Durcissement de l'Active Directory

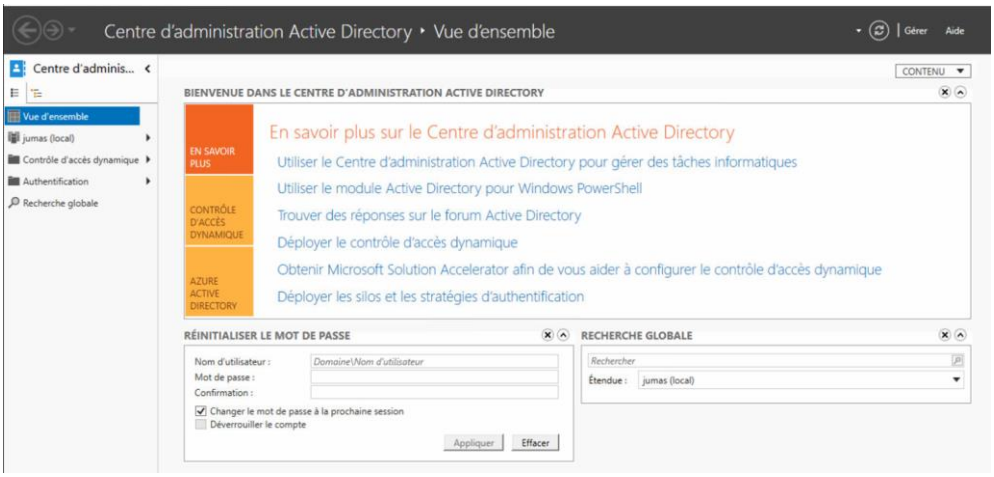
Version de Windows : Serveur 2022

Le hardening de l'Active Directory, ou encore le durcissement de l'Active Directory à pour but d'améliorer la sécurité de celui-ci en désactivant par exemple des protocoles qui sont connues pour ne plus être sur et en renforçant la sécurité via une stratégie de mot de passe forte et des groupes de sécurités.

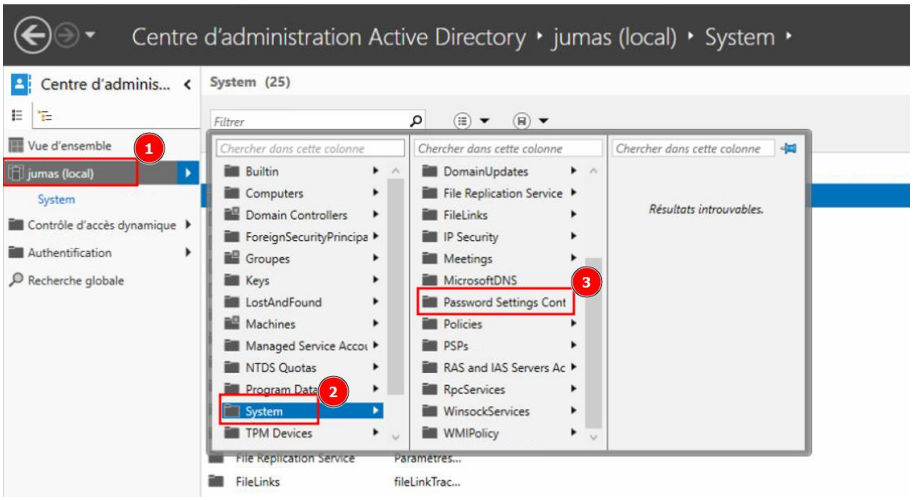
1 – Amélioration de la stratégie de mot de passe

La stratégie de mot de passe par défaut n'est plus suffisante dans un contexte de sécurité comme le connait actuellement notre société. De ce fait, nous allons améliorer cette stratégie et également bloquer les sessions après un nombre infructueux de tentative de connexion. Cela va notamment servir à éviter les attaques de type Brute force.

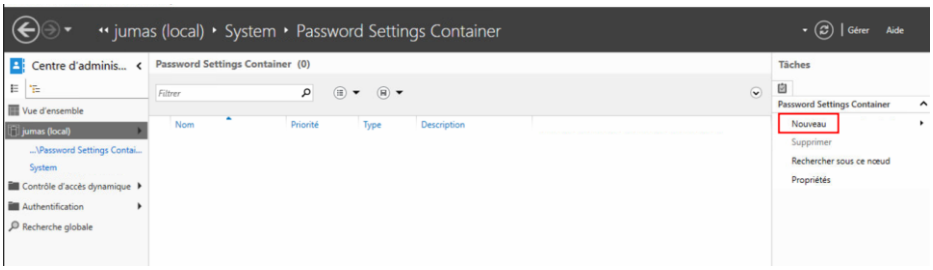
Sur votre contrôleur de domaine, ouvrez le **« Centre d'administration Active Directory ».**



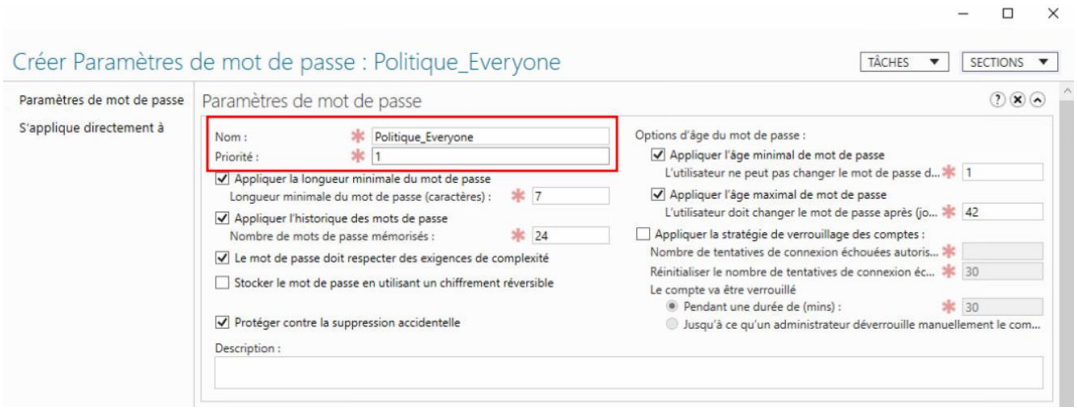
Rendez-vous ensuite dans **« Password Settings Container »**



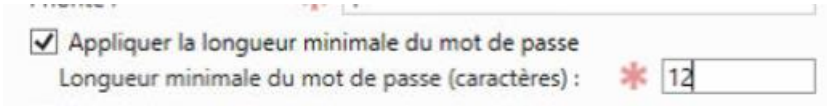
Cliquez maintenant sur **« Nouveau »** pour pouvoir créer notre politique



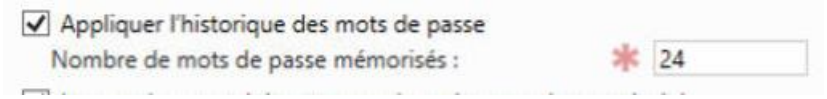
Nous allons commencer par donner un nom à notre politique, essayez d'utiliser quelque chose de logique et qui vous permettra de vous y retrouver.



