ATELIER PRO 1

GROUPE : Jérémie-Cephas SEGBEAME
Ali MIRNAMI
Valentin MISTRAL
Amir TAJIk
Rayane SOULAIMAN
Ferdinand NKONE

DOCUMENT TECHNIQUE

Fourniture d'une solution informatique nomade sécurisée

Date limite de réponse :

1) INTRODUCTION ET OBJECTIFS DU PROJET

1.1. Contexte et Problématique de l'Entreprise GSB

L'entreprise **GSB (Gabriel & Stéphane BETETA)** opère dans un secteur sensible, où l'activité repose sur une flotte d'environ cent postes de travail nomades utilisés par ses **Visiteurs Médicaux**. Ces équipements sont au cœur de la relation client et contiennent des données stratégiques et confidentielles (fichiers clients, comptes-rendus, données commerciales).

Historiquement, l'entreprise a fait face à des **incidents de sécurité récurrents**, notamment des **vols et des pertes de matériel**, qui ont potentiellement mené à des vols de données, impactant directement son Chiffre d'Affaires et sa réputation. Un audit de sécurité externe a confirmé la fragilité de l'environnement, identifiant des failles tant au niveau de la **sécurité physique** (gestion des équipements par l'utilisateur) qu'au niveau des **systèmes d'exploitation** (Windows 10 Enterprise et GNU/Linux Mint Cinammon).

De plus, l'entreprise est soumise à l'obligation de se conformer au **Règlement Général sur la Protection des Données (RGPD)**, rendant indispensable la protection des données personnelles stockées sur ces équipements mobiles.

1.2. Objectifs Stratégiques du Projet

Face à ces constats, le projet de **Sécurisation des Postes de Travail Nomades** a été lancé avec un objectif clair : concevoir et déployer une solution informatique résiliente et conforme, en s'appuyant sur une stratégie de **Défense en Profondeur**. Ce projet s'inscrit autour de deux axes stratégiques majeurs :

1. **Sécurité Physique (Axe 1.a) :** Définir et documenter un **processus de protection physique** des laptops (transport, stockage, utilisation), rendant le risque de vol et de perte de données moins critique.

2. **Enrichissement de la Base de Connaissances (Axe 1.b) :** Fournir une **documentation technique complète** (Livrable 3) servant de référence et de mode d'emploi pour le service informatique (IT) de GSB.

1.3. Objet de la Documentation Technique (LIVRABLE 3)

Le présent document, rédigé au **format DOCX obligatoire** et totalisant environ cent pages, constitue le mode d'emploi complet de la solution de sécurisation. Il est le pilier de l'objectif d'enrichissement de la Base de Connaissances de GSB. Il a pour vocation de :

- **Prouver la Faisabilité Technique :** Démontrer, à travers des procédures détaillées et des captures d'écran, que toutes les exigences du Cahier des Charges ont été implémentées avec succès sur les deux systèmes d'exploitation.
- **Assurer la Reproductibilité :** Servir de guide pas-à-pas pour le service IT, permettant de répliquer le durcissement sur l'ensemble de la flotte nomade de GSB de manière standardisée et uniforme.
- **Justifier les Choix :** Fournir l'analyse technique derrière chaque mesure de sécurité (Hardening) pour justifier la conformité aux bonnes pratiques (ex : désactivation de protocoles obsolètes, chiffrement de disque).

2. PRÉSENTATION DU PROJET

2.1. Descriptif de l'Existant (Situation Actuelle de GSB)

L'analyse de l'existant est la phase initiale qui a permis d'identifier les vulnérabilités et de motiver le projet de sécurisation. L'entreprise GSB, avec son modèle économique basé sur une force de vente nomade, possède un Système d'Information (SI) dont les pratiques actuelles exposent l'organisation à des risques significatifs.

2.1.1. La Flotte Informatique Nomade

L'infrastructure de travail repose sur une flotte d'environ **cent postes de travail nomades** utilisés par les Visiteurs Médicaux.

- **Responsabilité Individuelle :** Chaque salarié est responsable de son équipement. Cette approche, si elle favorise l'autonomie, entraîne un manque de standardisation et de traçabilité des configurations.
- **Préparation Manuelle :** La préparation des postes par le Service Informatique est réalisée **individuellement**, sans outil d'automatisation centralisé, rendant la tâche fastidieuse, coûteuse en temps et source d'erreurs de configuration.
- **Hétérogénéité des Systèmes :** Le parc est réparti entre deux systèmes d'exploitation :
    - **Microsoft Windows 10 Enterprise** (pour environ la moitié de la flotte).
    - **GNU/Linux Mint Cinammon** (pour l'autre moitié). Cette dualité requiert des solutions de sécurité spécifiques pour chacun.

2.1.2. Failles de Sécurité et Incidents Historiques

L'audit de cybersécurité externe a révélé des faiblesses critiques qui ont déjà eu des conséquences opérationnelles :

- **Pertes et Vols de Matériel :** L'entreprise a enregistré des cas avérés de **pertes ou de vols** de laptops. Le risque principal n'est pas la valeur du matériel, mais le **vol de données** qu'ils contenaient.
- **Conséquences sur le Chiffre d'Affaires :** Ces incidents sont fortement suspectés d'avoir causé des fuites d'informations, entraînant des **pertes de contrats** et une **baisse du Chiffre d'Affaires**.
- **Vulnérabilités Logicielles :** L'audit a pointé du doigt des failles au sein des systèmes d'exploitation (absence de *hardening* suffisant, protocoles obsolètes actifs) et des failles physiques (absence de procédure de protection du matériel sur le terrain).
- **Manque de Traçabilité :** Le matériel ne revient en maintenance que très tardivement (panne ou départ du salarié), ce qui empêche un suivi régulier de l'état de sécurité et la correction proactive des vulnérabilités.

2.1.3. Contraintes Réglementaires et Usage

- **Conformité RGPD :** L'entreprise doit se mettre en conformité avec le **Règlement Général sur la Protection des Données**. La présence de données sensibles (clients, prospects) sur des postes nomades non chiffrés constitue une violation potentielle majeure.
- **Travail Collaboratif Non Sécurisé :** L'utilisation de services tiers et d'échanges par courriel pour le travail collaboratif manque de sécurité et augmente le risque d'interception ou de fuite de données.

2.2. Expressions de Besoins

Le projet doit donc impérativement répondre aux besoins suivants, traduisant les remèdes aux faiblesses de l'existant :

- **Besoin de Sécurité Maximale :** Appliquer les meilleures pratiques de durcissement (Hardening) sur **Windows 10 Enterprise** et **LinuxMint Cinammon**.

- **Besoin d'Automatisation :** Mettre en place un processus (via **scripts PowerShell**) pour standardiser et automatiser le déploiement des configurations de sécurité Windows.
- **Besoin de Chiffrement :** Protéger les données sensibles en cas de vol, via le **chiffrement de disque complet** (BitLocker / LVM-LUKS).
- **Besoin de Procédures :** Définir un **processus clair de protection physique** et des règles strictes de **politique de mot de passe** (12 caractères, 90 jours, verrouillage après 3 tentatives).

2.3. Objectifs du Projet

La solution proposée vise à réaliser un niveau de sécurité optimal pour les Visiteurs Médicaux de GSB. Pour cela, le projet est structuré autour d'objectifs stratégiques, techniques et documentaires clairement définis.

2.3.1. Axes Stratégiques à Atteindre

Le succès du projet sera mesuré par l'atteinte de deux objectifs stratégiques majeurs, qui constituent le cœur de la réponse au Cahier des Charges (CDC) :

Axe Stratégique	Objectif Qualitatif du Projet	Impact Attendu
Sécurité Physique (Axe 1.a)	Définition et documentation d'un **processus de protection physique** efficace pour le poste de travail nomade (transport, stockage, utilisation).	Réduction significative du risque de vol et de l'exposition du matériel, et donc des données.
Documentation (Axe 1.b)	**Enrichissement de la Base de Connaissances GSB** par la fourniture de ce Livrable 3, une documentation technique complète et un mode d'emploi pour la réplication des configurations.	Garantie de la pérennité et de la standardisation de la solution pour les futures installations par le service IT.

2.3.2. Objectifs Techniques et Fonctionnels Attendus

Le projet s'engage à implémenter le durcissement complet des systèmes d'exploitation afin de remédier aux vulnérabilités logicielles identifiées :

A. Objectifs de Durcissement pour Microsoft Windows 10 Enterprise (Binôme 1)

- **Automatisation :** Fournir un **script PowerShell exécutable** pour le déploiement rapide et standardisé de toutes les configurations de sécurité.
- **Contrôle d'Accès :** Mise en œuvre de la **Politique de Mots de Passe** (12 caractères, 90 jours, verrouillage 3 tentatives).
- **Chiffrement :** Activation de **BitLocker** pour le chiffrement intégral du disque, soutenu par le module TPM 2.0.
- **Réseau :** Désactivation des protocoles obsolètes et vulnérables (NTLMv1, SMBv1, diffusion DNS Multicast) et activation de la **Signature SMB**.
- **Défense :** Configuration avancée de **Windows Defender** et du Pare-feu Windows, ainsi que l'activation du **Contrôle de Compte Utilisateur (UAC)** à son niveau maximal.
- **Traçabilité :** Activation de la **Journalisation des lignes de commande** et sécurisation des journaux d'événements.

B. Objectifs de Durcissement pour GNU/Linux Mint Cinammon (Binôme 2)

- **Chiffrement :** Mise en place du **chiffrement de disque LVM/LUKS** pour la protection des données au repos.
- **Réseau et Périmètre :** Configuration stricte des pare-feu **UFW et Iptables** (politique "deny all incoming").
- **Prévention d'Intrusion :** Installation et configuration de **fail2ban** pour contrer les attaques par force brute (notamment sur SSH).
- **Audit et Détection :** Installation des outils d'audit (**Lynis**) et antivirus (**ClamAV**).
- **Accès Distant :** Sécurisation du protocole **SSH** par authentification par clé et désactivation de l'accès root.
- **Hygiène :** Mise à jour régulière du système et désactivation des services non nécessaires.

2.3.3. Éléments à Fournir et Responsabilités

Le projet s'est concrétisé à travers une série de livrables et d'évaluations, nécessitant une répartition claire des responsabilités entre les trois binômes du groupe :

Éléments à Fournir	Date Limite	Binômes Responsables
LIVRABLE 2 (Réponse au CDC, Devis)	26/09/2025	Binômes 2 et 3
ORAL 1 (Présentation de la Solution)	29/09/2025	**Binôme 3** (Présentation, Argumentation)
LIVRABLE 3 (Ce document) (Documentation Technique)	**13/10/2025 - 18H**	**Binôme 1** (Édition Finale, Windows), **Binôme 2** (Linux, Physique), **Binôme 3** (Validation Usage)
ORAL 2 (Démonstration Technique)	**13/10/2025** (20 minutes)	**TOUS** (Chaque étudiant doit pratiquer et démontrer une partie de la solution technique.)

Rappel de la Répartition des Tâches :

- **Binôme 1 (Ali & Amir) :** Expert Windows (Durcissement/Script PowerShell) et Responsable de la mise en forme et de l'édition finale du **LIVRABLE 3** (format DOCX).
- **Binôme 2 (Jérémie & Valentin) :** Expert Linux (Durcissement/Chiffrement LVM/UFW) et Architecte Infrastructure (Matériel, Devis, Procédures Physiques).
- **Binôme 3 (Ferdinand & Rayane) :** Responsable de la Solution et des Soutenances (Oral 1 et 2), garant de la validation de la conformité aux usages professionnels et de la séparation des profils.

Solutions techniques et logicielles et justification des choix

. Solutions Techniques et Logicielles

La solution proposée s'articule autour d'une stratégie de Défense en Profondeur (Defense in Depth). Au lieu de se fier à une seule couche de protection, nous avons mis en place des mesures de sécurité à plusieurs niveaux : physique, système d'exploitation (durcissement), accès et réseau.

Le choix des solutions repose sur la priorisation des outils natifs (pour Windows) et des solutions Open Source reconnues (pour Linux) afin de minimiser les coûts d'acquisition de licences, tout en maximisant la sécurité.

Stratégie Transversale (Applicable aux Deux Environnements)

Ces solutions répondent aux exigences de conformité RGPD et à la politique de sécurité générale de l'entreprise.

Domaine	Solution Retenue	Justification Technique et Avantage
Sécurité des Données (RGPD)	**Chiffrement de disque complet** : **BitLocker** sur Windows 10 Enterprise (avec support TPM 2.0) et **LVM (Logical Volume Manager) avec LUKS** sur LinuxMint.	Réponse directe aux risques de vol et de perte de matériel. Le chiffrement rend les données illisibles en cas d'accès non autorisé au matériel, assurant ainsi la **confidentialité** des informations clients et la **conformité RGPD**.
Sécurité des Accès (Stratégie Locale)	Configuration stricte des politiques de mots de passe locales (Windows) et des modules **PAM** (Linux).	Permet d'imposer la politique de sécurité GSB : **12 caractères minimum, renouvellement tous les 90 jours, et verrouillage du compte après 3 tentatives infructueuses**. Cette mesure améliore l'hygiène de sécurité des utilisateurs.
Sécurité Physique (Processus)	Utilisation et procédure documentée des **Antivols de type Kensington**.	Mesure de prévention essentielle pour la sécurité physique, réduisant le vol d'opportunité dans les lieux publics (hôtels, gares) et remplissant l'un des deux axes stratégiques du projet.

Solutions Techniques pour Microsoft Windows 10 Enterprise

Le durcissement (Hardening) de l'environnement Windows repose sur la puissance des outils natifs et sur l'automatisation.

Domaine	Solution Technique Retenue	Justification Technique et Avantage
Automatisation/Déploiement	**Scripts PowerShell** (exécutables en tant qu'Administrateur).	Réponse à l'exigence de standardisation et d'efficacité. Le script permet d'appliquer rapidement et de manière reproductible tous les réglages du *hardening* (registre, politiques de sécurité, désactivation de services) sur les 50 postes Windows, garantissant l'uniformité du parc.
Sécurité Réseau	Désactivation de **SMBv1** et **NTLMv1**.	Ces protocoles sont obsolètes et présentent des vulnérabilités connues (ex : attaques de type *Man-in-the-Middle*, rançongiciels). Leur suppression réduit la surface d'attaque du poste de manière significative.
Défense et Système	Configuration avancée de **Windows Defender** (y compris la Protection contre les exploits) et activation stricte de **l'UAC**.	Windows Defender est gratuit et intégré, offrant une protection anti-malware robuste. L'UAC (Contrôle de Compte Utilisateur) au niveau maximal prévient l'escalade de privilèges par des applications malveillantes.
Traçabilité	Activation de la **Journalisation des lignes de commande** (Process Creation).	En cas d'incident, cette fonctionnalité permet à l'équipe IT de remonter le fil des actions exactes effectuées par un attaquant ou un malware (chaque commande exécutée est tracée), facilitant l'investigation et la réponse à incident.

Documentation – Durcissement Windows 10 Entreprise (Projet GSB)

Cette documentation présente l'ensemble des actions de sécurisation Windows 10 mises en place conformément au Cahier des Charges du projet GSB. Elle couvre uniquement la partie Windows, pour laquelle vous étiez responsable.

Sommaire

1. Introduction

Dans le cadre du projet GSB, les postes Windows 10 Entreprise utilisés par les visiteurs médicaux doivent être sécurisés afin de renforcer la résilience contre les attaques. Les actions décrites ci-dessous ont été réalisées avec succès sur le poste.

2. Méthodologie

Chaque étape comporte :

- L'objectif de sécurité
- La commande PowerShell utilisée
- Le résultat obtenu
- Une analyse expliquant l'intérêt de la mesure

3. Étapes de durcissement Windows

Étape 1 – Activation du pare-feu sur tous les profils

Objectif :
Garantir que le pare-feu Windows Defender est activé sur les trois profils réseau (Domaine, Privé et Public), afin de protéger le poste contre les connexions non autorisées et les attaques réseau.

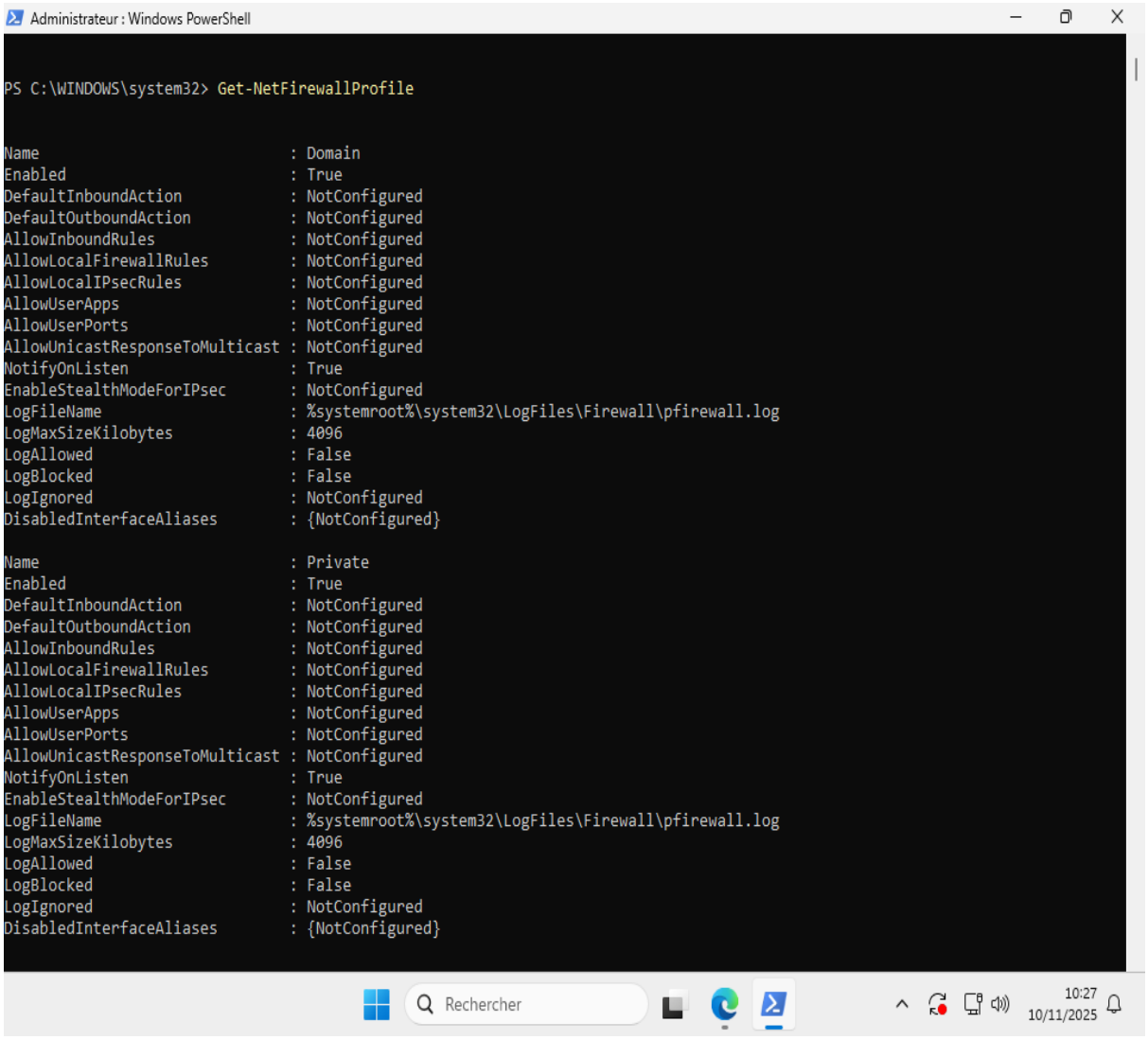
Commande PowerShell utilisée :

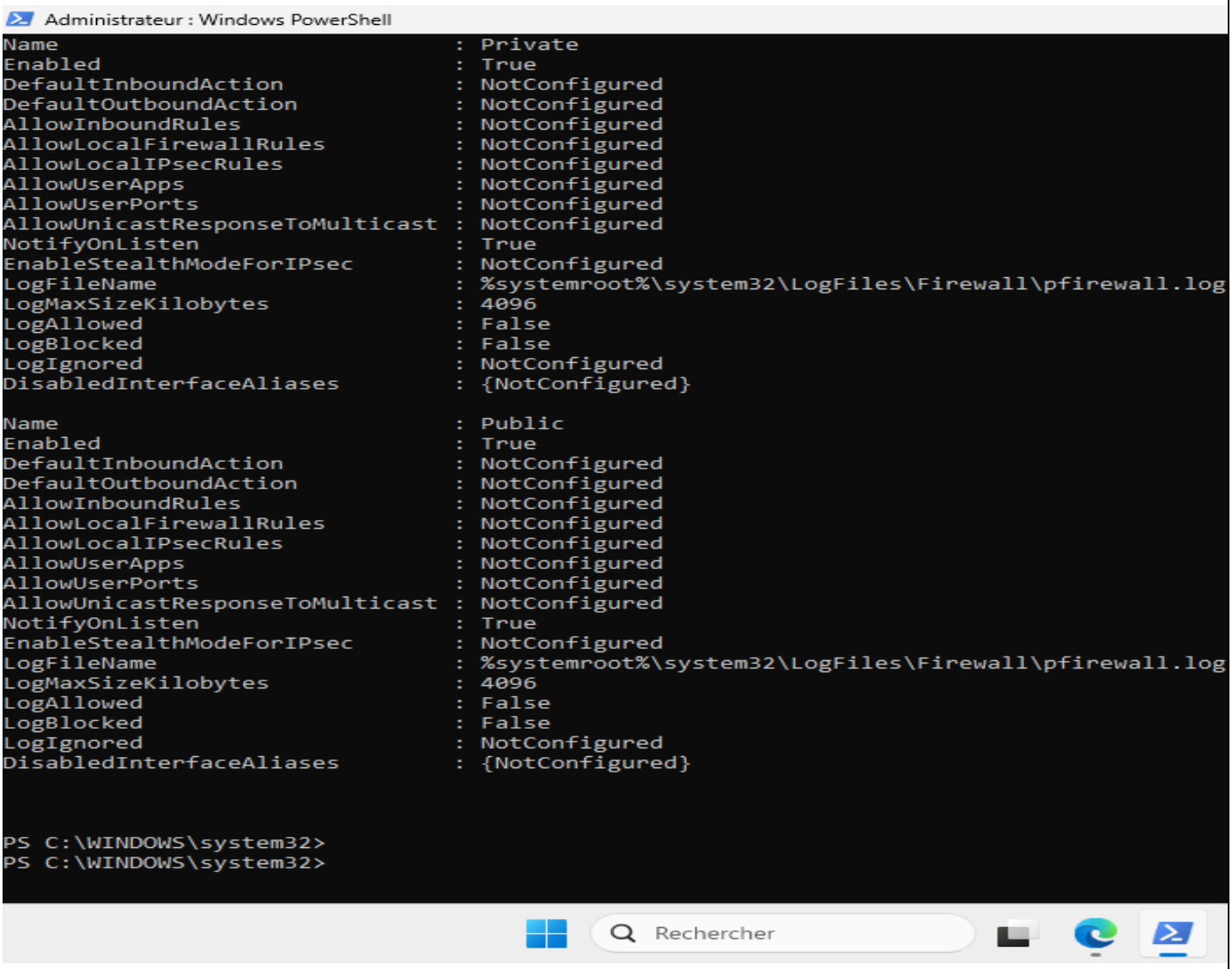
GetNetFirewallPr

ofile Résultat

obtenu :
Les trois profils affichent **Enabled : True,** ce qui confirme que le pare-feu est activé sur l'ensemble des contextes réseau.

