13/12/2023

AUDIT DE SECURITE

ACTIVE DIRECTORY / MYLAB

CONFIDENTIEL

Par
NICOLAS WAILLY

Fiche de suivi du document

Historique des modifications

Version	Date	Redacteur	Modicfication
1.0	13/12/2023	WAILLY Nicolas	Création du document
1.1	14/12/2023	WAILLY Nicolas	Correction

Liste de diffusion

Société	Service / Personne	Objet de la Diffusion

SOMMAIRE

01 PRESENTATION DE LA DEMARCHE

01.1 RAPPEL DU BESOIN

L'objectif de cet audit est d'évaluer les risques de l'Active Directory de MYLAB, par une démarche présentée ci-dessous. Pour chaque risques identifiés des recommandations seront effectuées afin de limiter le défaut et atteindre un niveau de sécurité acceptable.

01.2 PRESENTATION DE LA DEMARCHE

Démarche spécifique permettant l'évaluation de la sécurité de l'active directory :

1 CARTOGRAPHIE DE L'ACTIVE DIRECTORY
2 LISTE DES DIFFERENTS UTILISATEURS / UO / GROUPES
3 TEST D'INTRUSION / CHEMIN D'ATTAQUE POSSIBLE
4 ANALYSE DES RISQUES ET DES FAILLES POTENTIEL

La méthodologie de test d'intrusion se découpe en 4 phases :

- **Cartographie de l'Active Directory** : Cette première phase permet d'obtenir un premier niveau d'exposition de l'Active Directory. C'est un premier passage sur les potentiels manque de sécurité de celui-ci et permet d'adapter la suite de la démarche.
- **Listes des différents utilisateurs / UO / Groupes :** On complète ici la démarche initiale en venant analyser les parties prenantes de l'Active Directory. Cette étape à pour but de mettre en lumière une nouvelle fois des risques et des failles de l'organisation de celui-ci.
- **Test d'intrusion / Chemin d'attaque :** A l'aide de l'outil BloodHound, avec autorisation de Directeur du service informatique, nous allons analyser des chemins d'attaques possible pour prendre le contrôle, modifier ou endommager l'Active Directory.
- **Analyse des risques et des failles potentielles :** On termine par un contrôle plus large de l'active directory, par exemple l'utilisation des mots de passe, contrôle des sessions d'administration, autorisation Kerberos, etc.

01.3 OBJECTIFS VISES

La prestation de test d'intrusion a pour objectif de dresser un état des lieux de la sécurité d'un système d'information ou d'une application à un instant donné. L'objectif est de mettre en lumière les failles de sécurité réellement exploitables par un individu malveillant dans un temps volontairement limité.

01.4 MODE OPERATOIRE

Les tests d'intrusions et le contrôle de l'Active Directory à été réalisés du 05/12/2023 au 11/12/2023.

Afin de réalisés les tests les outils suivants ont été utilisés :

