PROJET COOK MASTER

# PRÉSENTATION

## Description du projet

## Schéma du réseau

Une image contenant diagramme, schématique

Description générée automatiquement

## Organisation du site

Une image contenant diagramme

Description générée automatiquement

Récapitulatif écrit des informations sur les versions des systèmes d’exploitation utilisés :

SRVAD-03 :

Windows server 2019 datacenter (avec expérience de bureau)

Version : 1809

Sortie : Septembre 2019

Installé le : 30/03/2023

Build du système d’exploitation : 17763.2114

NAS :

Os  : TRUENAS

PC-X :

Windows 10 PRO

Version : 21H22

Sortie : Septembre 2019

Installé le : 30/03/2023

Build du système d’exploitation : 19044.1288

Tableau détaillé des spécifications techniques relatives aux composants (modèle, taille, fréquence, génération) :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nom | Carte Mère | Processeur | Mémoire RAM | Disque | Réseau |
| SRVAD-03 | ASUSTeK COMPUTER INC.  GA401QM  Bus Specs :  PCI-Express 4.0 (16.0 GT /s) | AMD Ryzen 9 5900HS with Radeon Graphics  Vitesse de base : 3,30 GHz  Cœurs : 2  VCPU : 2 | Samsung  Type : DDR4  Vitesse : 3200 MHz  Facteur de forme : SODIMM  Disponible : 8,0 Go | SAMSUNG MZVLQ1T0HBLB-00B00  Capacité : 60 Go  Disque système : Oui  Type : SSD | Wi-Fi MediaTek Wi-Fi 6 MT7921 Wireless LAN Card  Nom de la carte :  Wi-Fi |
| SRVNAS-03 | ASUSTeK COMPUTER INC.  GA401QM  Bus Specs :  PCI-Express 4.0 (16.0 GT /s) | AMD Ryzen 9 5900HS with Radeon Graphics  Vitesse de base : 3,30 GHz  Cœurs : 2  VCPU : 2 | Samsung  Type : DDR4  Vitesse : 3200 MHz  Facteur de forme : SODIMM  Disponible : 8,0 Go | SAMSUNG MZVLQ1T0HBLB-00B00  Capacité : 60 Go  Disque système : Oui  Type : SSD  SAMSUNG MZVLQ1T0HBLB-00B00  Capacité : 4 To  Disque système : Oui  Type : SSD  SAMSUNG MZVLQ1T0HBLB-00B00  Capacité : 4 To  Disque système : Oui  Type : SSD  SAMSUNG MZVLQ1T0HBLB-00B00  Capacité : 4 To  Disque système : Oui  Type : SSD  SAMSUNG MZVLQ1T0HBLB-00B00  Capacité : 4 To  Disque système : Oui  Type : SSD | Wi-Fi MediaTek Wi-Fi 6 MT7921 Wireless LAN Card  Nom de la carte :  Wi-Fi |
| PC-X | ASUSTeK COMPUTER INC.  GA401QM  Bus Specs :  PCI-Express 4.0 (16.0 GT /s) | AMD Ryzen 9 5900HS with Radeon Graphics  Vitesse de base : 3,30 GHz  Cœurs : 2  VCPU : 2 | Samsung  Type : DDR4  Vitesse : 3200 MHz  Facteur de forme : SODIMM  Disponible : 8,0 Go | SAMSUNG MZVLQ1T0HBLB-00B00  Capacité : 60 Go  Disque système : Oui  Type : SSD | Wi-Fi MediaTek Wi-Fi 6 MT7921 Wireless LAN Card  Nom de la carte :  Wi-Fi |

Tableau de la configuration réseau de chaque interface :

SRVAD-03

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Interface | Adresse IP | DNS 1 | DNS 2 | Gateway | Type | Nom réseau |
| Ethernet 0 | 172.16.2.254 | 127.0.0.1 | 1.1.1.1 | 172.16.2.3 | HOST ONLY | LAN |

SRVNAS-03

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Interface | Adresse IP | DNS 1 | DNS 2 | Gateway | Type | Nom réseau |
| Ethernet 0 | 172.16.2.253 | 172.16.2.254 |  | 172.16.2.3 | HOST ONLY | LAN |

