UNIVERSITÉ DE LA RÉUNION

DE LA RÉUNION
Institut Universitaire de Technologie
Réseaux et Télécommunications

Rapport

Audit de Sécurité - Windows Server 2022

Présenté par

Hoareau Anthony

Encadré par

M. Fontaine

BUT 3 Réseaux & Télécoms
Année universitaire 2025-2026
Janvier 2026

Table des matières

1. Executive Summary

1.1. Score Global de Sécurité

L'audit réalisé via PingCastle sur l'environnement Windows Server 2022 a révélé un niveau de risque élevé.

- **Score de Risque Domaine :** 70 / 100
- **Interprétation :** Le score dépasse **le seuil critique de 30**. Des actions correctives majeures sont nécessaires pour sécuriser le serveur et le domaine.

1.2. Top 3 des Risques Identifiés

L'analyse met en évidence trois axes critiques basés sur les indicateurs rouges du tableau de bord :

- **Anomalies de Sécurité (Score 70/100) :** Présence de vulnérabilités critiques de type « Pass-the-credential », facilitant le vol d'identifiants et les mouvements latéraux d'un attaquant.
- **Comptes à Privilèges (Score 60/100) :** Des problèmes de « Account take over » (prise de contrôle de compte) et « Admin control » indiquent que les comptes administrateurs sont mal protégés ou trop nombreux.
- **Objets Obsolètes (Score 31/100) :** Utilisation détectée de « Old authentication protocols » (probablement NTLMv1 ou pré-Kerberos), offrant une surface d'attaque facile.

1.3. Recommandations Prioritaires

- Restreindre et sécuriser les comptes administrateurs (Groupe Admins du domaine).
- Désactiver les protocoles d'authentification obsolètes
- **Investiguer les configurations** permettant le « Pass-the-credential »

2. Contexte et Périmètre

L'objectif principal de cet audit est d'évaluer le niveau de sécurité du serveur cible afin d'identifier les vulnérabilités techniques, les erreurs de configuration et les écarts par rapport aux bonnes pratiques de sécurité.

2.1. Objectif de l'audit

Les objectifs spécifiques incluent :

- Identifier les vulnérabilités connues liées au système d'exploitation Windows Server 2022 et aux services installés (gestion des correctifs/patch management).
- Vérifier la robustesse de la configuration (Hardening) en se basant sur les standards de l'industrie (ex: CIS Benchmarks ou ANSSI).
- Contrôler la gestion des identités et des accès, incluant la politique de mots de passe et les privilèges administratifs.
- Analyser la surface d'attaque réseau, notamment la configuration du pare-feu (Windows Defender Firewall) et les ports ouverts non nécessaires.
- Fournir un plan d'action priorisé pour la remédiation des failles identifiées.

2.2. Périmètre audité

L'audit porte exclusivement sur le serveur Windows Server 2022 identifié ci-dessous.

- Cible : Serveur Win_Serv_2022 (IP : [192.168.56.10]).
- Système d'exploitation : Microsoft Windows Server 2022.
- Couches auditées :
  - Système de fichiers : Permissions NTFS, partages réseaux, présence de données sensibles non chiffrées.
  - Gestion des comptes : Utilisateurs locaux, groupes administrateurs, complexité des mots de passe.
  - Services et Rôles : Configuration des rôles actifs.
  - Réseau local : Configuration TCP/IP, règles de pare-feu entrant/sortant.
  - Journaux d'événements : Configuration de l'audit et de la rétention des logs (Event Viewer).

- Type d’accès : Audit en « Boîte Blanche » (White Box) avec privilèges administrateur complets.

2.3. Limitations

Les limitations suivantes s’appliquent à la présente mission d’audit :

- Validité temporelle : L’audit représente une « photographie » de l’état de sécurité du système. Les modifications ultérieures du système ne sont pas couvertes.
- Non-intrusivité : Afin de garantir la disponibilité du service, aucune attaque par déni de service (DoS) ni aucune exploitation active de vulnérabilité (Exploit) risquant de crasher le système ne sera tentée.
- Périmètre réseau étendu : L’audit se limite à la configuration du serveur lui-même. Les équipements réseaux intermédiaires (switchs, routeurs, pare-feux périmétriques) ne font pas partie de ce périmètre.
- Ingénierie sociale : Les attaques visant le facteur humain (phishing, appels téléphoniques) sont exclues du périmètre.
- Menaces inconnues : L’audit se base sur les bases de connaissances de vulnérabilités connues à ce jour. Les failles de type « Zero-day » ne peuvent être garanties comme détectées.

3. Méthodologie

3.1. Référentiel utilisé

L'évaluation de la conformité du serveur s'appuie sur plusieurs standards reconnus, intégrés à la base de connaissance de PingCastle :

- **ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information) : Recommandations issues du guide d'hygiène informatique et des guides de configuration sécurisée pour Microsoft Windows.
- **Base de connaissances PingCastle** : Règles spécifiques développées par l'éditeur de l'outil, ciblant les mauvaises configurations courantes de l'Active Directory et de l'environnement Windows.

