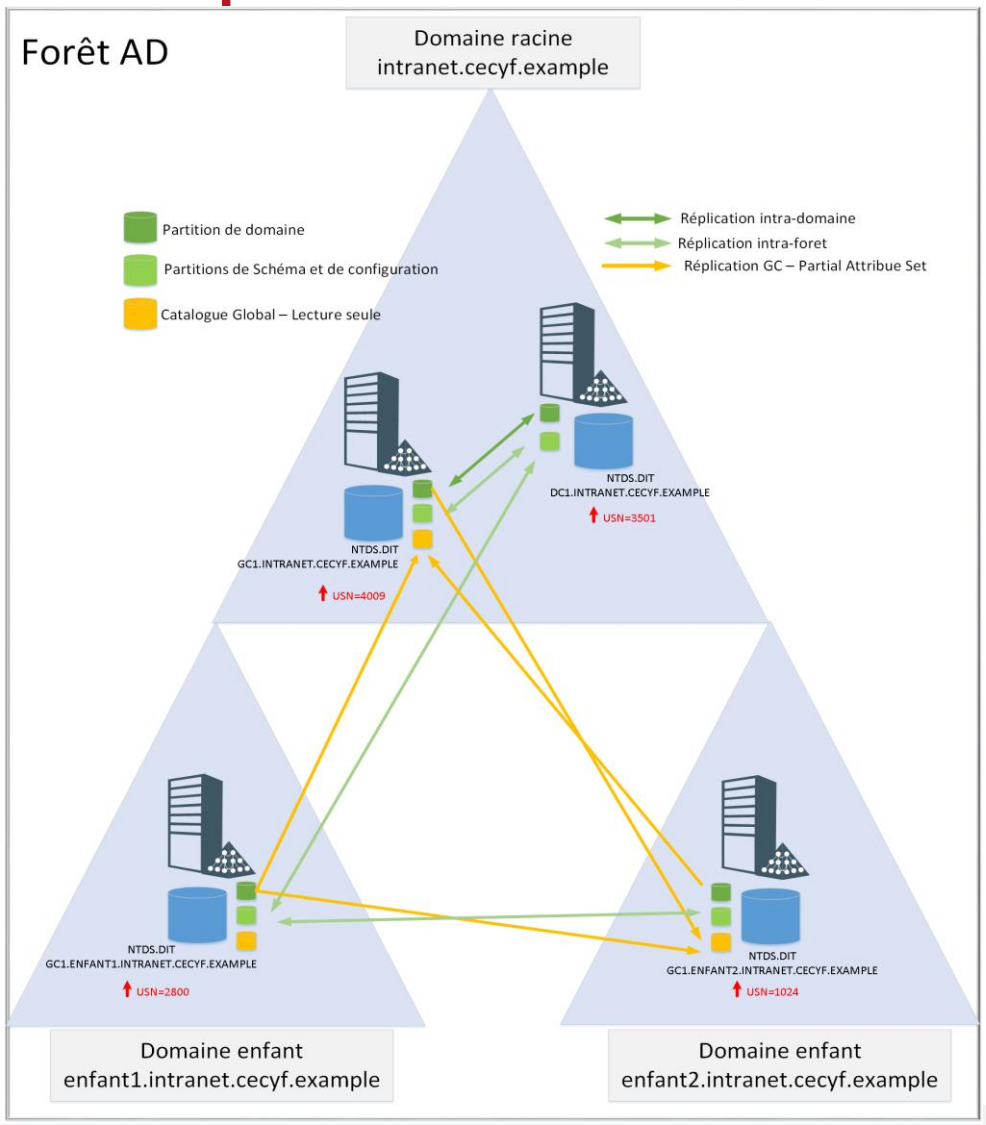
Un ou plusieurs domaines dans une forêt.

AD est un service qui doit être hautement disponible.

Plusieurs DCs dans un domaine, qui répliquent les partitions présentes dans la base NTDS.

Réplication intra Domaine, intra Forêt et Catalogue Global (*Partial Attribute Set*).

Le GUID d'un DC et l'USN (*Update Sequence Number*) identifient de manière unique un changement dans la base NTDS.



