

CLOUD.TAAF.INTERNAL

AUDIT DE SECURITÉ

ALAMELOU
ROHAN



1. Introduction.....	2
Objectifs de l'audit :.....	2
1.2 Contexte et Périmètre.....	2
1.3 Limites.....	3
2. Résumé Exécutif (Management Summary).....	3
2.1 Synthèse globale.....	3
2.2 Score de sécurité :.....	3
3. Méthodologie et Outils.....	4
4. Résultats de l'Audit (Vulnérabilités et mauvaises configurations).....	4
4.1 Absence de LAPS (Local Administrator Password Solution).....	4
4.2 Sauvegarde Active Directory obsolète (> 100 jours).....	6
4.3 Print Spooler actif sur un DC.....	7
4.4 Politique d'audit insuffisante sur les contrôleurs de domaine.....	9
4.5 Politique de mots de passe insuffisante (< 8 caractères).....	10
4.6 Absence de redondance des contrôleurs de domaine.....	11
4.7 Analyse des comptes utilisateurs (User Information).....	12
4.8 Analyse des comptes ordinateurs (Computer Information).....	14
5. Plan d>Action, synthèse des recommandations (Roadmap).....	15
5.1 Échelle de criticité des vulnérabilités.....	15
5.2 Synthèse des vulnérabilités :.....	16
6. Conclusion.....	17
6.1 Actions à mener après l'audit.....	17
6.2 Conclusion synthétique.....	18

1. Introduction

Cet audit constitue une **évaluation méthodique** et indépendante du système d'information. Il s'agit d'un état des lieux de la sécurité à un **instant T**, visant à vérifier la conformité par rapport aux bonnes pratiques de l'ANSSI et de Microsoft.

L'Active Directory est la **clé de voûte du système d'information**. Sa compromission équivaut souvent à une **compromission totale du réseau**. La plupart des attaques modernes (Ransomware) ciblent l'AD pour se propager.

Objectifs de l'audit :

- Identifier les vulnérabilités techniques et organisationnelles.
- Mesurer l'efficacité des mesures de sécurité déjà en place.
- Recommander un plan d'actions correctives priorisé.

Cet audit s'inscrit dans une démarche de mise en conformité. L'objectif est d'identifier les défauts de configuration et d'hygiène pouvant être exploités par des attaquants (Ransomware, vol de données).

Cet audit a été réalisé dans le strict respect de la confidentialité et du périmètre défini. Bien qu'il s'agisse d'un exercice, il s'inscrit dans la logique d'une intervention couverte par une **Lettre de Mission**, garantissant l'autorisation d'accès aux systèmes et la non-divulgation des données sensibles

1.2 Contexte et Périmètre

Cet audit s'inscrit dans une démarche de **mise en conformité**. L'objectif est d'identifier les défauts de configuration et d'hygiène pouvant être exploités par des attaquants (Ransomware, vol de données).

L'audit couvre les éléments suivants :

- **Domaine audité :** taaf.internal
- **Infrastructure :** Contrôleurs de domaine de taaf.internal

1.3 Limites

Il est important de noter les limites intrinsèques à cet exercice, pas de garantie à 100% et cet audit est une photographie à un instant T.

Ce n'est pas un Pentest complet, il s'agit d'une analyse de configuration et non d'une tentative d'exploitation active et l'audit technique ne couvre pas les failles liées à l'ingénierie sociale.

Ce qui est exclu de cet audit sont les tests d'intrusion offensive (Pentest), l'ingénierie sociale, la sécurité physique des serveurs et l'audit des applications tierces.

2. Méthodologie et Outils

Conformément aux standards d'audit, notre approche a suivi les 5 phases clés:

- i. **Préparation :** Cadrage du périmètre et choix des référentiels.
- ii. **Collecte :** Récupération de l'état des lieux via l'outil PingCastle.
- iii. **Analyse :** Évaluation technique des écarts de configuration.
- iv. **Évaluation :** Qualification des risques selon leur impact et leur probabilité.
- v. **Reporting :** Rédaction du présent rapport et du plan d'action.