3.2. Outils

Outil principal : PingCastle

- **Usage :** Cartographie du niveau de sécurité, détection des mauvaises configurations, analyse des relations de confiance et calcul du score de risque global.

Outils natifs Microsoft (pour vérification) :

- **PowerShell / CMD :** Pour interroger manuellement certaines configurations (Get-Acl, net user, etc.).
- **Éditeur de gestion des stratégies de groupe :** Pour valider les GPO appliquées.
- **Observateur d'événements:** Pour l'analyse des journaux d'audit.

4. Résultats Détaillés

Résultat de PingCastle:

4.1. Anomalies de Sécurité (Score : 70/100)

> ℹ **Cette section regroupe les écarts de configuration critiques sur le serveur.**

- **Gestion des Mots de Passe Locaux :** La solution Local Administrator Password Solution (LAPS) n'est pas installée. En cas de compromission, l'attaquant peut se déplacer latéralement si les mots de passe locaux sont identiques.
- **Sauvegardes (Backup) :** Dernière sauvegarde AD effectuée il y a 85 jours. C'est un risque opérationnel critique (non-conformité PCA/PRA).
- **Service Spouleur (Print Spooler) :** Le service est accessible à distance. Sur un contrôleur de domaine, cela expose à la faille PrintNightmare (exécution de code à distance).
- **Politique de Mots de Passe :** La longueur minimale est inférieure à 8 caractères (recommandation ANSSI : 12 à 14 caractères minimum).
- **Audit Policy :** La politique d'audit ne collecte pas les événements clés, aveuglant les équipes de surveillance (SOC/SIEM).

4.2. Gestion des Comptes à Privilèges (Score : 60/100)

> ℹ **Cette section analyse la protection des administrateurs du domaine.**

- **Compte Administrateur Natif :** Le compte « Administrateur » a été utilisé il y a 0 jour. Ce compte ne devrait être utilisé qu'en cas d'urgence. Son usage courant est dangereux car il n'est pas verrouillable.
- **Délégation Kerberos :** Des comptes admins n'ont pas l'attribut « Account is sensitive and cannot be delegated », les exposant au vol de tickets Kerberos.
- **Groupe Schema Admins :** Ce groupe n'est pas vide. Il ne devrait contenir des membres que temporairement lors de modifications d'architecture, jamais en permanence.
- **Corbeille AD :** La fonctionnalité « Recycle Bin » n'est pas activée, compliquant la restauration d'objets supprimés accidentellement ou malveillamment.

4.3. Objets Obsolètes et Protocoles (Score : 31/100)

> ℹ **Cette section couvre l'hygiène du domaine.**

- **Protocole NTLMv1 / LM :** La configuration LAN Manager Authentication Level permet l'usage de NTLMv1 ou LM. Ces protocoles sont cryptographiquement cassés et permettent de récupérer les mots de passe en clair très facilement.
- **Ajout de machines au domaine :** Les utilisateurs non-admins peuvent ajouter jusqu'à 10 ordinateurs au domaine. Cela permet à un attaquant d'ajouter une machine malveillante pour exploiter des failles AD.
- **Subnets :** La déclaration des sous-réseaux est incomplète (2 IPs de DC non trouvées), ce qui peut impacter l'application des GPO et l'authentification.

5. Classification des Vulnérabilités

Impact / Probabilité	Faible	Moyenne	Élevée
Critique		Backup > 85j	NTLMv1 / Spouleur Actif
Majeur		LAPS manquant	Admin Natif utilisé
Mineur	Subnets incomplets	Ajout de machines au domaine	

6. Plan d’Actions

Voici les actions correctives priorisées pour réduire le score de risque en dessous de 30.

ID	Vulnérabilité	Action Technique Recommandée
1	Service Spouleur Actif	Arrêter et désactiver le service Spooler sur tous les DC.
2	Absence de Sauvegarde	Lancer une sauvegarde complète « System State » immédiatement. Vérifier la tâche planifiée de backup.
3	NTLMv1 autorisé	Configurer GPO : Network Security: LAN Manager authentication level sur « Send NTLMv2 response only. Refuse LM & NTLM ».
4	Usage Admin Natif	Créer des comptes admin nominatifs. Cesser l’usage du compte « Administrateur » et changer son mot de passe (très complexe + coffre-fort).
5	Ajout de machines au domaine	Mettre l’attribut ms-DS-MachineAccountQuota à 0 dans l’éditeur ADSI à la racine du domaine.
6	LAPS manquant	Déployer le client LAPS et configurer la GPO pour randomiser les pwd admins locaux.
7	Mot de passe < 8 chars	Mettre à jour la « Default Domain Policy » : Longueur min = 12 ou 14 caractères.

DE LA RÉUNION
Institut Universitaire de Technologie
Réseaux et Télécommunications

Hoareau Anthony

anthony.hoareau@rt-iut.re

40 Av. De Soweto, Saint-Pierre 97410, La Réunion

MINISTÈRE
DE L'ENSEIGNEMENT
SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'ESPACE
Liberté
Égalité
Fraternité