Les métadonnées de réplication AD – msDS-ReplAttributeMetaData

- Attribut construit (*constructed attribute*) format XML.

```
PS Z:\> Get-ADGroup HR_RW -Properties msDS-ReplAttributeMetaData | Select-Object -ExpandProperty  msDS-ReplAttributeMetaData
<DS_REPL_ATTR_META_DATA>
        <pszAttributeName>objectCategory</pszAttributeName>
        <dwVersion>1</dwVersion>
        <ftimeLastOriginatingChange>2018-07-17T15:27:16Z</ftimeLastOriginatingChange>
        <uuidLastOriginatingDsaInvocationID>d391fb4c-852c-418f-9fe2-015cc980cf38</uuidLastOriginatingDsaInvocationID>
        <usnOriginatingChange>532806</usnOriginatingChange>
        <usnLocalChange>532806</usnLocalChange>
        <pszLastOriginatingDsaDN>CN=NTDS Settings,CN=RWDC,CN=Servers,CN=SIEGE,CN=Sites,CN=Configuration,DC=labo,DC=local</pszLastOriginatingDsaDN>
</DS_REPL_ATTR_META_DATA>

<DS_REPL_ATTR_META_DATA>
        <pszAttributeName>groupType</pszAttributeName>
        <dwVersion>1</dwVersion>
        <ftimeLastOriginatingChange>2018-07-17T15:27:16Z</ftimeLastOriginatingChange>
        <uuidLastOriginatingDsaInvocationID>d391fb4c-852c-418f-9fe2-015cc980cf38</uuidLastOriginatingDsaInvocationID>
        <usnOriginatingChange>532806</usnOriginatingChange>
        <usnLocalChange>532806</usnLocalChange>
        <pszLastOriginatingDsaDN>CN=NTDS Settings,CN=RWDC,CN=Servers,CN=SIEGE,CN=Sites,CN=Configuration,DC=labo,DC=local</pszLastOriginatingDsaDN>
</DS_REPL_ATTR_META_DATA>
```

- Pour chaque objet, nous avons la dernière modification de chacun des attributs.
- Ne contient que les informations des attributs répliqués de l'objet.

Les métadonnées de réplication AD – msDS-ReplAttributeMetaData

Pour chaque attribut répliqué msDS-ReplAttributeMetaData contient :

- **pszAttributeName** : nom de l'attribut ;
- **ftimeLastOriginatingChange** : date de la dernière modification de l'attribut ;
- **dwVersion** : Incrémenté à chaque modification de l'attribut ;
- **usnOriginatingChange** : USN du DC sur lequel la modification a lieu, lors de la dernière modification de l'attribut ;
- **pszLastOriginatingDsaDN** : objet NTDS (DC), sur lequel la dernière modification de l'attribut a lieu ;
- **uuidLastOriginatingDsaInvocationID** : ID correspondant à pszLastOriginatingDsaDN ;
- **usnLocalChange** : USN du DC interrogé par votre commande, une fois la dernière modification de l'attribut répliquée sur ce dernier.

Les métadonnées de réplication AD – msDS-ReplValueMetaData

Métadonnées de réplication pour les attributs liés (*linked attribute*):

Couple d'attributs dont le système calcule la valeur d'un attribut (*back link, ex MemberOf*) à partir de son pair (*forward link, ex Member*).

Dans le cas d'un objet groupe et l'attribut member, nous avons les mêmes informations que pour msDS-ReplAttributeMetaData mais avec en plus :

- **pszObjectDn** : le DistinguishedName du membre du groupe ;
- **ftimeCreated** : date où le membre a été mis dans le groupe ;
- **ftimeDeleted** : date où le membre a été retiré du groupe.

