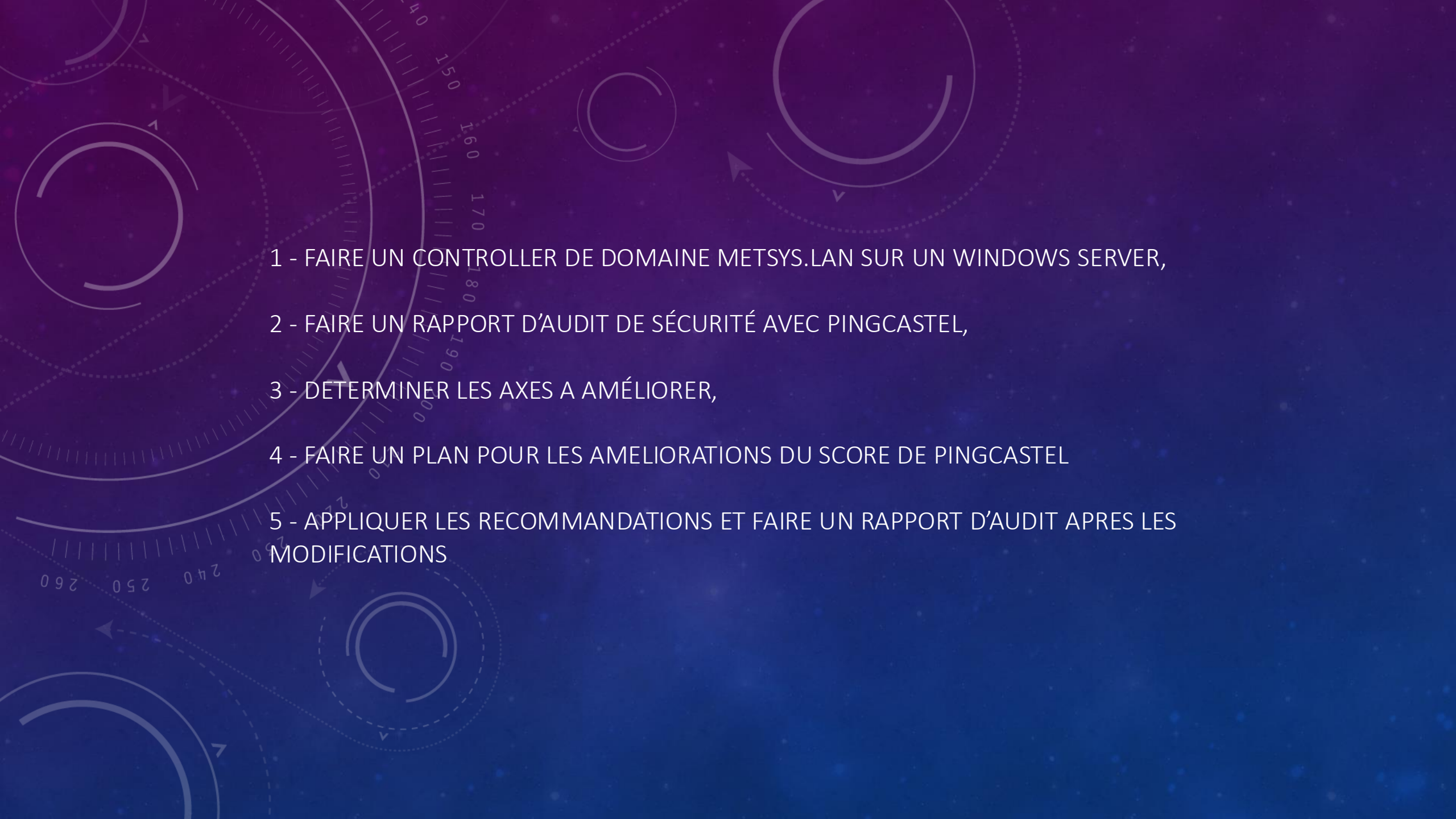


The background is a dark blue gradient with a subtle pattern of white dots. Overlaid on the left side are several concentric circles and arcs in a lighter blue color. Some of these arcs have degree markings, such as 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 250, and 260. There are also small arrows pointing in various directions, suggesting a circular or rotational theme.

TP CONTROLLER DE DOMAINE ET AUDIT PINGCASTEL

PRISCILLA

- 
- 1 - FAIRE UN CONTROLLER DE DOMAINE METSYS.LAN SUR UN WINDOWS SERVER,
 - 2 - FAIRE UN RAPPORT D'AUDIT DE SÉCURITÉ AVEC PINGCASTEL,
 - 3 - DETERMINER LES AXES A AMÉLIORER,
 - 4 - FAIRE UN PLAN POUR LES AMELIORATIONS DU SCORE DE PINGCASTEL
 - 5 - APPLIQUER LES RECOMMANDATIONS ET FAIRE UN RAPPORT D'AUDIT APRES LES MODIFICATIONS

1 - CREATION DU CONTROLLER DE DOMAINE

1 – j'ai renommé le serveur en SRV1

2- j'ai mis une adresse ip fixe et le DNS

Propriétés de : Protocole Internet version 4 (TCP/IPv4)

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

☐ Obtenir une adresse IP automatiquement

☒ Utiliser l'adresse IP suivante :

Adresse IP : 192 . 168 . 100 . 10

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 192 . 168 . 100 . 2

☐ Obtenir les adresses des serveurs DNS automatiquement

☒ Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : 127 . 0 . 0 . 1

Serveur DNS auxiliaire : . . .