PC-X

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Interface | Adresse IP | DNS 1 | DNS 2 | Gateway | Type | Nom réseau |
| Ethernet 0 | 172.16.2.4 | 172.16.2.254 |  | 172.16.2.3 | HOST ONLY | LAN |

Routeur (Pfsense)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Interface | Adresse IP | DNS 1 | DNS 2 | Gateway | Type | Nom réseau |
| WAN | 192.168.162.1 | 1.1.1.1 | 8.8.8.8 | 192.168.162.254 | NAT | NAT |
| LAN 2 | 172.16.2.1 | 172.16.2.254 |  |  | LAN | VMNET19 |
| DMZ | 172.16.3.1 |  |  |  | DMZ | VMNET11 |
| BDD | 172.16.4.1 |  |  |  | BDD | VMNET10 |

Pour les SRVNAS voici la liste non exhaustives des dossiers partagés :

-IT  
-Direction  
-Comptabilité  
-Ressources Humaines  
-Logistique

Accès administrateur du SRVNAS :

-root

-SecureAV24!

Accès utilisateur :

-user

-UserAV24!

Il faudrait aussi créer des groupes sur le Nas :

* Comptabilité
* Direction
* Techniciens
* RH

## I – Les mesures de protection face aux logiciels malveillants

Mise en place des mesures appropriées peut aider à protéger votre environnement contre les ransomwares et d'autres types de logiciels malveillants.

1. Mettre à jour les logiciels et les systèmes d'exploitation : Configurez les paramètres de Windows Update pour vous assurer que les systèmes d'exploitation et les logiciels sont régulièrement mis à jour avec les derniers correctifs de sécurité.

Une image contenant texte, lettre

Description générée automatiquement

1. Restrictions logicielles : Utilisation des GPO de restrictions logicielles (SRP) ou AppLocker pour limiter l'exécution de programmes non approuvés. Vous pouvez définir des règles basées sur des chemins, des signatures ou des hachages pour contrôler les applications autorisées à s'exécuter.

Une image contenant texte

Description générée automatiquement

1. Désactiver les macros Office : Les macros Office sont couramment utilisées pour propager des ransomwares. Vous pouvez désactiver les macros Office dans les documents provenant d'Internet via les GPO en définissant des paramètres appropriés pour les applications Office (Word, Excel, PowerPoint).

Une image contenant texte

Description générée automatiquement

1. Bloquer les fichiers exécutables dans les pièces jointes des e-mails : Utilisez les GPO pour configurer les paramètres de Microsoft Outlook afin de bloquer les fichiers exécutables en pièces jointes

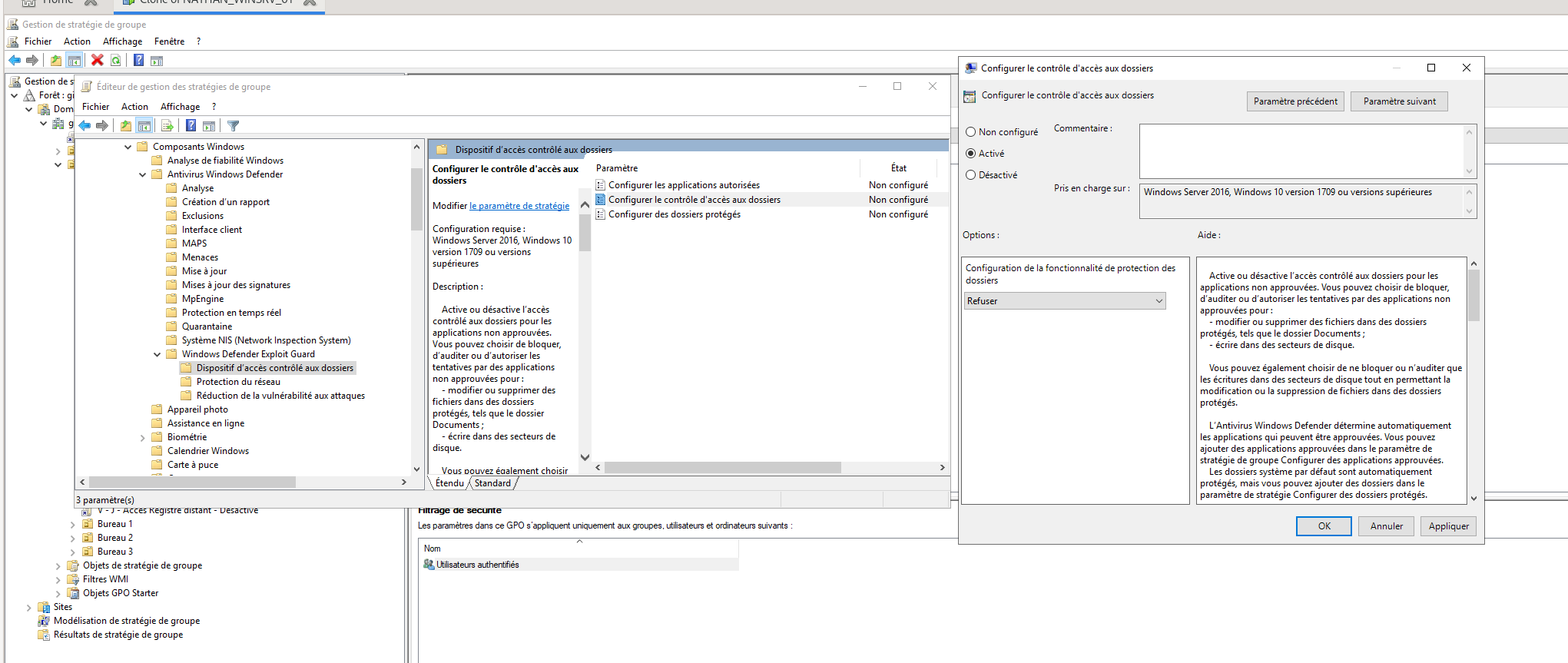
Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