Les métadonnées de réplication AD – Outils

> Repadmin.exe /showobjmeta:

```
PS C:\> repadmin /showobjmeta rwdc.labo.local "CN=HR_RW,DC=labo,DC=local"

12 entrées.msDS-ReplAttributeMetaData
USN loc                          DSA source       USN org. Heure/date org.      Attribut ver
=======                          ==========       ======== ===============      === ========
 532806                               SIEGE\RWDC     532806 2018-07-17 17:27:16    1 objectClass
 532806                               SIEGE\RWDC     532806 2018-07-17 17:27:16    1 cn
 532842                               SIEGE\RWDC     532842 2018-07-17 17:39:28    2 description
 532806                               SIEGE\RWDC     532806 2018-07-17 17:27:16    1 instanceType
 532806                               SIEGE\RWDC     532806 2018-07-17 17:27:16    1 whenCreated
 532806                               SIEGE\RWDC     532806 2018-07-17 17:27:16    1 nTSecurityDescriptor
 532806                               SIEGE\RWDC     532806 2018-07-17 17:27:16    1 name
 532806                               SIEGE\RWDC     532806 2018-07-17 17:27:16    1 objectSid
 532806                               SIEGE\RWDC     532806 2018-07-17 17:27:16    1 sAMAccountName
 532806                               SIEGE\RWDC     532806 2018-07-17 17:27:16    1 sAMAccountType
 532806                               SIEGE\RWDC     532806 2018-07-17 17:27:16    1 groupType
 532806                               SIEGE\RWDC     532806 2018-07-17 17:27:16    1 objectCategory
2 entrées.msDS-ReplValueMetaData
Type    Attribut      Heure dern mod.                    DSA source       USN loc USN org Ver
======= ============  ===============                    ===============  ======= ======= ===
        Nom unique
        ==============================
PRéSENT       member 2018-07-17 17:30:14                 SIEGE\RWDC  532836  532836   1
        CN=Rick,DC=labo,DC=local
ABSENT        member 2018-07-17 17:44:03                 SIEGE\RWDC  532855  532855   2
        CN=Morty,DC=labo,DC=local
```

> Avec Powershell 4.0+ : Get-ADReplicationAttributeMetadata

```
PS C:\> Get-ADReplicationAttributeMetadata "CN=HR_RW,DC=labo,DC=local" -Server rwdc.labo.local | select -last 1


AttributeName                           : member
AttributeValue                          : CN=Morty,DC=labo,DC=local
FirstOriginatingCreateTime              : 17/07/2018 17:30:14
IsLinkValue                             : True
LastOriginatingChangeDirectoryServerIdentity     : CN=NTDS Settings,CN=RWDC,CN=Servers,CN=SIEGE,CN=Sites,CN=Configuration,DC=labo,DC=local
LastOriginatingChangeDirectoryServerInvocationId : d391fb4c-852c-418f-9fe2-015cc980cf38
LastOriginatingChangeTime               : 17/07/2018 17:44:03
LastOriginatingChangeUsn                : 532855
LastOriginatingDeleteTime               : 17/07/2018 17:44:03
LocalChangeUsn                          : 532855
Object                                  : CN=HR_RW,DC=labo,DC=local
Server                                  : RWDC.labo.local
Version                                 : 2
```

Les métadonnées de réplication AD - Travaux existants

- Pierre Audonnet :

https://blogs.technet.microsoft.com/pie/2014/08/25/metadata-0-metadata-what-is-it-and-why-do-we-care

- Gregory Lucand :

https://social.technet.microsoft.com/wiki/contents/articles/25946-metadata-de-replication-et-analyse-forensic-active-directory-fr-fr.aspx

https://adds-security.blogpost.com

- Will Schroeder :

