HARDEN-AD

Sommaire

Qu’est-ce que Harden AD :

Le projet HARDEN AD est une initiative de renforcement de la sécurité et de la résilience de l'Active Directory, une infrastructure critique pour la gestion des identités et des accès dans les entreprises. Ce projet vise à protéger l'Active Directory contre les cybermenaces, en particulier les attaques avancées telles que les ransomwares et les compromissions de comptes administratifs. Il met en œuvre des stratégies et des outils pour renforcer la sécurité, améliorer la détection des anomalies, et assurer une récupération rapide en cas d'incident. L'objectif principal de HARDEN AD est de garantir la continuité des opérations et de sécuriser les données sensibles en rendant l'Active Directory plus résistant aux attaques et plus rapide à restaurer après une compromission.

A quoi sert-il :

Harden AD permet de sécuriser son Active directory face à des menaces d’attaques, pour cela il va déployer un modèle sur 5 tiers :

- **Tiers 0** : serveurs liés aux services d'authentification, d'infrastructure et de sauvegarde. Le meilleur exemple : les contrôleurs de domaine
- **Tiers 1** : serveurs liés aux applications métiers
- **Tiers 2** : les postes de travail des utilisateurs et la gestion des comptes utilisateurs
- **Tiers 1 Legacy** : serveurs avec un système d'exploitation obsolète (plus supporté par l'éditeur)
- **Tiers 2 Legacy** : stations de travail avec un système d'exploitation obsolète (plus supporté par l'éditeur), ce qui est parfois utile pour la compatibilité applicative

En ce qui concerne l'administration des différents tiers, et en l'absence d'un bastion, elle devra s'effectuer par des machines d'administration qui servent de points de connexion sécurisés pour se connecter sur les serveurs. Par exemple, à partir de son poste de travail, l'administrateur système doit se connecter en bureau à distance sur une machine, pour ensuite se connecter sur le serveur cible. Pour aller plus loin, il est recommandé d'avoir un second rebond intermédiaire vers une machine spécifique au tiers que l'on souhaite administrer, avant de se connecter à la ressource cible. Ceci complique certes le processus d'utilisation mais améliore la sécurité du réseau car en cas de piratage d'un compte admin, l'hackeur ne pourra pas avoir accès à tous les autres tiers du réseau.

Installation :

Création d'un active directory sur une machine Windows serveur pour pouvoir installer Harden AD et le tester.

Nous avons configuré un Active Directory en lab. Nous y avons ajouté un utilisateur et un ordinateur au domaine « ***test.lan*** » à l'adresse ip ***172.20.28.65*** le mot de passe du compte ***administrateur*** est ***lote5axa.36***.

Pour installer et mettre en place Harden AD nous suivons la documentation fourni sur le site ***hardenad.net*** ainsi que la documentation fourni par le site ***It connect***.

Récupération du Zip d'installation :

Vérification que les rôles FSMO sont disponibles avec la commande :

(Optionnelle)

Les rôles FSMO sont un ensemble de services et de processus, qui sont gérés par les DC dans une configuration AD multi-modèle. Ces rôles assurent le bon fonctionnement de toutes les capacités d'AD, y compris la réplication en temps voulu et aussi la cohérence des informations dans l'ensemble de la forêt d'AD de toute l'organisation.

```
> netdom query fsmo
```

```
Administrateur : C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur.WIN-7CRA1U18A8S>hostname
harden-ad

C:\Users\Administrateur.WIN-7CRA1U18A8S>netdom query fsmo
Contrôleur de schéma        harden-ad.test.lan
Maître des noms de domaine  harden-ad.test.lan
Contrôleur domaine princip. harden-ad.test.lan
Gestionnaire du pool RID    harden-ad.test.lan
Maître d'infrastructure     harden-ad.test.lan
L'opération s'est bien déroulée.
```