1. Contrôler l'accès aux dossiers : Activez le contrôle d'accès aux dossiers (CFD) pour surveiller et empêcher les applications non autorisées d'accéder aux dossiers protégés.



1. Désactiver l'accès aux lecteurs amovibles sur l’UO Immeuble RP : Utilisez les GPO pour désactiver l'accès aux lecteurs amovibles (clés USB, disques durs externes) afin de réduire la propagation de ransomwares par ce biais.Une image contenant texte

   Description générée automatiquement
2. Appliquer le principe de moindre privilège : Configurez les GPO pour limiter les droits d'administrateur et d'accès aux ressources aux utilisateurs qui en ont réellement besoin.

Une image contenant texte

Description générée automatiquement

La règle "Appliquer le principe de moindre privilège : Configurez les GPO pour limiter les droits d'administrateur et d'accès aux ressources aux utilisateurs qui en ont réellement besoin" est une mesure de sécurité importante qui recommande de limiter les droits d'administrateur et d'accès aux ressources des utilisateurs à ceux qui en ont réellement besoin pour effectuer leur travail.

Le principe de moindre privilège consiste à accorder aux utilisateurs le niveau de privilège le plus bas possible pour effectuer leur travail, plutôt que de leur donner des droits d'administrateur complets ou des accès à toutes les ressources du système. En limitant les droits d'accès, vous pouvez réduire le risque d'attaques malveillantes ou d'erreurs humaines qui pourraient causer des dommages à votre système.

1. Activer l'audit des événements : Configurez les GPO pour activer l'audit des événements, notamment les échecs d'ouverture de session, les modifications de sécurité et les modifications de fichiers. Cela peut aider à détecter et à analyser les activités suspectes.