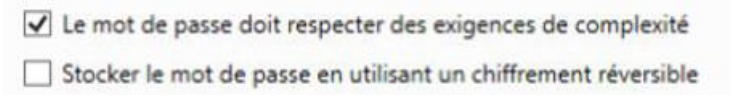
Nous allons maintenant mettre une longueur minimale de mot à 12 caractères (recommandation de la CNIL)



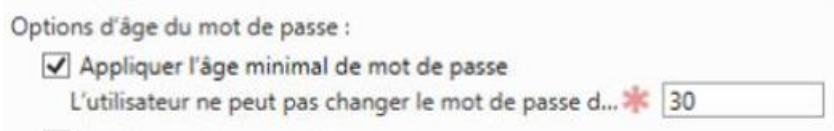
L'historique des mots de passe empêche un utilisateur de réutiliser un ancien mot de passe, la valeur par défaut est correcte nous n'allons donc pas modifier ce paramètre.



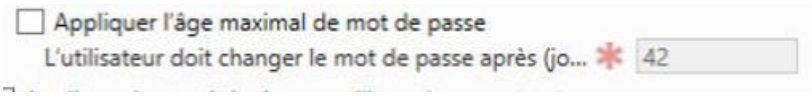
Cochez la case afin de respecter les exigences de complexité et SURTOUT ne cochez pas la case permettant un chiffrement réversible (cela signifie que le mot de passe peut être retrouver en clair)



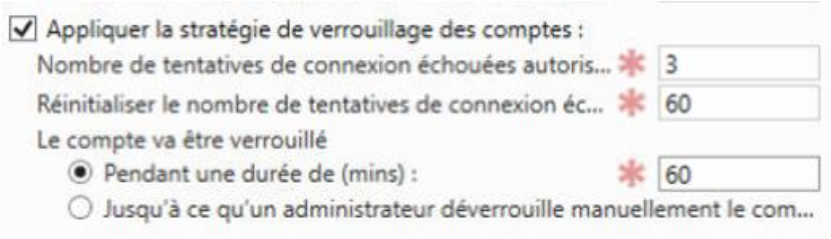
L'âge minimal de mot de passe représente la durée de vie d'un mot de passe en jour, ce qui permet de changer plusieurs fois d'affilée de mot de passe. La valeur à mettre est en jour.



Désactiver l'application d'un âge maximal afin de respecter les recommandations de l'ANSSI

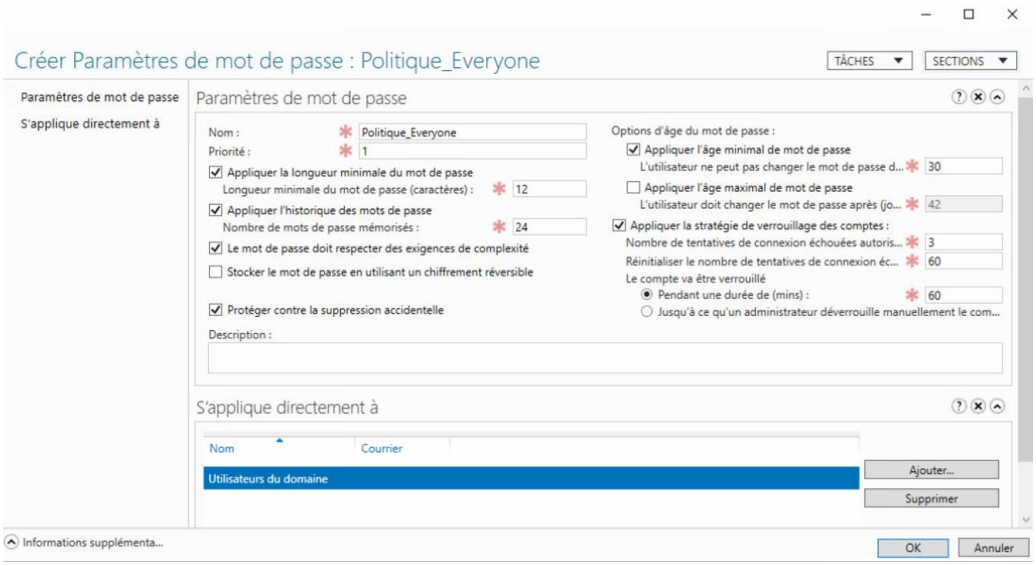


Nous allons maintenant activer la stratégie de verrouillage des comptes, cela va permettre d'empêcher les attaques de type brute force. Nous allons ainsi verrouiller le compte après 3 échecs et autoriser à nouveau la connexion après 60 min



Ajoutez ensuite le groupe sur lequel vous voulez appliquer cette politique, pour ma part je vais appliquer cette politique sur tous les utilisateurs du domaine

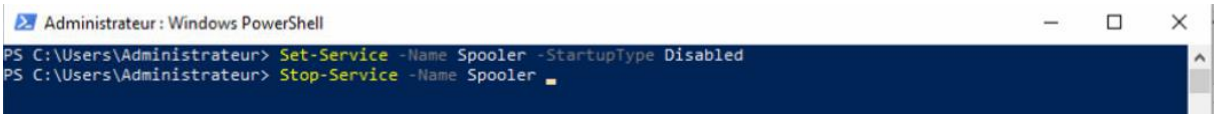
Vous devriez vous retrouver avec une politique ressemblante à l'image ci-dessous



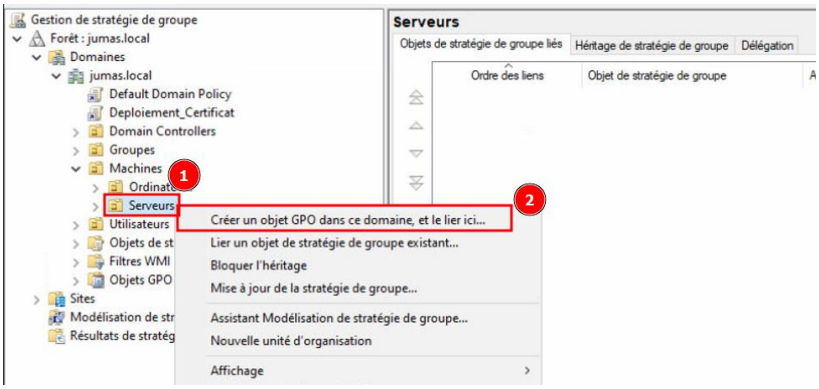
2 – Désactiver le Print Spooler service

Si ce service est activé sur le contrôleur de domaine, alors il rend celui-ci vulnérable à l'attaque nommée « PrintNightmare » et qui permet d'obtenir les droits SYSTEM, à savoir les droits les plus élevés !
Afin de se prémunir contre cela, il est important de désactiver ce service.