☐ Valider les paramètres en quittant

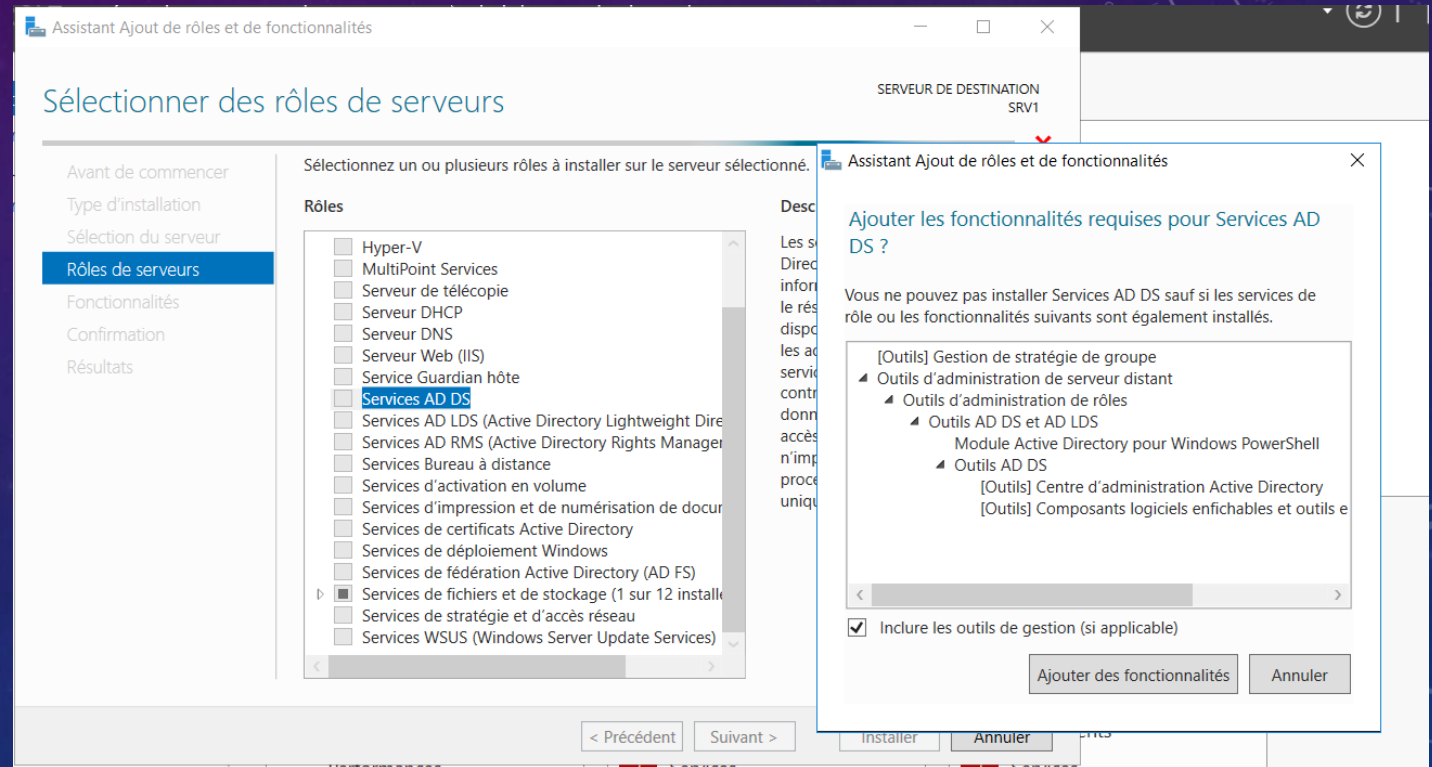
Avancé...

OK Annuler

1 - CREATION DU CONTROLLER DE DOMAINE

3 – on ajoute un rôle de serveurs

On coche Services ADDS



1 - CREATION DU CONTROLLER DE DOMAINE

4 – On ajoute une nouvelle forêt

Assistant Configuration des services de domaine Active Directory

Configuration de déploiement

SERVEUR CIBLE
SRV1

Configuration de déploie...

Options du contrôleur de...

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

Sélectionner l'opération de déploiement

☐ Ajouter un contrôleur de domaine à un domaine existant

☐ Ajouter un nouveau domaine à une forêt existante

☒ Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine :

[En savoir plus sur la configurations de déploiement](#)