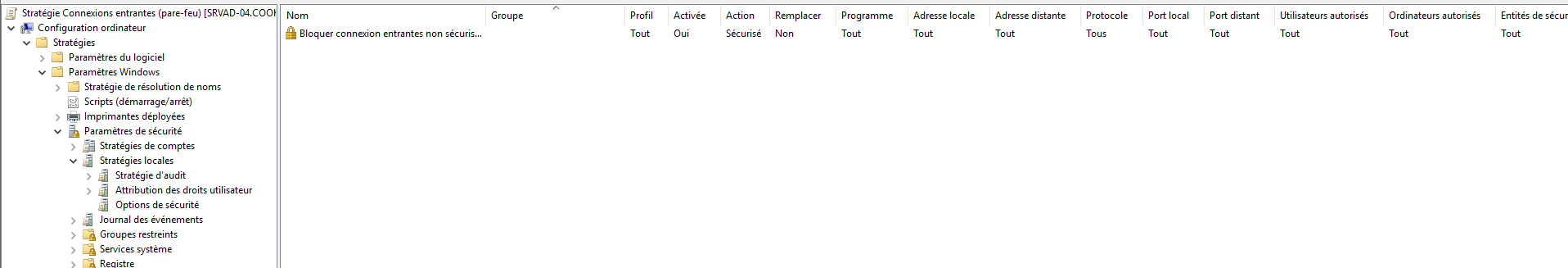
Une image contenant texte

Description générée automatiquement

La règle "Activer l'audit des événements : Configurez les GPO pour activer l'audit des événements, notamment les échecs d'ouverture de session, les modifications de sécurité et les modifications de fichiers" est une mesure de sécurité importante qui recommande d'activer l'audit des événements sur votre système d'exploitation.

L'audit des événements permet de surveiller les activités qui se produisent sur un système, telles que les échecs d'ouverture de session, les modifications de sécurité et les modifications de fichiers. En activant l'audit des événements, vous pouvez détecter et analyser les activités suspectes qui pourraient indiquer une tentative de compromettre la sécurité de votre système.

1. Renforcer les paramètres de pare-feu : Utilisez les GPO pour configurer les paramètres de pare-feu Windows et bloquer les connexions entrantes non autorisées.



La règle "Renforcer les paramètres de pare-feu : Utilisez les GPO pour configurer les paramètres de pare-feu Windows et bloquer les connexions entrantes non autorisées" est une mesure de sécurité importante pour protéger votre système contre les attaques provenant d'Internet ou du réseau local.

Le pare-feu Windows permet de bloquer les connexions entrantes non autorisées en filtrant le trafic réseau. En utilisant les stratégies de groupe (GPO), vous pouvez configurer les paramètres de pare-feu Windows pour bloquer les connexions entrantes non autorisées.

## II - Paramètres de sécurité généraux

1. Désactivez tous les services inutiles inclus dans l'installation par défaut pour réduire la vulnérabilité du serveur.

* Imprimante spouleur

Une image contenant texte

Description générée automatiquement

* Services de transferts intelligents en arrière-plan Une image contenant texte

  Description générée automatiquement

1. Supprimez les rôles et fonctionnalités inutiles de Windows Server.

Une image contenant texte

Description générée automatiquement

1. Affichez une notice légale comme suit avant que l'utilisateur se connecte : “ L'utilisation non autorisée de cet ordinateur et des ressources de mise en réseau est interdite ... ”

Une image contenant texte

Description générée automatiquement

1. Exiger Ctrl + Alt + Suppr pour les connexions et configurer une limite d'inactivité pour mettre fin aux sessions inactives.

Une image contenant texte

Description générée automatiquement

La première mesure consiste à exiger l'utilisation de la combinaison de touches "Ctrl + Alt + Suppr" lors de la connexion à un système informatique. Cette combinaison de touches est souvent utilisée comme une méthode de sécurité pour empêcher les logiciels malveillants de se connecter à un ordinateur sans autorisation. Elle peut également être utilisée pour se connecter à un système à distance ou pour accéder à certaines fonctions de sécurité supplémentaires.

La seconde mesure de sécurité consiste à configurer une limite d'inactivité pour mettre fin aux sessions inactives. Cela signifie que si un utilisateur est connecté à un système informatique mais qu'il n'a pas utilisé son clavier ou sa souris pendant une certaine période de temps prédéfinie, la session sera automatiquement fermée. Cette mesure est importante pour empêcher les personnes mal intentionnées d'accéder à des données sensibles ou de causer des dommages à un système en utilisant une session inactive laissée ouverte par un utilisateur.

1. (si ce n’est pas déjà fait) Activez le système de fichiers de chiffrement intégré ( EFS ) avec NTFS ou BitLocker pour les serveurs et les clients.

Une image contenant texte

Description générée automatiquement

## III - Durcissement de la sécurité du compte d'utilisateur

1. Désactivez le compte invité sur les serveurs

Une image contenant texte

Description générée automatiquement

Le compte invité est un compte utilisateur générique et communément utilisé qui n'est pas associé à un utilisateur spécifique. Ce compte peut être utilisé pour donner un accès limité à un utilisateur qui n'a pas de compte d'utilisateur dédié sur un système.