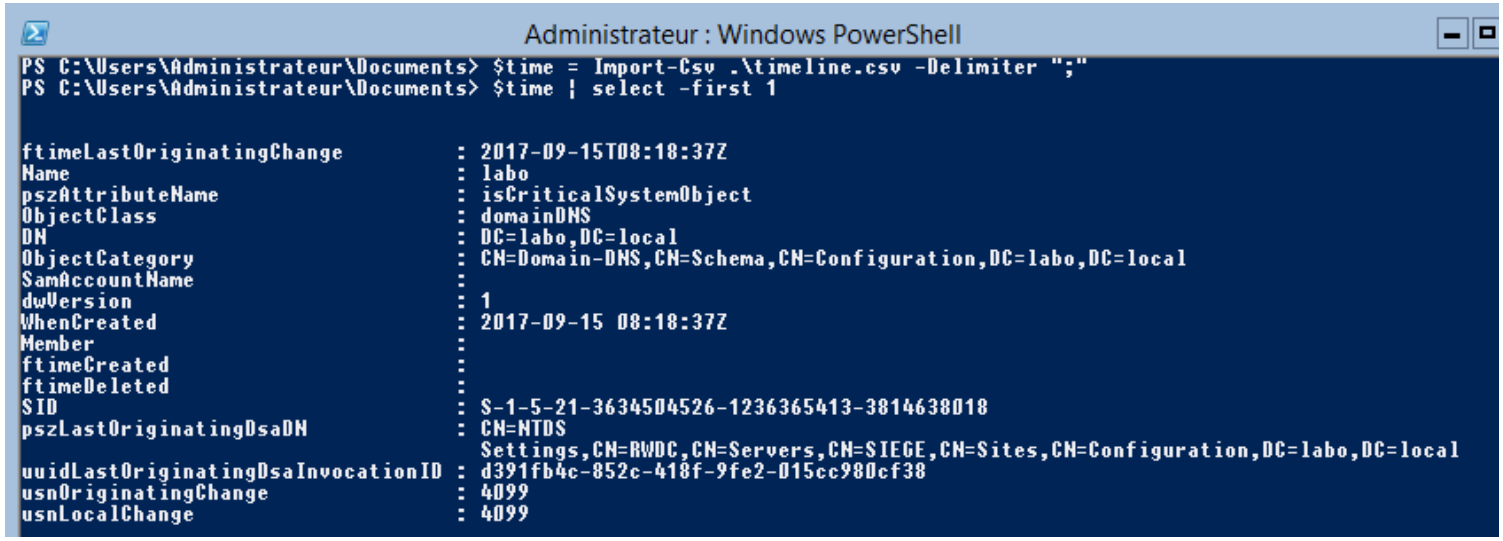
https://harmj0y.net/blog/defense/hunting-with-active-directory-replication-metadata

Présentation de l'outil ADTimeline - Concept

- Prendre de l'annuaire les objets considérés comme d'intérêt.
- Extraire pour ces objets leurs métadonnées de réplication AD : *msDS-ReplAttributeMetaData* pour tous ces objets. Pour les groupes, *msDS-ReplValueMetaData* est récoltée en plus.
- Générer une timeline en triant toutes ces métadonnées par *ftimeLastOriginatingChange*.
- Proposer un mode en ligne et un mode hors-ligne.

Présentation de l'outil ADTimeline – Fichiers générés

Timeline format CSV (métadonnées + qqes attributs): *Import-Csv –delimiter ';'*



Objets avec tous leurs attributs récupérés via LDAP (ADObjects.xml) et Global Catalog (GCADObjects.xml) : *Import-CliXML*.

log-adexport.log : fichier journal.