L'audit a été réalisé à l'aide de **PingCastle (version 3.3.0.1)**, un outil reconnu par l'industrie pour l'évaluation de la sécurité Active Directory. Il base son analyse sur un référentiel de règles (Healthcheck) couvrant les aspects d'architecture, de priviléges et d'anomalies.

L'analyse s'appuie sur les recommandations de :

- L'ANSSI (Guide d'hygiène informatique).
- Microsoft (Best Practices Analyzer).
- MITRE ATT&CK (Référentiel des tactiques d'attaque).
- ISO 27000

Afin de cibler les contrôles les plus pertinents, nous avons considéré les menaces de type **STRIDE** pesant sur l'Active Directory, notamment :

- **Élévation de privilèges :** Prise de contrôle d'un compte admin.
- **Divulgation d'informations (Information Disclosure) :** Accès au contenu de l'annuaire par des utilisateurs non autorisés.

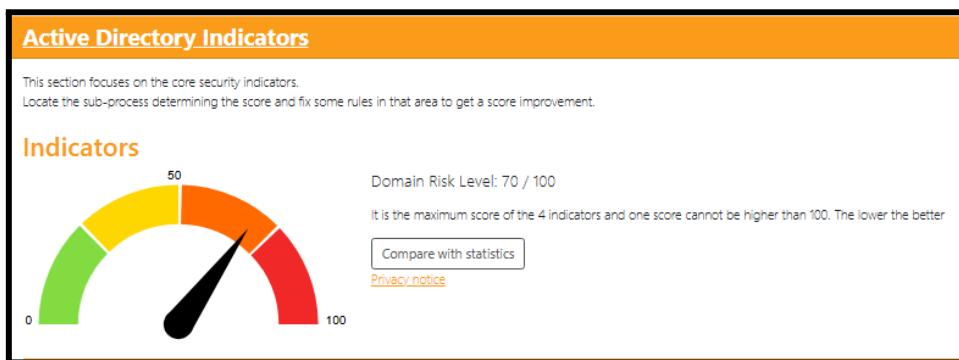
3. Résumé Exécutif (Management Summary)

3.1 Synthèse globale

L'audit de sécurité réalisé sur le domaine **taaf.internal** a permis d'évaluer le niveau de robustesse de l'annuaire Active Directory. L'analyse met en évidence un niveau de sécurité global **faible** par rapport aux standards de l'ANSSI et de Microsoft.

3.2 Score de sécurité :

L'outil d'audit a attribué un score de risque de **70/100** (où 0 est le meilleur et 100 le pire). Ce score indique que l'infrastructure est actuellement exposée à des risques **élevés**.



Les vulnérabilités suivantes nécessitent une attention immédiate :

- **L'absence de LAPS**
- **L'absence de sauvegardes récentes de l'Active Directory**
- **Le maintien du service Print Spooler actif sur un contrôleur de domaine**

Ces vulnérabilités exposent l'organisation à un risque élevé d'arrêt de production par Ransomware et de vol de données confidentielles.

L'Active Directory, étant la clé de voûte du système d'information, nécessite un plan de durcissement **immédiat et progressif**. Les faiblesses identifiées permettent potentiellement à un attaquant présent sur le réseau de compromettre l'ensemble du domaine en **quelques heures**.

3.3 Score de sécurité :

Gravité				
1				
2				
3				
4			X	
	1	2	3	4
	Vraisemblance			

- La **vraisemblance** correspond à la probabilité que la **vulnérabilité** soit **réellement exploitée**.
- La **gravité** correspond aux **conséquences si la vulnérabilité est exploitée**.

La vraisemblance a été évaluée en fonction de la facilité d'exploitation et du contexte Active Directory observé lors de l'audit. La gravité correspond à l'impact potentiel sur la confidentialité, l'intégrité et la disponibilité du système d'information. La combinaison de ces deux critères permet de déterminer le niveau de risque et la priorité de traitement.