Captures d’écran :





✅ **Statut : Réussi**

Analyse :

L'activation du pare-feu sur tous les profils assure un niveau de protection réseau de base sur l'ensemble des environnements, qu'il s'agisse d'un réseau professionnel, domestique ou public. Cette configuration est conforme aux bonnes pratiques de sécurité recommandées par l'ANSSI et Microsoft.

Étape 2 – Désactivation du protocole SMBv1

Objectif :
Désactiver le protocole SMBv1, obsolète et vulnérable aux attaques (notamment *WannaCry* et *Petya*), afin d'empêcher toute communication utilisant cette version non sécurisée.

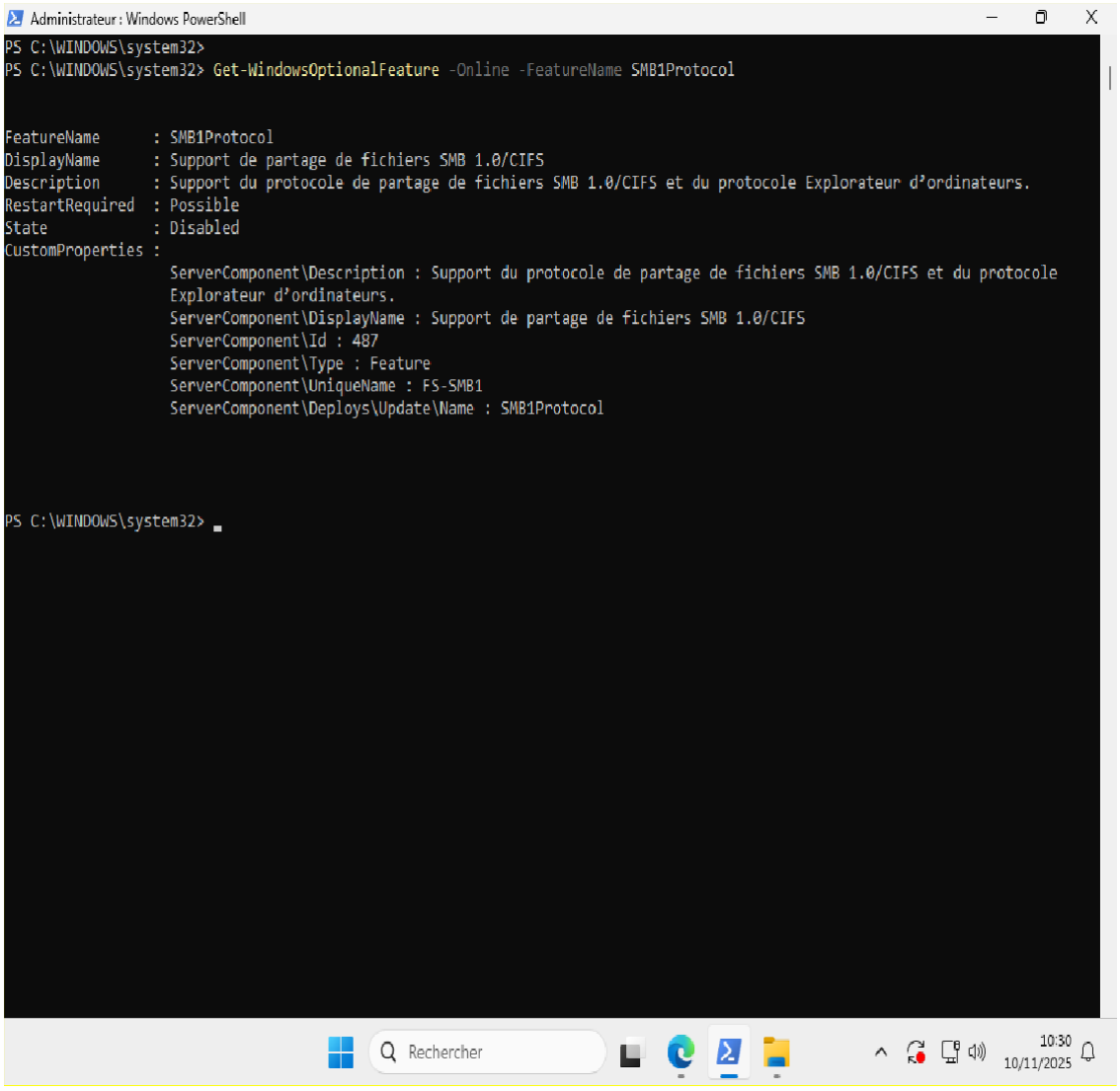
Commande PowerShell utilisée :

Get-windowsOptionsFeature

Résultat obtenu :

State: Disabled

Capture d'écran :



- ***02_SMBv1_Desactive.png*** **— Affiche l'état Disabled confirmant la désactivation du protocole.**

✅ **Statut : Réussi**

Analyse :

La désactivation du protocole SMBv1 renforce significativement la sécurité du système. Ce protocole, vieux de plus de 30 ans, ne prend pas en charge le chiffrement ni les mécanismes d'authentification modernes. Sa suppression empêche les attaques exploitant des partages réseau vulnérables et réduit la surface d'exposition du poste.

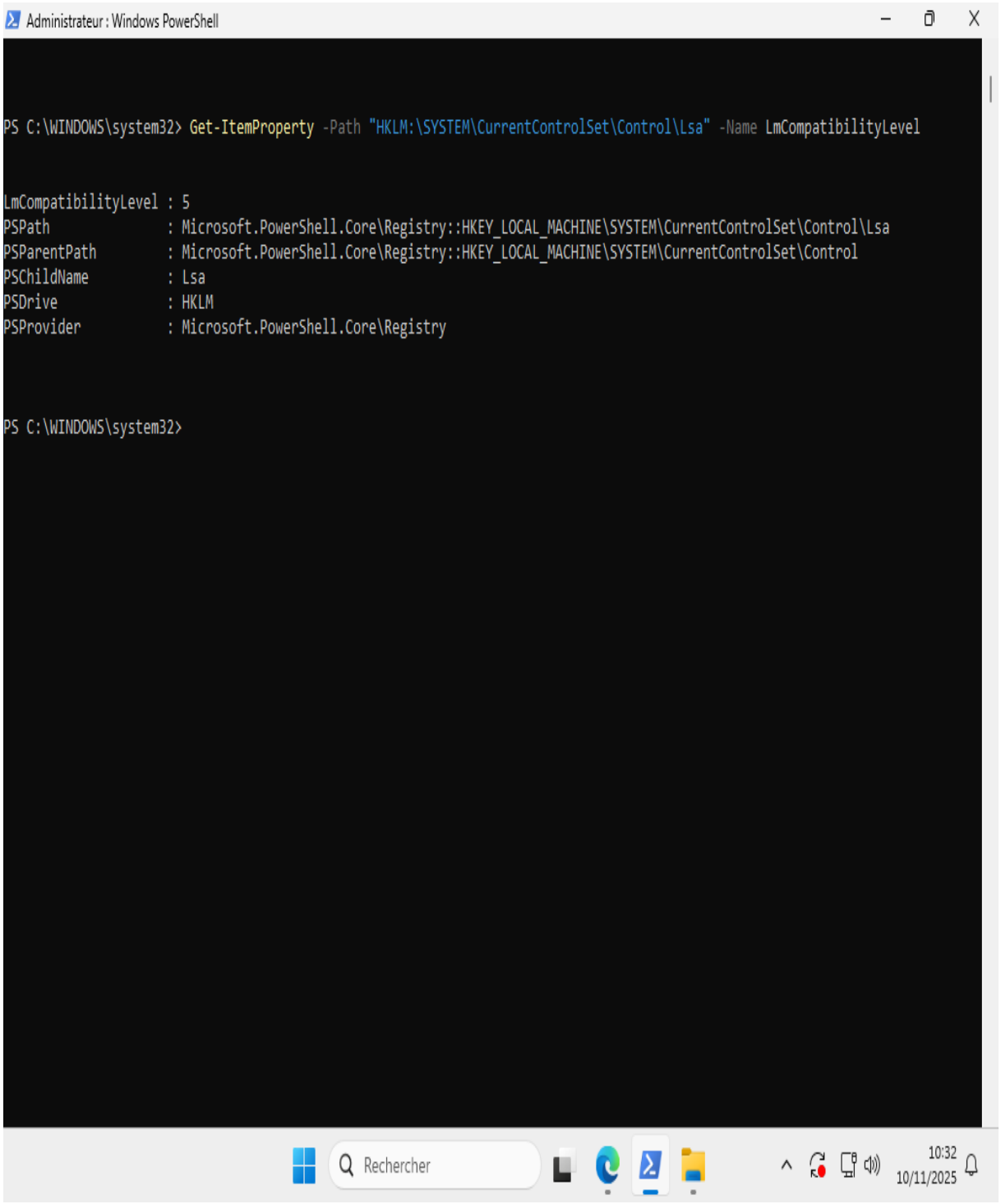
Étape 3 – Forcer NTLMv2 (interdire NTLMv1) Objectif :

Renforcer la sécurité de l'authentification réseau Windows en interdisant NTLMv1, obsolète et vulnérable aux attaques par interception, et en imposant NTLMv2, plus sécurisé grâce à un hachage renforcé et un échange de clés de session.

Commande PowerShell utilisée :

Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name LmCompatibilityLevel

Résultat obtenu :



LmCompatibilityLevel : 5

Capture d'écran :

- *03_NTLMv2_Active.png* — Affiche la valeur 5, correspondant à l'utilisation obligatoire de NTLMv2.

✅ Statut : Réussi

Analyse :

La valeur 5 signifie que l'ordinateur **n'envoie plus jamais d'authentification NTLMv1** et **n'accepte que**

NTLMv2, empêchant ainsi l'usage d'un protocole obsolète vulnérable aux attaques de type *pass-the-hash*.
Cette configuration est conforme aux recommandations de l'ANSSI et du CIS Benchmark Windows 10.

Étape 4 – Exiger la signature SMB et LDAP

🎯 Objectif :

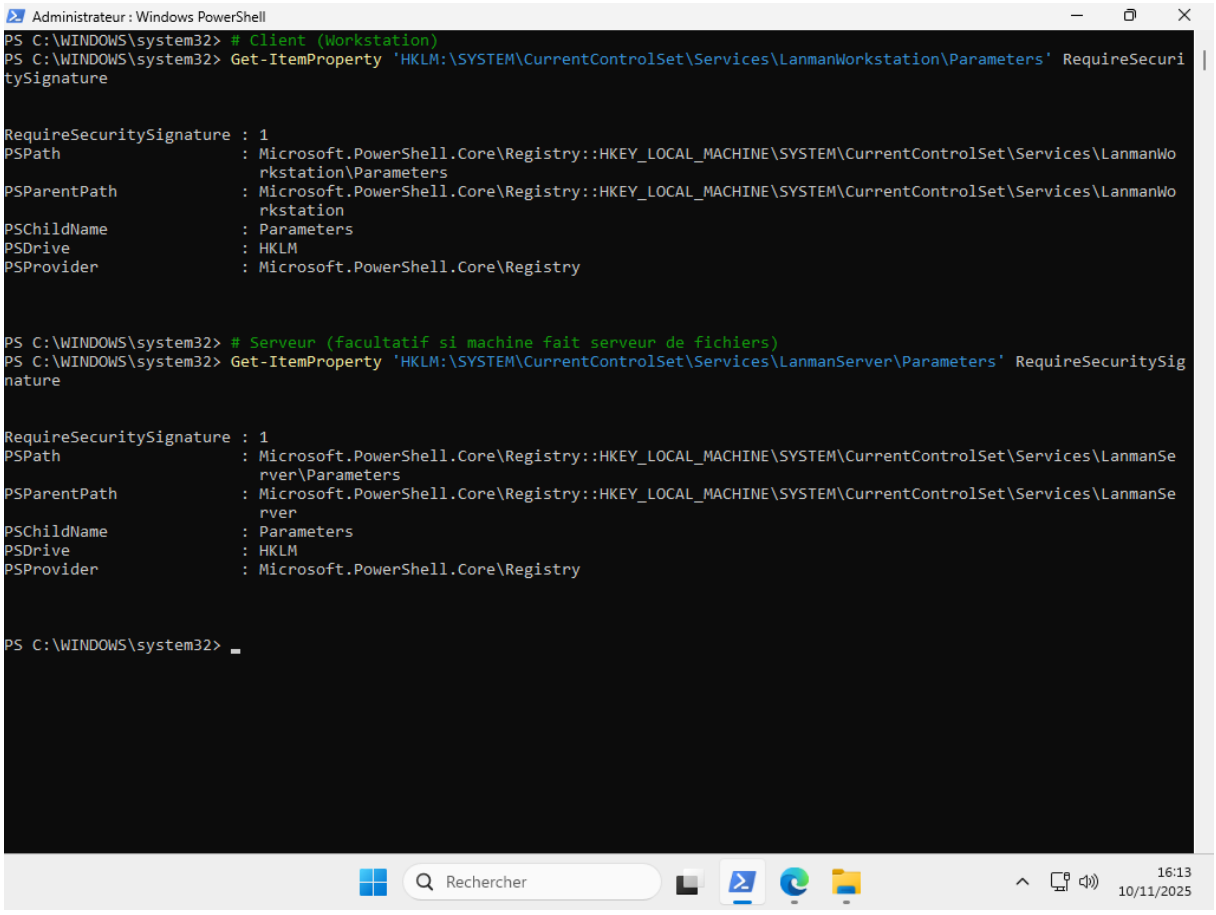
Renforcer la sécurité des communications réseau internes en **imposant la signature numérique des échanges SMB et LDAP**.
Cette mesure empêche les attaques de type *Man-in-the-Middle* (MiTM) et garantit l'intégrité des données échangées entre les postes et les serveurs.

💻 Commandes PowerShell utilisées :

```
# Client (Workstation)
Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters' RequireSecuritySignature

# Serveur (facultatif si la machine fait serveur de fichiers)
Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters' RequireSecu- rity Signature
```

📸 Capture d'écran :



• 04_Exiger_la_signature_SMB_et_LDAP.png — Affiche pour les deux clés de registre la valeur **RequireSecuritySignature = 1**, confirmant que la signature SMB est **activée** pour le client et le serveur.

✅ **Statut : Réussi**

🔍 **Analyse :**

La valeur **RequireSecuritySignature = 1** signifie que toutes les connexions SMB doivent être **signées numériquement** avant d'être acceptées.
Cela permet de :

- Empêcher toute altération ou falsification des paquets SMB,
- Bloquer les attaques d'interception ou d'usurpation de session (*session hijacking*),
- Garantir la confiance dans les communications internes du réseau.

L'activation de cette option est **recommandée par Microsoft et l'ANSSI** dans les environnements professionnels, notamment dans les domaines Active Directory et les réseaux d'entreprise.

Étape 5 – Activer et configurer l'UAC (User Account Control)

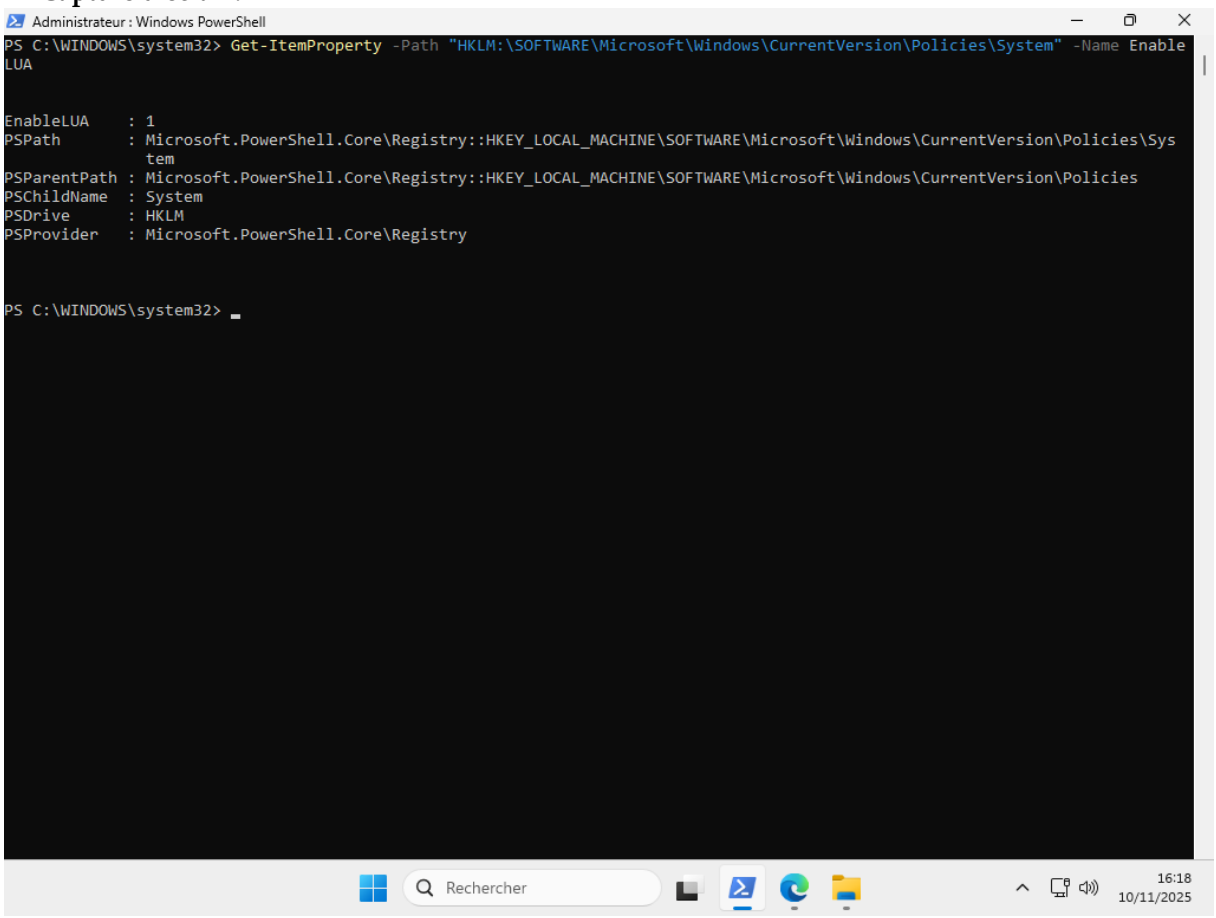
🎯 **Objectif :**

Vérifier que le **contrôle de compte utilisateur (UAC)** est activé afin de limiter les risques d'élévation de privilèges non autorisées.
L'UAC permet d'empêcher qu'un logiciel ou un utilisateur modifie des paramètres système sans autorisation explicite de l'administrateur.

💻 **Commande PowerShell utilisée :**

Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name EnableLUA

📸 **Capture d'écran :**



• 05_Activer_Config_UAC.png — Affiche la clé de registre **EnableLUA** avec la valeur **1**.

✅ **Statut : Réussi**

🔍 **Analyse :**

La valeur **EnableLUA = 1** confirme que le contrôle de compte utilisateur est **activé**.
Cette configuration est conforme aux bonnes pratiques de sécurité : elle protège le système contre l'exécution non autorisée de commandes nécessitant des privilèges élevés.
Si la valeur avait été **0**, cela aurait signifié que l'UAC était désactivé, exposant l'ordinateur à des risques accrus d'attaques par élévation de privilèges.

Étape 6 – Vérifier et configurer la politique de mot de passe

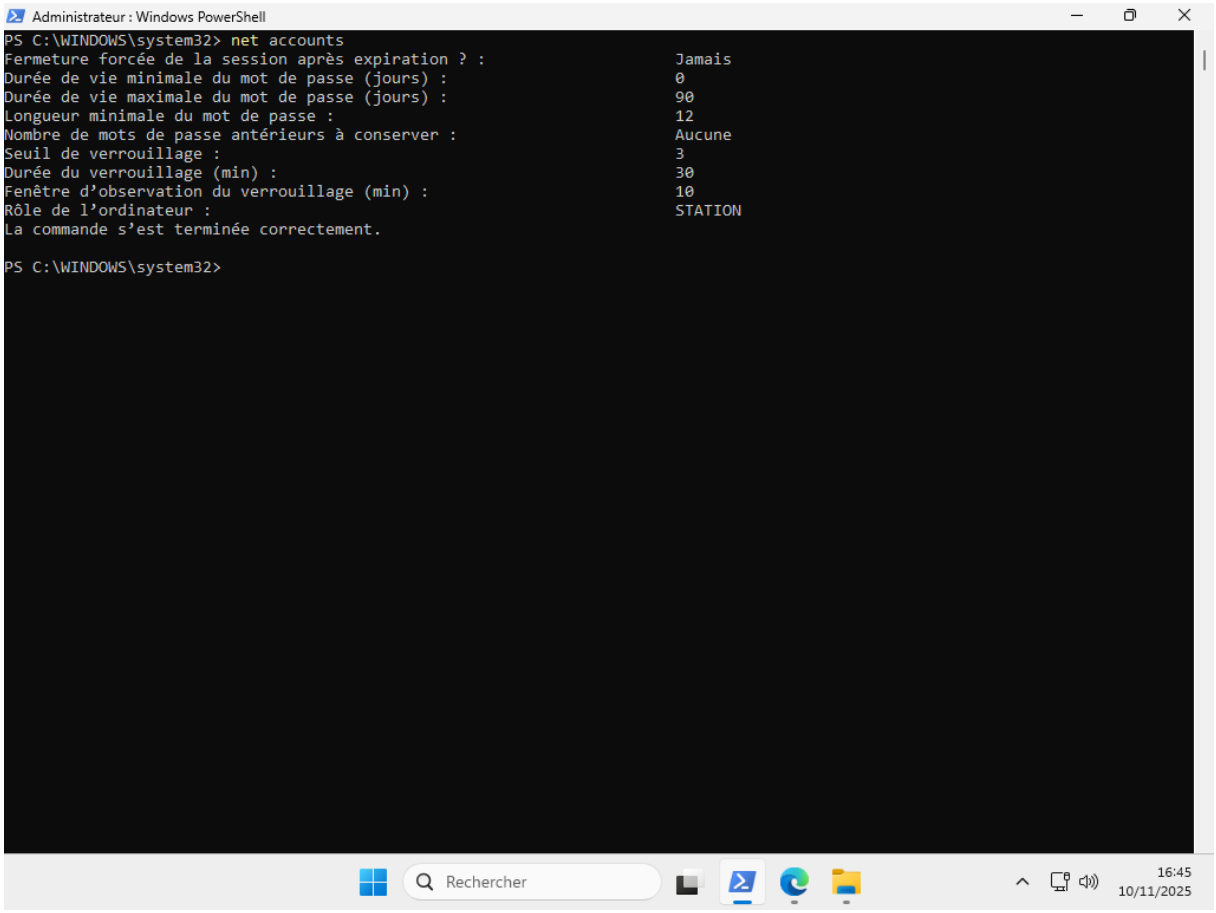
🎯 **Objectif :**

Contrôler les paramètres de la politique de mot de passe afin de garantir la robustesse et la gestion sécurisée des identifiants utilisateurs.
Une politique de mot de passe bien configurée limite les risques d'accès non autorisé au système.