< Précédent

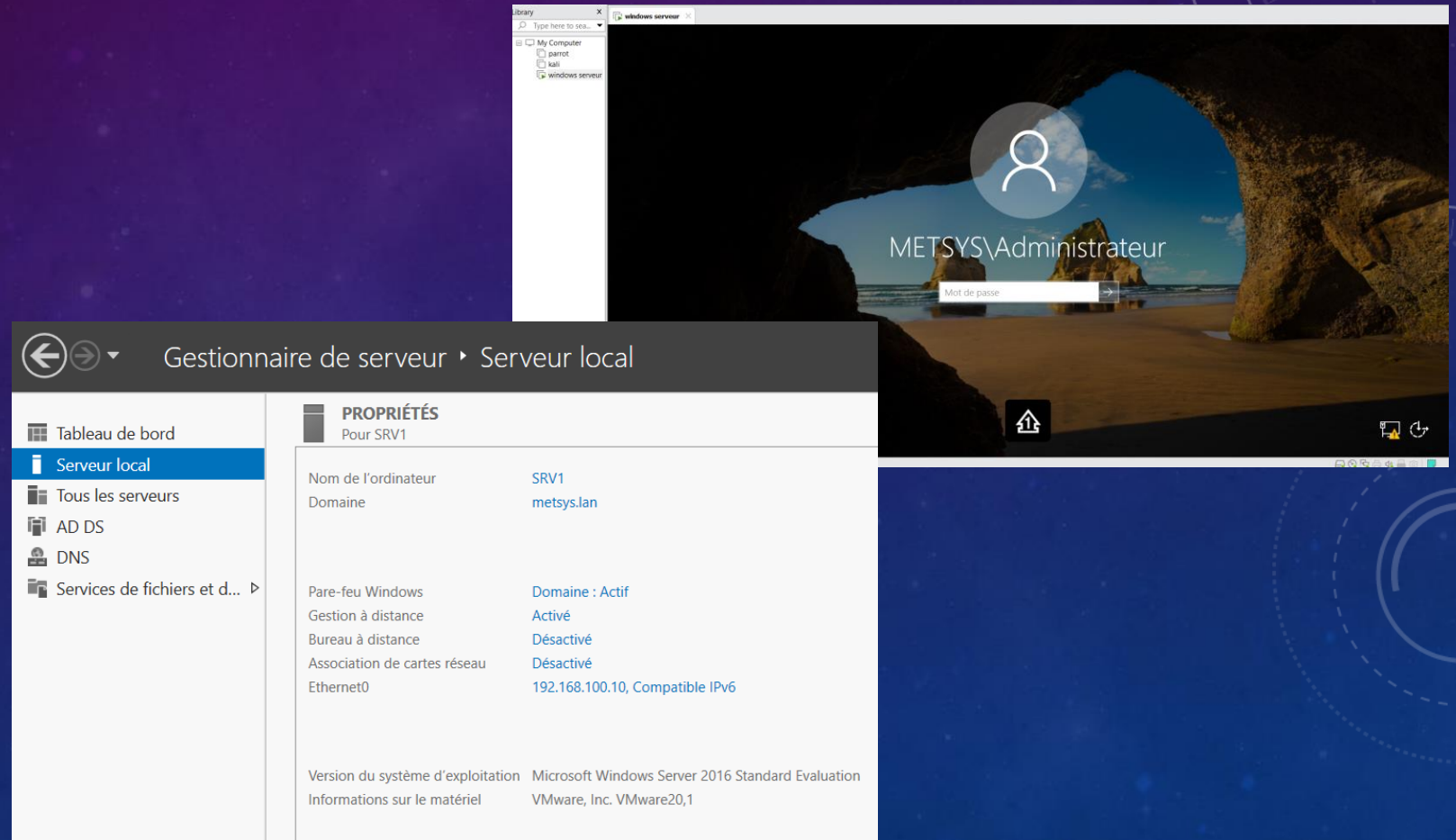
Suivant >

Installer

Annuler

1 - CREATION DU CONTROLLER DE DOMAINE

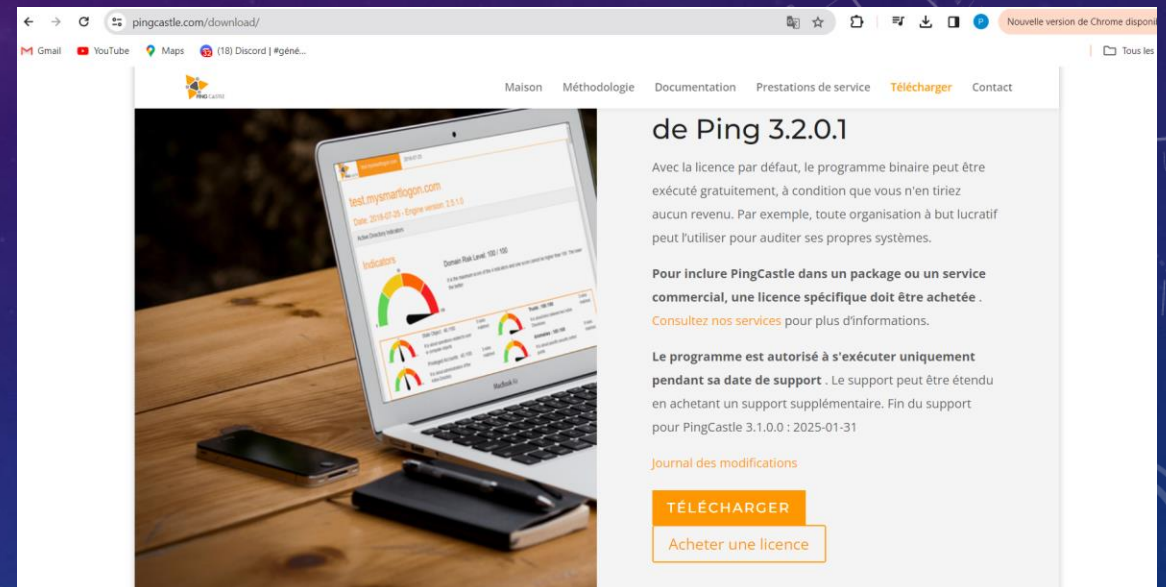
4 – Création du contrôleur de domaine



2 - INSTALLATION DE PINGCASTEL

PINGCASTEL est un outil qui va nous permettre d'auditer les annuaires AD :

pour améliorer la sécurité de l'annuaire AD,
générer un rapport complet qui indique un score qui reflète le niveau de risque de l'AD.