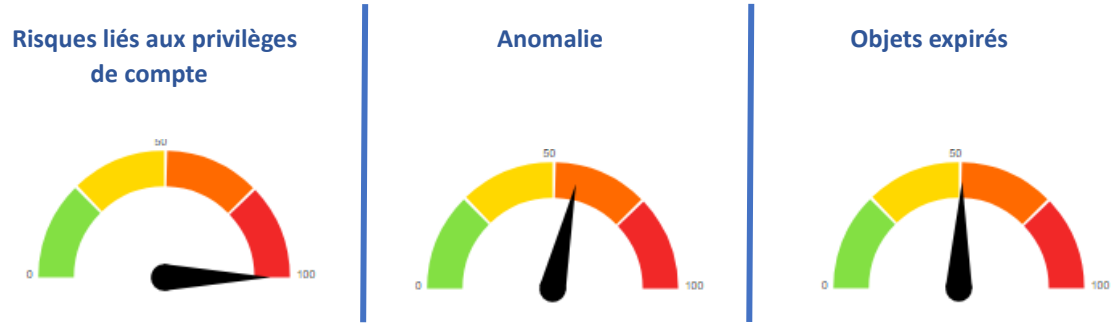
- BloodHound
- Ping Castle

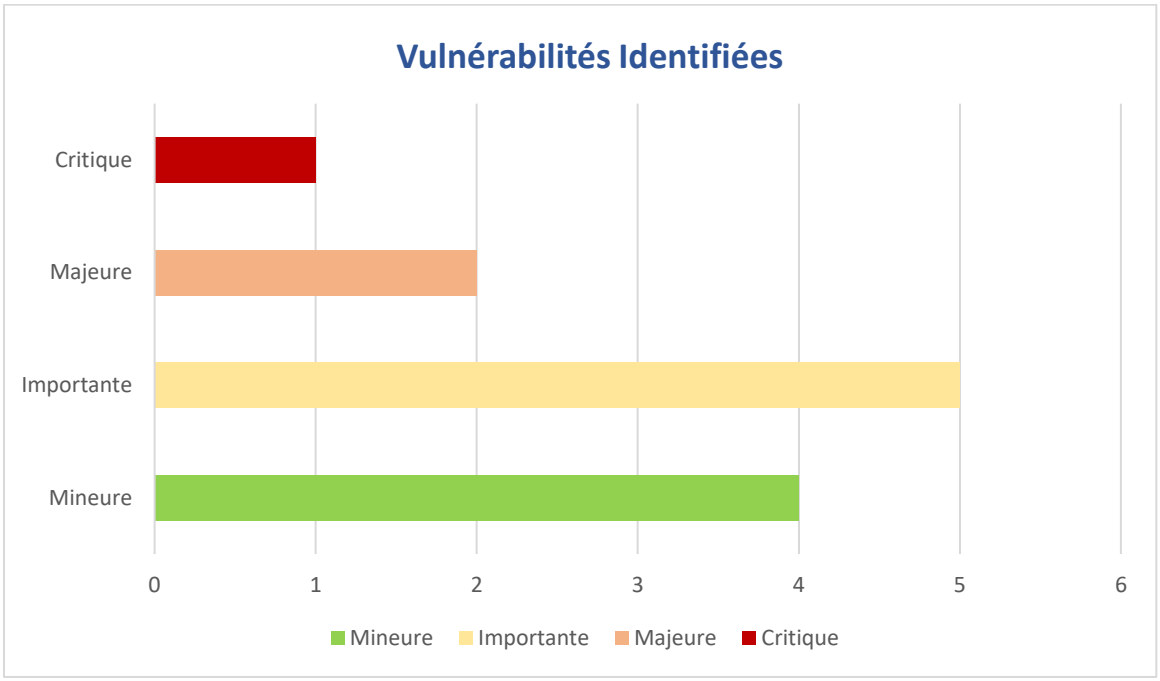
L'active directory étant accessible par la session administrateur de celui-ci.

01.5 EXHAUSTIVITE DES RESULTATS

Les résultats ont été réalisés sur une durée de test prédéfinie et limitée, cette démarche s'appuie sur une durée de test et n'a pas vocations à être exhaustive. Seuls les fonctionnalités accessibles lors de l'audit ont été analysées.

02 SYNTHESE MANAGERIALE





Les tests réalisés sur l'Active Directory MYLAB, ont permis de mettre en évidence **un niveau général de sécurité assez faible**. De nombreuses précautions de sécurités n'étant pas mises en place où appliquées.

Nous avons mis en évidence **l'absence de vérification des sessions disposant de droits administrateurs,** de nombreuses GPO qui ne sont pas appliquées et qui participe à sécuriser l'Active Directory, comme bannir les anciens protocole NTLMv1 ou LM. L'utilisation de la session administrateur native, de manière récurrente, 90% des sessions administrateurs sont inactives et au moins une session critique à son **mot de passe accessible en clair**.

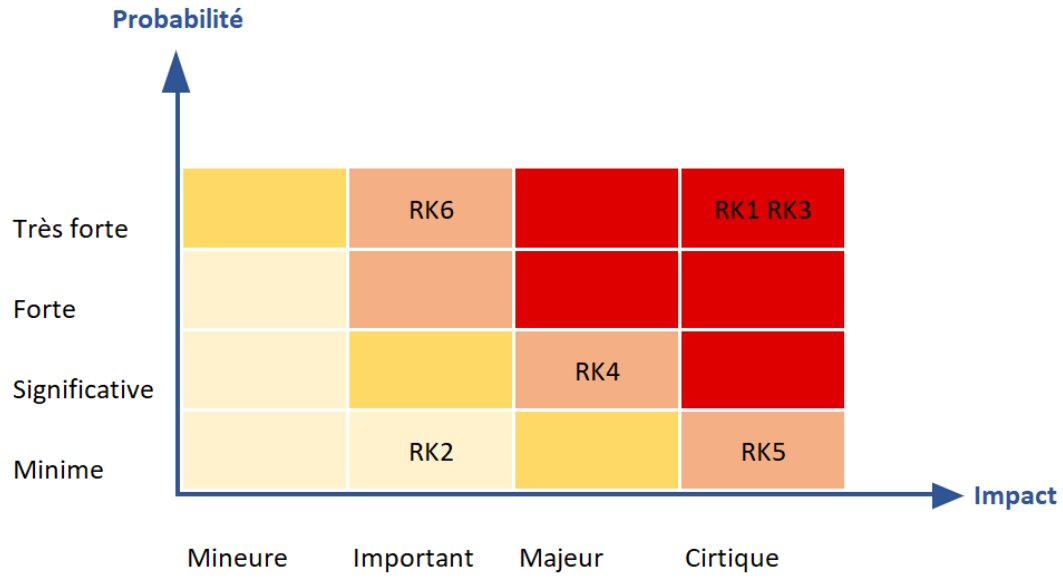
Un attaquant peut donc avoir des chemins d'attaque simple d'accès pour prendre le contrôle de l'Active Directory. Ils seront expliqués après dans la rubrique :

03 SYNTHESE DES RISQUES

Voici ci-dessous la liste des vulnérabilités identifiées :

Synthèse des risques

- **RK1 :** Un attaquant peut trouver une session avec des droits élevés sans mots de passe ou un mot de passe en clair.
- **RK2 :** Un utilisateurs à des informations récupérées par « print spooler » en absence de mesure prise contre.
- **RK3 :** L'active directory ne possède pas de back-up et un arrêt imprévu de celui-ci endommage les données.
- **RK4 :** Un attaquant accède à des données techniques et exploite des défauts dans les composants logiciels de l'environnement
- **RK5 :** Un utilisateur laisse fuiter des informations critiques
- **RK6 :** l'infrastructure et victime d'une campagne de ransomware ou de phishing



Cette matrice des risques pourra être adaptée vis-à-vis de votre éventuel référentiel interne de gestion des risques.