💻 **Commande PowerShell utilisée :**

net accounts

📸 **Capture d'écran :**



• 0G_Politique_MotDePasse.png — Affiche les paramètres de la stratégie de mot de passe (durée, longueur minimale, verrouillage, etc.).

✅ **Statut : Réussi**

🔍 **Analyse :**

Les paramètres affichés indiquent une configuration cohérente avec les bonnes pratiques de sécurité :

- **Durée maximale du mot de passe : 50 jours**, ce qui impose un renouvellement régulier.
- **Longueur minimale : 12 caractères**, garantissant un mot de passe robuste.
- **Seuil de verrouillage : 3 tentatives**, réduisant le risque d'attaques par force brute.
- **Durée du verrouillage : 30 minutes**, assurant une période de blocage raisonnable avant réessaie.

Cette configuration contribue à renforcer la **sécurité des comptes locaux** en imposant des mots de passe forts et une gestion stricte des tentatives de connexion.

Étape 7 – Restreindre Kerberos à AES only

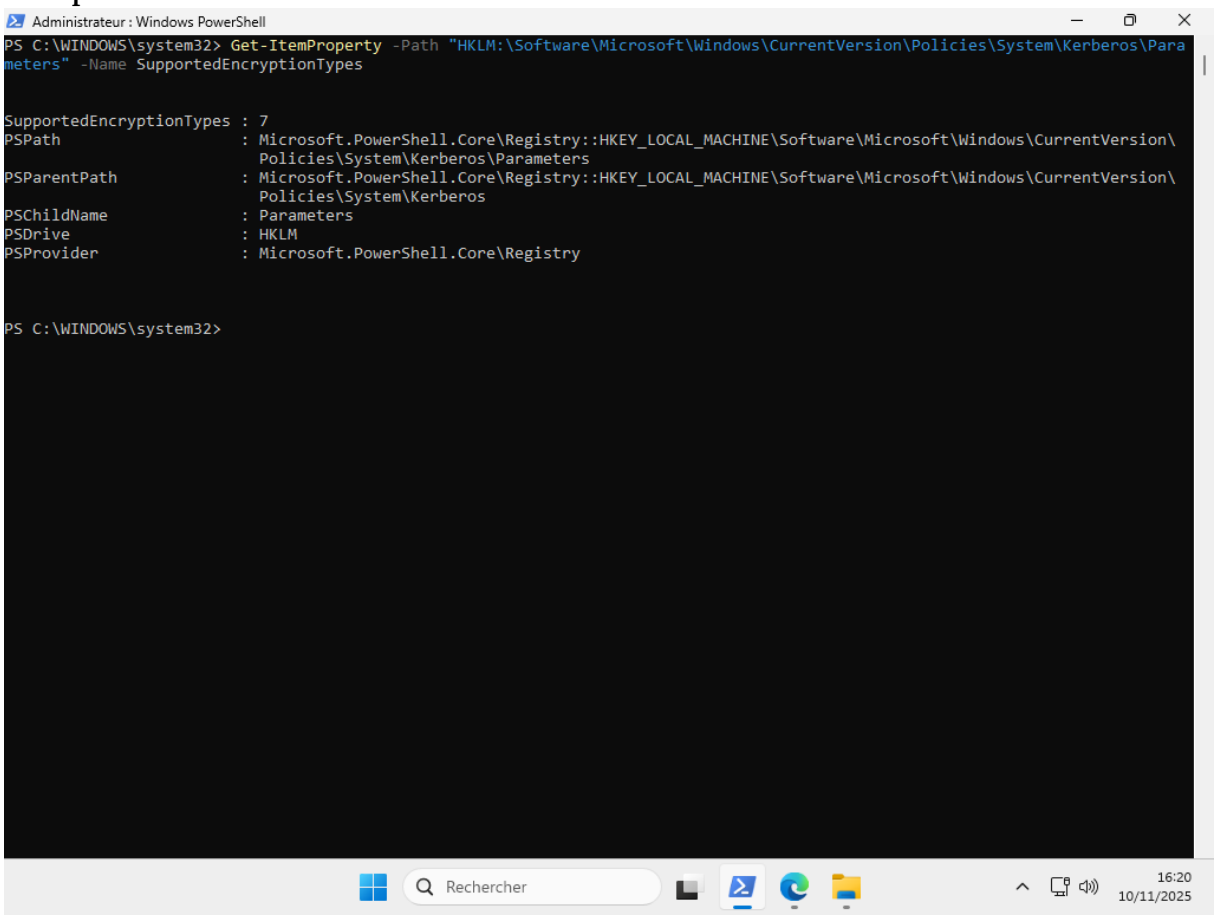
🎯 **Objectif :**

Renforcer la sécurité du protocole d'authentification **Kerberos** en limitant les types de chiffrement utilisés aux algorithmes **AES (Advanced Encryption Standard)**, considérés comme sûrs et modernes.
Cela empêche l'utilisation d'algorithmes obsolètes ou vulnérables (comme RC4 ou DES).

Commande PowerShell utilisée :

Get-ItemProperty -Path "HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System\Ker- beros\Parameters" -Name SupportedEncryptionTypes

Capture d'écran :



• 07_Kerberos_AESonly.png — Affiche la valeur du paramètre **SupportedEncryptionTypes = 7** confirmant l'activation des algorithmes AES.

Statut : Réussi

Analyse :

La valeur **7** correspond à la combinaison des algorithmes de chiffrement **AES128** et **AES256**, conformément aux recommandations de sécurité actuelles.
Cette configuration garantit que seules des méthodes de chiffrement robustes sont utilisées lors de l'authentification via Kerberos, protégeant ainsi les échanges d'identifiants contre les attaques de type **replay**, **brute force** ou **downgrade**.

L'utilisation d'AES uniquement améliore la **confidentialité** et l'**intégrité** des communications dans l'environnement Windows.

Étape 8 – Désactiver WDigest

🎯 Objectif :

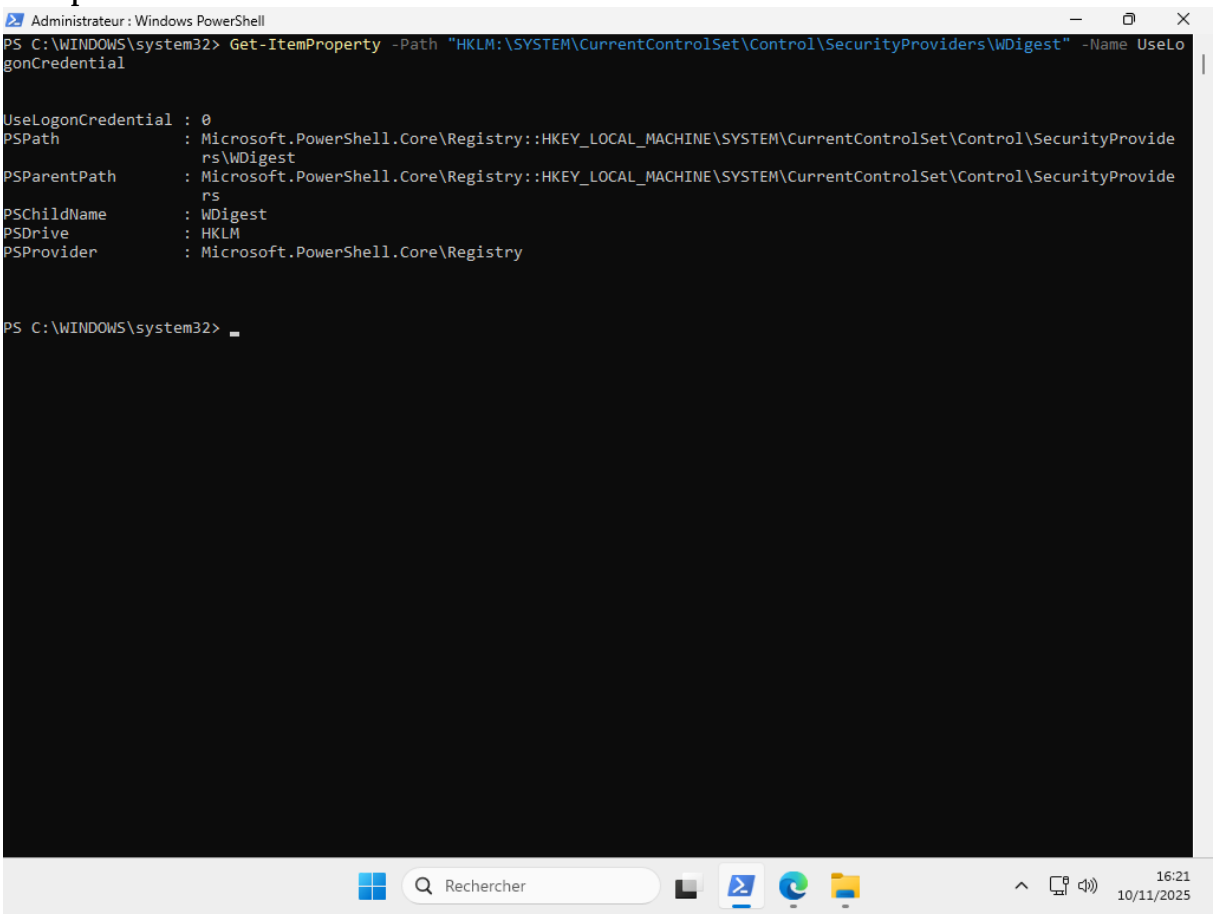
Désactiver le stockage en mémoire des identifiants en texte clair utilisé par **WDigest**, un ancien mécanisme d'authentification Windows.
Cette configuration empêche les attaquants d'extraire les mots de passe en clair de la mémoire du processus **LSASS**, renforçant ainsi la protection contre les attaques de type **credential dumping**.

💻 Commande PowerShell utilisée :

Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest" -Name UseLogonCredential

---

📸 Capture d'écran :



• 08_Désactiver_WDigest.png — Montre la valeur **UseLogonCredential = 0** confirmant la désactivation du stockage en mémoire.

✅ Statut : Réussi

🔍 Analyse :

La valeur **UseLogonCredential = 0** signifie que Windows **ne conserve pas les identifiants en clair dans la mémoire** du système.
Cette configuration est conforme aux recommandations de sécurité de Microsoft et de l'ANSSI.
Elle empêche les outils malveillants (tels que **Mimikatz**) d'extraire les mots de passe des utilisateurs depuis

la mémoire, réduisant ainsi considérablement le risque d'escalade de privilèges et de compromission totale du système.

Étape 5 – Protéger LSASS (RunAsPPL)

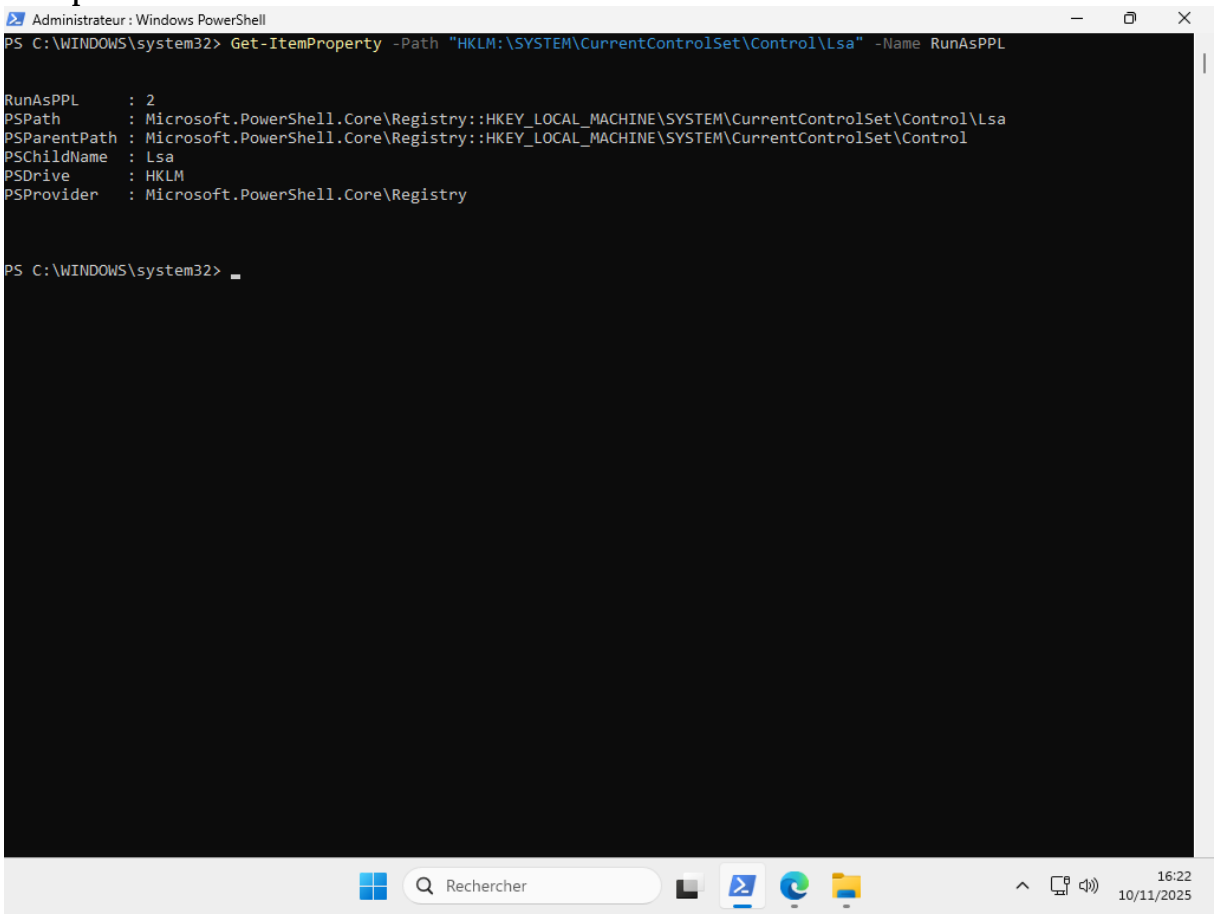
🎯 Objectif :

Renforcer la protection du processus **LSASS (Local Security Authority Subsystem Service)** en l'exécutant en mode **Protected Process Light (PPL)**.
Ce mode empêche les programmes non autorisés (y compris les malwares ou outils d'extraction comme Mimikatz) d'accéder à la mémoire de LSASS, qui contient des secrets d'authentification.

💻 Commande PowerShell utilisée :

```
Get-ItemProperty  -Path  "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa"  -Name  RunAsPPL
```

📸 Capture d'écran :



• 05_Protéger_LSASS.png — Affiche la valeur **RunAsPPL = 2**, confirmant que le mode protégé est activé.

✅ Statut : Réussi

🔍 Analyse :

La valeur **RunAsPPL = 2** indique que **LSASS s'exécute en mode protégé (PPL)**.
Ce mode empêche tout processus non signé ou non autorisé d'interagir avec LSASS, limitant ainsi les risques de **vol de mots de passe** ou de **dump mémoire**.

Cette configuration est une **mesure de défense essentielle** dans tout environnement Windows moderne, notamment pour contrer les techniques d'attaque post-exploitation ciblant les identifiants administratifs. Elle est conforme aux recommandations de **Microsoft** et de **l'ANSSI** pour la sécurisation des postes de travail et serveurs.

Étape 11 – Vérifier la journalisation PowerShell et sécurité

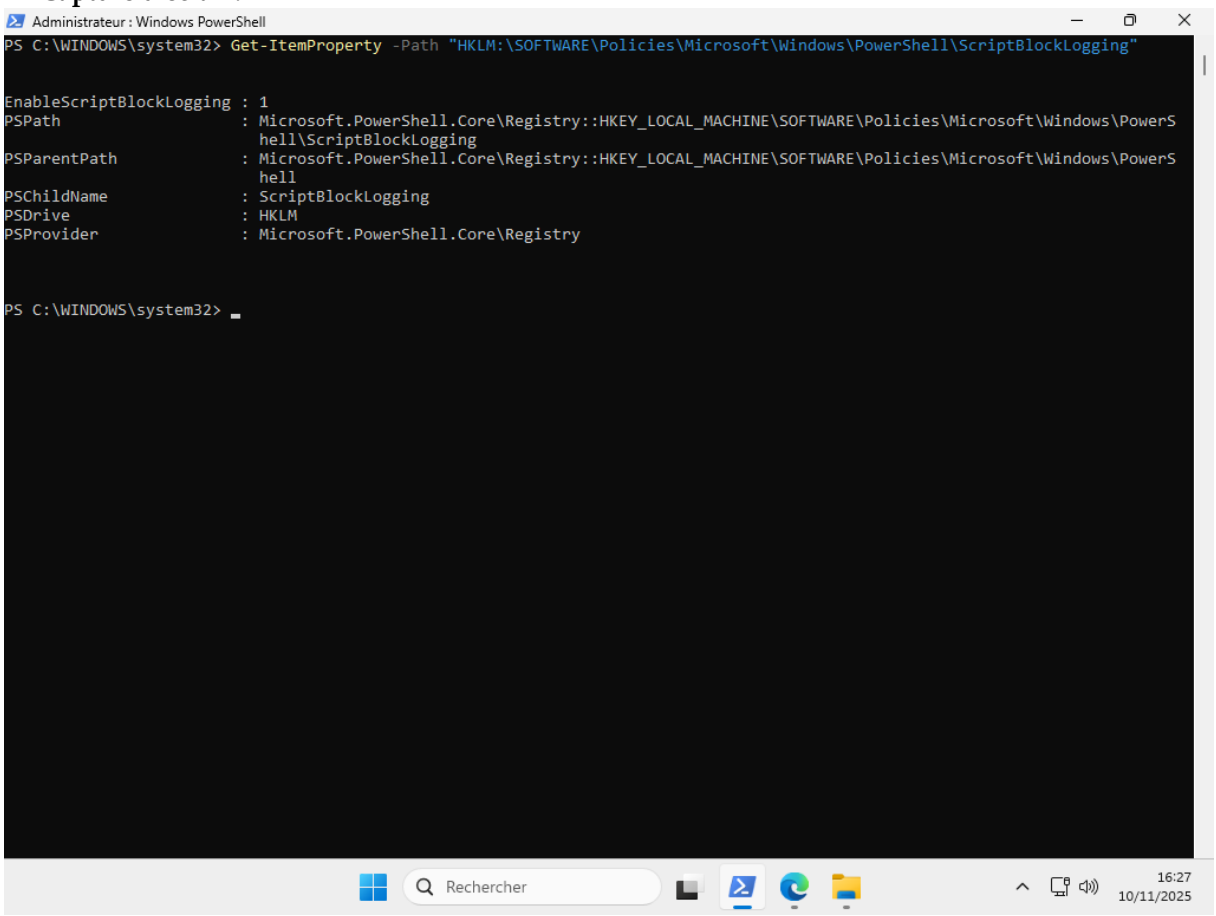
🎯 **Objectif :**

S'assurer que les **journaux d'événements Windows** dédiés à PowerShell et à la sécurité sont **activés**, afin de garantir la conservation des traces d'exécution des scripts et des activités système critiques.

💻 **Commandes PowerShell utilisées :**

wevtutil gl Security
wevtutil gl "Windows PowerShell"

📸 **Capture d'écran :**



• 11_Vérifier_Journalisation_PowerShell.png — Montre que les deux canaux d'événements **Security** et **Windows PowerShell** sont activés (enabled: true).

✅ **Statut : Réussi**

🔍 **Analyse :**

Les résultats affichent **enabled: true** pour les deux journaux :

- **Security** → enregistre les événements liés à l'authentification, à l'accès aux ressources et aux modifications de sécurité.
- **Windows PowerShell** → consigne toutes les commandes exécutées dans l'interpréteur PowerShell.

Cette configuration permet une **traçabilité complète des activités système** et contribue à la détection rapide d'actions suspectes ou non autorisées.
Elle est conforme aux **recommandations de Microsoft et de l'ANSSI** pour la supervision des postes de travail et des serveurs Windows.

