Mr JACQUEMIN



Compte rendu TP

Sécurisation Windows Server – Active Directory - LAPS

TEWES Arnaud BTS SIO SISR 2ÈME ANNÉE

Introduction

Dans ce TP, nous avons vu comment mieux sécuriser un serveur sous Windows Server avec certaines configurations de bases, comment sécuriser un contrôleur de domaine Active Directory en 7 étapes et comment paramétrer et installer Windows LAPS. C'est toutes ces étapes que je vais vous présenter dans ce compte-rendu.

Sécurisation de Windows Server

Pour sécuriser un serveur sous Windows Server, il est essentiel de suivre certaines configurations de base :

- Activer le pare-feu Windows : Cela aide à protéger le serveur contre les accès non autorisés.
- Faire les mises à jour : Assurer que le système d'exploitation et les logiciels sont à jour pour corriger les vulnérabilités.
- Activer BitLocker : Chiffrer les disques pour protéger les données sensibles.
- Activer Windows Defender : Utiliser Windows Defender si aucun autre antivirus ou solution IPS/IDS n'est disponible.
- **Désactiver le service spouleur d'impression** : Désactiver et supprimer ce service du démarrage automatique pour réduire les risques d'attaques.
- **Désactiver SMB V1** : Désactiver cette version obsolète du protocole SMB pour éviter les vulnérabilités connues.
- Activer les clichés instantanés : Utiliser les clichés instantanés pour sauvegarder et restaurer les données en cas de besoin.

Sécurisation d'un contrôleur de domaine Active Directory

Pour sécuriser un contrôleur de domaine Active Directory, voici les étapes à suivre :

- Activer la corbeille AD : Permet de restaurer facilement les objets supprimés.
- Modifier le quota d'utilisateur dans ADSI : Réduire le quota d'utilisateurs autorisés à joindre des machines au domaine à 0 au lieu de 10 par défaut.
- Supprimer "Utilisateur authentifié" du groupe "Accès compatible pré-Windows 2000" : Réduire les permissions par défaut pour améliorer la sécurité.
- Supprimer "Administrateur" du groupe "Administrateur du schéma" : Limiter les privilèges pour réduire les risques de modifications non autorisées.
- Ajouter "Administrateur" au groupe "Protected Users" : Renforcer la sécurité des comptes administratifs.
- **Créer une stratégie de groupe pour désactiver NTLM** : Désactiver NTLM pour utiliser des protocoles d'authentification par mot de passe plus sécurisés.

Paramétrage et installation de Windows LAPS

Windows Local Administrator Password Solution (LAPS) permet de gérer les mots de passe des comptes administrateurs locaux de manière sécurisée :

- 1. Installer LAPS : Déployer le logiciel sur les machines cibles.
- 2. **Configurer les paramètres de LAPS** : Définir les politiques de gestion des mots de passe, comme la longueur et la complexité.
- 3. **Déployer les stratégies de groupe** : Appliquer les stratégies de groupe pour automatiser la gestion des mots de passe sur les machines.

1. Sécurisation Windows Server

Activer le pare-feu Windows

Dans notre première configuration de Windows Server, il est préférable de désactiver le pare-feu pour éviter les soucis. La première étape de notre sécurisation va donc être de réactiver tous les pare-feux.

Si un souci venait à surgir après l'activation, on pourrait donc savoir que ce n'est pas un souci « logiciel » mais plus un souci réseau que le pare-feu bloquerait.



Faire les mises à jour

La deuxième étape va être d'effectuer toutes les mises à jour disponible sous Windows Update. En effet, Microsoft déploie tous les mois des mises à jour et correctifs de sécurité qu'il est essentiel d'installer sur nos serveurs pour éviter les risques d'actions malveillantes. Nous avons la possibilité de créer des planificateurs d'événements pour que les mises à jour se télécharge et/ou s'installent en dehors des heures d'activités. Mais il est impératif de toujours les effectuer.



Activer Windows Defender

La troisième étape est bien sûr d'utiliser et d'activer la protection via Windows Defender si aucun autre logiciel antivirus est installé sur le poste et/ou si nous n'avons pas de solutions IPS/IDS.

Sécurité Windows		- 0	×
≘ ລົ Accueil	Paramètres de protection contre les virus et menaces Consultez et metez à jour les paramètres de protection contre les virus et		
Protection cor Pare-feu et pro	menaces de l'antivirus Windows Defender. Modifier vo. ze les virus et menaces de l'antivirus Windows Defender. confidential tacilion du vizant	; paramètres de ité nodifiez les paramètre	s
 Pare-feu et pr Contrôle des a Bécurité des a 	Protection en temps réel de confiden yplications et du navigateur Ce paramètre permet di dentifier et d'empêcher l'installation ou l'exclution de programmes malveillants sur votre appareil. Vous pouvez le désactiver temporairement, mais nous le réactiverons automatiquement. Paramètres or désacture temporairement, mais nous le réactiverons automatiquement. Déclaration de Déclaration de	tialité de votre apparei I. le confidentialité ord de confidentialité de confidentialité	1
	Protection dans le cloud Offre une protection renforcée et plus rapide grâce à l'accès aux données de protection les plus récentes dans le cloud. Fonctionne de manière optimale une fois la soumission automatique d'échantilions activée. Déclaration de confidentialité		
© Paramètres ■	Envoi automatique d'un échantillon Envoyez des échantillons de fichier à Microsoft pour vous protéger et protéger les autres utilisateurs contre d'éventuelles menaces. Nous vous	토 d <mark>s 02/12/202</mark>	. 🖓