04 SYNTHESE DES VULNERABILITES IDENTIFEES

04.1 SYNTHESE TECHNIQUE

Les tests réalisé sur l'Active Directory MYLAB, ont permis de mettre en évidence plusieurs problèmes :

- **Au niveau de la sécurisation des sessions d'administrations :**
  - La majorité des sessions d'administrations sont inactives, ce qui constitue une zone de vulnérabilité, concerne 90% des sessions.
  - Les sessions administrateurs on leurs mots de passe qui n'expirent jamais. Au moins une session à son mot de passe disponible en clair dans sa description active directory.
  - Les sessions administrateurs n'ont pas de groupe spécifique « protect users ».

- **Au niveau des sauvegardes de « back-up » :**
  - L'active directory et la machine Windows serveur, ne disposent pas d'une session de back-up qui permettrait la récupération de la base de données en cas d'une coupure par exemple qui endommagerai la celle-ci.

- **Au niveau des GPO ou des fonctionnalités :**
  - Nous avons constaté qu'aucune politique n'est mise en place pour définir une longueur minimale aux mots de passe, ce qui pourrait facilité une attaque par « brut force » sur ces mots de passe.
  - Aucune session administrateur ne présente une mention « ne peut pas être délégués ».
  - La possibilité d'utiliser le print spooler n'est pas désactivé nativement dans l'AD, ce qui pourrait permettre de récupérer des documents dans la liste d'impression, ou dans les suppressions d'impressions.
  - Dans la même problématique que précédemment, aucune mesure n'est prise pour supprimer automatiquement la corbeille de la machine Windows server de l'active directory, ce qui permettrait de récupérer des documents dans celle-ci.

04.2 LISTES DES VULNERABILITES IDENTIFIEES

ID	DESCRIPTION	RISQUE AVERE	PERIMETRE	CVSS
V3	L'Active Directory est vulnérable à une attaque par brut force ou à une intrusion extérieure	Oui	MYLAB	4.5
V2	Aucune sauvegarde n'est mise en place sur l'AD	Oui	MYLAB	4.3
V1	Le print spooler ou la récupération via la corbeille est possible	Oui	MYLAB	3.2

04.3 SYNTHESE DES REMARQUES

ID	DESCRIPTION	PERIMETRE
R1	La politique de mot de passe pourrait être amélioré	MYLAB
R2	Les GPO pourrait être améliorés	MYLAB

05 SYNTHESE DES MESURES CORRECTIVES

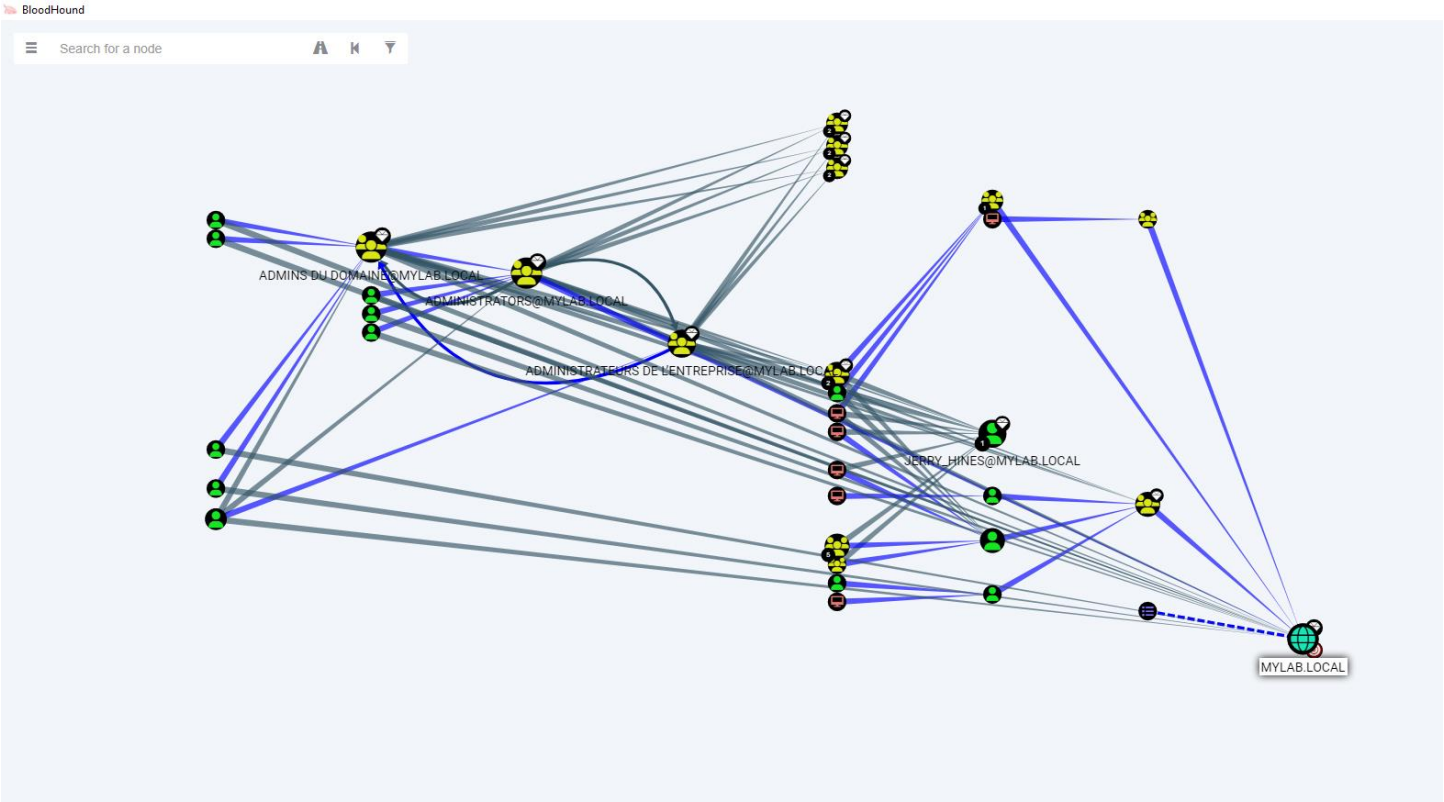
ID	DESCRIPTION	COMPLEXITE DE MISE EN ŒUVRE	VULNERABILITE ASSOCIEES	PERIMETRE	PRIORITE
C1	Limiter les sessions administrateurs et supprimer les mots de passe des descriptions de compte	Faible	V3	MYLAB	1
C2	Réaliser des sauvegardes de back-up	Moyenne	V2	MYLAB	1
C3	Modifier ou ajouter des GPO et des règles pour sécuriser l'AD	Moyenne	V1	MYLAB	2