Étape 12 – Vérifier la taille et l'état des journaux Windows

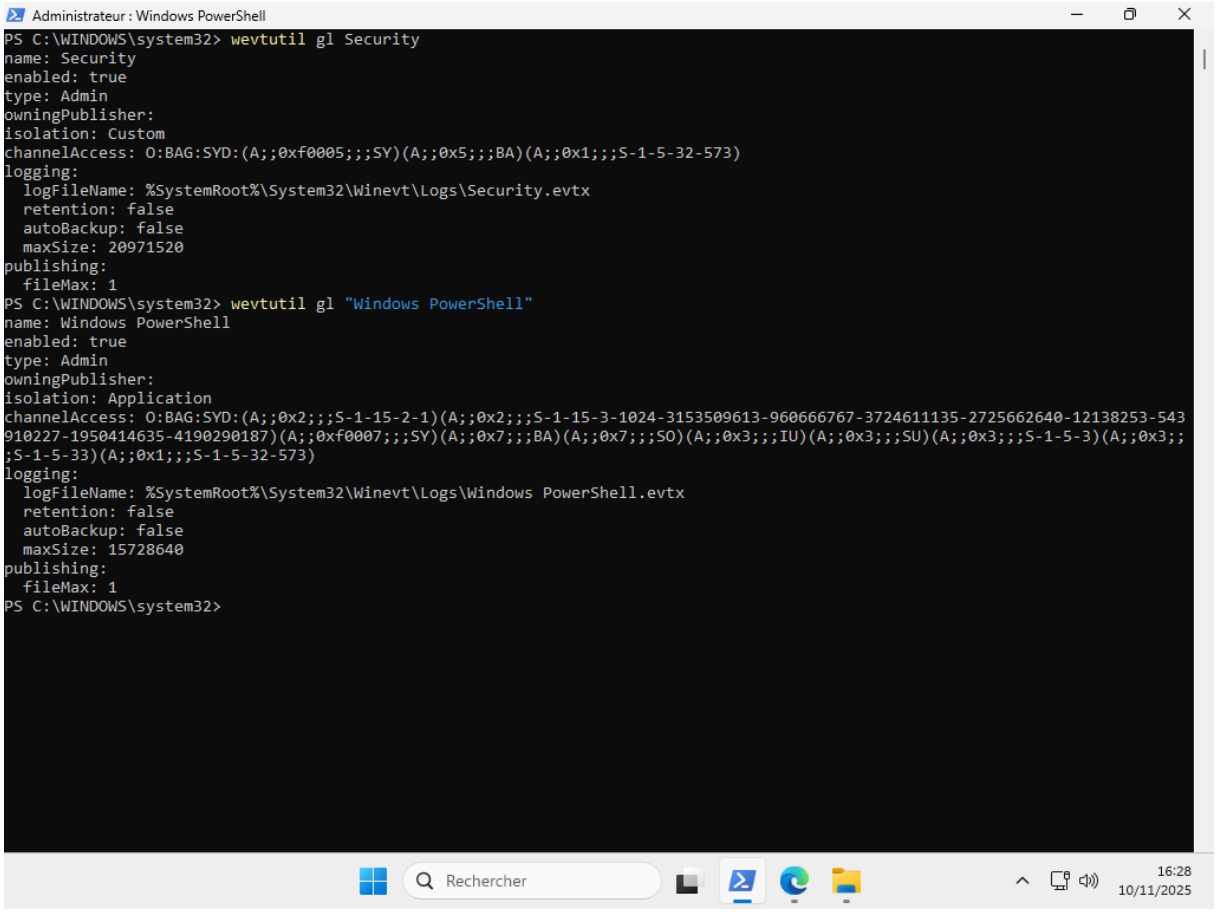
🎯 **Objectif :**

Vérifier que les **journaux d'événements Windows** liés à la sécurité et à PowerShell sont **activés** et correctement configurés en termes de **taille maximale et de rétention**.
Cela permet de garantir la **conservation suffisante des traces** pour les besoins d'audit et d'investigation.

💻 **Commandes PowerShell utilisées :**

```
wevtutil gl Security
wevtutil gl "Windows PowerShell"
```

📸 **Capture d'écran :**



• 12_Taille_Journaux_Windows.png — Affiche l'état des journaux *Security* et *Windows PowerShell*, tous deux activés avec une taille maximale définie.

✅ **Statut : Réussi**

🔍 **Analyse :**

Les deux journaux sont **activés (enabled: true)**, ce qui signifie que le système **enregistre correctement les événements critiques** :

- **Security** : événements d'authentification, de connexion et de gestion des comptes.
- **Windows PowerShell** : commandes et scripts exécutés sur le système.

Les valeurs observées (ex. *maxSize = 209/1520* pour *Security* et *15/28640* pour *PowerShell*) garantissent une **capacité suffisante pour stocker les événements récents** sans perte prématurée.

Cette configuration est conforme aux **bonnes pratiques de supervision de la sécurité** sous Windows, permettant un suivi complet et une meilleure réponse aux incidents.

Étape 13 – Activer SmartScreen

🎯 **Objectif :**

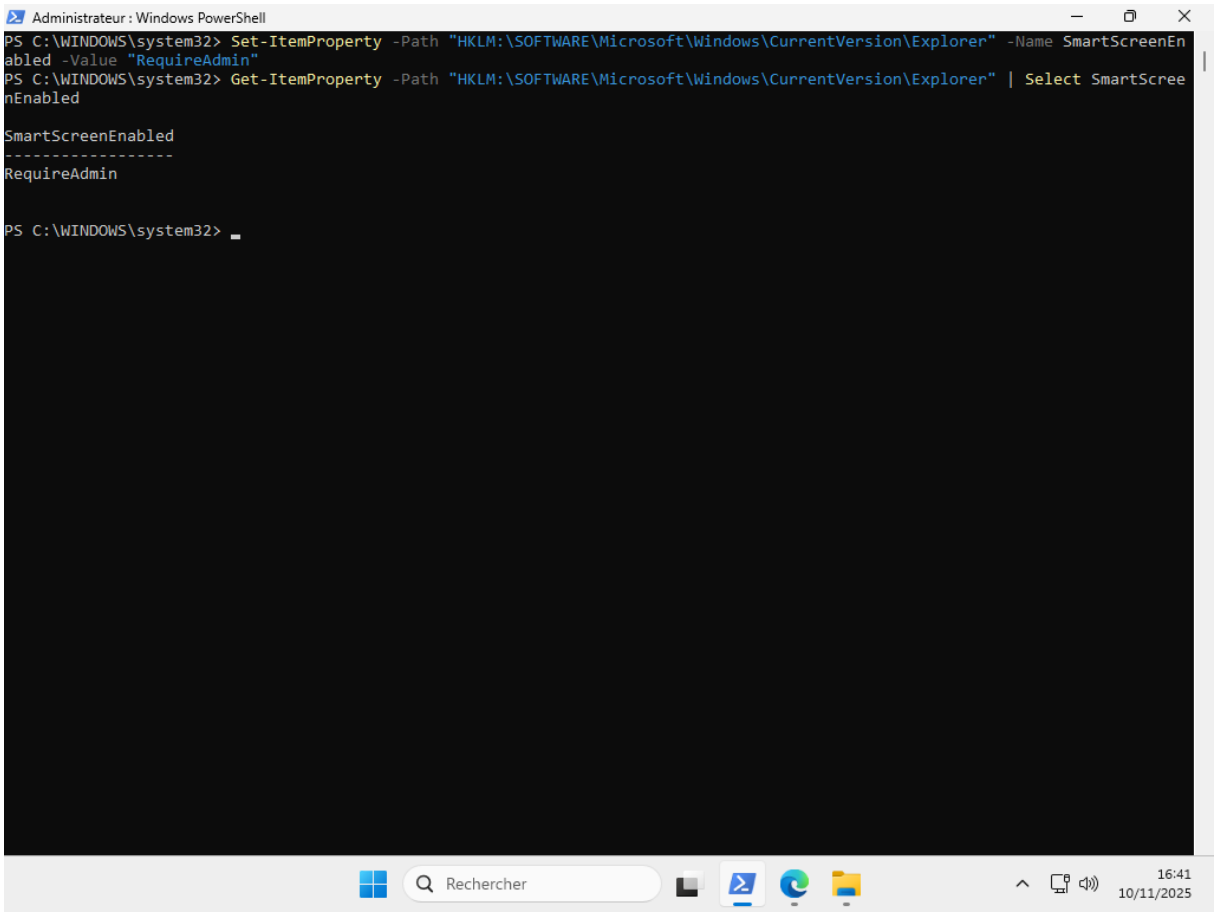
Activer **Windows SmartScreen**, une fonctionnalité de protection intégrée qui analyse les fichiers et applications téléchargés afin de bloquer ou d'avertir l'utilisateur en cas de contenu potentiellement dangereux ou non reconnu.

💻 Commandes PowerShell utilisées :

Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer" -Name SmartScreenEnabled -Value "RequireAdmin"
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer" | Select SmartScreenEnabled

---

📸 Capture d'écran :



• 13_Activer_SmartScreen.png — Montre la valeur **SmartScreenEnabled = RequireAdmin**, confirmant que la protection SmartScreen est bien activée et requiert une validation administrateur.

✅ Statut : Réussi

🔍 Analyse :

La valeur **RequireAdmin** indique que **SmartScreen est activé** et impose une **confirmation par un administrateur** avant l'exécution de tout fichier jugé suspect.
Cette configuration renforce la sécurité du système contre les **exécutables inconnus, les téléchargements malveillants et les attaques de phishing**.

Elle s'inscrit dans les bonnes pratiques recommandées par **Microsoft et l'ANSSI**, garantissant un **filtrage proactif** des menaces et une **protection accrue de l'utilisateur**.

Étape 14 – Désactiver AutoRun / AutoPlay

🎯 Objectif :

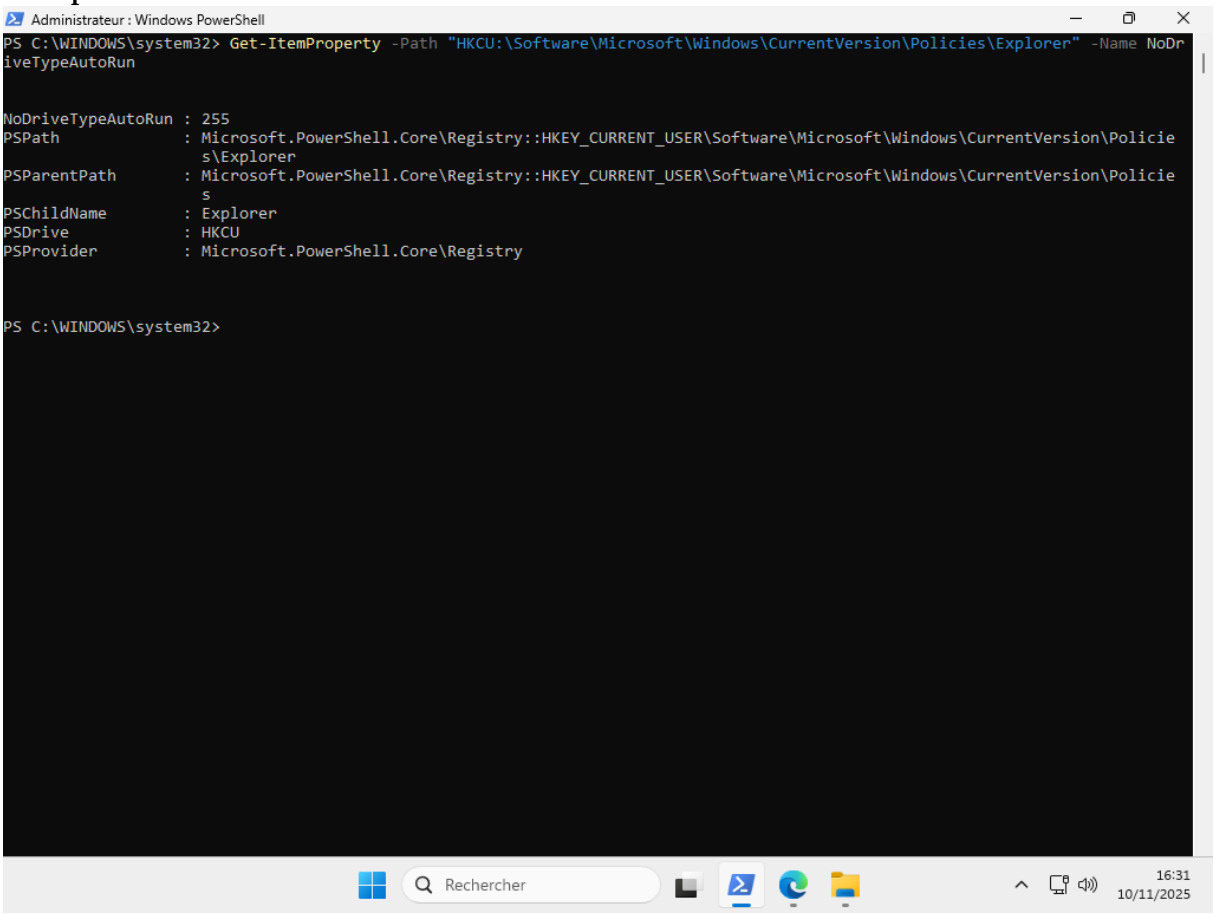
Empêcher l'exécution automatique des programmes lors de la connexion d'un périphérique externe (clé USB, disque dur, CD, etc.) afin de réduire les risques d'infection par des logiciels malveillants.

💻 Commande PowerShell utilisée :

Get-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" -Name NoDriveTypeAutoRun

---

📸 Capture d'écran :



• 14_Désactiver_AutoRun_AutoPlay.png — Affiche la valeur **NoDriveTypeAutoRun = 255**, confirmant que la fonction AutoRun est complètement désactivée pour tous les types de lecteurs.

✅ Statut : Réussi

🔍 Analyse :

La valeur **255** dans le registre signifie que **toutes les formes d'exécution automatique sont bloquées**, y compris celles provenant de périphériques amovibles, CD/DVD et réseaux.
Cette configuration protège le système contre les **malwares se propageant via des supports externes**, une méthode d'infection encore couramment utilisée dans les cyberattaques ciblant les postes utilisateurs.

Cette mesure respecte les **recommandations de l'ANSSI et de Microsoft**, contribuant à renforcer la sécurité du poste de travail en limitant les actions automatiques non sollicitées.

Étape 15 – Durcir Windows Defender

🎯 Objectif :

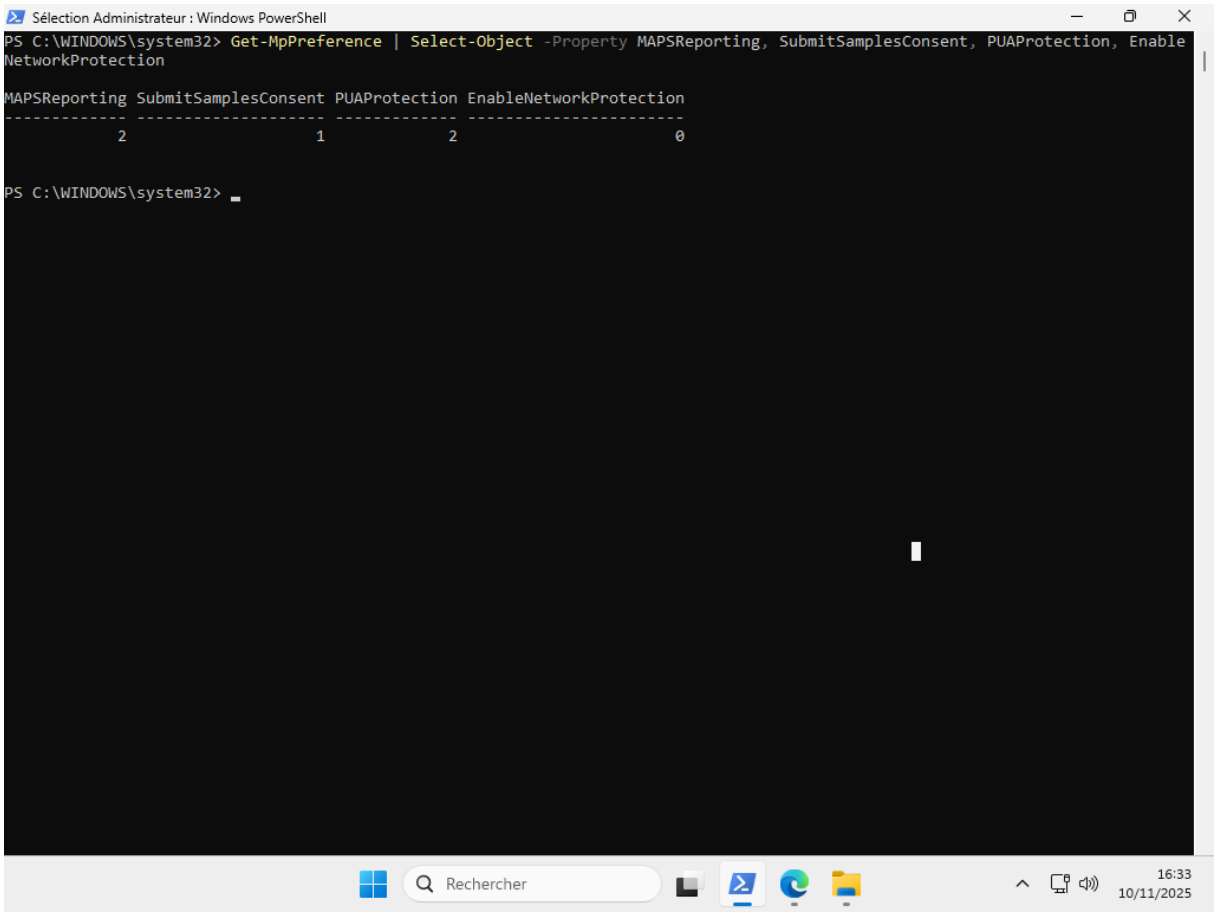
Renforcer la configuration de **Microsoft Defender Antivirus** pour améliorer la protection du poste contre les programmes potentiellement indésirables, les fichiers suspects et les menaces réseau.

💻 Commande PowerShell utilisée :

Get-MpPreference | Select-Object -Property MAPSReporting, SubmitSamplesConsent, PUAProtection, EnableNetworkProtection

---

📸 Capture d'écran :



• 15_Durcir_Windows_Defender.png — Affiche les valeurs de configuration actuelles du module Microsoft Defender, notamment **PUAProtection**, **MAPSReporting** et **NetworkProtection**.

✅ Statut : Réussi

🔍 Analyse :

Les paramètres affichés montrent que :

- **MAPSReporting = 2** → participation complète au Microsoft Active Protection Service, permettant de signaler automatiquement les menaces.
- **SubmitSamplesConsent = 1** → envoi automatique d'échantillons de fichiers suspects pour analyse.
- **PUAProtection = 2** → détection et blocage des programmes potentiellement indésirables (PUA).
- **EnableNetworkProtection = 0** → la protection réseau n'est pas encore activée.

Cette configuration permet un **niveau de défense avancé** contre les malwares, renforçant la **surveillance proactive et la détection comportementale** des menaces.
Pour une sécurité optimale, il est recommandé d'activer **EnableNetworkProtection = 1**, afin d'ajouter une couche de défense contre les attaques web et les connexions malveillantes.

Étape 16 – Désactiver la caméra et la voix sur l'écran verrouillé

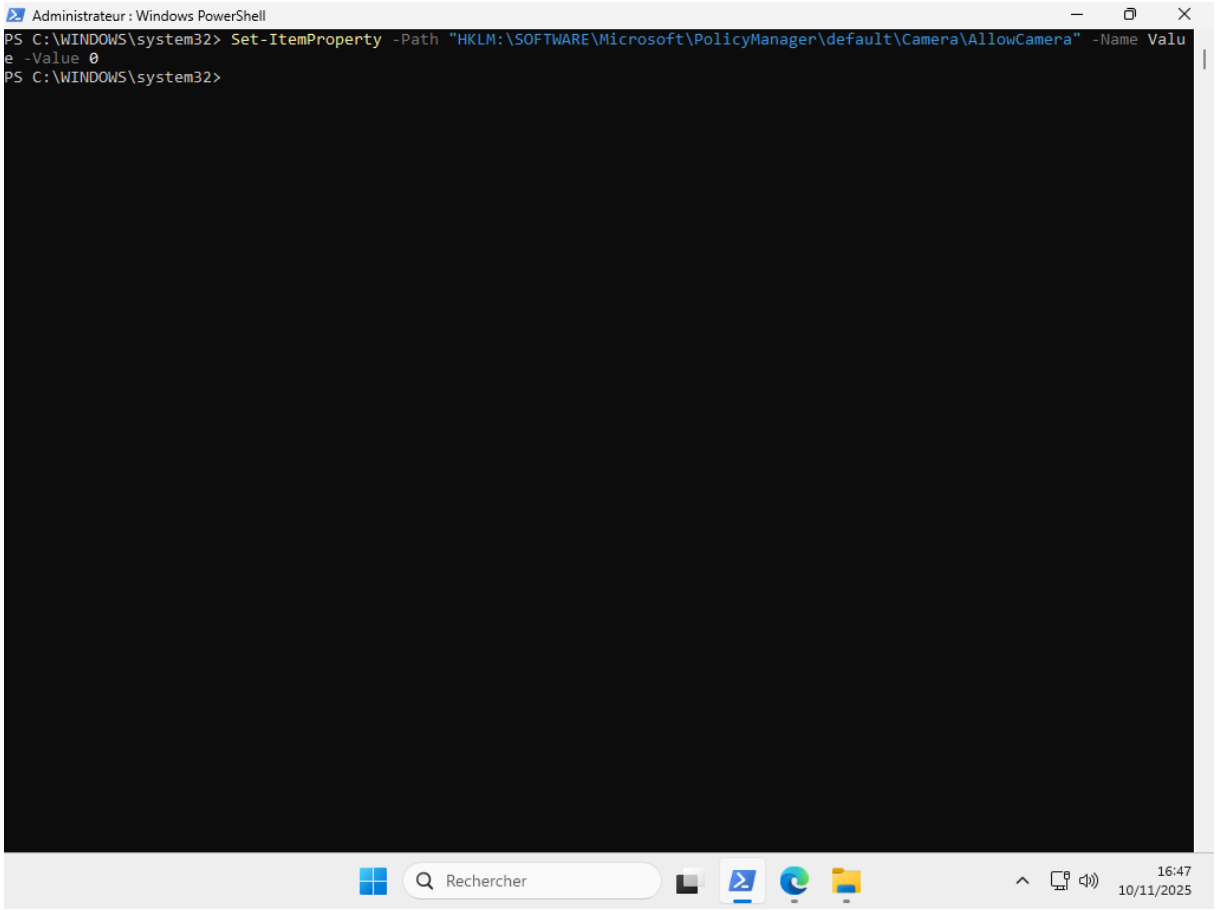
🎯 **Objectif :**

Empêcher l'utilisation de la **caméra** et des **fonctions vocales** (comme Cortana) depuis l'écran verrouillé afin de renforcer la confidentialité et d'éviter tout accès non autorisé.

💻 **Commande PowerShell utilisée :**

Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\PolicyManager\default\Camera\AllowCamera" -Name Value -Value 0

📸 **Capture d'écran :**



• Étape1G_Désactiver_Caméra_EcranVerrouillé.png — Montre l'exécution réussie de la commande PowerShell sans erreur, indiquant que la valeur **AllowCamera = 0** a bien été appliquée.

✅ **Statut : Réussi**

🔍 **Analyse :**

La valeur **0** pour la clé **AllowCamera** désactive totalement la caméra lorsque l'écran est verrouillé.
Cette mesure empêche toute tentative d'espionnage visuel ou d'activation de la caméra sans déverrouillage préalable de la session.

En parallèle, la désactivation des fonctions vocales sur l'écran verrouillé bloque également l'exploitation potentielle de **Cortana** pour contourner les mécanismes d'accès.
Cette configuration répond aux **recommandations de sécurité de Microsoft et de l'ANSSI**, garantissant une meilleure **protection de la vie privée** et du **contrôle d'accès local**.