2 - CREATION DE L'AUDIT AVEC PINGCASTLE

J'ai lancé l'analyse de mon domaine
pour la création de l'audit

```
C:\Users\Administrateur\Desktop\PingCastle\PingCastle.exe
\\---0_---> PingCastle (Version 3.2.0.1 13/02/2024 22:23:43)
Get Active Directory Security at 80% in 20% of the time
End of support: 2025-07-31

Vincent LE TOUX (contact@pingcastle.com)
twitter: @mysmartlogon https://www.pingcastle.com

What do you want to do?
=====
Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
1-healthcheck-Score the risk of a domain
2-azuread -Score the risk of AzureAD
3-conso -Aggregate multiple reports into a single one
4-carto -Build a map of all interconnected domains
```

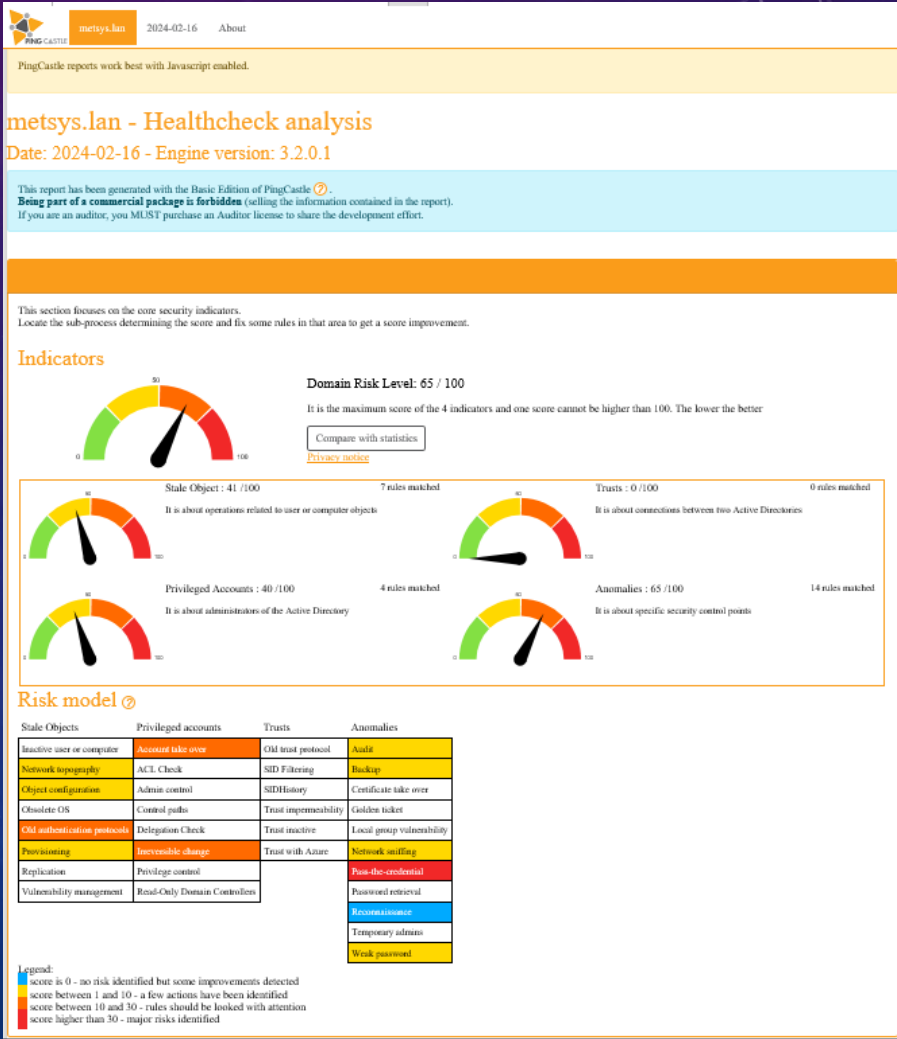
```
C:\Users\Administrateur\Desktop\PingCastle\PingCastle.exe

Free Edition of PingCastle 3.2.0 - Not for commercial use
Starting the task: Perform analysis for metsys.lan
[12:30:50] Getting domain information (metsys.lan)
[12:30:50] Gathering general data
[12:30:50] This domain contains approximatively 232 objects
[12:30:50] Gathering user data
[12:30:50] Gathering computer data
[12:30:50] Gathering trust data
[12:30:50] Gathering privileged group and permissions data
[12:30:50] - Initialize
[12:30:50] - Searching for critical and infrastructure objects
[12:30:51] - Collecting objects - Iteration 1
[12:30:51] - Collecting objects - Iteration 2
[12:30:51] - Collecting objects - Iteration 3
[12:30:51] - Collecting objects - Iteration 4
[12:30:51] - Collecting objects - Iteration 5
[12:30:51] - Completing object collection
[12:30:51] - Export completed
[12:30:51] Gathering delegation data
[12:30:51] Gathering gpo data
[12:30:51] Gathering pki data
[12:30:51] Gathering sccm data
[12:30:51] Gathering exchange data
[12:30:51] Gathering anomaly data
[12:30:51] Gathering dns data
[12:30:51] Gathering WSUS data
[12:30:51] Gathering MSOL data
[12:30:51] Gathering domain controller data (including null session) (including RPC tests)
```

it produces a report which will give you an overview of other domains by using the existing trust links.