Priorité 1 : Action à mettre en œuvre à court terme, corrigeant des faiblesses majeures
Priorité 2 : Action à mettre en œuvre à moyen terme, corrigeant des faiblesses non négligeables
Priorité 3 : Action pouvant être mise en œuvre à plus long terme pour accroître le niveau de sécurité

06 TEST ET CHEMINS D'INTRUSION

06.1 Les chemins d'attaques

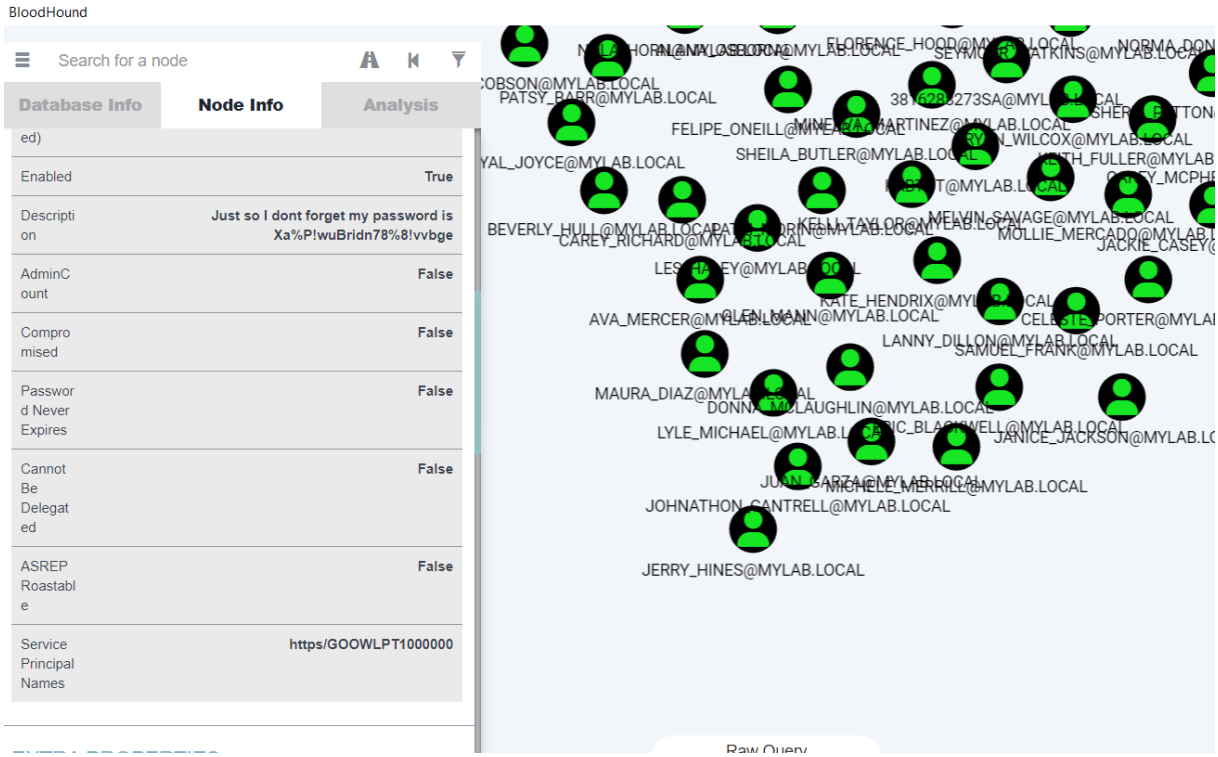
On se sert pour définir des chemins d'attaques possibles de notre Active Directory, de l'outil BloodHound, qui va établir le chemin le plus court pour prendre le contrôle de notre AD.