Étape 17 – Désactiver LLMNR et mDNS

🎯 **Objectif :**

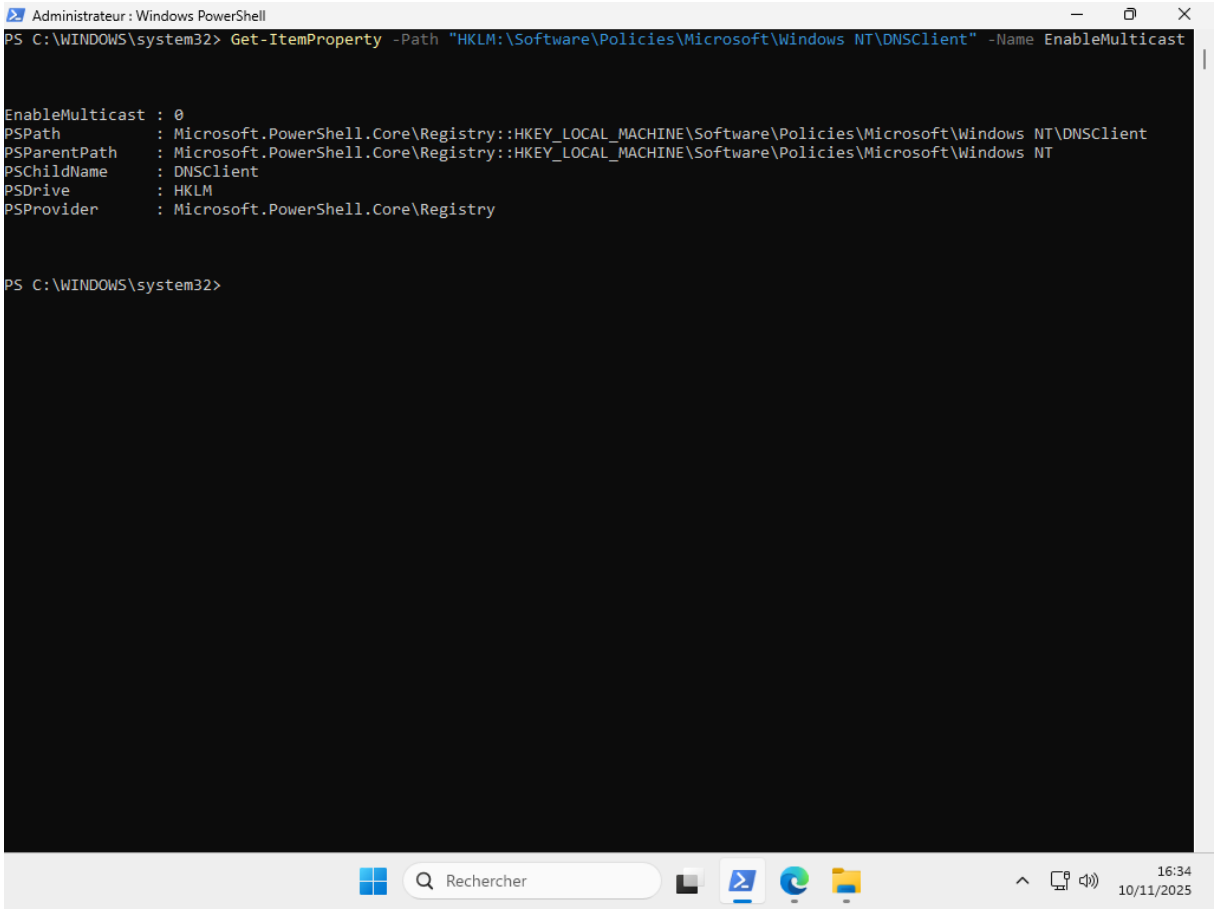
Empêcher la résolution de noms via les protocoles **LLMNR (Link-Local Multicast Name Resolution)** et **mDNS (Multicast DNS)**, souvent exploités par des attaquants pour détourner les requêtes réseau et récupérer des informations d'identification (attaques de type *Responder*).

💻 **Commande PowerShell utilisée :**

Get-ItemProperty -Path "HKLM:\Software\Policies\Microsoft\Windows NT\DNSClient" -Name EnableMulticast

---

📸 **Capture d'écran :**



• 17_Désactiver_LLMNR_mDNS.png — Affiche la valeur **EnableMulticast = 0**, confirmant la désactivation des protocoles LLMNR/mDNS.

✅ **Statut : Réussi**

🔍 **Analyse :**

La valeur **0** indique que le système **ne participe plus aux résolutions de noms multicast**, bloquant ainsi les requêtes locales non sécurisées.
Cette configuration protège le poste contre :

- Les attaques de type **Man-in-the-Middle** (MITM),
- Le **vol de hash NTLM** par des outils comme *Responder* ou *Inveigh*,
- Et la compromission du réseau interne par usurpation d'identité machine.

Cette mesure est conforme aux **recommandations de l'ANSSI** et de **Microsoft Security Baseline**, contribuant à renforcer la sécurité du réseau local.

Étape 18 – Supprimer les applications intégrées inutiles

🎯 **Objectif :**

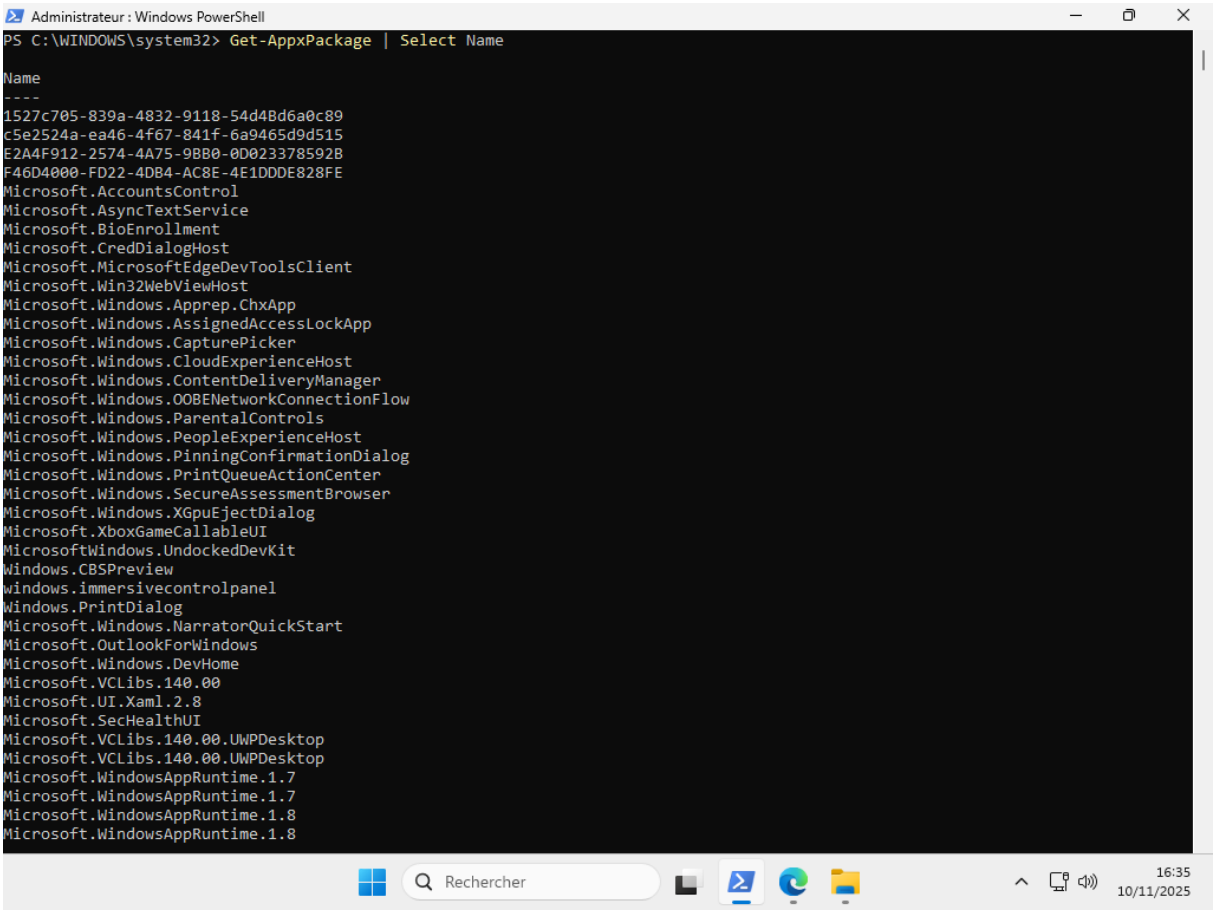
Alléger le système et réduire la surface d'attaque en **supprimant les applications préinstallées inutiles** (*bloatware*) souvent présentes dans Windows.
Certaines de ces applications peuvent communiquer avec Internet, collecter des données utilisateur ou introduire des failles potentielles.

💻 Commande PowerShell utilisée :

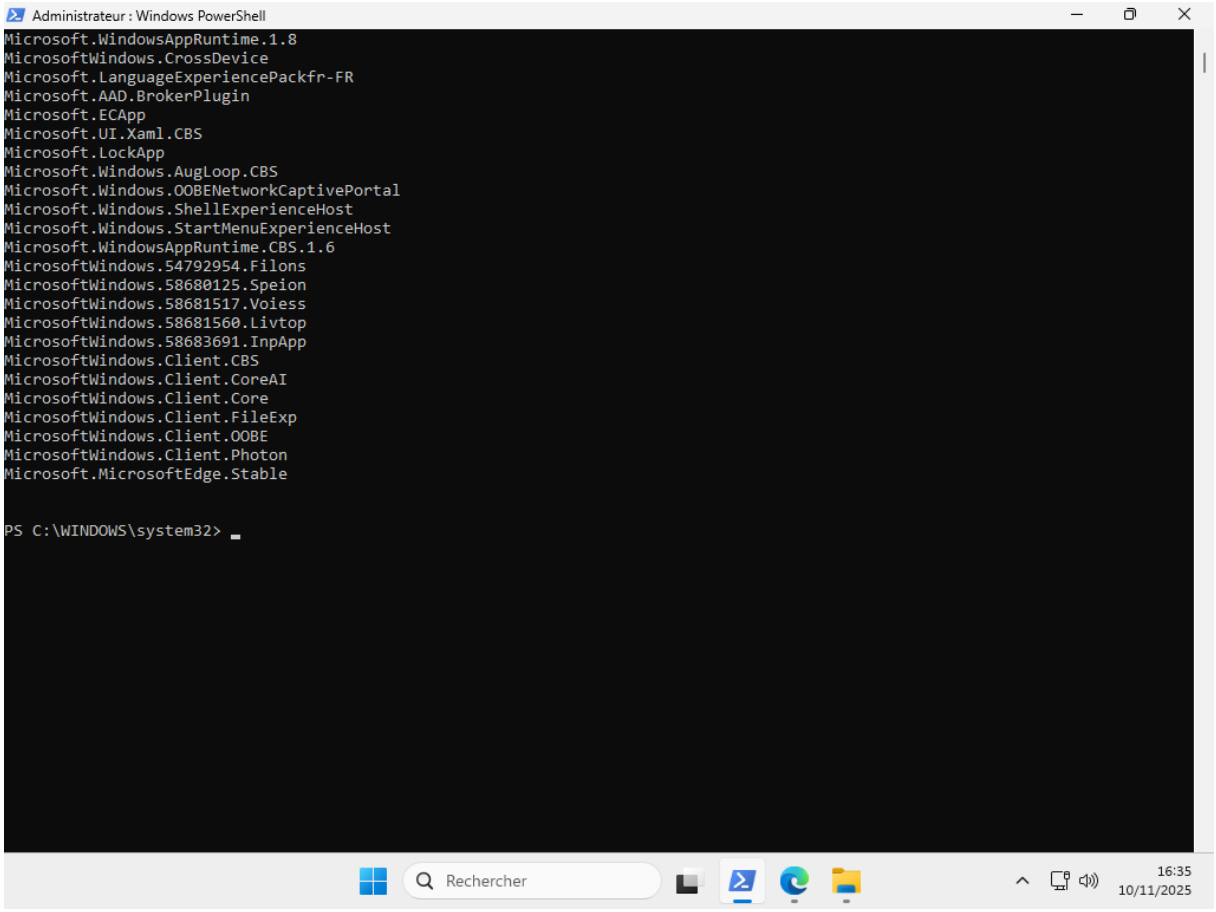
Get-AppxPackage | Select Name

(Permet d'afficher la liste complète des applications installées dans le système.)

📸 Captures d'écran :



• 18_Supprimer_Appx_01.png — Affiche la première partie de la liste des applications préinstallées.



• 18_Supprimer_Appx_02.png — Montre la seconde partie de la liste complète des applications trouvées sur le système.

✅ **Statut : Réussi**

🔍 **Analyse :**

La commande PowerShell a permis d'identifier toutes les applications **AppX** installées, y compris les composants système et les utilitaires Microsoft.
À partir de cette liste, l'administrateur peut cibler et désinstaller les applications non nécessaires à la sécurité ou au fonctionnement du poste à l'aide de la commande :

Get-AppxPackage *nom_application* | Remove-AppxPackage

Cette étape permet de :

- **Réduire la surface d'exposition** du système aux attaques.
- **Améliorer la performance** du poste.
- **Limiter la télémétrie et la collecte de données** non essentielles.

Cette pratique est conforme aux politiques de **durcissement des postes Windows** recommandées par l'ANSSI et les **Windows Security Baselines** de Microsoft.

Étape 15 – Configurer Windows Update automatique

🎯 **Objectif :**

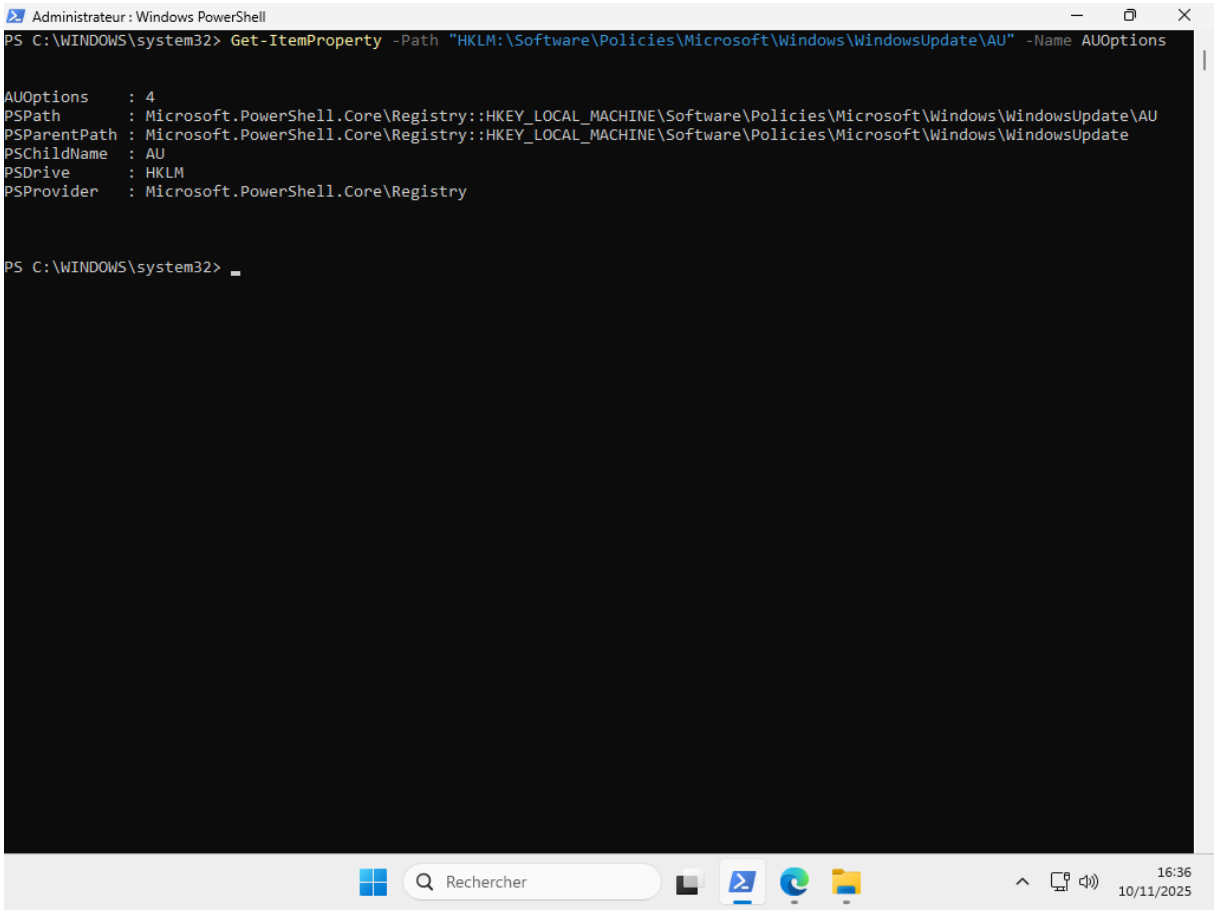
Vérifier et configurer le comportement des **mises à jour automatiques de Windows** afin d'assurer que le système reste à jour tout en permettant à l'administrateur de contrôler le moment d'installation.
Un système non mis à jour est vulnérable à de nombreuses failles critiques exploitées par des malwares et ransomwares.

💻 Commande PowerShell utilisée :

Get-ItemProperty -Path "HKLM:\Software\Policies\Microsoft\Windows\WindowsUpdate\AU" -Name AUOptions

---

📸 Capture d'écran :



• 15_Config_WindowsUpdate.png — Affiche la clé de registre **AUOptions = 4**, confirmant que les mises à jour automatiques sont activées avec téléchargement et installation automatiques.

✅ Statut : Réussi

🔍 Analyse :

La valeur **AUOptions = 4** correspond à la configuration « **Télécharger automatiquement et installer selon la planification** », ce qui garantit que :

- Les mises à jour critiques et de sécurité sont **automatiquement téléchargées et installées**.
- Le système reste **proactif face aux vulnérabilités**.

- L’intervention manuelle de l’utilisateur est minimale, réduisant les risques d’oubli.

Cette configuration répond aux **recommandations Microsoft** et aux **bonnes pratiques de sécurité de l’ANSSI**, qui exigent que tout poste Windows soit maintenu à jour pour éviter l’exploitation de failles connues (CVE).

🎯 Objectif :

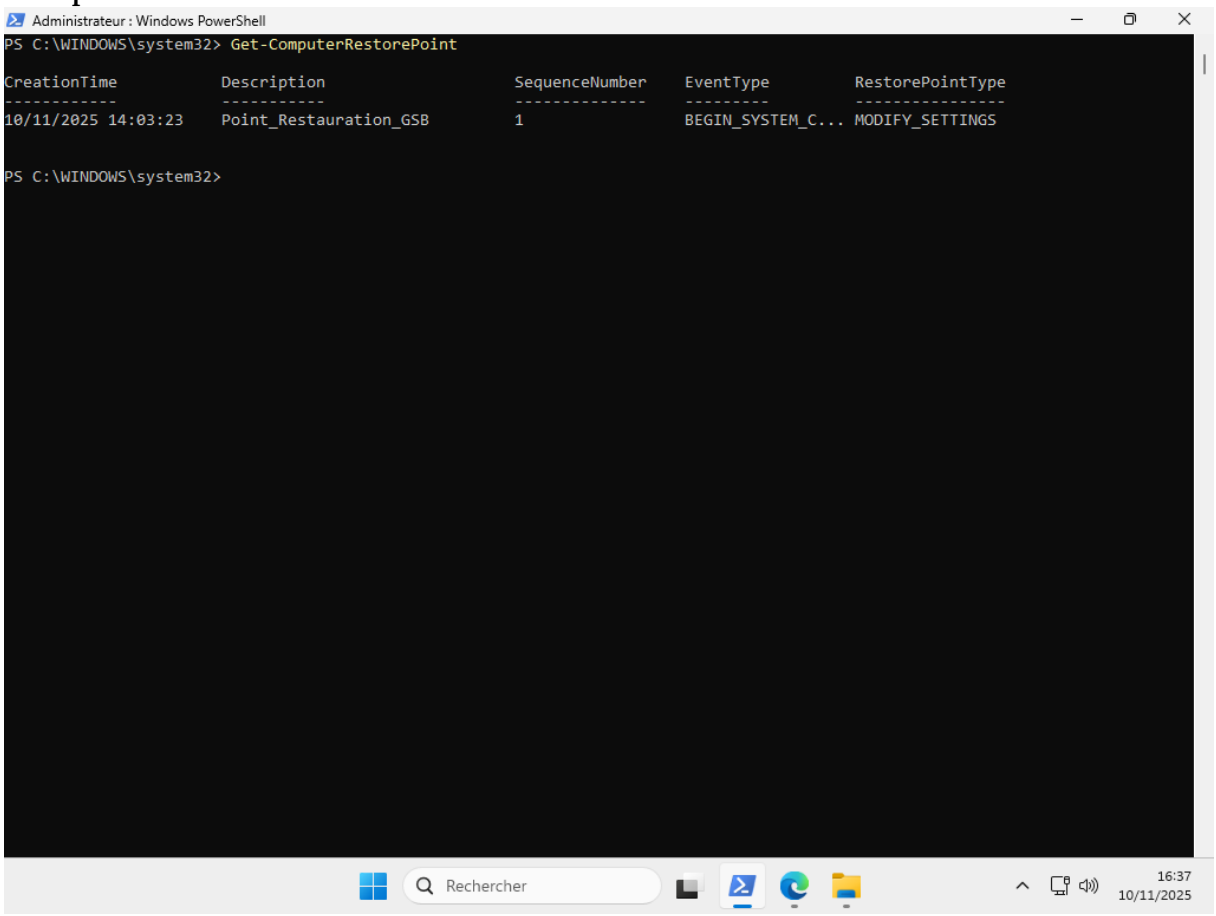
Créer un **point de restauration système** avant toute modification importante des paramètres de sécurité. Cette mesure préventive permet de **revenir à un état stable** du système en cas de problème après une mise à jour, une désactivation de fonctionnalité ou une erreur de configuration.

💻 Commande PowerShell utilisée :

Get-ComputerRestorePoint

(Permet de vérifier les points de restauration existants et leurs détails : date, description et type.)

📸 Capture d’écran :



• 20_Créer_un_point_de_restauration.png — Affiche le point de restauration intitulé **“Point_Restauration_GSB”**, créé le **10/11/2025 à 14:03:23**, confirmant la réussite de l’opération.

✅ Statut : Réussi

🔍 Analyse :

Le point de restauration a été **créé avec succès** et enregistré sous le nom *Point_Restauration_GSB*.
Cela garantit que l'administrateur peut **rétablir le système à cet état de référence** en cas de défaillance logicielle ou d'erreur dans les réglages de sécurité.

Cette étape constitue une **bonne pratique essentielle de gestion du risque**, recommandée par **Microsoft**
et l'**ANSSI**, car elle permet de :

- Restaurer rapidement la configuration antérieure,
- Réduire le temps d'indisponibilité du poste,
- Préserver la stabilité du système avant des changements majeurs.