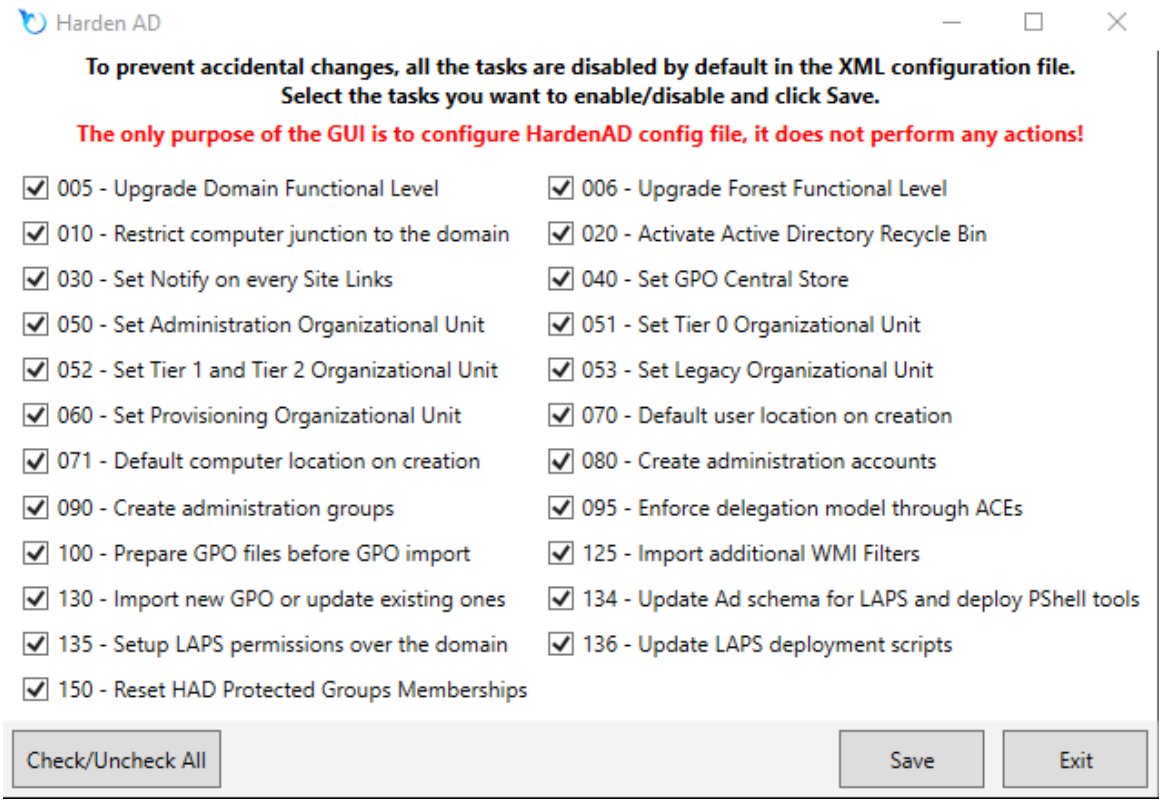
Lancement Harden AD :

Extraire le zip dans le C déployer le script « Run-HardenADGui.ps1 »

```
PS C:\HardenAD-Master\HardenAD-Master>
PS C:\HardenAD-Master\HardenAD-Master> .\Run-HardenADGui.ps1
```

(En cas de non droit d'exécution, utiliser la commande PowerShell **Set-executionPolicy unlock**)

Coché le paramétrage voulu et sauvegarder la sélection :