Solution à apporter : établir des accès qui seraient plus restreins, réduire les sessions ou les machines pouvant accéder à l'AD, mettre en place une politique renforcée de mots de passe sur les sessions critiques.

R1	L'attaquant dispose de plusieurs chemins d'attaque possible
	Lors de notre test d'intrusion on a établi que plusieurs chemins d'attaques étaient possibles, certains plus complexe que d'autres.
	Périmètre concerné : MYLAB

06.2 Risques relatifs aux accès à des secrets d'authentification(3.3) :



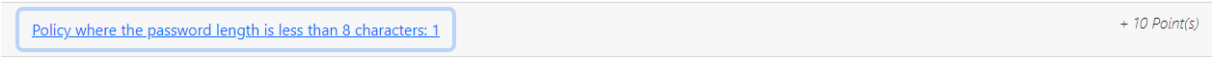
Dans le test précédent on peut voir l'utilisateur « JERRY HINES », cet utilisateur remonte avec son mot de passe notée en clair en description.

Solution à apporter : Faire une communication générale sur les bonnes pratiques en matière de mot de passe. Appeler à la responsabilité des utilisateurs, supprimer les mots de passe de la description. Utiliser un gestionnaire de mot de passe.

R1	L'utilisateur ne respecte pas la politique de mot de passe
	Au moins un utilisateur, ne respecte pas la politique de sécurité des mots de passe.
	Périmètre concerné : MYLAB

06.3 Active Directory vulnérable à une attaque par brut force

Lors d'une analyse réalisée par Pingcastle, il est remonté que l'AD ne présente pas de GPO qui force l'utilisation d'un mot de passe fort ou d'un minimum de 8 caractères. Ce qui pourrait faciliter une attaque par brut force et une intrusion dans l'infrastructure.



<table>
<tr><td rowspan="4">V3

Important

CVSS 4.5</td><td colspan="3">L'Active Directory est vulnérable à une attaque par brut force ou à une intrusion extérieure</td></tr>
<tr><td colspan="3"><u>Vulnérabilité :</u>
Lors de nos tests il est apparu qu'aucune politique n'est mise en place pour le contrôle des mots de passe.
Il n'y a pas de demande de renouvellement de mot de passe ou de politique en matière de la sécurité de celui-ci (confidentialité, non divulgation, changement mensuels)

<u>Recommandation :</u>
Nous recommandons la mise en place d'une politique de mot de passe plus poussé, avec sensibilisation du personnel aux bonnes pratiques en matière de mots de passe.</td></tr>
<tr><td colspan="3"><u>Mesures associées :</u> Limiter les sessions administrateurs et supprimer les mots de passe des descriptions de compte

<u>Périmètre concernés :</u> MYLAB</td></tr>
<tr><td>Impact</td><td>Difficulté d'exploitation</td><td>Risque avéré</td></tr>
<tr><td>Important</td><td>Faible</td><td>Oui</td></tr>
</table>

06.4 Les sauvegardes de secours

<table>
<tr><td rowspan="4">V3

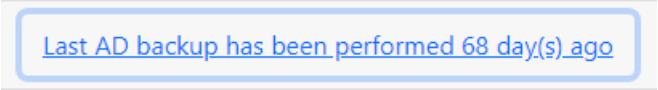
Important

CVSS
4.3</td><td colspan="3">Aucune sauvegarde n'est mise en place sur l'AD</td></tr>
<tr><td colspan="3"><u>Vulnérabilité :</u>
L'active directory ne dispose d'aucune sauvegarde de back-up et d'aucun logiciel permettait de faire une restauration de la base de données en cas de besoin.

<u>Recommandation :</u>
Nous recommandons la mise en place d'un logiciel de Back-up type Veam par exemple.</td></tr>
<tr><td colspan="3"><u>Mesures associées :</u> Modifier ou ajouter des GPO et des règles pour sécuriser l'AD