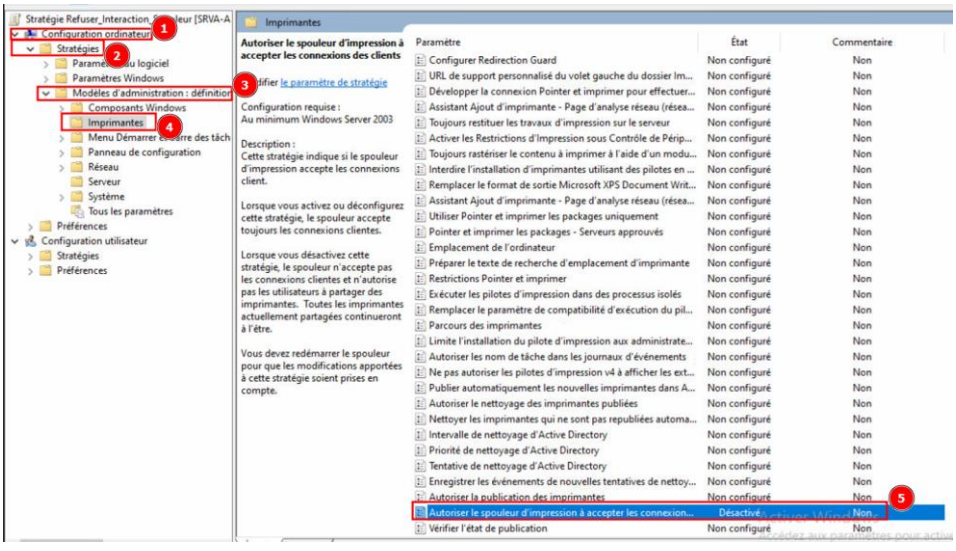
Pour ce faire nous allons utiliser une simple commande PowerShell sur notre contrôleur de domaine



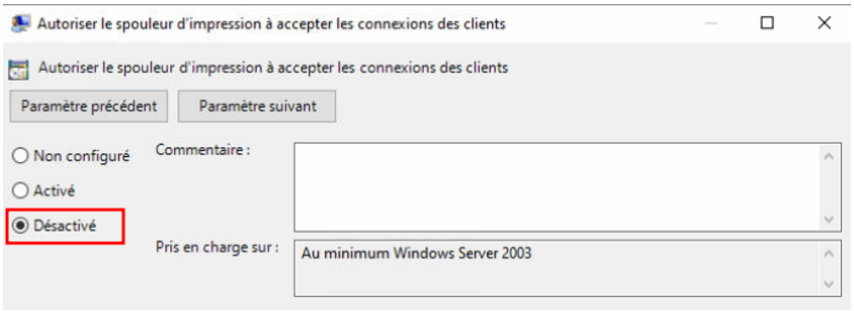
Maintenant, nous allons faire en sorte de bloquer les interactions distantes sur le Spouleur d'impression, il va falloir appliquer cette GPO sur une OU pour vos serveurs



Il va falloir ensuite désactiver la GPO **« Autoriser le spouleur d'impression à accepter les connexions des clients »** dans **Configuration ordinateur -> Stratégies -> Modèles d'administration -> Imprimantes**



Mettez cette GPO sur **« Désactivé »**

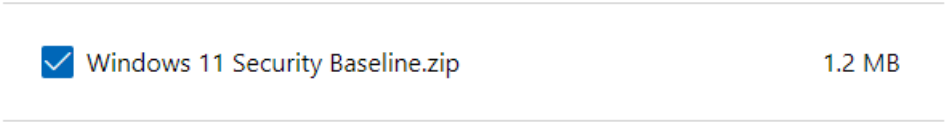


3 – Désactiver SMBv1

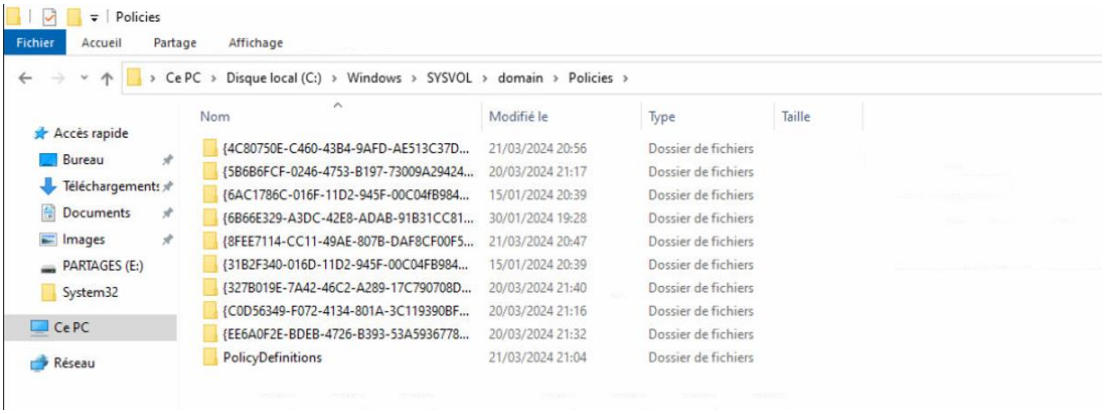
SMBv1 est la toute première version de SMB (Server Message Block) du protocol permettant le partage de ressources. Cette version est vulnérable à la vulnérabilité nommé **« EternalBlue »** qui permet de devenir SYSTEM sur le contrôleur de domaine et tout ordinateur utilisant cette version de SMB en seulement 5 minutes.

Nous allons donc utiliser une GPO qui s'appliquera sur l'ensemble du parc pour interdire l'utilisation de cette version.