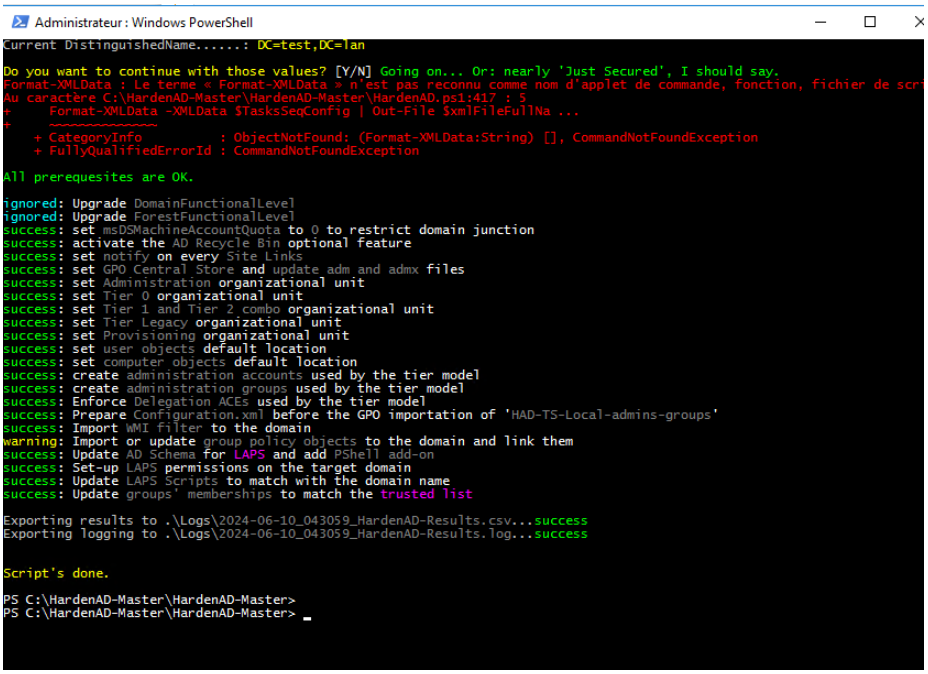


À la suite de l'activation des paramètre de configuration vous pouvez lancer une analyse Ping Castle pour comparer le avant/après de l'Active Directory

Lancer le script principal « HardenAD.ps1 » :

À la suite du lancement nous retrouvons un problème de lecture du format des **Fichiers XLM** dans les scripts, probablement dû as l'ancienneté du script d'Harden qui ne passe plus avec les mises à jour récentes.

(Ceci est le deuxième test d'Harden AD lors du premier essaie l'update du schéma d'AD n'avait pas fonctionner)