4.Résultats de l'Audit (Vulnérabilités et mauvaises configurations)

4.1 Absence de LAPS (Local Administrator Password Solution)

L'audit de sécurité de l'Active Directory met en évidence l'absence de déploiement de la solution **Local Administrator Password Solution (LAPS)**. Cette solution vise à assurer une gestion centralisée et sécurisée des mots de passe des comptes administrateurs locaux des postes et serveurs membres du domaine. En l'absence de LAPS, ces mots de passe sont généralement identiques ou peu différenciés entre les machines, et leur cycle de vie n'est pas maîtrisé. Cette situation constitue une faiblesse majeure d'hygiène de sécurité, fréquemment exploitée lors d'attaques ciblant les environnements Active Directory.

[LAPS doesn't seem to be installed](#)

+ 15 Point(s)

Problème :

L'analyse met en évidence que la solution LAPS n'est pas déployée sur le domaine Active Directory. Cela signifie que les mots de passe des comptes administrateurs locaux des postes ne sont ni uniques ni gérés de manière centralisée.

Risque

En l'absence de LAPS, la compromission d'un seul poste de travail permet à un attaquant de réutiliser le mot de passe administrateur local sur d'autres machines. Ce scénario est fréquemment exploité lors des phases de mouvement latéral.

Impact

Cette faiblesse peut conduire à une élévation de privilèges rapide, puis à une compromission complète du domaine Active Directory. Elle facilite notamment la propagation de ransomwares à l'échelle du SI.

Scénario d'attaque plausible

Un attaquant obtient un accès initial à un poste utilisateur via un hameçonnage ou un logiciel malveillant. Le mot de passe administrateur local étant identique sur plusieurs machines, il peut se connecter avec des privilèges élevés sur d'autres postes du domaine. Cette élévation progressive lui permet d'atteindre un serveur ou un compte à privilèges, puis de compromettre le contrôleur de domaine.

Recommandation

Déployer LAPS sur l'ensemble des postes et serveurs membres du domaine afin d'assurer l'unicité et la rotation automatique des mots de passe administrateurs locaux.

Alignement avec les référentiels de sécurité

L'absence de LAPS est contraire aux recommandations du **Guide d'hygiène informatique de l'ANSSI**, qui préconise une gestion stricte et centralisée des comptes à privilèges ainsi que la limitation des mots de passe partagés. Elle va également à l'encontre des **bonnes pratiques Microsoft**, qui recommandent explicitement

l'utilisation de LAPS pour réduire les risques liés aux comptes administrateurs locaux et limiter les mouvements latéraux dans un environnement Active Directory.

Cette vulnérabilité s'inscrit clairement dans les tactiques de **mouvement latéral et d'élévation de privilèges** décrites par le référentiel **MITRE ATT&CK**, notamment via l'utilisation de comptes valides. Enfin, cette situation ne respecte pas les exigences de l'**ISO/IEC 27001**, en particulier les contrôles relatifs à la gestion des accès et au principe du moindre privilège, qui imposent de réduire l'exposition des comptes à hauts privilèges et de maîtriser leur cycle de vie.

4.2 Sauvegarde Active Directory obsolète (> 100 jours)

L'audit met en évidence que la **dernière sauvegarde** connue de l'Active Directory date de plus de **cent jours**. Cette situation traduit une politique de **sauvegarde inexisteante ou insuffisante** pour un composant critique du système d'information. Active Directory étant au **cœur des mécanismes d'authentification et d'autorisation**, l'absence de sauvegardes régulières constitue une **faiblesse majeure** en matière de résilience et de continuité d'activité.

[Last AD backup has been performed 101 day\(s\) ago](#)

+ 15 Point(s)

Problème

La dernière sauvegarde Active Directory recensée date de plus de 100 jours, ce qui indique une politique de sauvegarde insuffisante ou inexisteante pour un composant critique du système d'information.