2 - AUDIT AVEC PINGCASTEL

Il a généré l'audit
sur un fichier Html et xml
Et à détecter un risque de 65/100



3 - RISQUES DETECTES – AXES A AMELIORER

Les risques en rouge et orange sont élevés et doivent être traités en priorité.

Risk model ?

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust impermeability	Golden ticket
Old authentication protocols	Delegation Check	Trust inactive	Local group vulnerability
Provisioning	Irreversible change	Trust with Azure	Network sniffing
Replication	Privilege control		Pass-the-credential
Vulnerability management	Read-Only Domain Controllers		Password retrieval
			Reconnaissance
			Temporary admins
			Weak password

Legend:

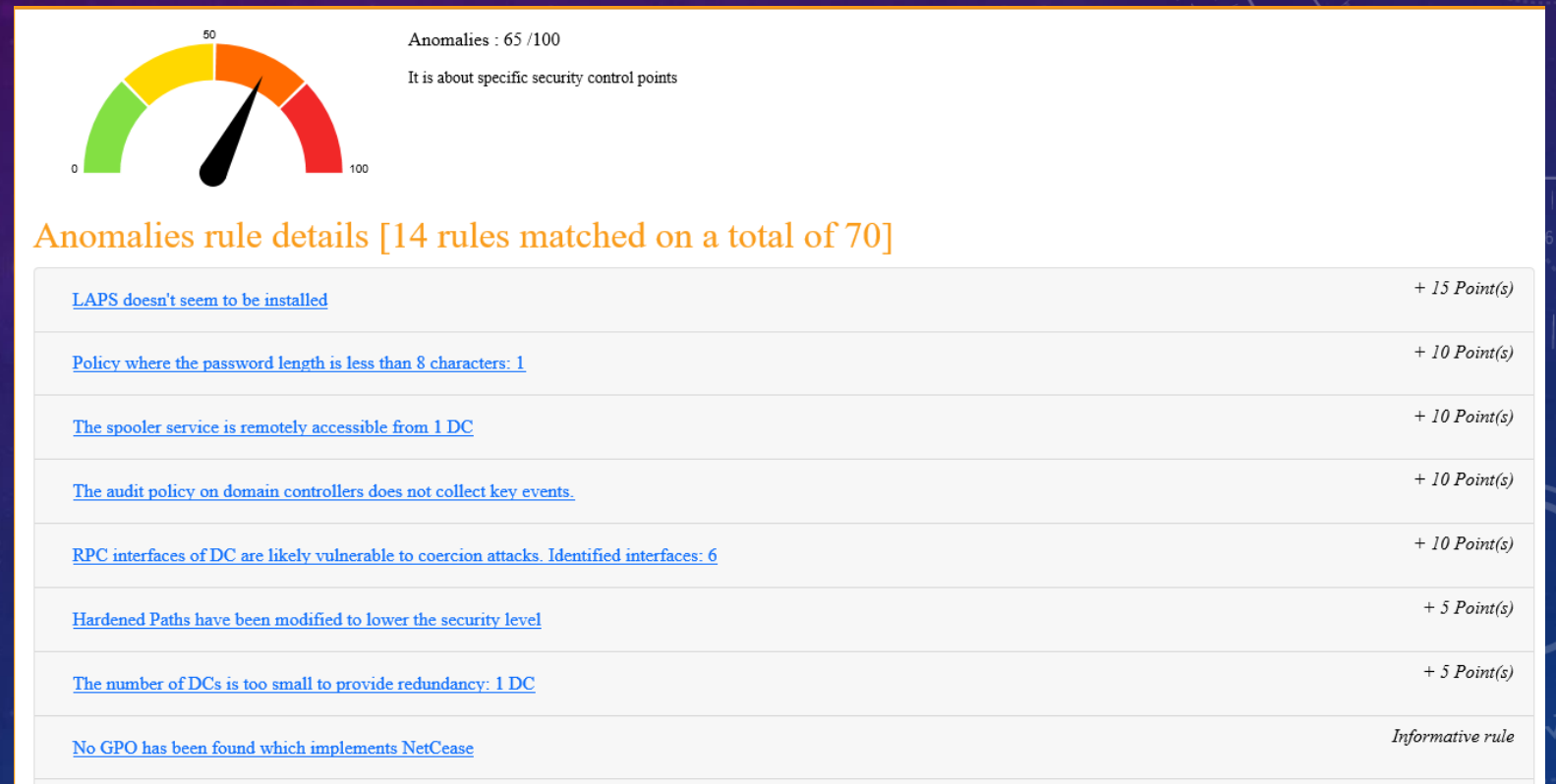
- score is 0 - no risk identified but some improvements detected
- score between 1 and 10 - a few actions have been identified
- score between 10 and 30 - rules should be looked with attention
- score higher than 30 - major risks identified

3 - RISQUES DETECTES - AXES A AMELIORER

Cela concerne les anomalies

Score de 65/100

En dessous les axes d'améliorations
à effectuer pour gagner des points
et remonter le score.