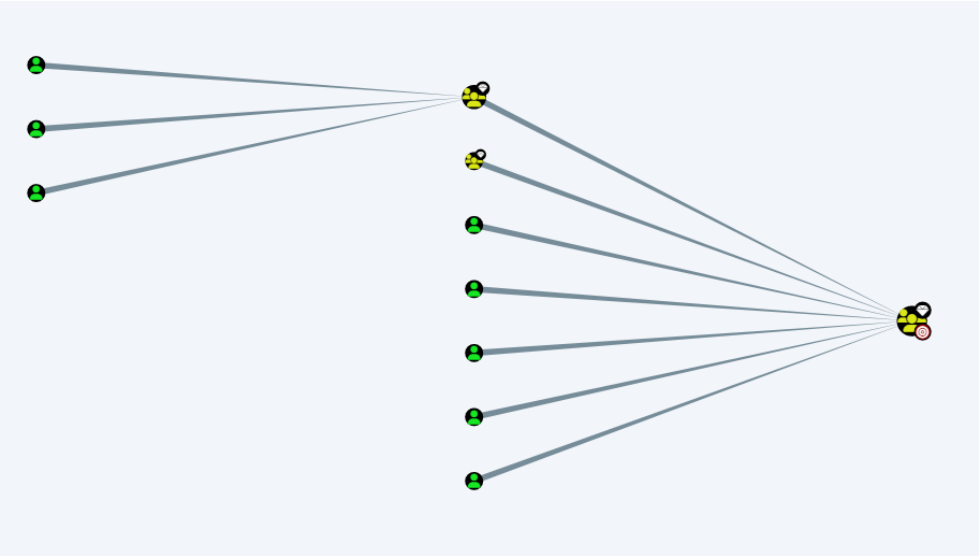
<u>Périmètre concernés :</u> MYLAB</td></tr>
<tr><td>Impact</td><td>Difficulté d'exploitation</td><td>Risque avéré</td></tr>
<tr><td>Important</td><td>Important</td><td>Oui</td></tr>
</table>

La session Windows serveur n'a pas de sauvegarde de mis en place depuis sa création. Si les données venaient à être perdu aucune solution n'est disponible pour les récupérer. Comme montré ci-après aucune sauvegarde depuis l'installation de la machine.

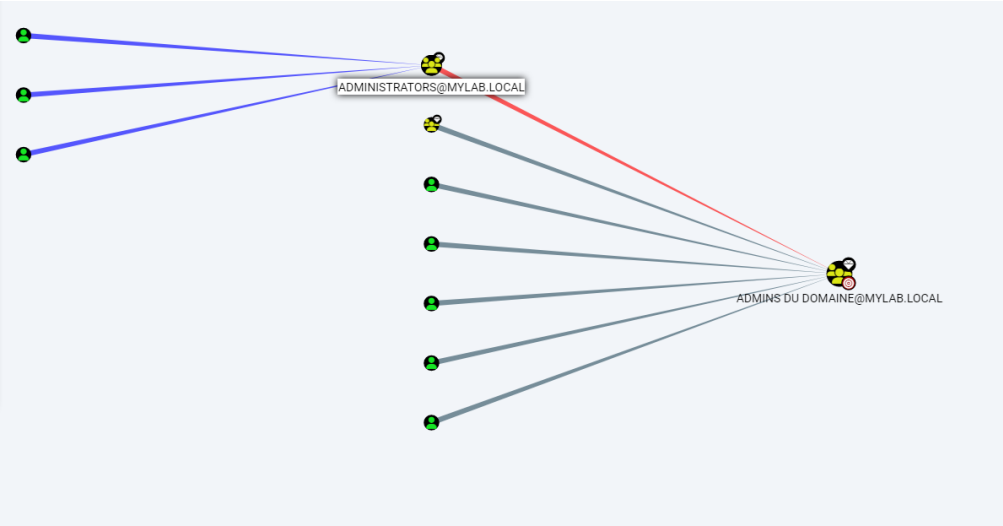


06.5 Principales sources d'attaques d'administrateurs du domaine

Lors de test il est remonté que de nombreux points d'attaques sont identifiés pour prendre le contrôle du domaine AD.



Ces points d'attaques sont des utilisateurs avec des mots de passe qui n'expire jamais et sans politique de mot de passe fort pour ses sessions à risques, ce qui fait écho aux points précédents. Ils sont pour la plupart inactif ou des sessions plus utilisées.



Pour les membres du groupe administrateur, aucun ne sont membre d'un groupe spécifique « protect users » et 1 n'a pas la reconnaissance administrateur sur son profil AD.

Solution à apporter : ajout de GPO et contrôle plus strict des droits et des sessions admin.

06.6 Mise en place de GPO

<table>
<tr><td rowspan="4">V1

Important

CVSS
4.3</td><td colspan="3">Le print spooler ou la récupération via la corbeille est possible</td></tr>
<tr><td colspan="3"><u>Vulnérabilité :</u>
L'active directory ne dispose d'une GPO pour sécuriser les impressions, supprimer les fils d'impression ou les données envoyées dans la corbeille

<u>Recommandation :</u>
Nous recommandons la mise en place de GPO permettant de supprimer automatiquement les contenus de la liste d'impression ou de la corbeille.</td></tr>
<tr><td colspan="3"><u>Mesures associées :</u> Réaliser des sauvegardes de back-up

<u>Périmètre concernés :</u> MYLAB</td></tr>
<tr><td>Impact</td><td>Difficulté d'exploitation</td><td>Risque avéré</td></tr>
<tr><td>Faible</td><td>Faible</td><td>Oui</td></tr>
</table>

07 DETAIL DES MESURES CORRECTIVES

C1

Limiter les sessions administrateurs et supprimer les mots de passe des descriptions

Vulnérabilité :
Nous avons constaté qu'aucune politique de mots de passe n'est mise en place sur les sessions administrateurs de l'AD, pas de longueur de mot de passe minimale, ou de renouvellement de mot de passe.

Recommandation :
Nous recommandons la mise en place d'une politique de mot de passe plus poussée, avec sensibilisation du personnel aux bonnes pratiques en matière de mot de passe.