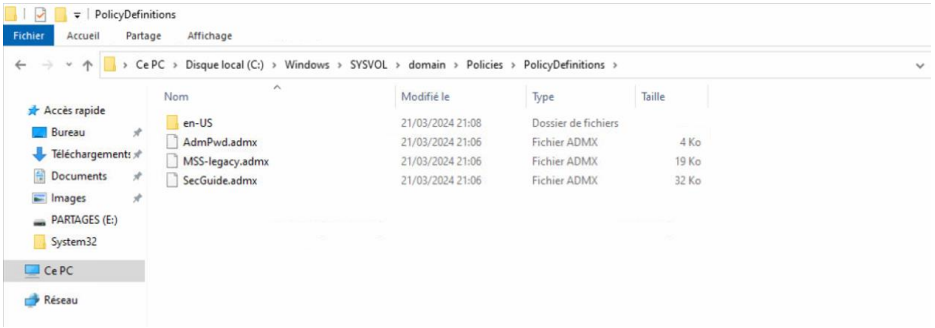
Il va falloir en premier lieu télécharger une GPO dans le magasin Microsoft.
Sélectionnez **« Windows 11 Security Baseline.zip »**



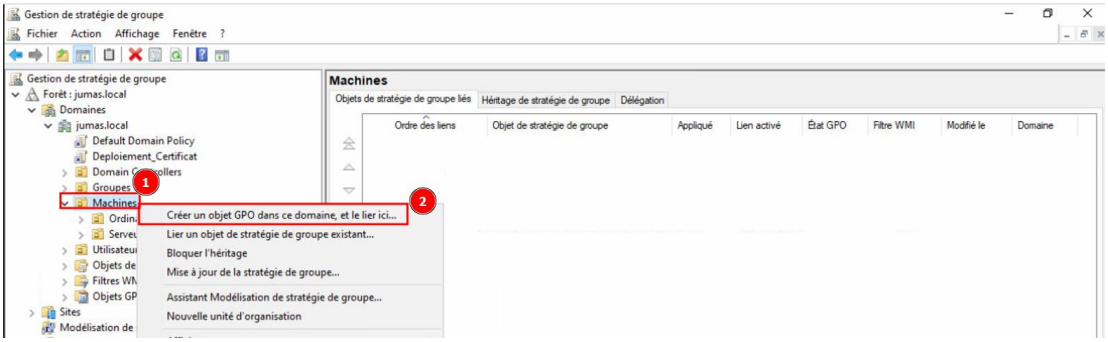
Maintenant, rendez-vous dans le chemin suivant **C:\Windows\SYSVOL\domain\Policies** et créez un nouveau dossier **« PolicyDefinitions »**



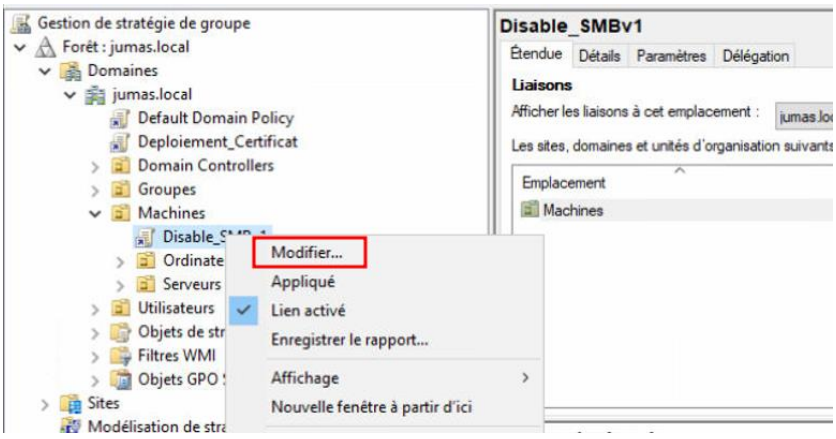
Dans ce dossier, il va falloir mettre les fichiers « admx » présent dans le fichier que nous avons téléchargé



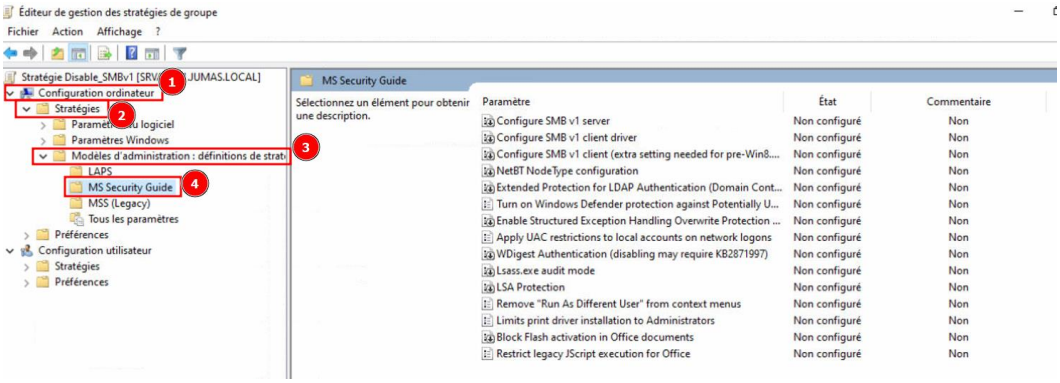
Je vais maintenant créer cette GPO dans mon OU **« Machines »**



Il va ensuite falloir modifier cette GPO

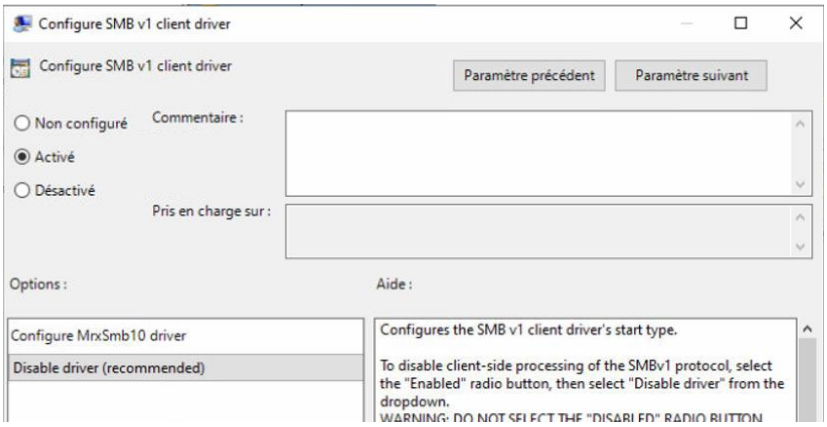


Il va maintenant falloir se rendre dans l'emplacement **Configuration ordinateur -> Stratégies -> Modèles d'administration -> MS Security Guide**



Il faut commencer par désactiver la stratégie **« Configure SMB v1 server »**

Nous allons ensuite désactiver la stratégie **« Configure SMB v1 client driver** ». Pour ce faire activez la stratégie et sélectionner **« Disable driver »**



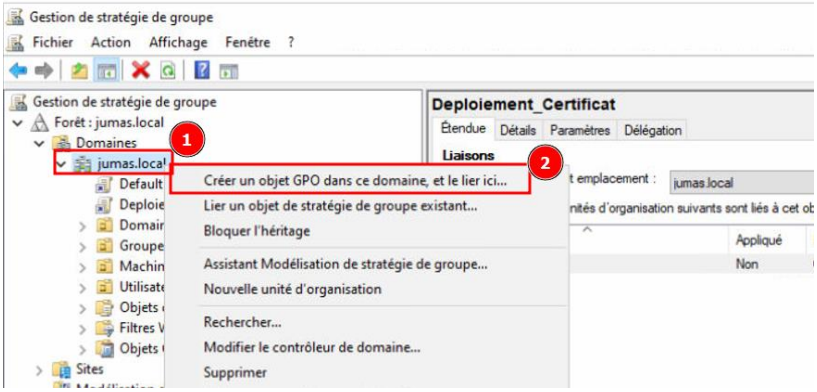
4 – Désactiver LLMNR et Netbios

Le protocole LLMNR (Local Link Multicast Name Resolution) permet la résolution de noms localement. Il est utilisé lorsque la résolution DNS échoue.
Le risque est qu'un attaquant s'étant introduit dans le réseau pourrait empoisonner les paquets en se faisant passer pour le nom recherché.