Risque

En cas d'attaque par ransomware, de corruption de l'annuaire ou d'erreur humaine, l'absence de sauvegarde récente rend la restauration du domaine impossible ou fortement dégradée.

Impact

Cela peut entraîner une indisponibilité prolongée du SI, une perte de données critiques et une interruption totale des activités métiers.

Scénario d'attaque plausible

Un attaquant déclenche un ransomware ciblant les contrôleurs de domaine, chiffrant la base Active Directory. En l'absence de sauvegarde récente, l'organisation est incapable de restaurer l'annuaire dans un état fonctionnel, entraînant une interruption prolongée des services d'authentification.

Recommandation

Mettre en place une politique de sauvegarde régulière et automatisée des contrôleurs de domaine, avec des tests de restauration périodiques.

Alignement avec les référentiels de sécurité

Cette faiblesse est contraire aux recommandations du **Guide d'hygiène informatique de l'ANSSI**, qui impose la mise en place de sauvegardes régulières et testées pour les composants critiques. Elle ne respecte pas non plus les exigences de l'**ISO/IEC 27001**, notamment les contrôles relatifs aux sauvegardes et à la continuité d'activité. Du point de vue opérationnel, **Microsoft** recommande des sauvegardes fréquentes des contrôleurs de domaine afin de garantir une restauration fiable en cas d'incident majeur.

4.3 Print Spooler actif sur un DC

L'audit révèle que le service **Print Spooler** est actif et accessible à distance sur un contrôleur de domaine. Or, ce service n'est pas nécessaire au fonctionnement normal d'un DC et son exposition augmente inutilement la surface d'attaque du système d'information. La présence de ce service sur un composant aussi critique constitue une mauvaise pratique de durcissement.

Le Print Spooler a été à l'origine de nombreuses vulnérabilités critiques ces dernières années, certaines permettant l'exécution de code à distance ou l'élévation de priviléges. Lorsqu'il est exposé sur un contrôleur de domaine, ce service devient une cible privilégiée, car son exploitation peut conduire directement à la compromission du cœur de l'Active Directory.

[The spooler service is remotely accessible from 1 DC](#)

+ 10 Point(s)

Problème



Le service Print Spooler est accessible à distance sur un contrôleur de domaine, alors que ce service n'est pas requis pour le fonctionnement normal d'un DC.

Risque

Le Print Spooler a été à l'origine de multiples vulnérabilités critiques, permettant l'exécution de code à distance ou l'élévation de privilèges.

Impact

Un attaquant pourrait exploiter ce service pour obtenir des privilèges élevés et compromettre le contrôleur de domaine.

Scénario d'attaque plausible

Un attaquant déjà présent sur le réseau exploite une vulnérabilité connue du service Print Spooler exposé sur un contrôleur de domaine. Cette exploitation lui permet d'exécuter du code avec des privilèges élevés et d'obtenir un accès administrateur au domaine.

Recommandation

Désactiver le service Print Spooler sur tous les contrôleurs de domaine.

Alignement avec les référentiels de sécurité

Cette configuration est contraire aux recommandations de l'**ANSSI**, qui préconise la réduction maximale de la surface d'attaque des composants critiques. Elle va également à l'encontre des bonnes pratiques **Microsoft**, qui recommandent explicitement la désactivation du Print Spooler sur les contrôleurs de domaine. D'un point de vue offensif, cette faiblesse s'inscrit dans les techniques d'**élévation de privilèges** décrites par le référentiel **MITRE ATT&CK**. Enfin, elle ne respecte pas les principes de durcissement et de gestion des vulnérabilités définis par l'**ISO/IEC 27001**.

4.4 Politique d'audit insuffisante sur les contrôleurs de domaine

L'audit de sécurité met en évidence que la politique d'audit appliquée aux contrôleurs de domaine ne permet pas de collecter l'ensemble des événements de sécurité critiques, en particulier ceux relatifs aux authentifications, à

l'utilisation des privilèges élevés et aux modifications des objets Active Directory. Cette configuration limite la visibilité sur les actions sensibles réalisées au sein du domaine, alors même que les contrôleurs de domaine constituent des composants centraux et critiques du système d'information.