Il est possible de mettre en place une GPO pour que les mots de passe ne fassent pas moins de 8 caractères par exemple, au moins sur les sessions administrateurs.

Il est également conseillé d'utiliser un coffre-fort de mot de passe sécuriser héberger en interne comme Bitwarden (gratuit) ou bastion (payant).

Coût/Charge : Faible

Vulnérabilité : V3

Périmètre concernés : MYLAB

Complexité de mise en œuvre	Gain en sécurité	Impact de la correction
Faible	Modéré	intégrité

C2

Réaliser des sauvegardes de back-up

Vulnérabilité :
L'active directory ne dispose d'aucune sauvegarde de back-up et d'aucun logiciel permettait de faire une restauration de la base de données en cas de besoin.

Recommandation :
Nous recommandons la mise en place d'un logiciel de Back-up type Veam par exemple.

Veam dispose d'une version gratuite, pour faire des sauvegardes du PC qui héberge le Windows server par exemple ou d'une version payante.

Coût/Charge : Modéré

Vulnérabilité : V2

Périmètre concernés : MYLAB

Complexité de mise en œuvre	Gain en sécurité	Impact de la correction
Modéré	**Fort**	intégrité

<table>
<tr><td rowspan="4">C2</td><td colspan="3">Modifier ou ajouter des GPO et des règles pour sécuriser l'AD</td></tr>
<tr><td colspan="3"><u>Vulnérabilité :</u>
L'Active Directory ne dispose d'une GPO pour sécuriser les impressions, supprimer les fils d'impression ou les données envoyées dans la corbeille

<u>Recommandation :</u>
Nous recommandons la mise en place de GPO permettant de supprimer automatiquement les contenus de la liste d'impression ou de la corbeille.</td></tr>
<tr><td colspan="3"><u>Coût/Charge :</u> Faible

<u>Vulnérabilité :</u> V1

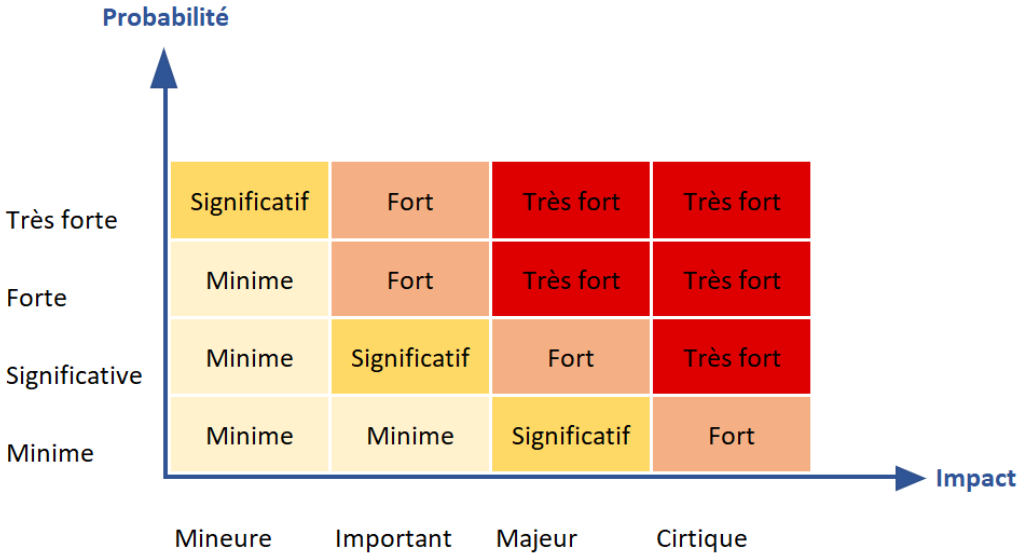
<u>Périmètre concernés :</u> MYLAB</td></tr>
<tr><td>Complexité de mise en œuvre</td><td>Gain en sécurité</td><td>Impact de la correction</td></tr>
<tr><td>Faible</td><td>Faible</td><td>intégrité</td></tr>
</table>

08 ANNEXES

08.1 échelles des risques

Les scénarios de risques sont évalués selon les échelles suivantes :

- Les impacts (sur une échelle de 1 à 4)
- Les probabilités d'occurrence du risque associé.



Pour une approche risques, la dimension probabilité est appréciée selon l'échelle suivante

- **Minime :** Le risque résulte d'une attaque complexe, difficile à réaliser ou ne permettant pas d'obtenir d'informations sensibles. Les conditions préalables à la réalisation de ce mode opératoire sont très difficilement réunies par la source de la menace. La motivation de la source pour mener l'attaque reste faible.
- **Significatif :** Le risque résulte d'une vulnérabilité exploitable mais complexe. Elle est exploitée par une source motivée disposant d'informations confidentielles ou profitant de complicité interne. La probabilité de survenance est significative.
- **Forte :** La risque résulte de l'exploitation d'une vulnérabilité connue qui peut être complexe. Un minimum de connaissances de l'application est requis pour conduire l'attaque mais l'attractivité du gain est forte. Elle a une forte probabilité de se produire.
- **Très forte :** Le risque surviendra si aucune mesure de sécurité n'est prise. Les vulnérabilités associées sont triviales et ne nécessitent pas forcement d'authentification préalable.