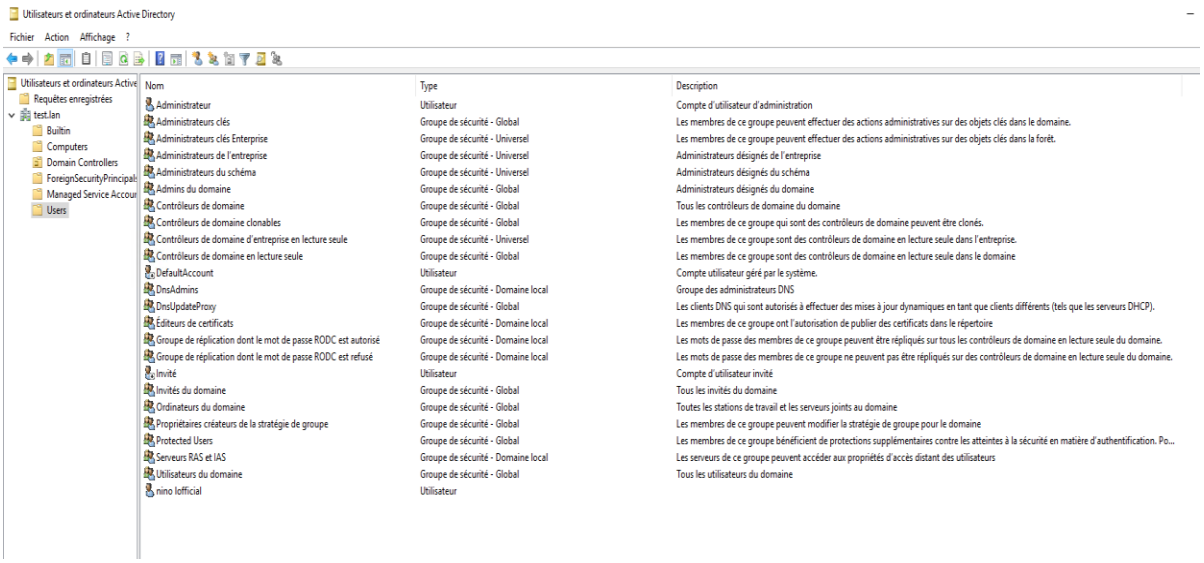


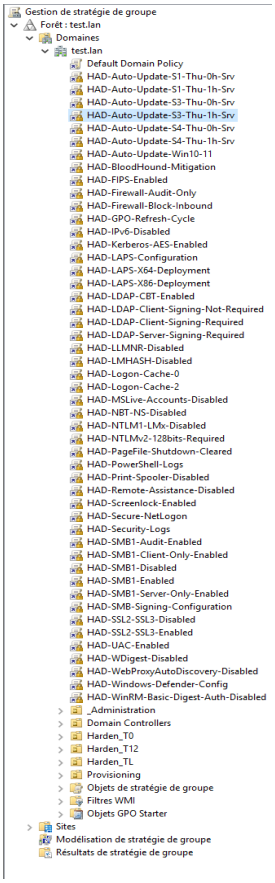
```
Script.....: Harden AD
Edition....: Community Edition
Version....: 02.09.008
Contact....: contact@hardenad.net
Our words..: improve the security of your directory in minutes!

Current forest .................: test.lan
Current domain .................: test.lan
Current NetBIOS.................: TEST
Current DistinguishedName......: DC=test,DC=lan

Do you want to continue with those values? [Y/N] Going on... Or: nearly 'Just Secured', I should say.
All prerequesites are OK.

Ignored: Upgrade DomainFunctionalLevel
Ignored: Upgrade ForestFunctionalLevel
Success: set msDSMachineAccountQuota to 0 to restrict domain junction
Success: activate the AD Recycle Bin optional feature
Success: set notify on every Site Links
Success: set GPO Central Store and update adm and admx files
Success: set Administration organizational unit
Success: set Tier 0 organizational unit
Success: set Tier 1 and Tier 2 combo organizational unit
Success: set Tier Legacy organizational unit
Success: set Provisioning organizational unit
Success: set user objects default location
Success: set computer objects default location
Success: create administration accounts used by the tier model
Success: create administration groups used by the tier model
Success: Enforce Delegation ACEs used by the tier model
Success: Prepare Configuration.xml before the GPO importation of 'HAD-TS-Local-admins-groups'
Success: Import WMI filter to the domain
Success: Import or update group policy objects to the domain and link them
Success: Update AD Schema for LAPS and add PShell add-on
Success: Set-up LAPS permissions on the target domain
Success: Update LAPS Scripts to match with the domain name
Success: Update groups' memberships to match the trusted list

Exporting results to .\Logs\2024-06-11_014039_HardenAD-Results.csv...success
Exporting logging to .\Logs\2024-06-11_014039_HardenAD-Results.log...success


Script's done.
```

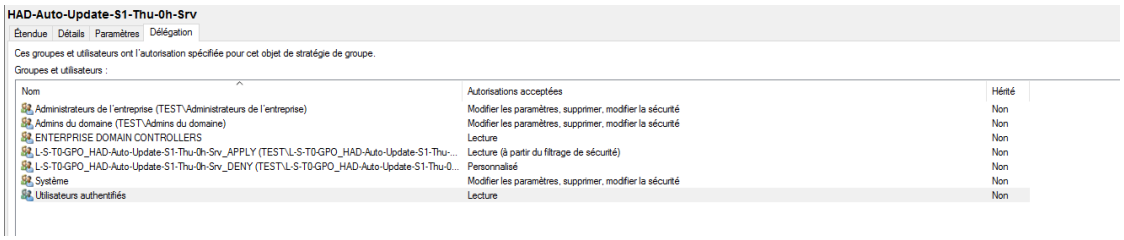
(En relançant le script pour tester, aucun message n'apparait pour l'erreur XML et l'import update n'a pas été mis en warning)

Résultat des scripts PowerShell :

Création des groupes de sécurité global et local, mais aussi d'une multitude de GPO après l'exécution des scripts sur l'Active Directory.







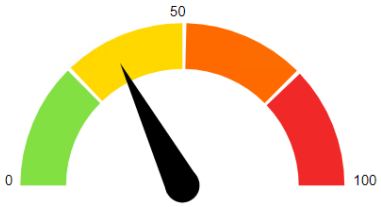
Pour chaque GPO crée celle-ci ne sont pas active pour permettre à l'administrateur d'avoir la main sur les règles établis et à qui elles sont établis.

Analyse et résultat de Ping Castle :

Après avoir regardé les résultats des scripts sur l'Active Directory faites une analyse de sécurité avec Ping Castle :

- Il nous donne après l'exécution des scripts de Harden AD un **score général de sécurité** du domaine de **35/100**.