Désactiver le service spouleur d'impression

La 4eme étape va être de désactiver le spouleur d'impression pour renforcer la sécurité de nos serveurs. En effet, ce service a été la cible de nombreuses vulnérabilités. En désactivant ce service, nous réduisons la surface d'attaque potentielle et protégeons nos systèmes contre des exploits connus. De plus, si le serveur n'a pas besoin de gérer des tâches d'impression, il est logique de désactiver ce service pour éviter des risques inutiles.

s (local)	Services (local)	2					
	Spouleur d'impression	Nom	Description	État	Type de démarrage	Ouvrir une session en tant que	
		Service utilisateur du Presse	Ce service u		Manuel	Système local	
	Arrêter le service	Service Windows Insider	Offre la pris		Désactivé	Système local	
	Redemarter le service	Service SSTP (Secure Socket	Prend en ch	En co	Manuel	Service local	
		Services Bureau à distance	Autorise les	En co	Manuel	Service réseau	
	Description :	Services de chiffrement	Fournit trois	En co	Automatique	Service réseau	
	Ce service met en spoule les travaux	Services de domaine Active	Service de c	En co	Automatique	Système local	
	avec l'imprimante. Si vous arrêtez ce	Services Web Active Directory	Ce service f	En co	Automatique	Système local	
	service, vous ne pourrez plus	Shared PC Account Manager	Manages pr		Désactivé	Système local	
	imprimer ni voir vos imprimantes.	SMP de l'Espace de stockag	Service hôte		Manuel	Service réseau	
		Spouleur d'impression	Ce service	En co	Automatique	Système local	
		Station de travail	Crée et mai	En co	Automatique	Service réseau	
		Stockage des données utilis	Gère le stoc		Manuel	Système local	
		Stratégie de retrait de la cart	Autorise le s		Manuel	Système local	
		SysMain	Gère et amé	En co	Automatique	Système local	
		Système d'événement COM+	Prend en ch	En co	Automatique	Service local	
		Système de fichiers EFS (En	Fournit la te		Manuel (Déclencher	Système local	
		🖏 Téléphonie	Prend en ch		Manuel	Service réseau	
		Carl Temps Windows	Conserve la	En co	Automatique (décle	Service local	
		Children Thèmes	Fournit un s	En co	Automatique	Système local	
		Children Update Orchestrator Service	Gère les mis	En co	Automatique (débu	Système local	
		Weeam Agent for Microsoft	Performs pe	En co	Automatique	Système local	
		Keeam Data Mover Service	Sends and r	En co	Automatique	Système local	
		Veeam Installer Service	Enables inst	En co	Automatique	Système local	
		Werificateur de points	Vérifie les e		Manuel (Déclencher	Système local	
		WalletService	Objets d'hô		Désactivé	Système local	
		WarpJITSvc	Provides a Jl		Manuel (Déclencher	Service local	
		Windows Installer	Ajoute, mo		Manuel	Système local	
		Windows Search	Fournit des		Désactivé	Système local	
		Windows Update	Active la dé	En co	Manuel (Déclencher	Système local	

Propriété	s de <mark>Spoul</mark> e	ur d'impression	Ordinateur local)	×
Général	Connexion	Récupération	Dépendances		
Nom du	service :	Spooler			
Nom co	mplet :	Spouleur d'impre	ssion		
Descrip	tion :	Ce service met e et gère l'interacti	en spoule les travaux ion avec l'imprimante	d'impression Si vous	
Chemin C:\Wind	d'accès des dows\System	s fichiers exécutal n32\spoolsv.exe	bles :		
Type de	e démarrage	: Désa	activé	~	
État du	service : /	Arrêté			
Dér	marrer	Arrêter	Suspendre	Reprendre	
Vous po service.	ouvez spécifi	ier les paramètres	qui s'appliquent au	démarrage du	
Paramè	tres de déma	arrage :]
		0	OK Annule	Applique	er

Désactiver SMB V1

La 5eme étape va être de désactiver SMB V1. Cette version obsolète du protocole SMB est connue pour ses nombreuses vulnérabilités, qui peuvent être exploitées par des attaquants pour accéder à nos systèmes.