Cependant, le compte invité peut également représenter une menace pour la sécurité des systèmes informatiques. Le fait que ce compte soit utilisé par de nombreux utilisateurs différents peut rendre difficile la traçabilité des activités effectuées sous ce compte, ce qui peut rendre plus difficile l'identification des utilisateurs malveillants qui cherchent à accéder à un système sans autorisation.

1. Désactiver l’énumération anonyme des comptes et actions SAM

Une image contenant texte

Description générée automatiquement

Le Security Accounts Manager (SAM) est une base de données locale utilisée par les systèmes d'exploitation Windows pour stocker les informations d'identification des utilisateurs et des groupes, ainsi que les paramètres de sécurité du système. L'énumération anonyme des comptes et actions SAM fait référence au fait qu'un utilisateur non authentifié peut accéder à ces informations de manière anonyme, sans fournir d'informations d'identification.

Cela peut être utilisé par des pirates informatiques pour collecter des informations sensibles sur le système, comme les noms d'utilisateur et les mots de passe, ce qui peut ensuite être utilisé pour lancer des attaques plus sophistiquées.

Pour cette raison, il est recommandé de désactiver l'énumération anonyme des comptes et actions SAM. Cette mesure de sécurité empêche les utilisateurs non authentifiés d'accéder aux informations de compte et de groupe stockées dans la base de données SAM, renforçant ainsi la sécurité du système.

1. Désactivez la traduction anonyme Nom/SID

Une image contenant texte

Description générée automatiquement

Dans les systèmes d'exploitation Windows, chaque compte utilisateur et groupe de sécurité est identifié par un identificateur de sécurité (SID), qui est unique pour chaque compte ou groupe. La traduction Nom/SID est le processus qui permet de convertir un nom de compte ou de groupe en son SID correspondant.

Cependant, si la traduction anonyme Nom/SID est activée, les utilisateurs non authentifiés peuvent accéder aux informations de nom de compte et de groupe ainsi qu'à leurs SID correspondants. Cela peut être utilisé par des pirates informatiques pour collecter des informations sensibles sur le système, comme les noms d'utilisateur et les groupes de sécurité, ce qui peut ensuite être utilisé pour lancer des attaques plus sophistiquées.

Pour cette raison, il est recommandé de désactiver la traduction anonyme Nom/SID. Cette mesure de sécurité empêche les utilisateurs non authentifiés d'accéder aux informations de nom de compte et de groupe ainsi qu'à leurs SID correspondants, renforçant ainsi la sécurité du système.

## IV - Configuration de la sécurité réseau et gestion des accès

1. Activez le pare-feu Windows et assurez-vous que le pare-feu est activé pour chacun des profils de pare-feu de domaine, privé et public. Configurez le comportement du pare-feu des ordinateurs clients pour chaque profil afin de bloquer le trafic entrant par défaut.

Une image contenant texte

Description générée automatiquement

1. Lorsqu'un accès entrant est requis à un serveur, limitez-le aux protocoles, ports et adresses IP nécessaires à l’aide d’une règle de trafic dans la gestion du pare-feu avancée.

Une image contenant table

Description générée automatiquement

1. Pour RDP, définissez le niveau de chiffrement de connexion RDP sur élevé.

Une image contenant texte

Description générée automatiquement

Le chiffrement est une technique de sécurité qui permet de protéger les données sensibles en les convertissant en une forme illisible et en utilisant une clé pour les rendre lisibles uniquement pour les personnes autorisées. Dans le contexte de la connexion RDP, le chiffrement est utilisé pour protéger les informations d'identification de l'utilisateur et les données de la session pendant le transfert entre l'ordinateur client et l'ordinateur hôte.

En définissant le niveau de chiffrement de la connexion RDP sur élevé, les communications entre le client et le serveur RDP seront cryptées avec un algorithme de chiffrement fort, offrant ainsi une protection accrue contre les attaques de type "man-in-the-middle" et la divulgation de données sensibles.

1. Configurez le gestionnaire LAN pour refuser l'authentification LM et NTLMv1 et autoriser le système local à utiliser l'identité de l'ordinateur pour l'authentification NTLMv2

Une image contenant table

Description générée automatiquement

Le protocole LM (LAN Manager) et le protocole NTLMv1 (NT LAN Manager version 1) sont des méthodes d'authentification obsolètes et vulnérables qui ont été utilisées dans les systèmes Windows. Ces protocoles présentent des failles de sécurité qui peuvent être exploitées pour accéder à des informations sensibles et lancer des attaques sur le système.