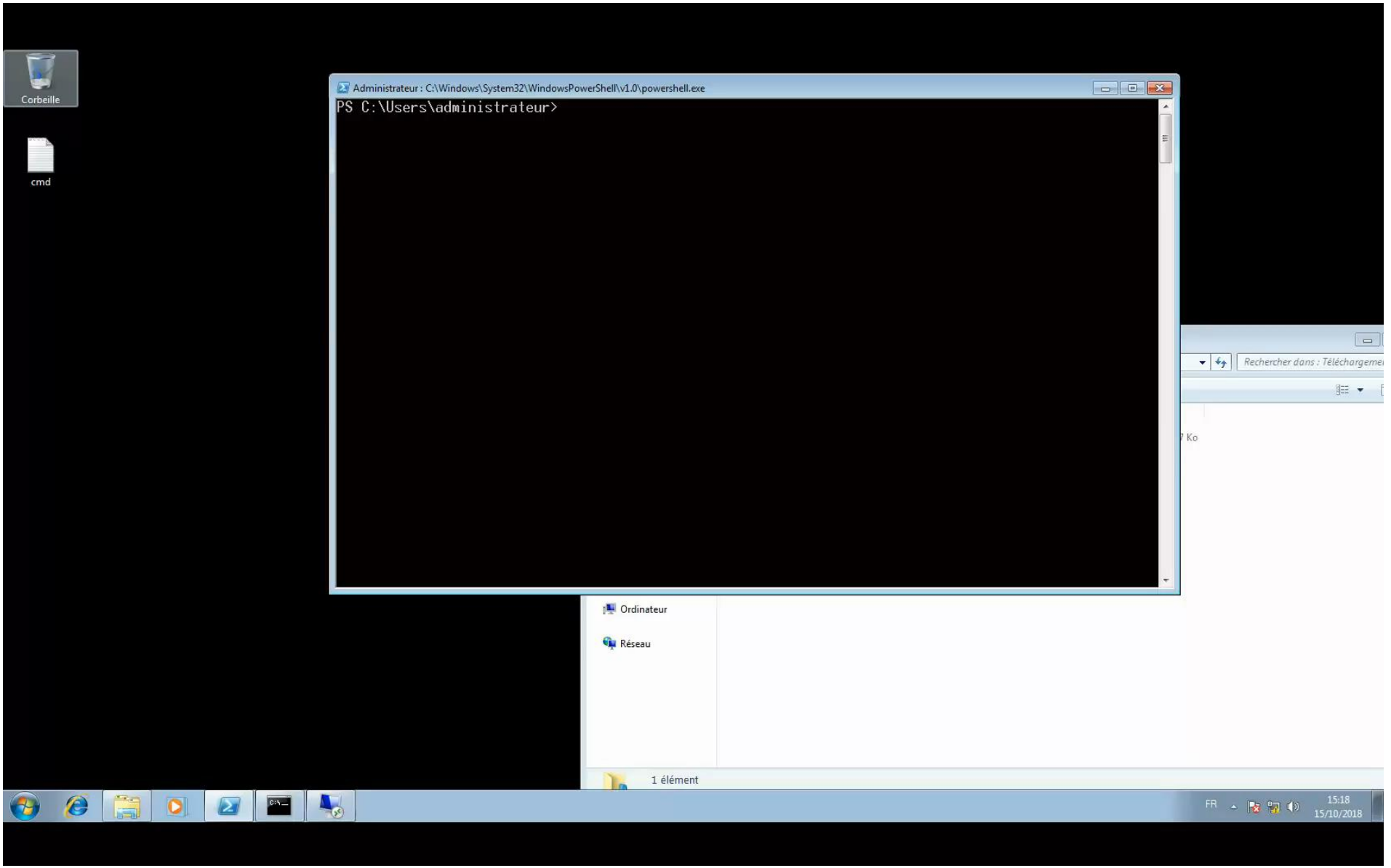
Démo 1 – Mimikatz DCSync + déploiement via GPO.

Scénario Attaquant:

- Mise en place d'une porte dérobée pour un compte non privilégié par modification du *NTSecurityDescriptor* à la racine du domaine avec *PowerSploit* afin de lui permettre la récupération des secrets d'authentificaion via *Mimikatz DCSync*.

- Déploiement d'un logiciel malveillant via la « *default domain policy* ».

- Reprise en main du domaine via la porte dérobée et le compte non privilégié.


Corbeille
cmd
Administrateur : C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PS C:\Users\administrateur>
Ordinateur
Réseau
1 élément
FR
15:18
15/10/2018

Exploitation des résultats de l'outil ADTimeline

- Modifications suspectes d'attributs : *NTSecurityDescriptor, SIDHistory, defaultSecurityDescriptor, UserAccountControl, Searchflags*…
- Effacements suspects d'objets (*Tombstone*).
- Comptes utilisateurs ajoutés/retirés de groupes.
- Incohérence timeline (*USN/ftimeLastOriginatingChange, dwVersion, WhenCreated*).

Quand un comportement suspect/défaut de configuration est trouvé, pivoter sur les journaux Windows (sauvegarde du DC *pszLastOriginatingDsaDN*).

Objets d'intérêt récoltés par ADTimeline

Objets partition domaine	Objets autres partitions
Racine et objets sous racine du domaine.	Rôles RBAC Exchange.
Objets protégés par SDProp.	Objets d'infrastructure Exchange.
Membres de DNSAdmins.	Zones DNS présentes et effacées.
GPOs présentes et effacées.	Objets effacés partition configuration.
Utilisateurs effacés et objets dynamiques.	Comptes Ordinateurs DCs via GC.
Les unités d'organisation.	Comptes nTDSDSA et Server des DCs.
Comptes délégation Kerberos.	Objets sites AD et Directory Service.
Objets sous conteneur System.	Objets de type PKI.
Comptes kerberoastables et AS-Reproastables.	Objets de type ClassSchema.
Groupes d'admin Exchange.	Admins domaine parent et Exchange via GC.
Membres de Cert Publishers.	Comptes SID history via GC.
Membres de GPO creators owners.	Droits étendus.
Groupes personnalisables.	AttributeSchema Searchflags particuliers.