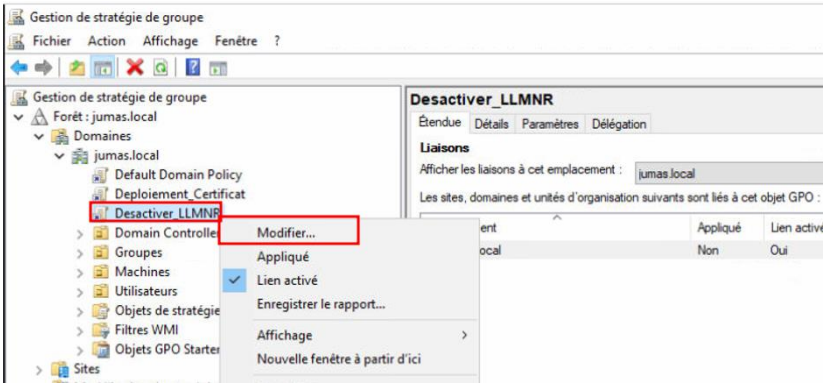
Netbios quant à lui est utilisé pour effectuer la recherche de ressources sur un réseau local. Ce protocol est aussi vulnérable à l'empoisonnement de paquet, un attaquant pourrait se faire passer pour une ressource réseau et tenter de récupérer le hash NTLM d'une machine avec des outils comme Responder.

4.1 – Désactiver LLMNR via une GPO

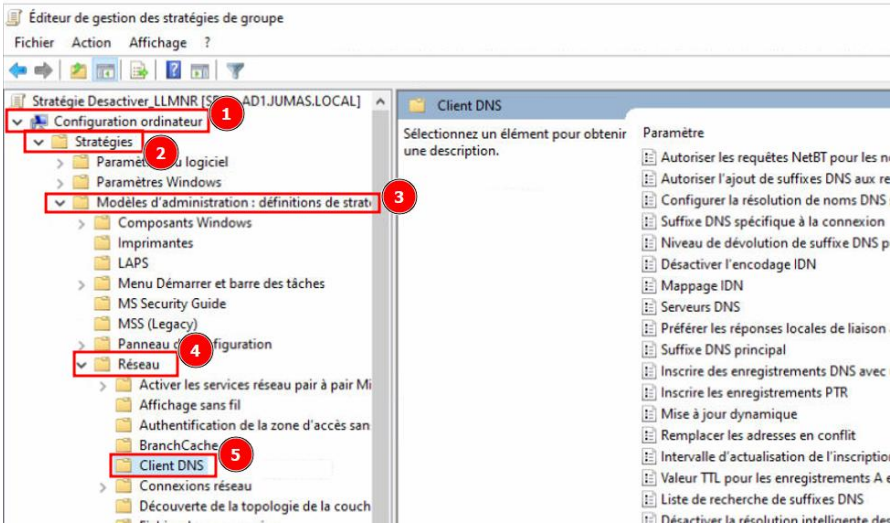
Nous allons créer une stratégie de groupe qui sera lié à la racine du domaine. Pour ce faire, rendez-vous dans la console de gestion de groupe et créer une GPO à la racine



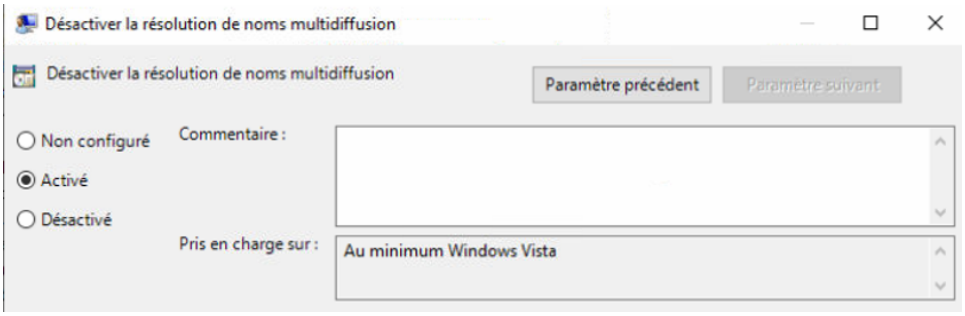
Nous allons ensuite modifier la GPO



Rendez-vous dans **Configuration ordinateur -> Stratégies -> Modèles d'administration -> Réseau -> Client DNS**



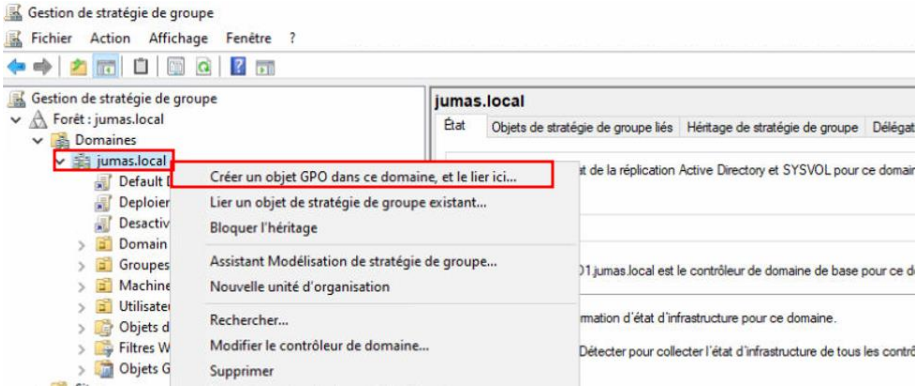
Activez ensuite la stratégie **« Désactiver la résolution de noms multidiffusion »**



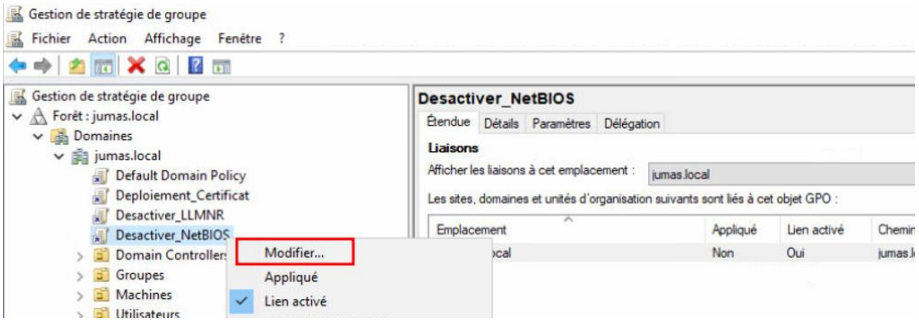
4.2 – Désactiver NetBIOS via une GPO

Afin de désactiver NetBIOS il va falloir jouer sur les clés de registre. Nous allons utiliser un script PowerShell déjà existant et faire en sorte qu'il s'exécute sur les machines.