[The audit policy on domain controllers does not collect key events.](#)

+ 10 Point(s)

Problème

La politique d'audit appliquée aux contrôleurs de domaine ne collecte pas l'ensemble des événements de sécurité critiques, notamment ceux liés à l'authentification et aux privilèges.

Risque

Cette configuration réduit fortement la capacité de détection des attaques et complique les investigations post-incident.

Impact

Une compromission du domaine pourrait passer inaperçue pendant une période prolongée, augmentant les dommages potentiels.

Scénario d'attaque plausible

Un attaquant déjà présent sur le réseau exploite une vulnérabilité connue du service Print Spooler exposé sur un contrôleur de domaine. Cette exploitation lui permet d'exécuter du code avec des privilèges élevés et d'obtenir un accès administrateur au domaine.

Recommandation

Activer une politique d'audit avancée sur les DC, couvrant les événements d'authentification, d'accès et de modification des objets AD.

Alignement avec les référentiels de sécurité

Cette configuration est contraire aux recommandations du **Guide d'hygiène informatique de l'ANSSI**, qui insiste sur la nécessité d'une journalisation complète et centralisée des événements de sécurité sur les composants critiques. Elle ne respecte pas non plus les exigences de l'**ISO/IEC 27001**, notamment celles relatives à la journalisation, à la surveillance et à la détection des incidents de sécurité. Les bonnes pratiques **Microsoft**



recommandent explicitement l'activation des stratégies d'audit avancées sur les contrôleurs de domaine afin d'assurer une traçabilité suffisante. Enfin, du point de vue du référentiel **MITRE ATT&CK**, cette faiblesse s'inscrit dans les tactiques d'évasion des défenses, où l'absence ou l'insuffisance de logs empêche la détection des activités malveillantes.

4.5 Politique de mots de passe insuffisante (< 8 caractères)

L'audit met en évidence que la **politique de sécurité du domaine** autorise l'utilisation de mots de passe d'une longueur inférieure à huit caractères. Cette configuration est largement insuffisante face aux capacités actuelles de calcul et ne **répond plus aux standards de sécurité modernes**. Elle traduit une **faiblesse structurelle** dans la gestion des identités et de l'authentification au sein de l'Active Directory.

[Policy where the password length is less than 8 characters: 1](#)

+ 10 Point(s)

Problème

La politique de sécurité autorise des mots de passe d'une longueur inférieure à huit caractères, ce qui est largement insuffisant face aux capacités de calcul actuelles.

Risque

Des mots de passe faibles sont vulnérables aux attaques par force brute et par cassage hors ligne, notamment dans des scénarios Kerberos ou NTLM.

Impact

La compromission d'un compte peut servir de point d'entrée pour une élévation de privilèges et un mouvement latéral dans le domaine.

Recommandation

Renforcer la politique de mots de passe (longueur, complexité, expiration) et appliquer des règles spécifiques aux comptes à privilèges et de service.

Scénario d'attaque plausible



Un attaquant réalise des tentatives répétées d'authentification et modifie certains objets Active Directory. En raison d'une journalisation incomplète, ces actions ne sont pas correctement tracées. L'attaquant peut ainsi maintenir une présence prolongée dans le domaine sans être détecté.

Alignement avec les référentiels de sécurité

Cette configuration est contraire aux recommandations du **Guide d'hygiène informatique de l'ANSSI**, qui préconise l'utilisation de mots de passe longs et robustes pour limiter les attaques par force brute. Elle ne respecte pas non plus les bonnes pratiques **Microsoft**, qui recommandent une longueur minimale significativement supérieure, notamment pour les comptes sensibles et de service. Du point de vue du référentiel **MITRE ATT&CK**, cette faiblesse s'inscrit dans les techniques d'accès aux identifiants et d'authentification abusive. Enfin, elle ne satisfait pas aux exigences de l'**ISO/IEC 27001** relatives au contrôle d'accès et à la protection des mécanismes d'authentification.