Utilisation de l'outil ADTimeline – Modes de l'outil

- Mode en ligne : à exécuter sur une console d'administration ayant le module PowerShell Active Directory avec un compte administrateur du domaine (lecture dans le *tombstone*).

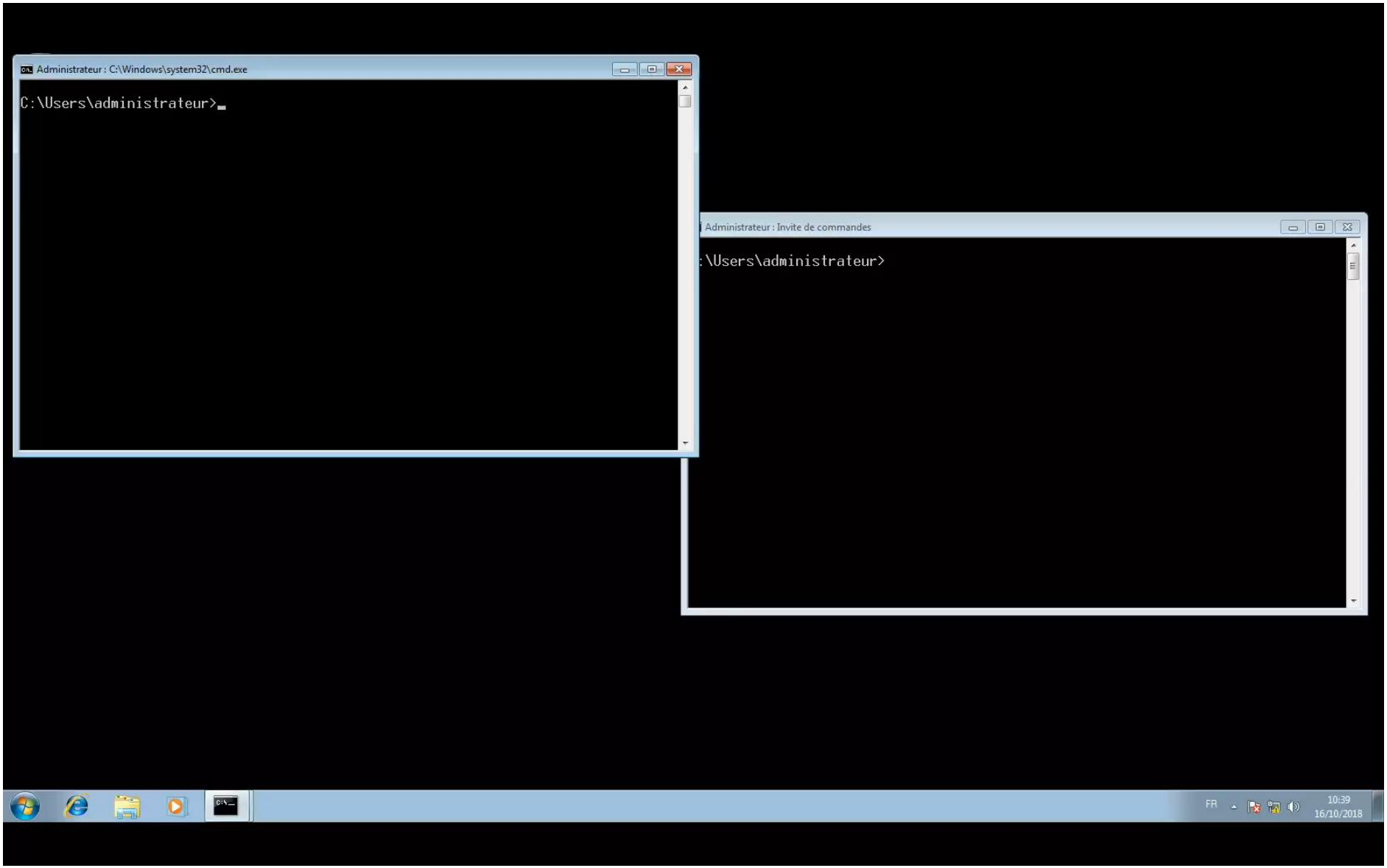
- Mode hors-ligne : dans le cas d'une image disque d'un DC, d'une sauvegarde ou snapshot de la base. Monter NTDS.DIT avec *dsamain.exe* (rôle ADLDS) sur une machine d'analyse ayant le module PowerShell Active Directory.