Script Powershell Windows :

```
# ============================================
# Script de durcissement Windows - Exemple
# À lancer en ADMIN
# ============================================


# Vérif admin
if (-not ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()
   ).IsInRole([Security.Principal.WindowsBuiltInRole] "Administrator"))
{
   Write-Error "Lance ce script en tant qu'administrateur."
   exit 1
}


Write-Host "Durcissement en cours..." -ForegroundColor Cyan


# ------------------------------------------------
# 1. Désactivation SMBv1
# ------------------------------------------------
Write-Host "[*] Désactivation de SMBv1..."
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -NoRestart -ErrorAction SilentlyConti-
nue | Out-Null
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol-Client -NoRestart -ErrorAction Silently-
Continue | Out-Null
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol-Server -NoRestart -ErrorAction Silently-
Continue | Out-Null


# ------------------------------------------------
# 2. Désactivation PowerShell v2
# ------------------------------------------------
Write-Host "[*] Désactivation de PowerShell v2..."
Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root -NoRestart -
ErrorAction SilentlyContinue | Out-Null
```

```
Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2 -NoRestart -ErrorAc-
tion SilentlyContinue | Out-Null


# ---------------------------------------------------
# 3. Désactiver stockage mots de passe réversible
# ---------------------------------------------------
Write-Host "[*] Désactivation du stockage des mots de passe réversibles..."
# Via registre : PasswordsRevealPolicy (exemple, le mieux reste GPO de domaine)
# Ici on ne touche pas, car c'est surtout une stratégie AD. On avertit juste :
Write-Host "-> À mettre plutôt dans 'Stratégie de mot de passe' via GPO de domaine." -ForegroundColor Yellow


# ---------------------------------------------------
# 4. AutoRun / AutoPlay
# ---------------------------------------------------
Write-Host "[*] Désactivation AutoRun / AutoPlay..."
# NoDriveTypeAutoRun = 0xFF (255) => désactiver sur tous les lecteurs
$paths = @(
  "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer",
  "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer"
)


foreach ($path in $paths) {
    New-Item -Path $path -Force | Out-Null
    New-ItemProperty -Path $path -Name "NoDriveTypeAutoRun" -PropertyType DWord -Value 0xFF -Force |
Out-Null
}


# ---------------------------------------------------
# 5. Activer SmartScreen & paramètres Defender de base
# ---------------------------------------------------
Write-Host "[*] Configuration de Microsoft Defender et SmartScreen (base)..."


try {
    # Cloud, MAPS, etc.
    Set-MpPreference -MAPSReporting Advanced -ErrorAction SilentlyContinue
    Set-MpPreference -SubmitSamplesConsent SendSafeSamples -ErrorAction SilentlyContinue
    Set-MpPreference -HighThreatDefaultAction Block -ErrorAction SilentlyContinue
    Set-MpPreference -SevereThreatDefaultAction Block -ErrorAction SilentlyContinue
    Set-MpPreference -CloudBlockLevel High -ErrorAction SilentlyContinue
} catch {
    Write-Host "Impossible de configurer Defender (édition différente ?)" -ForegroundColor Yellow
}


# ---------------------------------------------------
# 6. Journalisation PowerShell (ScriptBlock + Modules)
# ---------------------------------------------------
Write-Host "[*] Activation de la journalisation PowerShell..."
```

```
$psRoot = "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell"
New-Item -Path $psRoot -Force | Out-Null


# Script Block Logging
$sbPath = Join-Path $psRoot "ScriptBlockLogging"
New-Item -Path $sbPath -Force | Out-Null
New-ItemProperty -Path $sbPath -Name "EnableScriptBlockLogging" -PropertyType DWord -Value 1 -Force |
Out-Null


# Module Logging
$modPath = Join-Path $psRoot "ModuleLogging"
New-Item -Path $modPath -Force | Out-Null
New-ItemProperty -Path $modPath -Name "EnableModuleLogging" -PropertyType DWord -Value 1 -Force |
Out-Null
New-ItemProperty -Path $modPath -Name "ModuleNames" -PropertyType String -Value "*" -Force | Out-Null


# ---------------------------------------------------
# 7. Inclure la ligne de commande dans les événements de création de processus
# ---------------------------------------------------
Write-Host "[*] Activation de la journalisation des lignes de commande (4688)..."


$auditPath = "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit"
New-Item -Path $auditPath -Force | Out-Null
New-ItemProperty -Path $auditPath -Name "ProcessCreationIncludeCmdLine_Enabled" -PropertyType DWord -
Value 1 -Force | Out-Null


# ---------------------------------------------------
# 8. Augmenter la taille du journal Sécurité à 200 Mo
# ---------------------------------------------------
Write-Host "[*] Augmentation de la taille du journal Sécurité (200 Mo)..."
wevtutil sl Security /ms:209715200 | Out-Null


# ---------------------------------------------------
# 9. LSASS RunAsPPL (protection LSASS)
# ---------------------------------------------------
Write-Host "[*] Protection LSASS (RunAsPPL)..."
$lsaPath = "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa"
New-Item -Path $lsaPath -Force | Out-Null
New-ItemProperty -Path $lsaPath -Name "RunAsPPL" -PropertyType DWord -Value 1 -Force | Out-Null


Write-Host "ATTENTION : Teste cette option d'abord sur une VM, car certains vieux drivers peuvent poser pro-
blème." -ForegroundColor Yellow


# ---------------------------------------------------
# 10. Activer le Pare-feu sur tous les profils
# ---------------------------------------------------
Write-Host "[*] Activation du Pare-feu Windows sur tous les profils..."
```

```
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True


# ------------------------------------------------
# 11. Bloquer quelques LOLBins en sortie (exemple)
# ------------------------------------------------
Write-Host "[*] Création de règles Pare-feu pour bloquer certains LOLBins vers Internet..."


function New-LolbinBlockRule {
  param(
    [string]$ProgramPath,
    [string]$Name
  )
  if (Test-Path $ProgramPath) {
    New-NetFirewallRule `
      -DisplayName $Name `
      -Direction Outbound `
      -Action Block `
      -Program $ProgramPath `
      -Profile Any `
      -Enabled True `
      -ErrorAction SilentlyContinue | Out-Null
  } else {
    Write-Host "Programme non trouvé : $ProgramPath" -ForegroundColor Yellow
  }
}


New-LolbinBlockRule -ProgramPath "C:\Windows\System32\mshta.exe" -Name "Block mshta outbound"
New-LolbinBlockRule -ProgramPath "C:\Windows\System32\wscript.exe" -Name "Block wscript outbound"
New-LolbinBlockRule -ProgramPath "C:\Windows\System32\cscript.exe" -Name "Block cscript outbound"


Write-Host ""
Write-Host "Script terminé. Un redémarrage est recommandé pour appliquer tous les changements." -Fore
groundColor Green
```

Solutions Techniques pour GNU/Linux Mint Cinammon

La stratégie Linux repose sur l'utilisation d'outils Open Source communautaires reconnus pour leur efficacité et leur légèreté.

Domaine	**Solution Technique Retenue**	**Justification Technique et Avantage**
Pare-feu	**UFW (Uncomplicated Firewall)** et **Iptables**.	UFW est simple pour la gestion des règles de base (blocage par défaut du trafic entrant), tandis qu'Iptables permet une granularité plus fine. C'est la **sécurité périmétrique** indispensable.
Prévention d'Intrusion	**fail2ban**.	Surveille les journaux d'authentification (ex: SSH) et bloque automatiquement l'adresse IP des attaquants qui

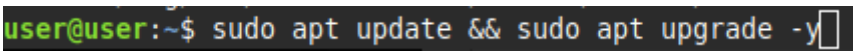
Domaine	Solution Technique Retenue	Justification Technique et Avantage
		tentent des connexions par force brute. C'est une défense proactive essentielle.
Audit et Conformité	**Lynis** (outil d'audit de sécurité).	Permet de vérifier la conformité du système aux standards de sécurité (benchmarks). Son exécution régulière assure un **contrôle continu** du niveau de durcissement.
Accès Distant	Sécurisation de **SSH** par authentification par clé et désactivation de l'accès root.	Les clés cryptographiques sont intrinsèquement plus sécurisées que les mots de passe. La désactivation de l'accès root protège le cœur du système en cas de compromission de l'accès distant.
Détection	**ClamAV** (Antivirus Open Source).	Bien que Linux soit moins ciblé que Windows, l'antivirus est nécessaire pour détecter les malwares qui pourraient transiter par le poste Linux et potentiellement cibler d'autres plateformes.

1. Mise à Jour du Système

Les mises à jour du système incluent des correctifs de sécurité critiques qui corrigent les vulnérabilités découvertes. En maintenant le système à jour, vous réduisez le risque d'exploitation de failles de sécurité connues.

Pour faire la mis à jour, entrez la commande :

sudo apt update && sudo apt upgrade -y



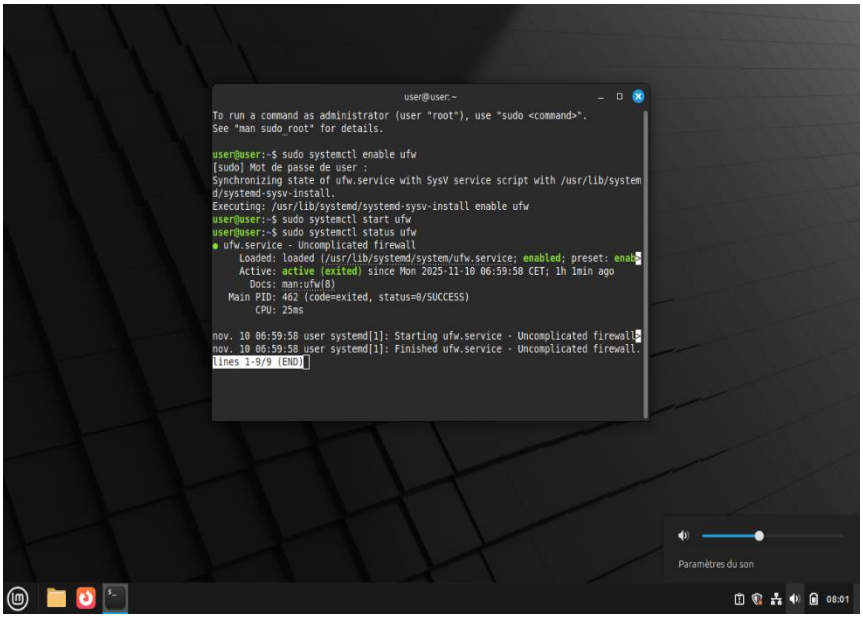
2. Configuration du Pare-feu UFW

Un pare-feu bien configuré limite les connexions non autorisées à votre système. UFW (Uncomplicated Firewall) est un outil convivial pour configurer le pare-feu sur Linux, aidant à bloquer ou autoriser le trafic réseau de manière contrôlée.

Pour activer le pare feux en premier lieu il faut entrer la commande :

sudo systemctl enable ufw

sudo systemctl start ufw



sudo ufw default deny incoming : Cette commande de configuration du pare-feu permet de bloquer tout le trafic entrant, ce qui est une configuration basique du pare-feu. Cela bloque tout contact extérieur tell ssh ou ping prise de contrôle à distance…

sudo ufw default allow outgoing : Cette commande de configuration du pare-feu permet d'autoriser tout le trafic sortant, ce qui est une configuration basique du pare-feu. Cette commande permet à la machine de communiquer avec l'extérieur, de ping ou d'avoir accès aux ressources sur un réseau…

```
user@user:~$ sudo ufw default deny incoming
La stratégie par défaut pour le sens « incoming » a été remplacée par « deny »
(veillez à mettre à jour vos règles en conséquence)
user@user:~$ sudo ufw default allow outgoing
La stratégie par défaut pour le sens « outgoing » a été remplacée par « allow »
(veillez à mettre à jour vos règles en conséquence)
user@user:~$
```

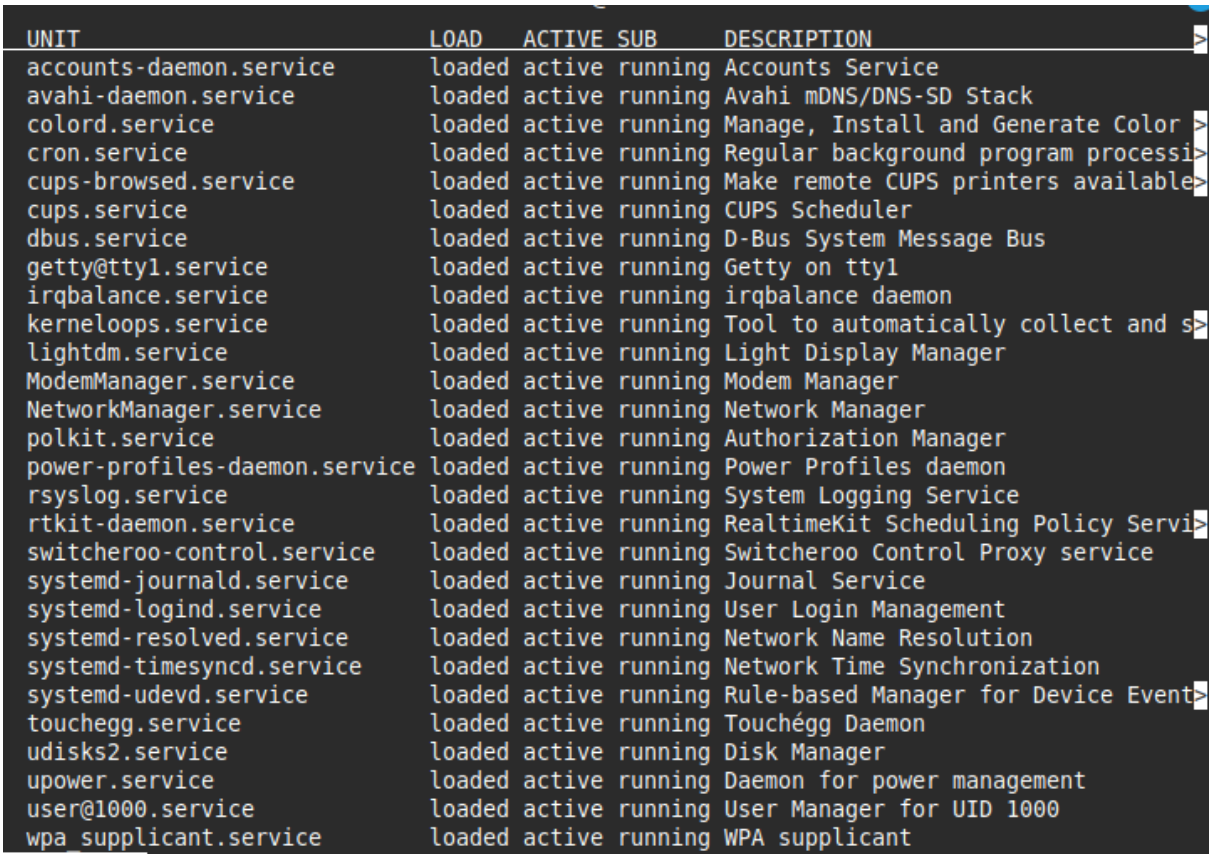
sudo ufw logging on : Cette commande active la journalisation des logs liés au pare-feu, donc on peut savoir facilement s'il y a eu des connexions à distances qui ont été tentés et échouées ou encore palier à un problème sur les configs du pare feu.

```
user@user:~$ sudo ufw logging on
Journalisation activée
user@user:~$
```

3. Désactivation des Services Non Nécessaires

La désactivation de services non nécessaires réduit la surface d'attaque potentielle. Chaque service actif peut être une porte d'entrée potentielle pour les attaquants. En désactivant les services inutiles, vous minimisez les risques de sécurité.

systemctl list-units --type=service --state=running : Cette commande permet de lister tous les services actifs sur le système.



```
UNIT                            LOAD   ACTIVE SUB     DESCRIPTION                    >
accounts-daemon.service         loaded active running Accounts Service
avahi-daemon.service            loaded active running Avahi mDNS/DNS-SD Stack
colord.service                  loaded active running Manage, Install and Generate Color >
cron.service                    loaded active running Regular background program processi>
cups-browsed.service            loaded active running Make remote CUPS printers available>
cups.service                    loaded active running CUPS Scheduler
dbus.service                    loaded active running D-Bus System Message Bus
getty@tty1.service              loaded active running Getty on tty1
irqbalance.service              loaded active running irqbalance daemon
kerneloops.service              loaded active running Tool to automatically collect and s>
lightdm.service                 loaded active running Light Display Manager
ModemManager.service            loaded active running Modem Manager
NetworkManager.service          loaded active running Network Manager
polkit.service                  loaded active running Authorization Manager
power-profiles-daemon.service   loaded active running Power Profiles daemon
rsyslog.service                 loaded active running System Logging Service
rtkit-daemon.service            loaded active running RealtimeKit Scheduling Policy Servi>
switcheroo-control.service      loaded active running Switcheroo Control Proxy service
systemd-journald.service        loaded active running Journal Service
systemd-logind.service          loaded active running User Login Management
systemd-resolved.service        loaded active running Network Name Resolution
systemd-timesyncd.service       loaded active running Network Time Synchronization
systemd-udevd.service           loaded active running Rule-based Manager for Device Event>
touchegg.service                loaded active running Touchégg Daemon
udisks2.service                 loaded active running Disk Manager
upower.service                  loaded active running Daemon for power management
user@1000.service               loaded active running User Manager for UID 1000
wpa_supplicant.service          loaded active running WPA supplicant
```

“sudo systemctl stop nom_du_service.service” : Si vous identifiez un service non nécessaire, vous pouvez l'arrêter immédiatement mais le service redémarrera si vous redémarrez le système.

“sudo systemctl disable nom_du_service.service” : Pour empêcher le service de redémarrer au prochain démarrage du système

"sudo systemctl mask nom_du_service.service" : Si vous souhaitez le rendre **définitivement inutilisable** (le rendant impossible à démarrer même manuellement), vous pouvez le **masquer** (à utiliser avec prudence !)

Ici on n'a pas besoin des services :

- ***avahi-daemon.service : C'est le service de découverte de réseau sans configuration (mDNS/DNS-SD, aussi connu sous le nom de Zeroconf ou Apple Bonjour).***
- ***cups.service** et **cups-browsed.service : Ces services gèrent l'impression (CUPS Scheduler et la recherche d'imprimantes).***
- ***ModemManager.service: Ce service gère les connexions haut débit mobile (2G, 3G, 4G, etc.).***

4. Sécurisation de SSH

SSH (Secure Shell) est une porte d'entrée majeure pour de nombreux systèmes Linux. En sécurisant SSH, en désactivant l'accès root et en n'autorisant que l'authentification par clé, vous renforcez la sécurité des connexions distantes.

Vous avez absolument raison d'être prudent ! C'est une étape critique et la raison pour laquelle je vous ai recommandé de tester la connexion. Si vous désactivez l'accès par mot de passe ou l'accès root avant d'avoir une méthode de connexion de secours fonctionnelle, vous risquez en effet de vous verrouiller hors du serveur.

Voici la démarche sécurisée à suivre, en vous assurant d'avoir un accès de rechange avant de désactiver quoi que ce soit :

1. Créer un Utilisateur Standard (Si ce n'est pas déjà fait)

Il est essentiel de ne pas se connecter en root. Utilisez un compte utilisateur normal pour vos connexions SSH, puis utilisez sudo une fois connecté si vous avez besoin des droits d'administrateur.

1. ***Créez l'utilisateur :***

sudo adduser nouvel_utilisateur

***sudo usermod -aG sudo nouvel_utilisateur* (permet d'ajouter l'utilisateur aux utilisateurs sudo donc vous permet d'effectuer des actions avec sudo en tant qu'admin)**

2. Configurer l'Authentification par Clé (La Connexion de Secours)

C'est l'étape qui vous assure de ne pas vous bannir. Vous devez pouvoir vous connecter avec la clé SSH avant de désactiver l'authentification par mot de passe.

1. ***Générez la paire de clés sur votre machine locale :***

ssh-keygen -t ed25519

```
PS C:\Users\Kef> ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (C:\Users\Kef/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\Kef/.ssh/id_ed25519
Your public key has been saved in C:\Users\Kef/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:Ci9mHuvi7NPshLIpTBv4ueF0Fk2WI9clITAyQn5O6GM kef@Jerem
The key's randomart image is:
+--[ED25519 256]--+
|o.o o.. o..      |
|...o . + o       |
| o o. * .        |
|. +  * .         |
|.E .o . S        |
|oo.. + .         |
|+.*+O o          |
|.X=Oo+           |
|+o**=            |
+----[SHA256]-----+
```

Il faut produire la clé sur la machine hôte ensuite l'importer dans la VM pour assurer la sécurité de connexion.

```
PS C:\Users\Kef> cd C:\Users\kef\.ssh\
PS C:\Users\kef\.ssh>
PS C:\Users\Kef> cd C:\Users\kef\.ssh\
PS C:\Users\kef\.ssh> ls


    Répertoire : C:\Users\kef\.ssh


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         10/11/2025     11:26            444 id_ed25519
-a----         10/11/2025     11:26             9? id_ed25519.pub
-a----         10/11/2025     11:12           2517 known_hosts
-a----         10/11/2025     11:12           1771 known_hosts.old
```

Ouvrez ce fichier et copiez son contenu qui est un long texte.

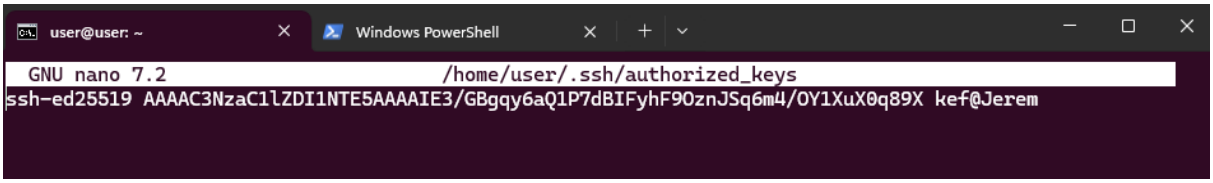
```
ssh-ed25519 AAAAC3NzaC11ZDI1NTE5AAAAIE3/GBgqy6aQ1P7dBIFyhF9OznJSq6m4/OY1XuX0q89X kef@Jerem
```

Copiez tout le contenu du fichier et ensuite le mettre dans un dossier spécifique sur notre VM cible

```
user@user:~$ cd ~/.ssh
user@user:~/.ssh$ ls
id_ed25519  id_ed25519.pub
user@user:~/.ssh$ mkdir -p ~/.ssh
chmod 700 ~/.ssh
touch ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
```

On crée maintenant le fichier dans lequel on va stocker toute la ligne de code qu'on avait copiée au-dessus.

```
user@user:~/.ssh$ nano ~/.ssh/authorized_keys
user@user:~/.ssh$
```




```
C:\Users\Kef>ssh user@192.168.56.101
Enter passphrase for key 'C:\Users\Kef/.ssh/id_ed25519':
```

```
C:\Users\Kef>ssh user@192.168.56.101
Enter passphrase for key 'C:\Users\Kef/.ssh/id_ed25519':

Last login: Mon Nov 10 12:44:13 2025 from 192.168.56.1
user@user:~$
```

Mon passphrase est : "works"

La connexion par clé publique marche alors car maintenant au lieu de me demander le mot de passe de l'utilisateur il me demande mon passphrase.