4.6 Absence de redondance des contrôleurs de domaine

L'analyse des systèmes d'exploitation montre que le domaine repose sur un **unique contrôleur de domaine sous Windows Server 2022**. Bien que la version du système soit récente, l'absence de redondance constitue une faiblesse structurelle majeure. Active Directory étant un service critique, cette architecture crée un point de défaillance unique, tant du point de vue de la disponibilité que de la sécurité.

[The number of DCs is too small to provide redundancy: 1 DC](#)

+ 5 Point(s)

Problème

Le domaine ne dispose que d'un seul contrôleur de domaine, ce qui constitue un point de défaillance unique.

Risque

La perte ou l'indisponibilité du DC entraîne une interruption immédiate des services d'authentification.

Impact

Arrêt des services critiques, impossibilité d'authentification et impact direct sur la continuité d'activité.

Recommandation

Déployer au minimum un second contrôleur de domaine pour assurer la redondance.

Scénario d'attaque plausible

Un attaquant provoque une indisponibilité du contrôleur de domaine unique via une attaque par déni de service ou une exploitation ciblée. L'ensemble des services dépendants de l'authentification Active Directory devient alors indisponible.

Alignment avec les référentiels de sécurité

Cette architecture n'est pas conforme aux recommandations du **Guide d'hygiène informatique de l'ANSSI**, qui insiste sur la nécessité de garantir la disponibilité des services critiques. Elle ne respecte pas non plus les exigences de l'**ISO/IEC 27001** relatives à la continuité d'activité et à la résilience des systèmes d'information. Les bonnes pratiques **Microsoft** recommandent la mise en place d'au moins deux contrôleurs de domaine afin d'assurer la tolérance aux pannes et de limiter les impacts liés à une défaillance ou à une attaque ciblée.

4.7 Analyse des comptes utilisateurs (User Information)

L'analyse des comptes utilisateurs révèle plusieurs éléments traduisant une **hygiène de gestion des identités perfectible**. Le rapport PingCastle indique la présence d'au moins un compte dont le mot de passe n'expire jamais, ainsi que des comptes utilisant des mécanismes Kerberos potentiellement incompatibles avec le chiffrement AES. Ces configurations sont contraires aux bonnes pratiques de sécurité, qui recommandent une rotation régulière des secrets et l'usage exclusif d'algorithmes cryptographiques robustes.

Account analysis

Nb User Accounts	Nb Enabled	Nb Disabled	Nb Active	Nb Inactive	Nb Locked	Nb pwd never Expire	Nb SidHistory	Nb Bad PrimaryGroup	Nb Password not Req.
2	1	1	1	0	0	1	0	0	0

[Objects with a password which never expires](#)

[Objects where AES usage with kerberos may be cause issues](#)

[Activer Windows](#) [Accédez aux paramètres](#)

Problème

Des comptes utilisateurs disposent de mots de passe sans expiration et certains mécanismes de chiffrement Kerberos ne sont pas alignés avec les standards actuels.

Risque

Les comptes à mot de passe non expirant constituent des cibles privilégiées, car ils sont souvent oubliés et peu surveillés. En cas de compromission, l'attaquant peut conserver un accès durable à l'annuaire sans déclencher d'alertes liées au renouvellement de mots de passe.

Impact

Ces comptes peuvent servir de point d'entrée persistant dans le domaine Active Directory et faciliter des attaques ultérieures d'élévation de privilèges ou de mouvement latéral.

Scénario d'attaque plausible

Un attaquant obtient l'accès à un compte utilisateur dont le mot de passe n'expire jamais via une attaque par hameçonnage. Ce compte, rarement utilisé et peu surveillé, lui permet de maintenir un accès persistant au domaine. L'attaquant peut ensuite exploiter cet accès pour collecter des informations Active Directory et préparer une élévation de privilèges.