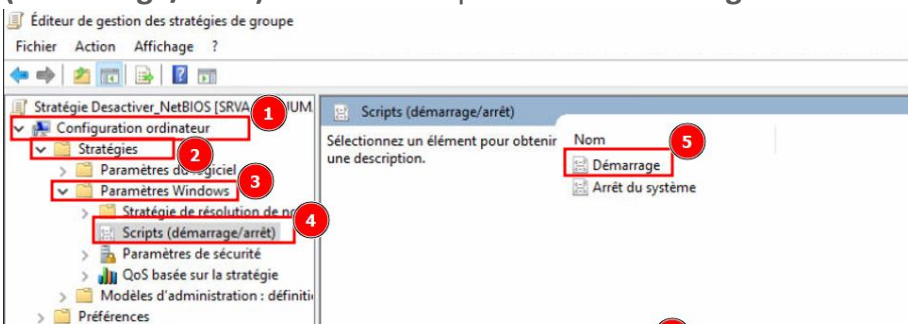
Créez une GPO à la racine de votre domaine



Modifiez cette GPO



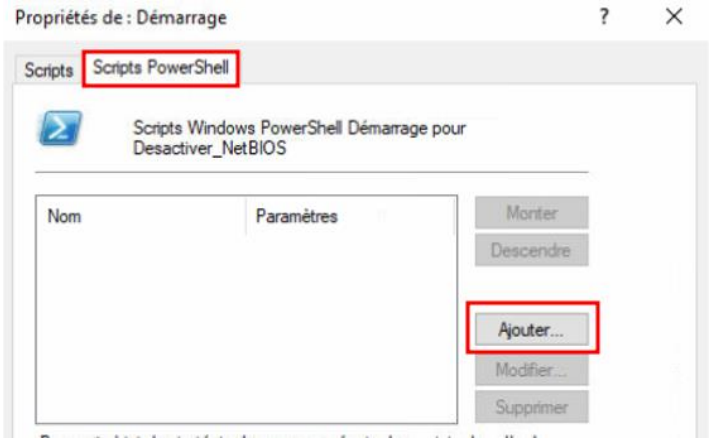
Rendez-vous dans **Configuration ordinateur -> Paramètres Windows -> Scripts (démarrage/arrêt)** et double cliquez sur **« Démarrage »**



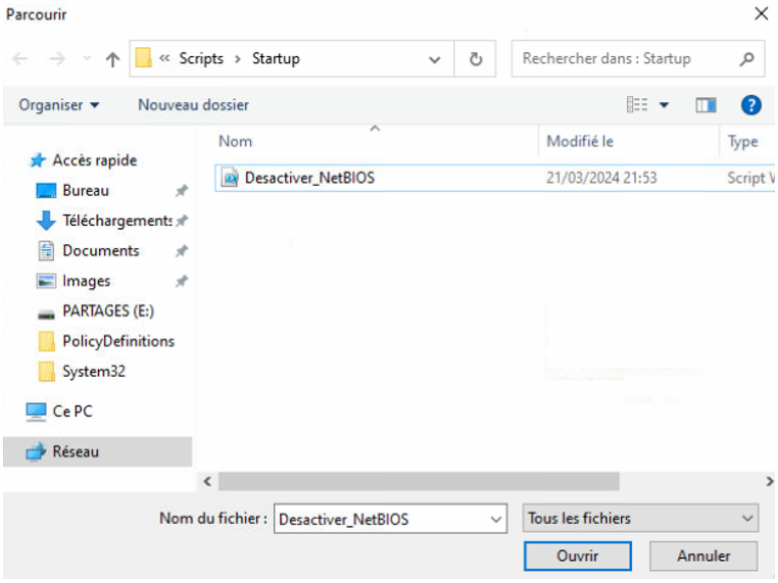
Rendez-vous dans le chemin suivant **« \\domaine\\SysVol\domaine\Policies\{C838EA2B-8B69....}\Machine\Scripts\Startup »,** créez un fichier PowerShell et coller le script suivant :

```
Set-ItemProperty -Path
'HKLM:\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\Interfaces\tcpip_*'
-Name NetbiosOptions -Value 2 -Verbose
```

Allez dans l'onglet **« Scripts PowerShell »** et cliquez sur **« Ajouter »**



Sélectionnez votre script précédemment créé



Une fois ajouté, ce script s'exécutera à chaque démarrage de toutes les machines.

5 – Protéger le compte krgbt

Le compte krgbt est sujet à des attaques de type « Golden Tickets ». Ce type d'attaque va permettre à un attaquant d'avoir accès à toutes les ressources du domaine en exploitant les vulnérabilités du protocole Kerberos.

Afin de se prémunir contre ce type d'attaque, il faut réinitialiser le mot de passe de ce compte 2 fois, car Windows garde un historique de 2 mots de passe. De plus, l'ANSSI recommande de changer le mot de passe de compte tous les ans.

Il va falloir suivre une méthode précise afin de ne pas perturber le bon fonctionnement de l'Active Directory. Il va falloir réinitialiser le mot de passe une première fois, puis attendre 10 heures avant de réinitialiser à nouveau le mot de passe afin de s'assurer que tous les tickets en cours récupèrent bien le mot de passe.

Pour mener à bien tout cela, nous allons utiliser un script publié par Microsoft.