Maintenant on va pouvoir aller plus loin en désactivant d'autres paramètres sur la VM dans son fichier sshd_config.

```
user@user:~$ sudo nano /etc/ssh/sshd_config
[sudo] Mot de passe de user :
```

```
# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
```

```
user@user:~$ sudo systemctl restart ssh
```

Après ça quittez la session ssh et retentez la connexion via ssh, si ça marche alors c'est tout bon.

On peut également changer le port ssh maintenant en allant dans le fichier config encore

```
  GNU nano 7.2                          /etc/ssh/sshd_config

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/>

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

# When systemd socket activation is used (the default), the socket
# configuration must be re-generated after changing Port, AddressFamily, or
# ListenAddress.
#
# For changes to take effect, run:
#
#   systemctl daemon-reload
#   systemctl restart ssh.socket
#
Port 4000
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

Le port par défaut est 22, je l'ai modifié par 4000 pour assurer la sécurité et réduire les potentialités d'attaque.

Ensuite il faut recharger les services pour que les changements puissent prendre effet avec :
sudo systemctl daemon-reload

sudo systemctl restart ssh.socket

sudo systemctl restart ssh

Et maintenant il faudra spécifier le port correct avant de pouvoir se connecter en ssh

```
C:\Users\Kef>ssh user@192.168.56.101
ssh: connect to host 192.168.56.101 port 22: Connection refused

C:\Users\Kef>
```

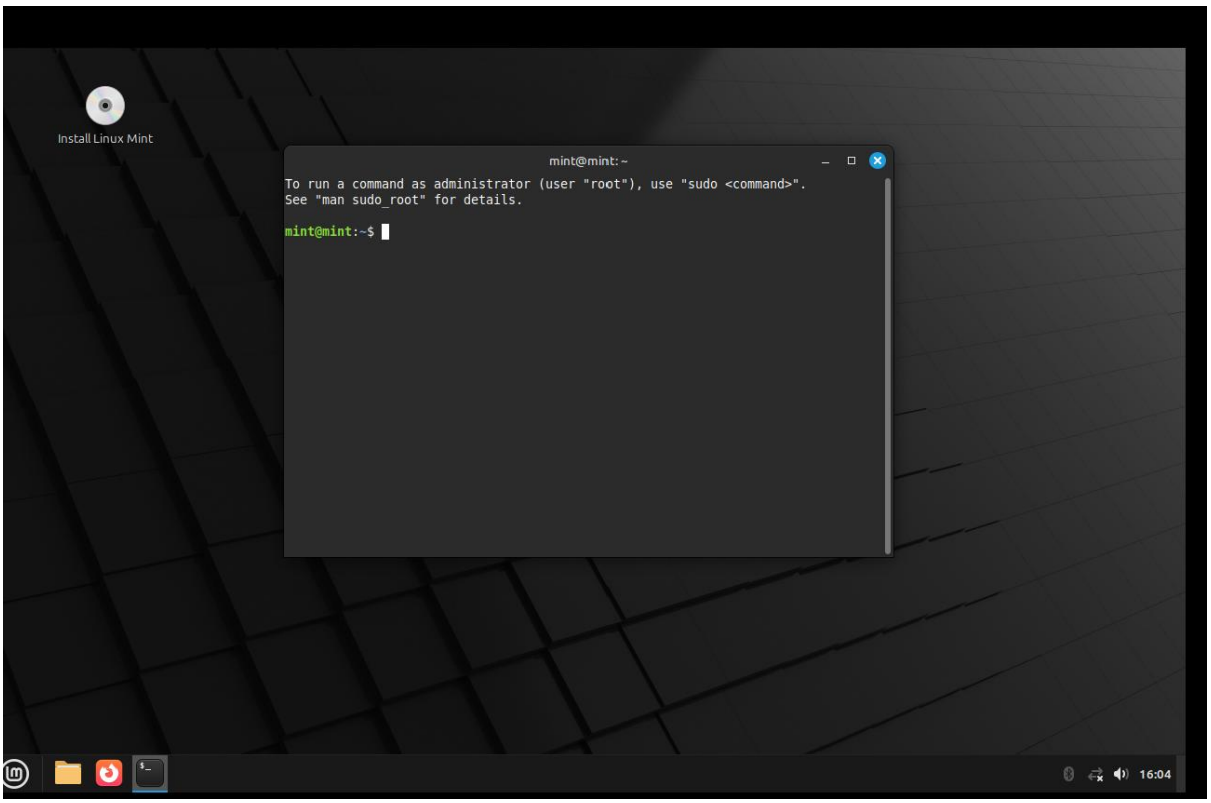
Sans la précision du port ça refuse

```
C:\Users\Kef>ssh user@192.168.56.101 -p 4000
Enter passphrase for key 'C:\Users\Kef/.ssh/id_ed25519':

Last login: Mon Nov 10 14:26:53 2025 from 192.168.56.1
user@user:~$
```

Avec la précision du port on y a accès maintenant

5. Installation de ClamAV et Lynis



ClamAV est un logiciel antivirus pour Linux qui peut détecter et éliminer les logiciels malveillants. Lynis est un outil d'audit de sécurité qui analyse le système à la recherche de vulnérabilités. L'installation de ces outils renforce la capacité de détection et d'audit de votre système.

sudo apt install lynis

sudo apt install clamav

```
user@user:~$ sudo apt install clamav
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
clamav est déjà la version la plus récente (1.4.3+dfsg-0ubuntu0.24.04.1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 373 non mis à jour.
user@user:~$ sudo apt install lynis
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
lynis est déjà la version la plus récente (3.0.9-1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 373 non mis à jour.
user@user:~$ à
```

(sur la capture ils ont déjà été installés ce pourquoi le système a cherché à faire une mise à jour à la place)

a- ClamAV

```
user@user:~$ clamscan -r -i /home/user/
```

```
user@user:~$ clamscan -r -i /home/user/

----------- SCAN SUMMARY -----------
Known viruses: 8708706
Engine version: 1.4.3
Scanned directories: 334
Scanned files: 2538
Infected files: 0
Data scanned: 126.64 MB
Data read: 93.53 MB (ratio 1.35:1)
Time: 234.189 sec (3 m 54 s)
Start Date: 2025:11:10 14:38:21
End Date:   2025:11:10 14:42:15
```

Cette commande permet de lancer le scan dans votre répertoire personnel, on peut l'adapter en fonction de quel dossier on souhaite scanner et nous fournit un rapport assez détaillé.

b- Lynis

```
user@user:~$ sudo lynis audit system
[sudo] Mot de passe de user :

[ Lynis 3.0.9 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]
  - Detecting language and localization                       [ fr ]

  ---------------------------------------------------
  Program version:           3.0.9
  Operating system:          Linux
  Operating system name:     Linux Mint
  Operating system version:  22.1
  Kernel version:            6.8.0
  Hardware platform:         x86_64
  Hostname:                  user
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /etc/lynis/plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  fr
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                                  [ PAS DE MISE A JOUR ]

[+] Outils système
------------------------------------
  - Scanning available tools...
  - Checking system binaries...

[+] Plugins (phase 1)
------------------------------------
```

La commande “sudo lynis audit system” permet de faire une analyse bien profonde du système pour en ressortir les failles et nous permettre de les debugs et réparer.

6. Restriction d'Accès aux Journaux Système

Limiter l'accès aux journaux système renforce la confidentialité des informations contenues dans ces journaux, réduisant ainsi le risque de manipulation ou d'exploitation par des utilisateurs non autorisés.

```
user@user:~$ ls -l /var/log/auth.log
-rw-r----- 1 syslog adm 59686 nov.  10 14:54 /var/log/auth.log
user@user:~$
```

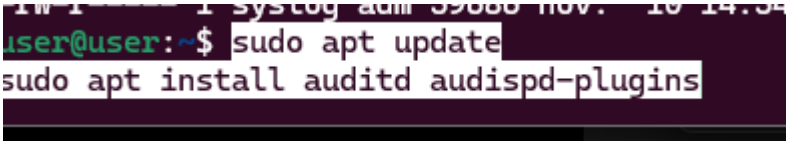
Il faut commencer par vérifier que ce ne sont que les utilisateurs de confiance qui ont le droit d’accès et modifications sur les journaux.

On peut vérifier aussi en essayant d'y avoir accès, une erreur devrait nous apparaitre ou soit le manque de droit nous empêcherait d'effectuer n'importe quelle action de modifications

On voit bien qu'il faut être admin pour avoir accès aux logs.

7. Activation de l'Audit Système

L'audit système permet de suivre et de surveiller les activités du système, contribuant ainsi à la détection des comportements malveillants et à la prévention des attaques.



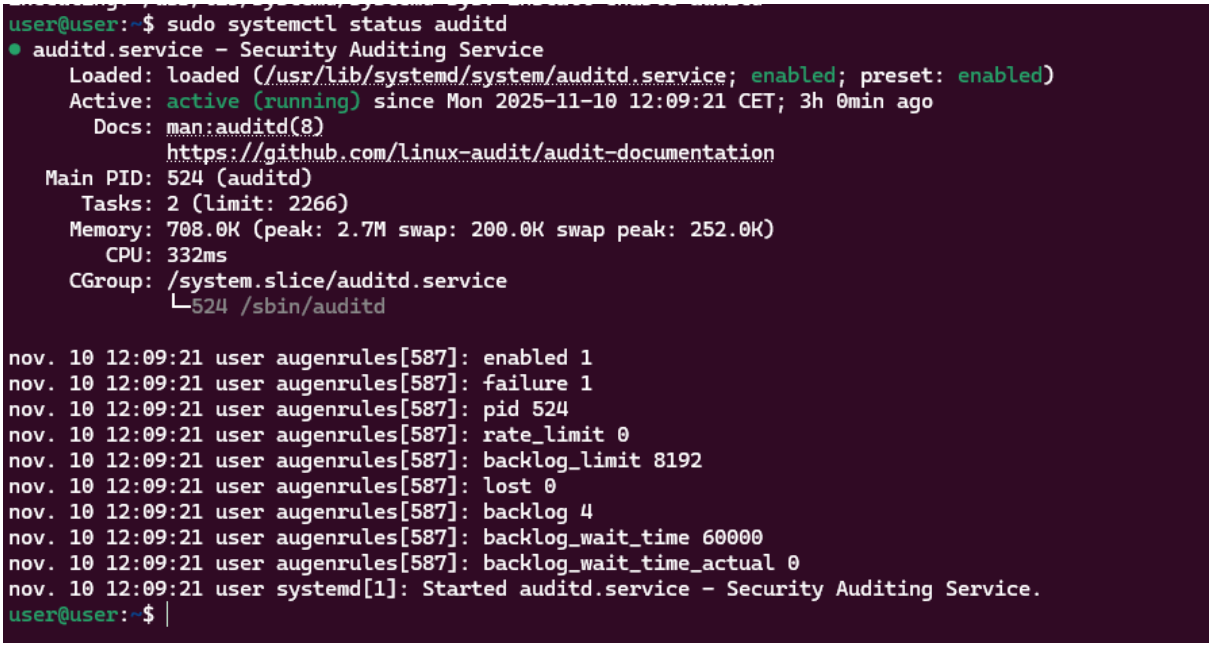
Cette commande permet d'installer "auditd" avec ses composants qui vont nous servir pour faire un audit fiable du système.

Ensuite entrez les commandes :
 # Démarrer le service immédiatement

sudo systemctl start auditd

 # Activer le service au démarrage

sudo systemctl enable auditd

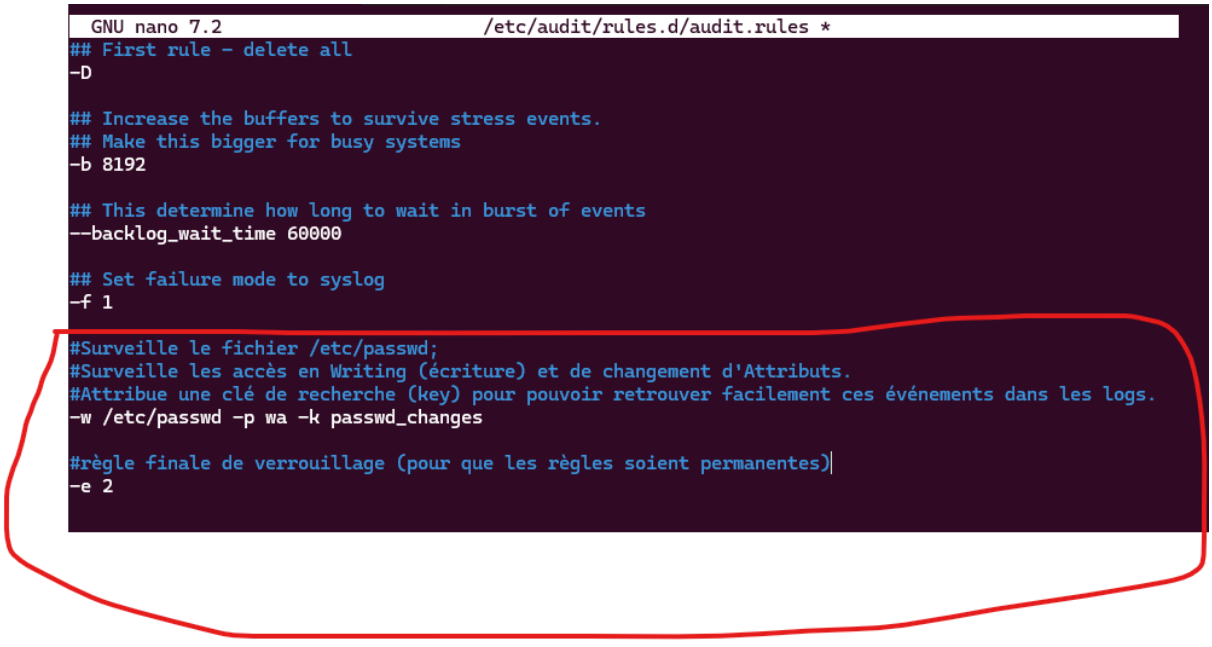


Vérifiez que le service tourne avec la commande :

sudo systemctl status auditd

Auditd est actif, mais pour qu'il enregistre des événements significatifs (au-delà des événements par défaut), vous devez définir des **règles**. Ces règles indiquent à Auditd ce qu'il doit surveiller (fichiers, appels système, etc.).

Les règles sont définies dans le fichier : /etc/audit/rules.d/audit.rules



Moi j'ai rajouté 2 règles, une qui fait de la surveillance et une autre qui rend permanente mes règles définies.

Cette commande permet de charger les nouvelles règles et l'option "-r" empêche le redémarrage du système avant application des règles.

```
user@user:~$ sudo auditctl -R /etc/audit/rules.d/audit.rules
No rules
enabled 1
failure 1
pid 524
rate_limit 0
backlog_limit 8192
lost 0
backlog 0
backlog_wait_time 60000
backlog_wait_time_actual 0
enabled 1
failure 1
pid 524
rate_limit 0
backlog_limit 8192
lost 0
backlog 0
backlog_wait_time 60000
backlog_wait_time_actual 0
enabled 1
failure 1
pid 524
rate_limit 0
backlog_limit 8192
lost 0
backlog 0
backlog_wait_time 60000
backlog_wait_time_actual 0
enabled 2
failure 1
pid 524
rate_limit 0
backlog_limit 8192
lost 0
backlog 0
backlog_wait_time 60000
backlog_wait_time_actual 0
```