Recommandation

Supprimer l'attribut « *mot de passe n'expire jamais* » sur l'ensemble des comptes utilisateurs, à l'exception des cas strictement justifiés et documentés.

Alignement référentiels

Ce constat va à l'encontre des recommandations de l'**ANSSI** en matière d'hygiène des comptes, des bonnes pratiques **Microsoft** sur la gestion des identités, ainsi que des exigences de l'**ISO 27001** relatives au contrôle d'accès. D'un point de vue offensif, ces faiblesses s'inscrivent dans les phases de *Credential Access* et *Persistence* du référentiel **MITRE ATT&CK**.

4.8 Analyse des comptes ordinateurs (Computer Information)

L'audit des comptes ordinateurs met en évidence des éléments de configuration pouvant affaiblir la sécurité globale du domaine. Le rapport indique notamment la présence d'un compte machine autorisé à utiliser une **délégation non contrainte**, mécanisme historiquement sensible dans les environnements Active Directory. Bien que le nombre de machines soit limité, ce type de configuration est particulièrement critique lorsqu'il concerne un environnement peu segmenté.

Computer Information

Account analysis

This section gives information about the computer accounts stored in the Active Directory

Nb Computer Accounts	Nb Enabled	Nb Disabled	Nb Active	Nb Inactive	Nb SidHistory	Nb Bad PrimaryGroup	Nb unconstrained delegations	Nb Reversible password
1	1	0	1	0	0	0	1	0

[Objects trusted to authenticate for delegation](#) [\[?\]](#)

Problème

Un ordinateur est configuré avec des droits de délégation excessifs.

Risque

La délégation non contrainte permet à un attaquant qui compromet une machine concernée de récupérer des tickets Kerberos valides, y compris ceux de comptes à priviléges.

Impact

Cette configuration peut conduire à une élévation de priviléges rapide et à une compromission complète du domaine Active Directory.

Scénario d'attaque plausible

Un attaquant compromet un poste disposant d'une délégation non contrainte. Lorsqu'un compte à priviléges s'authentifie sur cette machine, l'attaquant récupère un ticket Kerberos valide et l'utilise pour s'authentifier en tant qu'administrateur sur d'autres ressources du domaine.

Recommandation

Supprimer toute **délégation non contrainte** configurée sur les comptes ordinateurs et de la remplacer, lorsque cela est strictement nécessaire, par des mécanismes de délégation **contrainte ou basée sur des services spécifiques**

Alignement référentiels

Cette situation est contraire aux recommandations de durcissement **ANSSI** et **Microsoft** concernant Kerberos. Elle correspond à des techniques bien connues du référentiel **MITRE ATT&CK**, notamment en matière d'élévation de priviléges et de mouvement latéral, et viole les principes de moindre privilège définis par l'**ISO 27001**.

5. Plan d>Action, synthèse des recommandations (Roadmap)

5.1 Échelle de criticité des vulnérabilités

Criticité	Priorité	Délai recommandé	Description
****	P0 – Urgent	Correction immédiate	La vulnérabilité peut conduire à une prise de contrôle totale du service, de l'équipement ou du domaine Active Directory. Elle peut permettre une compromission complète du système d'information ou un arrêt majeur de l'activité.
***	P1 – Élevé	Correction rapide	La vulnérabilité permet un contrôle partiel du service ou de l'équipement, ou facilite fortement une élévation de priviléges ou un mouvement latéral.
**	P2 – Moyen	Correction planifiée	La vulnérabilité entraîne une divulgation d'informations ou une faiblesse exploitable en combinaison avec d'autres vulnérabilités plus critiques.

*	P3 - Faible	Amélioration continue	La vulnérabilité est potentielle ou informative et n'impacte pas directement la confidentialité, l'intégrité ou la disponibilité du système.
---	--------------------	-----------------------	--

5.2 Synthèse des vulnérabilités :

Le tableau ci-dessous présente l'application de cette grille de criticité aux vulnérabilités identifiées lors de l'audit Active Directory.