3 - RISQUES DETECTES - AXES A AMELIORER

Cela concerne les anomalies - suite

Score de 65/100

*En dessous les axes d'améliorations
à effectuer pour gagner des points
et remonter le score.*

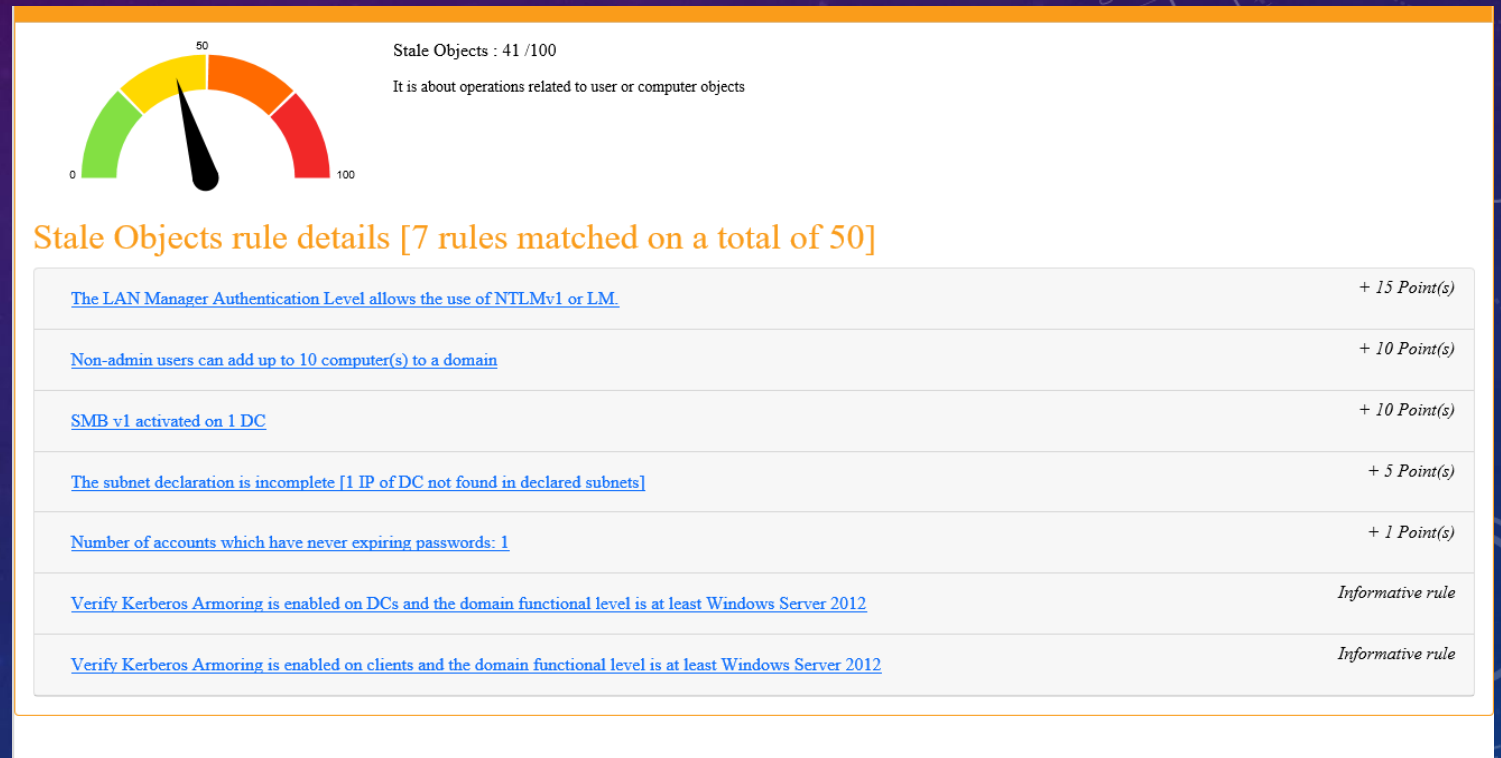
The PreWin2000 compatible group contains "Authenticated Users"	Informative rule
No GPO has been found which disables LLMNR or at least one GPO does enable it explicitly	Informative rule
DsHeuristics has not been set to enable the mitigation for CVE-2021-42291	Informative rule
Authenticated Users can create DNS records	Informative rule
No password policy for service accounts found (MinimumPasswordLength>=20)	Informative rule
The PowerShell audit configuration is not fully enabled.	Informative rule

3 - RISQUES DETECTES – AXES A AMELIORER

Cela concerne les objets, ordinateurs et utilisateurs

Score de 41/100

En dessous les axes d'améliorations à effectuer pour gagner des points et remonter le score.