Indicateurs

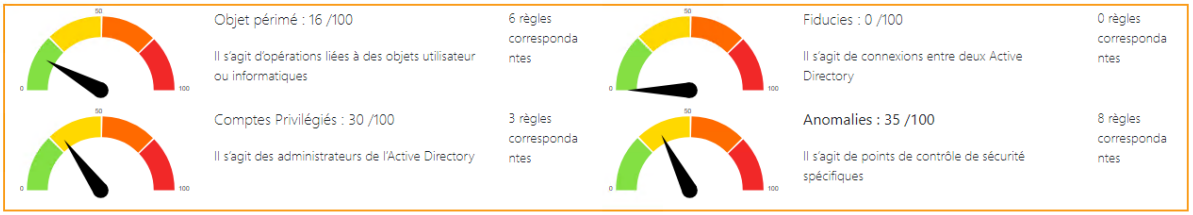


Niveau de risque du domaine : 35 / 100

C'est le score maximum des 4 indicateurs et un score ne peut pas être supérieur à 100. Plus c'est bas, mieux c'est

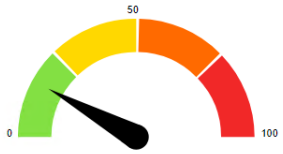
Comparer avec les statistiques

Avis de confidentialité



Pour les **Objets Périmé**. Cette partie est noté **16/100** car :

Objets périmés



Objets périmés : 16 /100

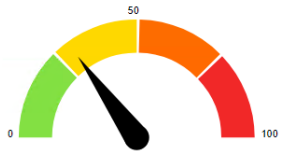
Il s'agit d'opérations liées à des objets utilisateur ou informatiques

Détails de la règle Objets périmés [6 règles correspondantes sur un total de 50]

SMB v1 activé sur 1 DC	*+ 10 point(s)*
La déclaration de sous-réseau est incomplète [1 adresse IP du contrôleur de domaine introuvable dans les sous-réseaux déclarés]	*+ 5 point(s)*
Nombre de comptes dont le mot de passe n'expire jamais : 1	*+ 1 point(s)*
Vérifiez que le blindage Kerberos est activé sur les contrôleurs de domaine et que le niveau fonctionnel du domaine est au moins Windows Server 2012	*Règle informative*
Vérifiez que le blindage Kerberos est activé sur les clients et que le niveau fonctionnel du domaine est au moins Windows Server 2012	*Règle informative*
Au moins une valeur par défaut de l'unité d'organisation par défaut a été modifiée	*Règle informative*

Pour les **Comptes privilégiés**. Cette partie est noté **30/100** car :

Comptes privilégiés



Comptes Privilégiés : 30 /100

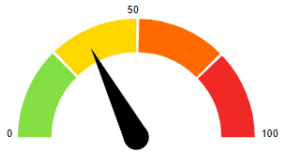
Il s'agit des administrateurs de l'Active Directory

Détails de la règle des comptes privilégiés [3 règles correspondantes sur un total de 45]

Présence de comptes Admin qui n'ont pas l'indicateur « Ce compte est sensible et ne peut pas être délégué » : 1	+ 20 point(s)
Le groupe Schema Admins n'est pas vide : 1 compte(s)	+ 10 point(s)
Des unités d'organisation sans protection contre la suppression accidentelle ont été trouvées	Règle informative

Pour les **Analyses des anomalies**. Cette partie est noté **35/100** car :

Analyse des anomalies



Anomalies : 35 /100

Il s'agit de points de contrôle de sécurité spécifiques

Détails de la règle Anomalies [8 règles appariées sur un total de 70]

Stratégie où la longueur du mot de passe est inférieure à 8 caractères : 1	+ 10 point(s)
Le service de spouleur est accessible à distance depuis 1 DC	+ 10 point(s)
Les interfaces RPC du DC sont probablement vulnérables aux attaques de coercition. Interfaces identifiées : 6	+ 10 point(s)
Le nombre de contrôleurs de domaine est trop faible pour assurer la redondance : 1 contrôleur de domaine	+ 5 point(s)
DsHeuristics n'a pas été configuré pour activer l'atténuation pour CVE-2021-42291	Règle informative
Le groupe compatible PreWin2000 contient « Utilisateurs authentifiés »	Règle informative
Aucune stratégie de mot de passe pour les comptes de service trouvée (MinimumPasswordLength>=20)	Règle informative
Les utilisateurs authentifiés peuvent créer des enregistrements DNS	Règle informative

Amélioration de la sécurité de l'Active directory de l'entreprise pour permettre la diminution du score de Ping Castle passant de 50/100 a 30/100 une diminution pas total car les stratégie de groupe ne sont pas encore activé dans les paramètre de groupe en rajoutant ceux-ci le score devrait encore baisser