08.2 ECHELLES DE CLASSIFICATION DES MESURES CORRECTIVES

Pour chaque mesure, les critères suivants sont évalués :

• Indication de complexité :

- Action de complexité élevée nécessitant de nombreuses interactions entre les équipes et une prise de décision de la part du management.
- Action de complexité moyenne nécessitant des interactions entre les équipes.
- Action de complexité faible pouvant être menée de manière autonome par l'équipe en charge.

• Indication de coûts et de charge, à définir en fonction du contexte client :

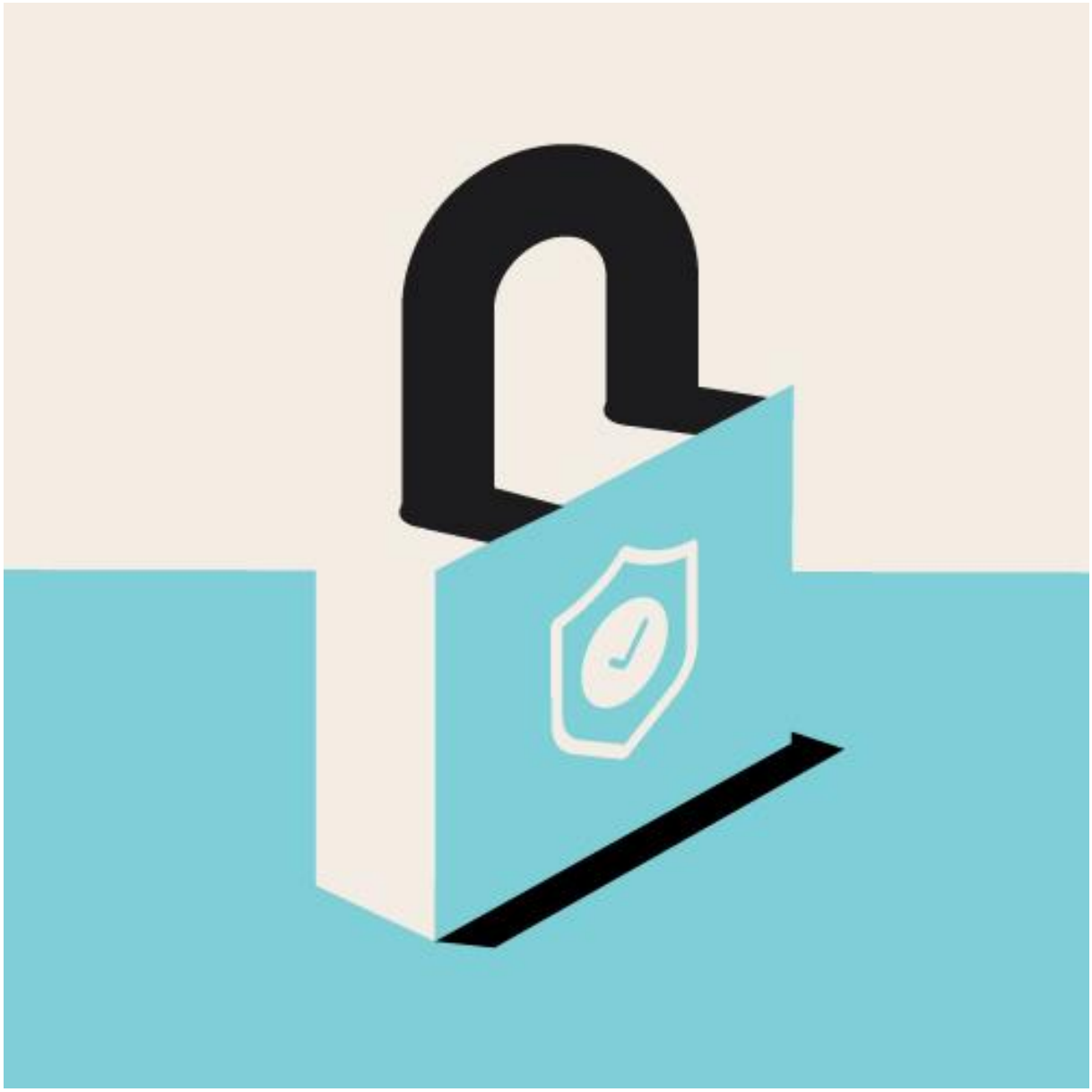
- Coût important.
- Coût modéré
- Coût faible.

• Indication de gain en sécurité par rapport à l'état des lieux, une fois l'action complètement terminée :

- Gain important (contribue de manière importante à la réduction des risques).
- Gain modéré (contribue correctement à la réduction des risques).
- Gain faible (contribue peu à la réduction des risques).

• Les mesures sont classées par priorité :

- Priorité 1 : action court terme, à mettre en place rapidement.
- Priorité 2 : action à mettre en œuvre à moyen terme, corrigeant des faiblesses non négligeables.
- Priorité 3 : action pouvant être mise en œuvre à plus long terme pour accroître le niveau de sécurité.



Par WAILLY Nicolas

@ : nicolaswailly7@gmail.com

Tel : 00 00 00 00 00