Démo 2 – Mimikatz DCShadow

Scénario Attaquant :

- Modification de l'attribut *PhoneNumber* des comptes administrateurs pour contourner l'authentification multi-facteur via SMS mise en place par l'équipe de sécurité.

- Utilisation de *Mimikatz DCShadow* pour contourner les alertes du SIEM et falsification des métadonnées de réplication pour ralentir l'investigation numérique (*ftimeLastOriginatingChange* uniquement).


Administrateur : C:\Windows\system32\cmd.exe
C:\Users\administrateur>
Administrateur : Invite de commandes
:\Users\administrateur>
FR
10:39
16/10/2018

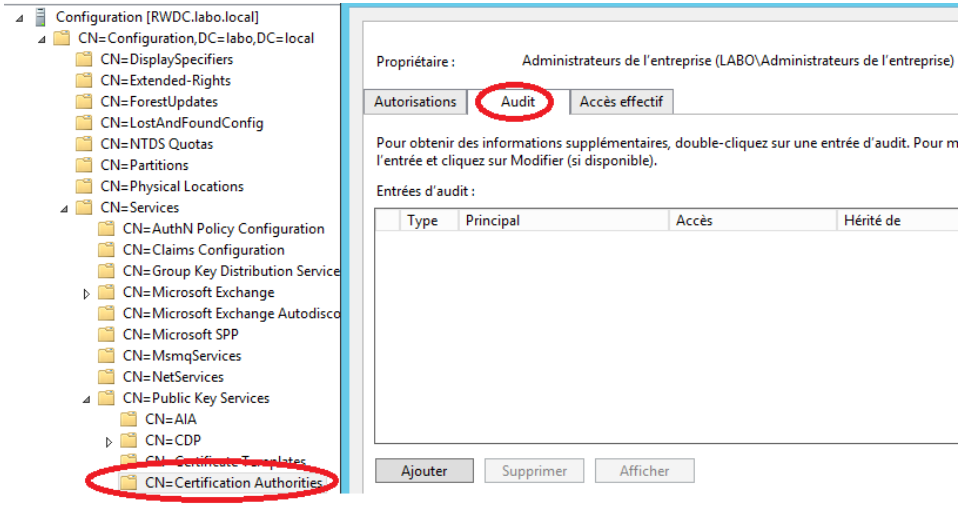
Les métadonnées de réplication AD vs journaux de sécurité

> Les métadonnées de réplication **ne remplacent pas** un système de centralisation, stockage et analyse des journaux de sécurité !

> Périmètre :

Métadonnées : tous les objets de l'annuaire mais seuls les attributs répliqués.

Journaux : dépend de votre stratégie d'audit.



Les métadonnées de réplication AD vs journaux de sécurité

> Centralisation :

Métadonnées : répliquées et stockées dans la base NTDS de chaque DC.

Journaux : solution de centralisation à mettre en place (http://aka.ms/WEF)

> Historique :

Métadonnées : données depuis la création de votre domaine mais uniquement la dernière modification de chaque attribut.

Journaux : dépend de la taille des journaux et votre stratégie de centralisation.

> Informations disponibles :

Métadonnées : vous ne savez pas quel compte a effectué la modification, ainsi que la valeur avant/après de l'attribut.

Journaux : toutes les données nécessaires sont présentes.

> Falsifiable par un attaquant :

Métadonnées : oui (ex *Mimikatz DCShadow*).

Journaux : oui (ex *DanderSpritz Eventlogedit*).

https://github.com/ANSSI-FR/ADTimeline

QUESTIONS?