Nous allons commencer par le télécharger à l'aide de PowerShell

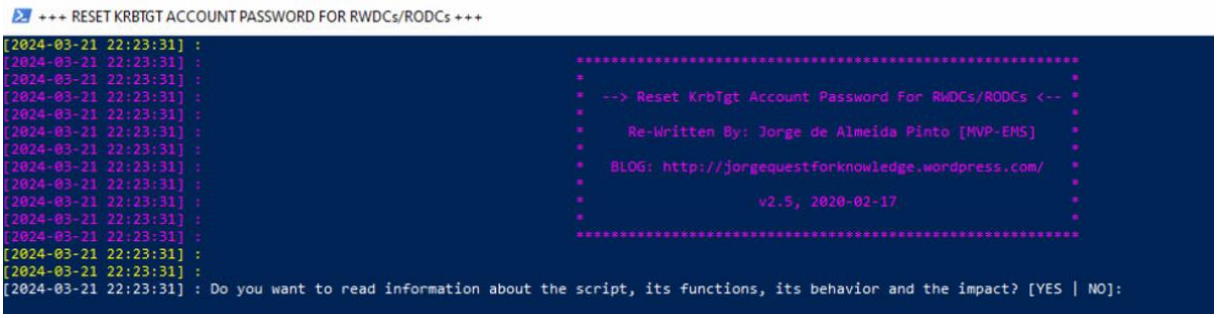
```
# Temporarily allow TLS1.2
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12

# Download the script.
Invoke-WebRequest https://raw.githubusercontent.com/microsoft/New-KrbtgtKeys.ps1/master/New-KrbtgtKeys.ps1 -O ./New-KrbtgtKeys.ps1
```

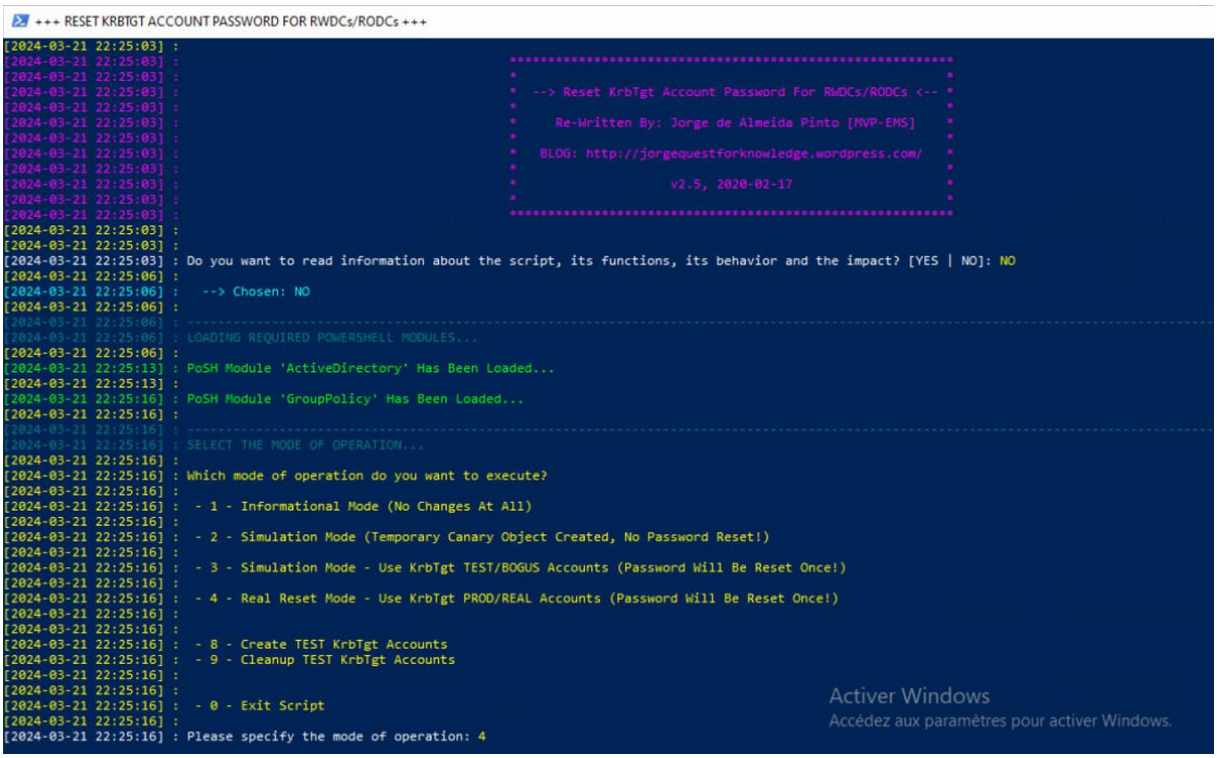
On va ensuite exécuter le script

```
# Temporarily allow srcipts to be run.
Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process
# Run the Microsoft script.
./New-KrbtgtKeys.ps1
```

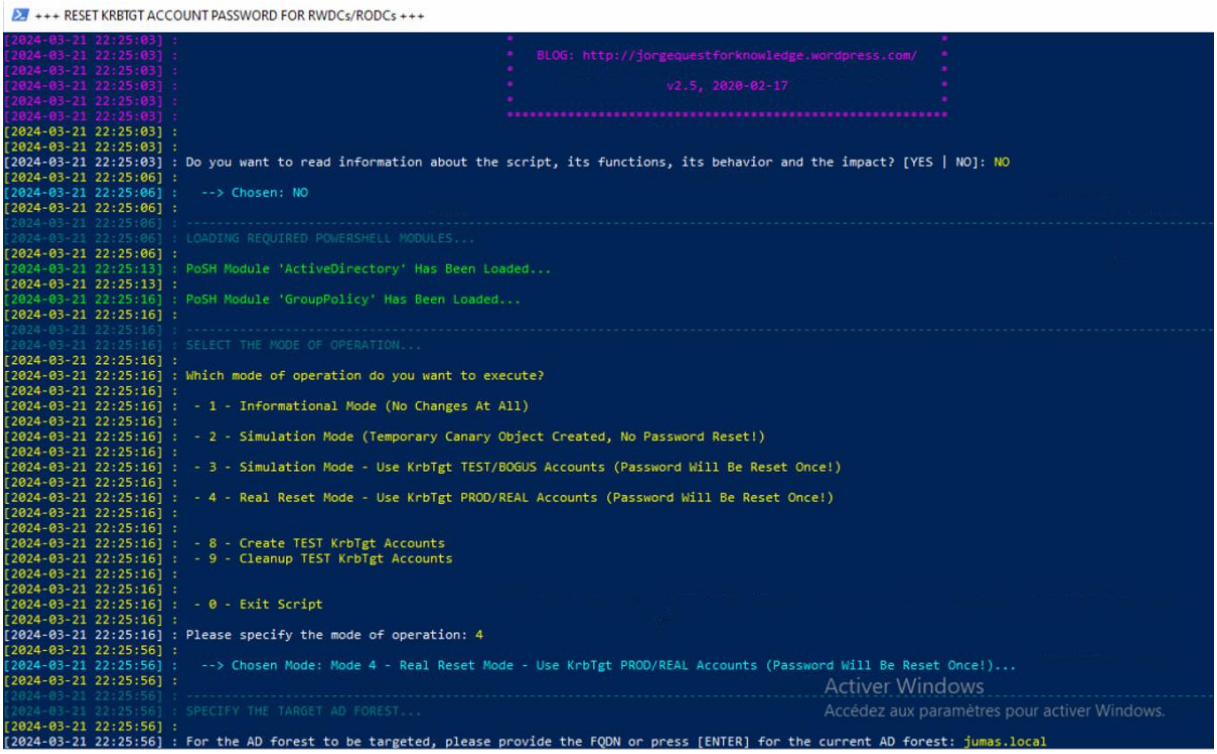
Au lancement du script, sélectionnez **[NO]**