En revanche, le protocole NTLMv2 (NT LAN Manager version 2) est une méthode d'authentification plus robuste et plus sécurisée qui doit être utilisée à la place des protocoles obsolètes LM et NTLMv1.

1. Désactiver la session se secours NULL du système local

Une image contenant texte

Description générée automatiquement

La session de secours NULL est une fonctionnalité de sécurité qui permet à l'utilisateur de se connecter à un système local en utilisant un compte d'utilisateur anonyme en cas d'échec de l'authentification normale. Cependant, cette fonctionnalité présente des risques de sécurité car elle permet à un utilisateur malveillant de se connecter au système sans avoir besoin d'un nom d'utilisateur ou d'un mot de passe.

Pour appliquer cette mesure de sécurité, il est recommandé de désactiver la session de secours NULL sur le système local. Cela permettra d'empêcher les utilisateurs malveillants d'exploiter cette fonctionnalité pour accéder au système sans autorisation et de renforcer la sécurité du système.

1. Configurez les types de chiffrement autorisés pour l'authentification Kerberos

Une image contenant texte

Description générée automatiquement

Choisir uniquement AES256 (pour un maximum de sécurité)

## V - Configuration de la sécurité du registre

1. Protégez le registre contre tout accès anonyme

Une image contenant texte

Description générée automatiquement

1. Désactivez l'accès au registre distant si ce n'est pas nécessaire

Une image contenant texte

Description générée automatiquement

1. Définissez MaxCachedSockets ( REG\_DWORD ) sur 0

Une image contenant texte

Description générée automatiquement

1. Set SmbDeviceEnabled ( REG\_DWORD ) à 0

Une image contenant texte

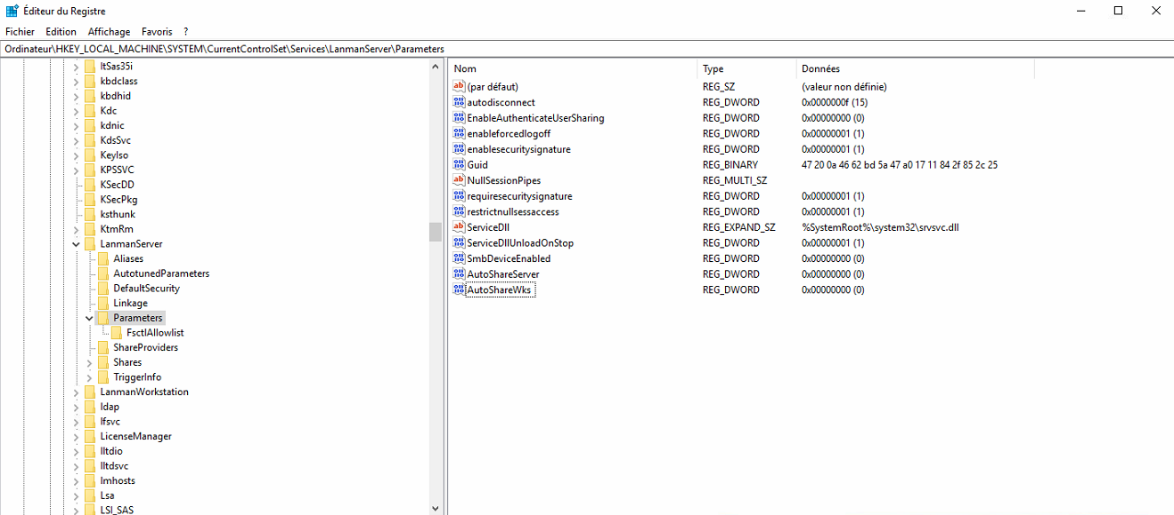
Description générée automatiquement

1. Définissez AutoShareServer sur 0

Une image contenant texte

Description générée automatiquement

1. Réglez AutoShareWks sur 0



1. Supprimez toutes les valeurs de NullSessionPipes

Une image contenant texte

Description générée automatiquement

1. Supprimez toutes les valeurs de NullSessionShares