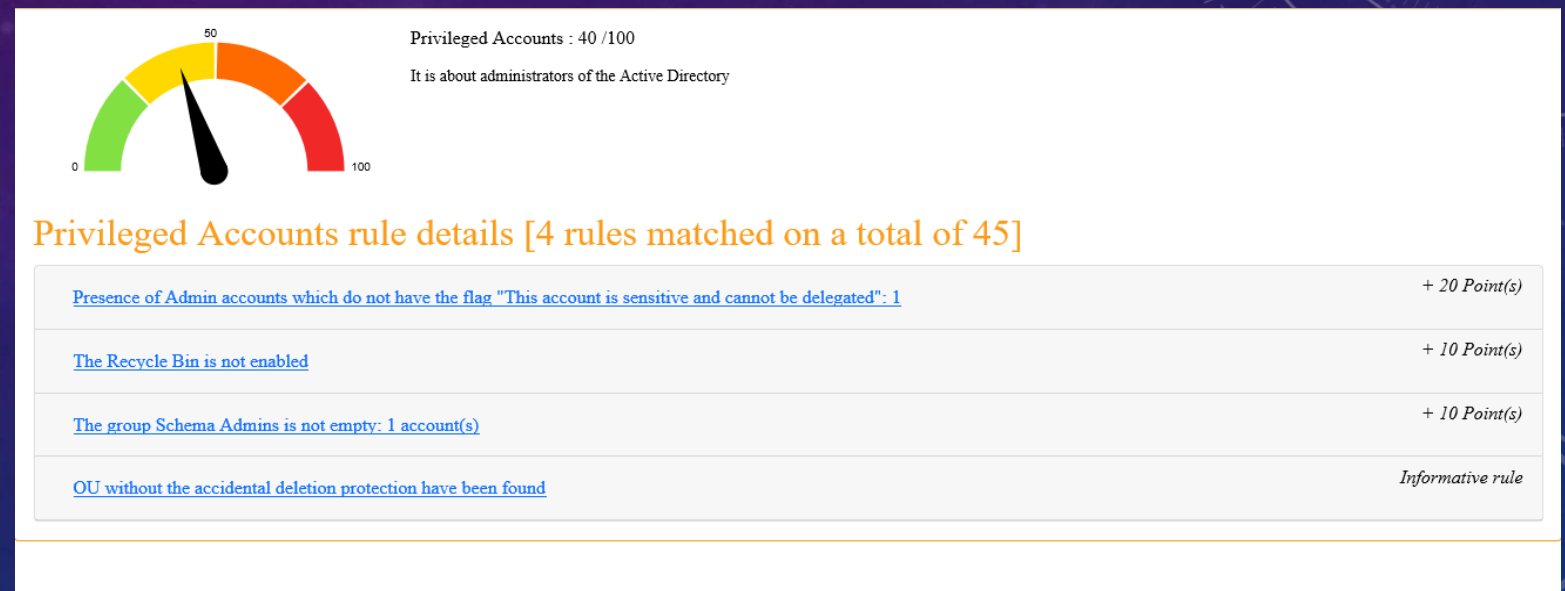


3 - RISQUES DETECTES - AXES A AMELIORER

Cela concerne les comptes
avec privilèges

Score de 40/100

*En dessous les axes d'améliorations
à effectuer pour gagner des points
et remonter le score.*



4 – PLAN POUR LES AMELIORATIONS DU SCORE

J'ai commencé par améliorer les anomalies qui affichaient un score de 65/100

1 - Vérification de la longueur du mdp dans la politique de mdp

J'ai mis 8 caractères à la place de 7 caractères

Vérifiez la longueur du mot de passe dans la politique de mot de passe

ID de règle :
A-MinPwdLen

Description:

Le but est de vérifier si la politique de mot de passe du domaine oblige les utilisateurs à avoir au moins 8 caractères dans leur mot de passe.

Explication technique :

Une vérification est effectuée pour identifier si le GPO concernant la politique de mot de passe autorise un mot de passe de moins de 8 caractères. Les mots de passe courts représentent un risque élevé car ils peuvent assez facilement être forcés ou pulvérisés. La plupart des CERT et des agences conseillent au moins 8 caractères (et souvent ce nombre va jusqu'à 12)

Solution conseillée :

Pour résoudre le problème, le meilleur moyen est soit de supprimer le mot de passe court d'activation du GPO, soit de le modifier afin d'augmenter la longueur du mot de passe à au moins 8 caractères.

Points:

10 points si présent

Documentation:

<https://www.microsoft.com/en-us/research/publication/password-guidance/>

[FR]ANSSI - Membres de groupes privilégiés avec une politique de mot de passe faible (vuln2_privileged_members_password) 2

[MITRE]Découverte de la politique de mot de passe T1201

Détails:

Le détail peut être trouvé dans [les politiques de mot de passe](#)

```
Administrateur : Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Tous droits réservés.

PS C:\Users\Administrateur> Get-ADDefaultDomainPasswordPolicy -Identity "metsys.lan"

ComplexityEnabled           : True
DistinguishedName           : DC=metsys,DC=lan
LockoutDuration              : 00:30:00
LockoutObservationWindow    : 00:30:00
LockoutThreshold             : 0
MaxPasswordAge               : 42,00:00:00
MinPasswordAge               : 1,00:00:00
MinPasswordLength            : 7
ObjectClass                  : {domainDNS}
ObjectGUID                   : 9d7258b2-8c7e-48ed-adb2-845fa7401183
PasswordHistoryCount         : 24
ReversibleEncryptionEnabled : False

PS C:\Users\Administrateur> gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

PS C:\Users\Administrateur> Get-ADDefaultDomainPasswordPolicy -Identity "metsys.lan"

ComplexityEnabled           : True
DistinguishedName           : DC=metsys,DC=lan
LockoutDuration              : 00:30:00
LockoutObservationWindow    : 00:30:00
LockoutThreshold             : 0
MaxPasswordAge               : 42,00:00:00
MinPasswordAge               : 1,00:00:00
MinPasswordLength            : 8
ObjectClass                  : {domainDNS}
ObjectGUID                   : 9d7258b2-8c7e-48ed-adb2-845fa7401183
PasswordHistoryCount         : 24
ReversibleEncryptionEnabled : False

PS C:\Users\Administrateur>
```

4 – PLAN POUR LES AMELIORATIONS DU SCORE

J'ai commencé par améliorer les anomalies qui affichaient un score de 65/100

2 – j'ai désactivé le service print spooler sur le contrôleur de domaine

Assurez-vous que le service Print Spooler ne peut pas être abusé pour obtenir les informations d'identification DC

ID de règle :
A-DC-Spooler

Description:

Le but est de garantir que les informations d'identification ne peuvent pas être extraites du DC via son service Print Spooler.