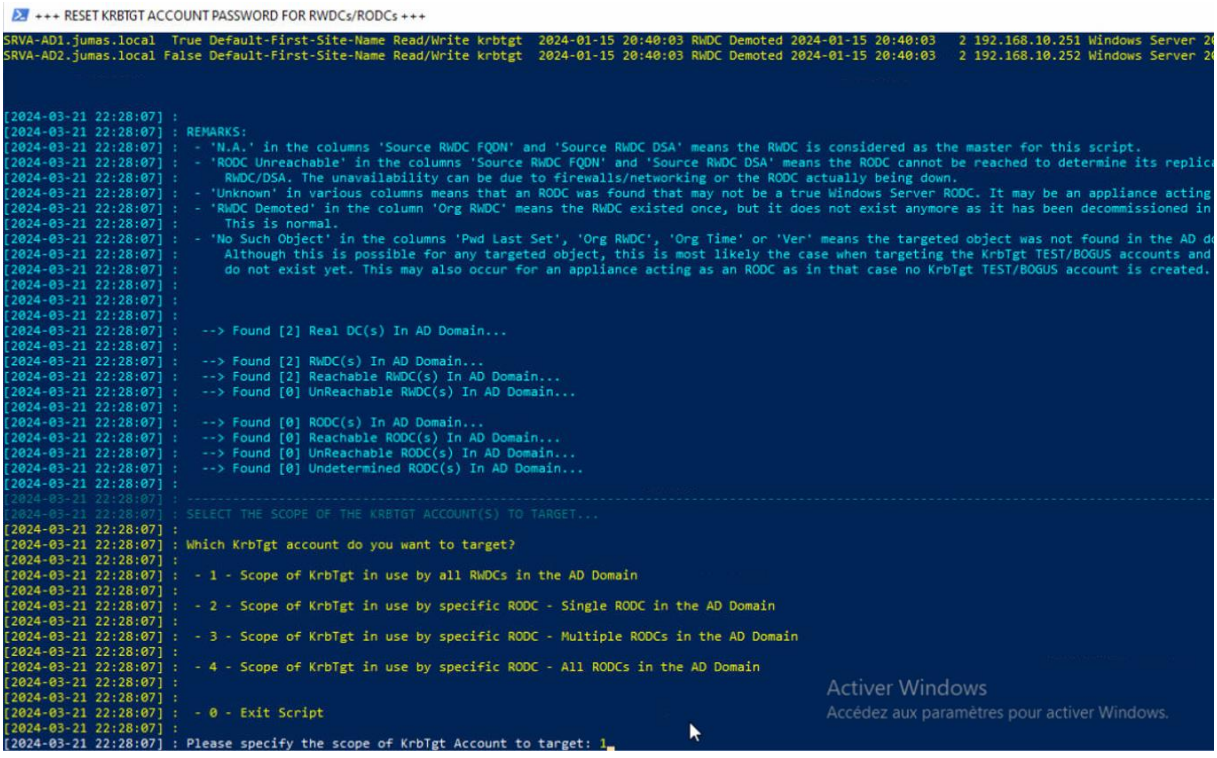
Sélectionnez ensuite le **mode 4**



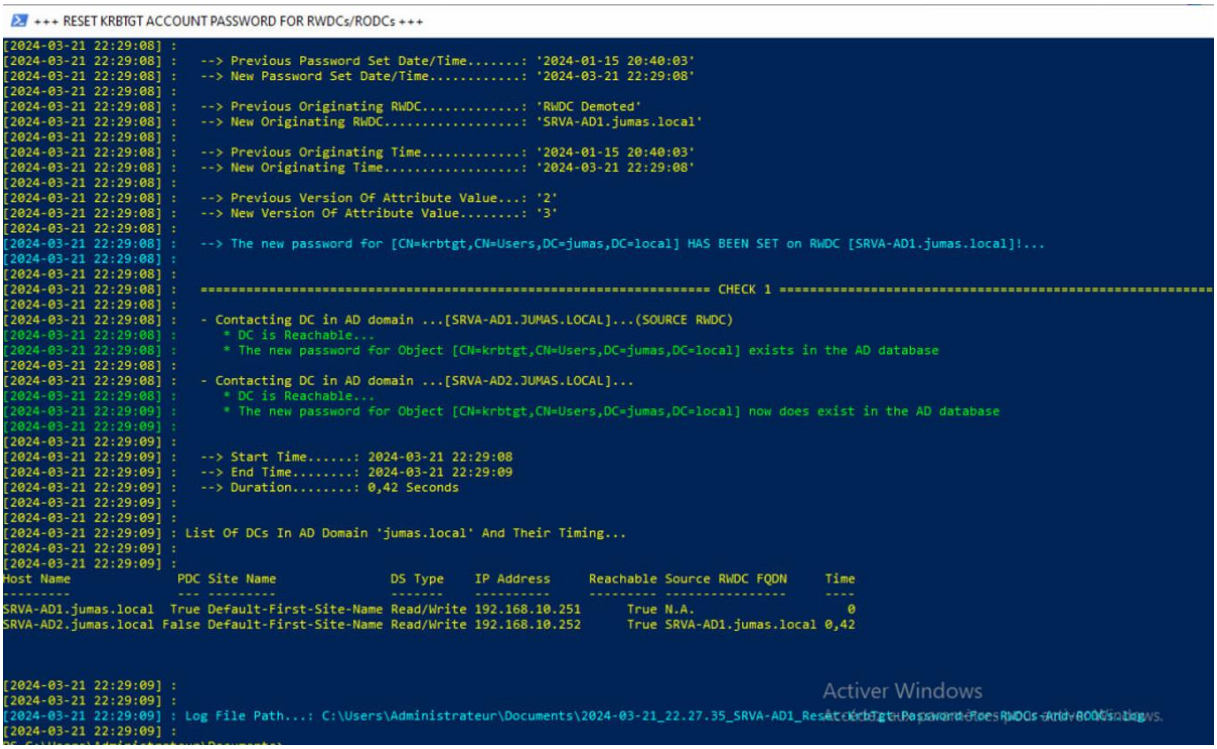
Insérez maintenant votre nom de domaine



Sélectionnez maintenant **l'option 1**



Le script va ensuite réinitialiser le mot de passe



Il faudra ensuite refaire cette opération après 10h car comme je l'ai dit précédemment, windows garde en historique 2 mots de passe.

Par la suite, ces étapes seront à réalisées tous les ans afin de maintenir un niveau de sécurité optimale en conformité avec les recommandations de l'ANSSI.

Fin de la procédure.