Priorité	Vulnérabilité identifiée	Risque associé	Action recommandée	Gain sécurité
P0 – Urgent	Absence de LAPS	Mouvement latéral et élévation rapide de priviléges via comptes administrateurs locaux	Déployer LAPS sur l'ensemble des postes et serveurs membres du domaine	Très élevé
P0 – Urgent	Sauvegarde Active Directory obsolète	Impossibilité de restauration du domaine en cas de ransomware ou corruption	Mettre en place une politique de sauvegarde régulière et testée des DC	Très élevé
P0 – Urgent	Print Spooler actif sur un DC	Exécution de code à distance et compromission directe du contrôleur de domaine	Désactiver le service Print Spooler sur tous les contrôleurs de domaine	Très élevé
P0 – Urgent	Politique de mots de passe insuffisante	Compromission de comptes par force brute ou cassage hors ligne	Renforcer la politique de mots de passe (longueur, complexité, rotation)	Élevé
P1 – Élevé	Politique d'audit insuffisante sur les DC	Attaques non détectées et investigations post-incident impossibles	Activer une politique d'audit avancée sur les contrôleurs de domaine	Élevé

P1 – Élevé	Comptes utilisateurs à mot de passe non expirant	Persistante discrète d'un attaquant dans le domaine	Supprimer l'attribut « mot de passe n'expire jamais » et imposer une rotation	Élevé
P1 – Élevé	Délégation non contrainte sur comptes ordinateurs	Récupération de tickets Kerberos et compromission du domaine	Supprimer les délégations non contraintes et appliquer le moindre privilège	Élevé
P2 – Moyen	Absence de redondance des contrôleurs de domaine	Interruption totale du SI en cas de panne ou d'attaque	Déployer un second contrôleur de domaine	Moyen

6. Conclusion

6.1 Actions à mener après l'audit

Objectif	Action principale	Fréquence
Suivre le niveau de sécurité	Relancer un audit Active Directory (PingCastle)	Trimestrielle
Limiter les priviléges excessifs	Revoir les comptes administrateurs et délégations	Semestrielle
Améliorer la détection	Centraliser et analyser les journaux des DC	Continue

Renforcer la résilience	Tester les sauvegardes et la restauration AD	Annuelle
Maintenir le durcissement	Vérifier les GPO et services exposés	Trimestrielle

6.2 Conclusion synthétique

L'audit de sécurité réalisé sur le domaine **taaf.internal** met en évidence une **posture de sécurité globalement insuffisante** au regard des bonnes pratiques recommandées par l'ANSSI, Microsoft et les standards internationaux. Bien que l'infrastructure Active Directory soit fonctionnelle et repose sur des composants récents, elle présente plusieurs faiblesses critiques de configuration et d'hygiène qui exposent directement le système d'information à des scénarios de compromission majeurs.

Les vulnérabilités identifiées concernent principalement la **gestion des comptes à priviléges**, la **résilience du cœur du système d'information** et la **réduction de la surface d'attaque des contrôleurs de domaine**. Certaines d'entre elles, classées de criticité "P0", pourraient permettre à un attaquant disposant d'un accès initial limité de compromettre l'ensemble du domaine Active Directory en un temps réduit, notamment dans un contexte d'attaque par ransomware ou de mouvement latéral.

Le plan d'action proposé fournit une **feuille de route claire, priorisée et réaliste**, permettant de réduire rapidement le niveau de risque global. Les actions prioritaires (P0) visent à supprimer les vecteurs d'attaque les plus critiques, tandis que les actions P1 et P2 s'inscrivent dans une démarche d'amélioration continue de la sécurité, de la détection et de la résilience de l'infrastructure.

La mise en œuvre progressive de ces recommandations permettrait de ramener le score de risque du domaine d'un niveau estimé à **70/100** vers une cible réaliste inférieure à **25/100**, tout en renforçant durablement la sécurité et la disponibilité de l'Active Directory.