Explication technique :

Lorsqu'un compte avec une délégation sans contrainte est configuré (ce qui est assez courant) et que le service Print Spooler s'exécute sur un ordinateur, vous pouvez obtenir les informations d'identification de cet ordinateur envoyées au système avec une délégation sans contrainte en tant qu'utilisateur. Avec un contrôleur de domaine, le TGT du DC peut être extrait, permettant à un attaquant de le réutiliser avec une attaque DCSync, d'obtenir tous les hachages des utilisateurs et de se faire passer pour eux.

Solution conseillée :

Le service Print Spooler doit être désactivé sur les contrôleurs de domaine. Veuillez noter en conséquence que la fonctionnalité Printer Pruning (rarement utilisée) sera indisponible.

Points:

10 points si présent

Documentation:

<https://adsecurity.org/?p=4056>

<https://www.slideshare.net/harmj0y/derbycon-the-unintended-risks-of-trusting-active-directory>

[\[MITRE\]Authentification forcée T1187](#)

Détails:

Le détail peut être trouvé dans [Contrôleurs de domaine](#)

```
PS C:\Users\Administrateur> Set-Service -Name Spooler -StartupType Disabled
PS C:\Users\Administrateur>
```


4 – PLAN POUR LES AMELIORATIONS DU SCORE

J'ai commencé par améliorer les anomalies qui affichaient un score de 65/100

3 – J'ai identifié et corrigé les paramètres d'audit à appliquer

Vérifiez s'il existe la politique d'audit attendue sur les contrôleurs de domaine.

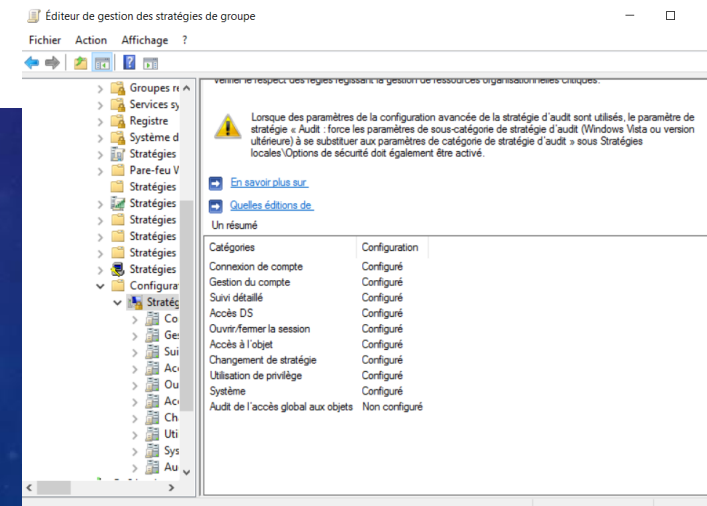
ID de règle :
A-AuditDC

Description:
L'objectif est de garantir que la politique d'audit sur les contrôleurs de domaine collecte le bon ensemble d'événements.

Explication technique :
Pour détecter et atténuer une attaque, le bon ensemble d'événements doit être collecté.
La politique d'audit est un compromis entre trop ou pas assez d'événements à collecter.
Pour résoudre ce problème, la politique d'audit suggérée par adsecurity.org est comparée à la politique d'audit en place.

Solution conseillée :
Identifiez les paramètres d'audit à appliquer et corrigez-les.
Sachez qu'il existe deux emplacements pour les paramètres d'audit.
Pour une configuration d'audit « simple » :
dans Configuration ordinateur -> Stratégies -> Paramètres Windows -> Paramètres de sécurité -> Stratégies locales -> Stratégies d'audit
Pour une configuration d'audit « Avancée » :
dans Configuration ordinateur -> Stratégies -> Paramètres Windows -> Paramètres de sécurité -> Configuration avancée de la politique d'audit
Assurez-vous également que le GPO d'audit est appliqué à tous les contrôleurs de domaine, car l'objet sous-jacent peut se trouver dans une unité d'organisation où le GPO n'est pas appliqué.

Points:
10 points si présent



5 – RAPPORT D'AUDIT APRES LES MODIFICATIONS

Suite aux modifications effectuées

Le nouvel audit indique un nouveau score de 45/100

L'audit a permis d'identifier et de remédier aux vulnérabilités majeures de l' Active Directory de metsys.lan.

Pingcastel a aidé au renforcement de la sécurité globale.

Recommandations pour le Suivi :

Planifier des audits réguliers avec PingCastle

Maintenir une sensibilisation continue à la sécurité informatique.

Documenter les changements apportés à l'Active Directory pour référence future.