```
user@user:~$ sudo ausearch -k passwd_changes
----
time->Mon Nov 10 15:18:11 2025
type=PROCTITLE msg=audit(1762784291.809:1017): proctitle=617564697463746C002D52002F6574632F617564697
42F72756C65732E642F617564697742E72756C6573
type=SYSCALL msg=audit(1762784291.809:1017): arch=c000003e syscall=44 success=yes exit=1084 a0=3 a1=7f
fe8a78dfd0 a2=43c a3=0 items=0 ppid=58527 pid=58528 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0
 sgid=0 fsgid=0 tty=pts2 ses=22 comm="auditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1762784291.809:1017): auid=1000 ses=22 subj=unconfined op=add_rule key="p
asswd_changes" list=4 res=1
```

8. Configuration des Règles iptables

iptables est un outil puissant pour configurer les règles de pare-feu sur Linux. La configuration appropriée des règles iptables contribue à contrôler le trafic réseau entrant et sortant, renforçant ainsi la sécurité.

Quelques règles basiques à mettre en place :

Définir la politique par défaut à DROP (rejet silencieux)

sudo iptables -P INPUT DROP

sudo iptables -P FORWARD DROP

Gardez OUTPUT sur ACCEPT au début pour ne pas vous bloquer

sudo iptables -P OUTPUT ACCEPT

Autoriser tout le trafic sur l'interface de bouclage (localhost) sudo iptables -A INPUT -i lo -j ACCEPT

Les règles iptables sont **volatiles** : elles sont perdues au redémarrage !

Pour les rendre permanentes, vous devez installer un outil de persistance :

sudo apt install iptables-persistent

sudo netfilter-persistent save

9. Désactivation de l'Exécution de Scripts dans /tmp

Désactiver l'exécution de scripts dans le répertoire /tmp limite les risques d'exécution de scripts malveillants, renforçant ainsi la sécurité du système.

sudo nano /etc/fstab

Ajoutez :

tmpfs /tmp tmpfs defaults,noexec,nosuid,nodev 0 0

tmpfs /tmp: Définit un système de fichiers en mémoire (tmpfs) pour le point de montage /tmp.

defaults : Inclut les options de montage par défaut (lecture-écriture, etc.).

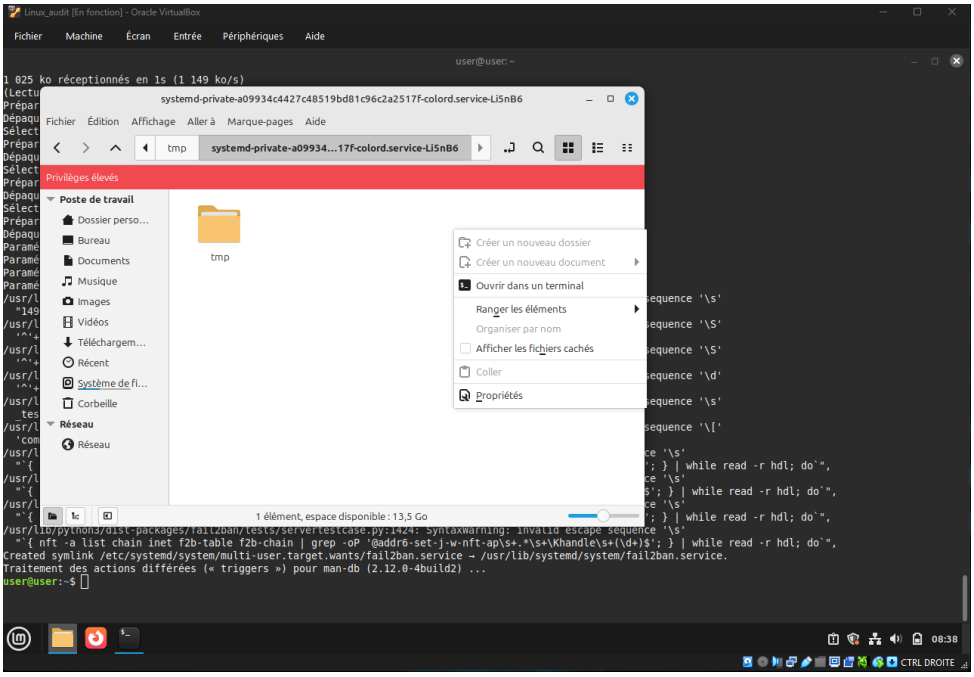
noexec: **Empêche l'exécution de binaires ou scripts** dans /tmp (l'objectif principal).

nosuid: Ignore les bits SUID et SGID pour empêcher l'escalade de privilèges.

nodev: Empêche la création de fichiers de périphériques.

Montez l'entrée /tmp (cela démontera l'ancien /tmp et le remontera avec les nouvelles options) :
sudo mount /tmp

Vérifiez les options de montage :
mount | grep /tmp



Il faut avoir les droits admins aussi pour configurer ou même avoir accès à tmp.

10. Restriction des Droits sur les Fichiers Sensibles

Pour garantir la sécurité des informations sensibles, il est essentiel d'appliquer une politique de droits d'accès stricte basée sur le **Principe du Moindre Privilège** et la **Séparation des Rôles**.

Points Clés :

1. **Administrateurs (Propriétaires) :** Doivent disposer des droits complets (Lecture, Écriture, Exécution — rwx ou rw-, par exemple 700 ou 600) pour gérer et modifier les fichiers sensibles.
2. **Utilisateurs Standards (Autres) :** L'accès en **Modification/Écriture (w) doit être strictement interdit**. Ils peuvent avoir un accès limité en Lecture (r, par exemple 444) si nécessaire, ou aucun accès (---, par exemple 000).
3. **Mise en Œuvre Technique (Linux/Unix) :** Utiliser les commandes chown et chgrp pour définir le propriétaire et le groupe, et chmod pour ajuster les permissions. L'exemple typique pour un fichier critique est chmod 600, assurant que seul l'administrateur peut lire et écrire.

En résumé, seuls les administrateurs doivent avoir les droits de modification, les autres utilisateurs étant limités à la lecture ou se voyant interdire tout accès.

En utilisant des lignes de commandes avec chmod ou shown

11. Installation de fail2ban

fail2ban est un outil de prévention des intrusions qui protège le système en détectant et en bloquant les adresses IP suspectes. Son installation renforce la sécurité du système contre les attaques par force brute.

“sudo apt install fail2ban”

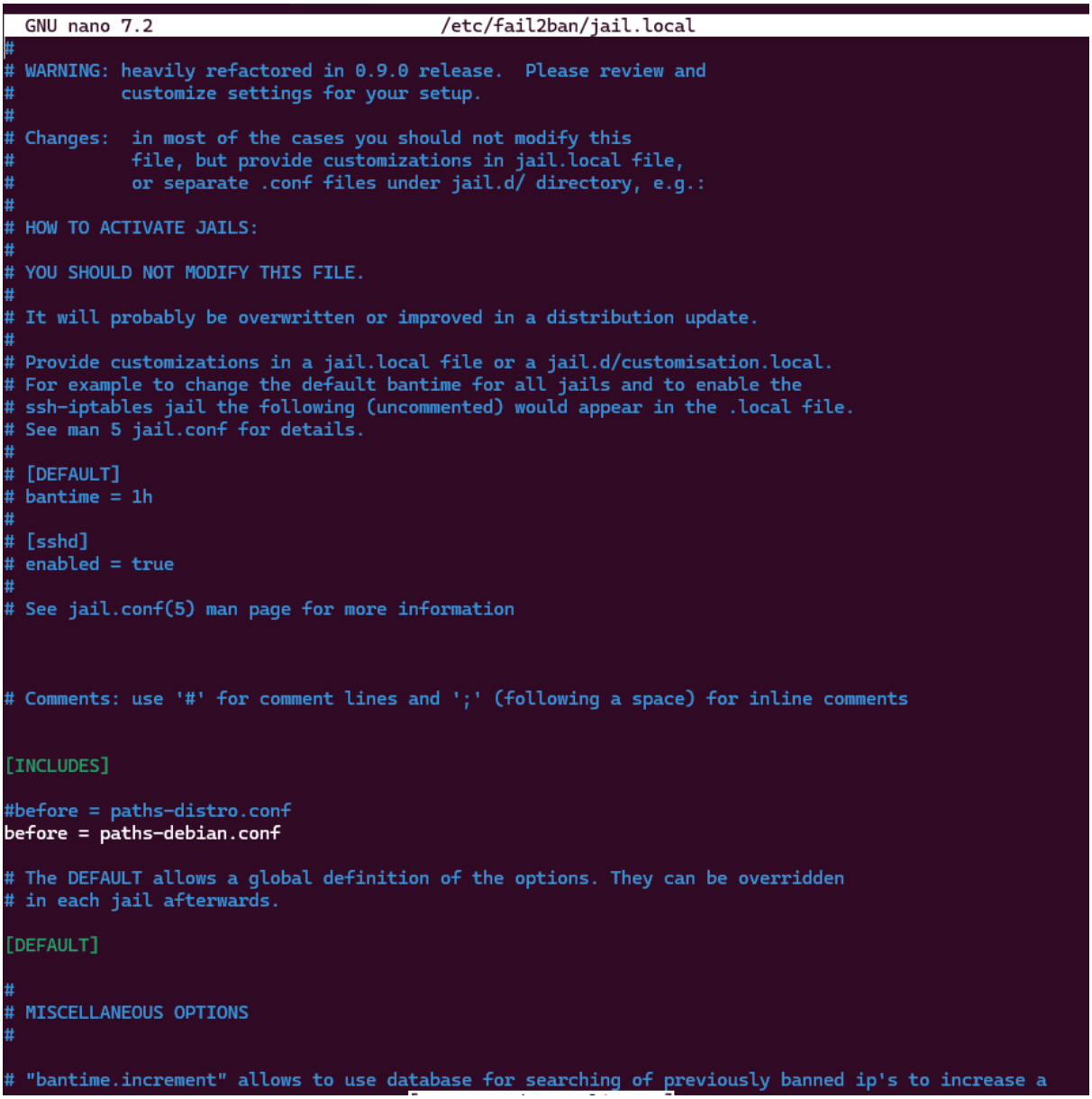
La configuration par défaut de Fail2ban se trouve dans /etc/fail2ban/jail.conf. Il est **fortement recommandé** de ne jamais modifier ce fichier directement. À la place, vous créez un fichier de configuration local, **jail.local**, pour y placer vos modifications. Cela permet de conserver vos paramètres même si le paquet est mis à jour.

Entrez la commande :

“sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local”

On peut configurer maintenant l’outil à notre aise

sudo nano /etc/fail2ban/jail.local



ex : Fail2ban utilise des sections appelées "Jails" pour chaque service. Puisque vous avez sécurisé SSH, c'est le jail le plus important à activer.

1. **Recherchez la section [sshd]** ou [sshd-ddos] dans le fichier jail.local.

Activez le service en ajoutant ou en modifiant la ligne enabled :
Extrait de code
[**sshd**]

Active le jail

enabled = **true**

Le filtre **sshd** par défaut est généralement déjà bon

filter = **sshd**

Cible les logs standard d'authentification

logpath = **/var/log/auth.log**

Utilisez le port **4000** que j'ai configuré !

Port= **4000**

Ensuite il faut redémarrer le service pour que les changements prennent effet, avec :

sudo systemctl restart fail2ban

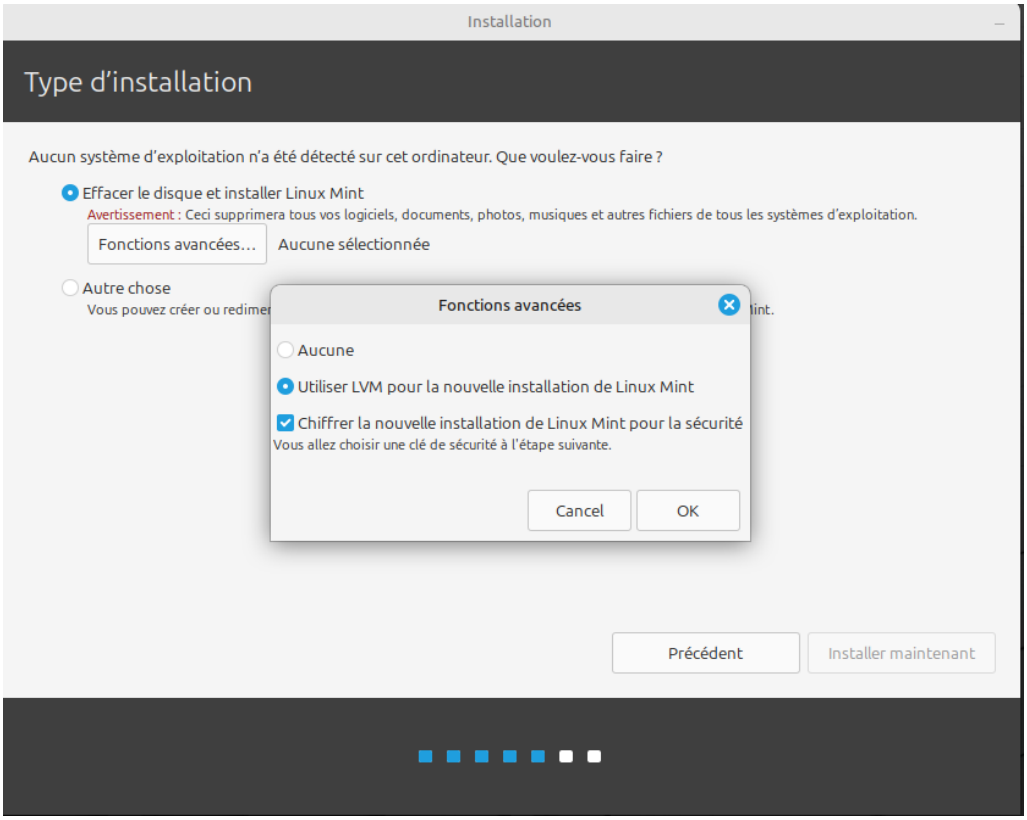
Pour vérifier que Fail2ban fonctionne et que le jail SSH est actif, utilisez la commande :

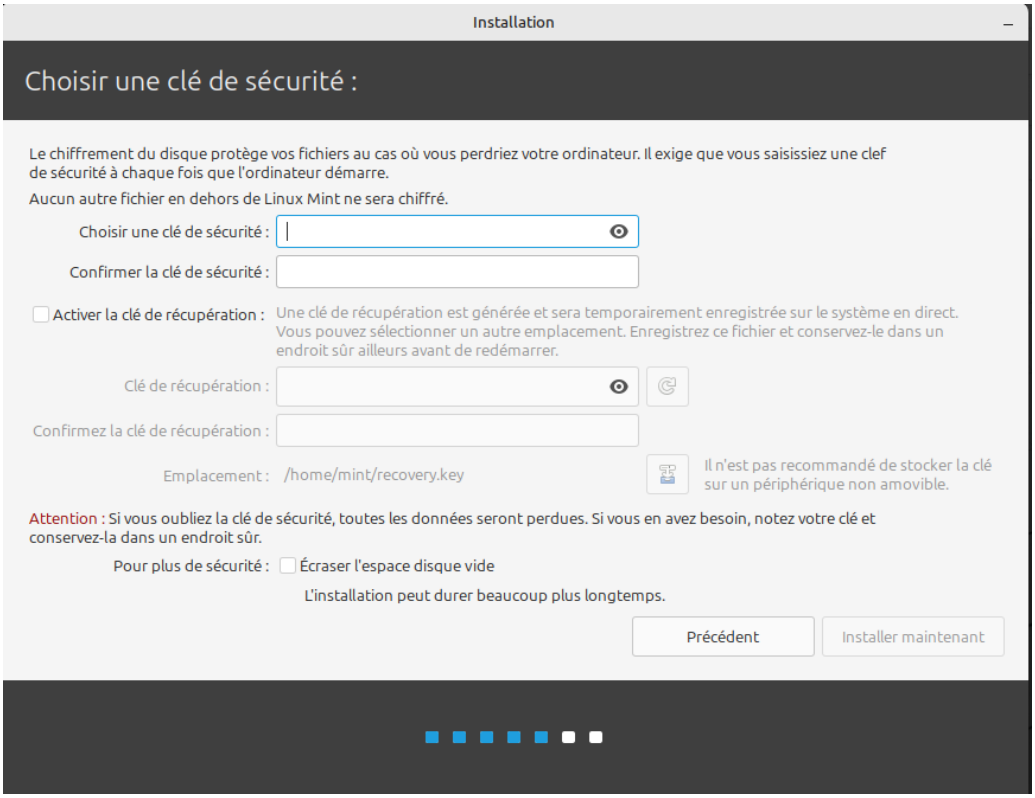
fail2ban-client status

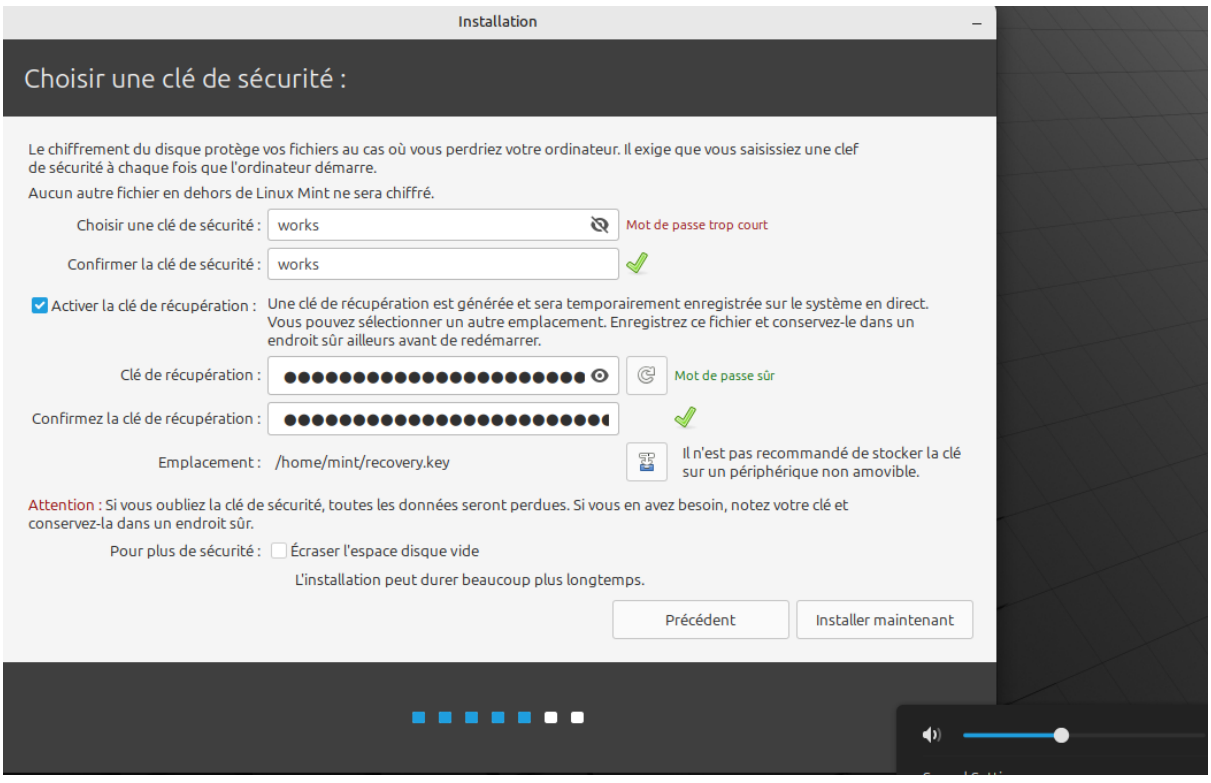
Vous devriez voir sshd listé comme un jail actif. Vous pouvez vérifier l'état détaillé de ce jail avec :

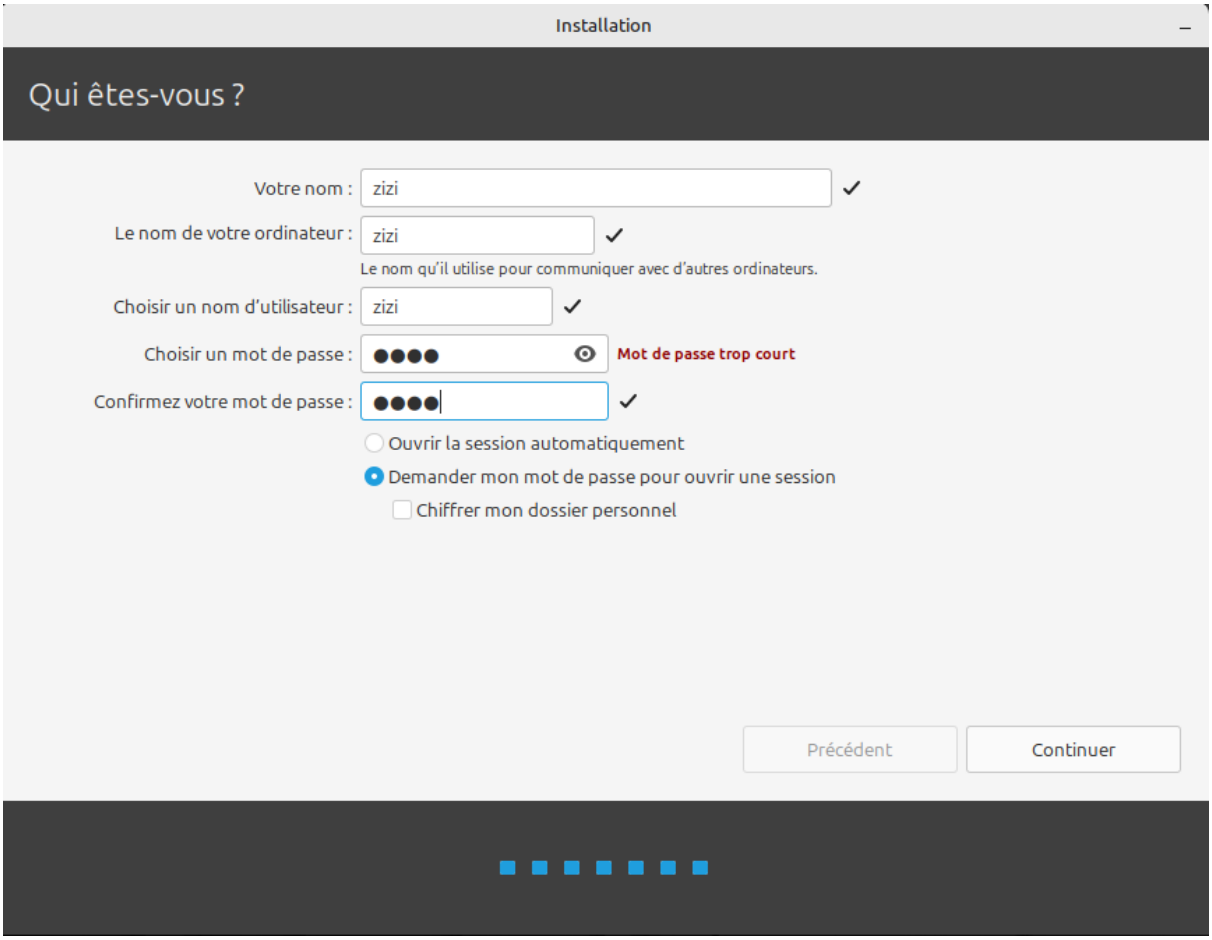
sudo fail2ban-client status sshd

12. Chiffrement du Disque avec LVM




Installation
Choisir une clé de sécurité :
Le chiffrement du disque protège vos fichiers au cas où vous perdriez votre ordinateur. Il exige que vous saisissiez une clef de sécurité à chaque fois que l'ordinateur démarre.
Aucun autre fichier en dehors de Linux Mint ne sera chiffré.
Choisir une clé de sécurité :
Confirmer la clé de sécurité :
Activer la clé de récupération :
Une clé de récupération est générée et sera temporairement enregistrée sur le système en direct. Vous pouvez sélectionner un autre emplacement. Enregistrez ce fichier et conservez-le dans un endroit sûr ailleurs avant de redémarrer.
Clé de récupération :
Confirmez la clé de récupération :
Emplacement : /home/mint/recovery.key
Il n'est pas recommandé de stocker la clé sur un périphérique non amovible.
Attention : Si vous oubliez la clé de sécurité, toutes les données seront perdues. Si vous en avez besoin, notez votre clé et conservez-la dans un endroit sûr.
Pour plus de sécurité : Écraser l'espace disque vide
L'installation peut durer beaucoup plus longtemps.
Précédent
Installer maintenant


Installation
Choisir une clé de sécurité :
Le chiffrement du disque protège vos fichiers au cas où vous perdriez votre ordinateur. Il exige que vous saisissiez une clef de sécurité à chaque fois que l'ordinateur démarre.
Aucun autre fichier en dehors de Linux Mint ne sera chiffré.
Choisir une clé de sécurité : works
Mot de passe trop court
Confirmer la clé de sécurité : works
Activer la clé de récupération :
Une clé de récupération est générée et sera temporairement enregistrée sur le système en direct. Vous pouvez sélectionner un autre emplacement. Enregistrez ce fichier et conservez-le dans un endroit sûr ailleurs avant de redémarrer.
Clé de récupération :
Mot de passe sûr
Confirmez la clé de récupération :
Emplacement : /home/mint/recovery.key
Il n'est pas recommandé de stocker la clé sur un périphérique non amovible.
Attention : Si vous oubliez la clé de sécurité, toutes les données seront perdues. Si vous en avez besoin, notez votre clé et conservez-la dans un endroit sûr.
Pour plus de sécurité : Écraser l'espace disque vide
L'installation peut durer beaucoup plus longtemps.
Précédent
Installer maintenant



Installer Ubuntu avec LVM sur une partition chiffrée via dm-crypt

. Conclusion Générale et Bilan du Projet 🚀

Synthèse et Validation de la Solution

Le projet de sécurisation des postes de travail nomades de GSB a atteint l'ensemble des objectifs fixés par le Cahier des Charges. La solution implémentée et documentée dans ce Livrable 3 garantit une **Défense en Profondeur** en agissant sur tous les vecteurs de risques, qu'ils soient physiques ou logiciels.

Les deux axes stratégiques majeurs ont été validés :

1. **Sécurité Physique :** Une procédure stricte a été définie (Chapitre 6) et peut être immédiatement déployée auprès des Visiteurs Médicaux (utilisation de l'antivol Kensington, règles de transport et de stockage sécurisé).
2. **Enrichissement de la Base de Connaissances :** Ce document (Livrable 3) constitue le mode d'emploi de référence, permettant au service IT de GSB de répliquer la solution de manière uniforme et pérenne sur l'ensemble de la flotte.

Bilan des Gains de Sécurité :

Objectif de Sécurité	Windows 10 Enterprise	GNU/Linux Mint Cinammon	Impact Principal
Protection des Données	Chiffrement intégral **BitLocker** (3.4).	Chiffrement intégral **LVM/LUKS** (4.4).	Conformité **RGPD** et neutralisation du risque de fuite en cas de vol.
Protection Réseau	Désactivation **SMBv1/NTLMv1** (3.3).	Pare-feu **UFW/Iptables** actif (4.3).	Réduction drastique de la surface d'attaque contre les rançongiciels et les attaques de réseau local.
Contrôle d'Accès	Politique de mot de passe stricte + **Windows Hello** (3.2).	Politique de mot de passe stricte + **fail2ban** (4.2/4.3).	Prévention des attaques par force brute et amélioration de l'hygiène de sécurité utilisateur.
Standardisation	**Script PowerShell** automatisé (5).	Procédures Open Source documentées (Chap. 4).	Efficacité et reproductibilité du déploiement à l'échelle des 100 postes.

. Validation des Usages et des Profils

Le durcissement a été réalisé sans compromettre la productivité des Visiteurs Médicaux.

- **Séparation des Profils (Usage Pro / Perso) :** La solution garantit la séparation des environnements. Le profil **"Visiteur Médical"** est un **utilisateur standard** aux privilèges limités, ce qui prévient les erreurs de manipulation et les installations malveillantes. Le compte **"Administrateur IT"** est utilisé uniquement pour les tâches de maintenance.
- **Validation Fonctionnelle :** Après le *hardening*, l'ensemble des outils métiers (suite bureautique, logiciels de présentation, accès aux documents) reste pleinement opérationnel. Le chiffrement de disque est transparent et n'impacte pas les performances grâce aux disques SSD NVMe.

Le poste de travail est désormais non seulement fonctionnel, mais résilient, garantissant la continuité de l'activité de GSB même en cas d'incident de sécurité.

Perspectives et Évolutions Futures

Bien que ce projet représente une étape majeure, la sécurité informatique est un processus continu. Les évolutions futures pourraient inclure :

1. **Gestion Centralisée des Correctifs :** Mettre en place un outil de gestion des correctifs (type WSUS ou solution MDM) pour automatiser la mise à jour des systèmes d'exploitation et des logiciels métiers, assurant la conformité continue (Chapitre 4.1).
2. **Supervision des Journaux (SIEM) :** Centraliser les journaux d'événements Windows (Journalisation des commandes, Chapitre 3.1) et les logs Linux/fail2ban sur une plateforme SIEM (Security Information and Event Management). Cela permettrait à GSB de détecter les attaques en temps réel, transformant la réponse à incident en surveillance proactive.
3. **Authentification Forte :** Explorer l'utilisation de clés physiques de sécurité (type YubiKey)

pour une authentification multi-facteurs systématique et plus robuste que la seule biométrie.