électionner des	fonctionnalités	SERVEUR DE DESTINAIC SRV-V-AD1-AT.miami.loc
Avant de commencer	Sélectionnez une ou plusieurs fonctionnalités à installer sur le s	erveur sélectionné.
Type d'installation	Fonctionnalités	Description
Sélection du serveur		Support for the SMB 1.0/CIFS file
Rôles de serveurs	Service de réceau local sans fil	sharing protocol, and the Comput
Fonctionnalités	Service de transfert intelligent en arrière-plan (BIT)	Browser protocol.
Confirmation	Service Serveur iSNS	
	Service SNMP Simple TCP/IP Services	
	Simpler Local Service Simpler Local Service Simpler Local Service Simpler Local Service Sous-système Windows pour Linux Stockage étendu Storage Migration Service Storage Migration Storage Migration	

Activer les clichés instantanés

La 6eme étape va être d'activer les clichés instantanés, ce qui permet de sauvegarder et de faire un instant afin de restaurer les données en cas de besoin. Cette fonctionnalité crée des copies de sauvegarde des fichiers à des moments précis, ce qui facilite la récupération des données en cas de perte ou de corruption.

□ I Gérer Ce PC Ercher Ordinateur Affrichane Outlis de lecteur	. Descriftés de l	Vienus la sel (Cr)			~		× ~ 0
Fichler Orainateur Attichage Outris de recteur ← → ^ ▲ ★ Accès rapide ✓ Dossiers (7) ■ Bureau ★ ■	Propriétés de : D Général Clichés instant Les clichés instanta existait dans le pass <u>cliquez ici</u> .	lisque local (C:) Outils M. anés V. nés permettent de voir é. Pour obtenir plus d'ir	atériel Pr ersions précédentes le contenu des dos nformations sur les d	artage Sécurité s Quota siers partagés tel qu'il clichés instantanés,	×	Rechercher dans : Ce PC	٩
Téléchargement: # Documents Musique Images Soft System32 Vidéos	Sélectionnez un vol Volume ()\? () C:\	ume : Heure de la procha Désactivé 03/12/2024 07:00	Partages 0 3	Utilisé 320 Mo sur C:\			
Ce PC	Clichés instantané	Désa is du volume sélectionn :30	activer	Paramètres			
				Supprimer Rétablir			
9 élément(s) 1 élément sélectionné			OK	Annuler Appliqu	ler		

Activer BitLocker

La 7eme étape est, bien entendu, d'activer BitLocker pour protéger les données sensibles sur nos serveurs. BitLocker chiffre les disques durs, rendant les données illisibles pour toute personne non autorisée. En cas de vol ou de perte de l'appareil, les informations restent sécurisées car elles sont chiffrées

	le fonctionnalités			×			
Sélectionner de	s fonctionnal	ités	SRV-V-AD1-AT.miami.lo	cal			
🔥 Le serveur de destinati	on fait état d'un redémar	rrage en attente. Il est recommandé de le redé	marrer avant l'installation ou la	×			
Avant de commencer	Sélectionnez une	ou plusieurs fonctionnalités à installer sur le s	serveur sélectionné.				
Type d'installation	Fonctionnalités	Fonctionnalités Desc					
Sélection du serveur	Assistanc	ce à distance	Le Chiffrement de lecteur BitLocke	er			
Rôles de serveurs	Base de c	données interne Windows	favorise la protection des donnée sur des ordinateurs perdus volés	S OIL			
Fonctionnalités	Chiffrem	ache ent de lecteur BitLocker	désaffectés de façon inappropriée				
Confirmation	Client d'in	impression Internet	en chiffrant tout le volume et en vérifiant l'intégrité de chaque				
	Clusterin	g de basculement	composant d'amorçage. Les				
	Collection	n des événements de configuration et de sion différentielle à distance	la vérification de ces composants	51			
	Containe	rs	aboutit et si le lecteur chiffré se trouve dans l'ordinateur d'origine	La			
	Data Cen	uillage réseau BitLocker	vérification de l'intégrité nécessite				
	Direct Pla	ay ge de la charge réseau	(TPM).	e			
		ce audio-vidéo haute qualité Windows					
	Extension	n ISS Management OData n WinRM IIS					
		···· · · · · · · · · · · · · · · · · ·					
		< Précédent Suivar	nt > Installer Annule	r			
		< Précédent Suivar	t > Installer Annule	r			
		< Précédent Suivar	it > Installer Annule	r			
🖸 🗖 🖛 🖛		< Précédent Suivar	Installer Annule	er.			
│ ✔ _ ≂ │ hier Ordinateur /	Affichage Out	< Précédent Suivar Ouvrir Ouvrir dans une nouvelle fenêtre	it > Installer Annule	er			
I ☑ _ = I hier Ordinateur ✓	Affichage Out	Ouvrir Ouvrir dans une nouvelle fenêtre Épingler à Accès rapide	nt > Installer Annule	er			
$ \bigcirc = = $ hier Ordinateur \rightarrow \rightarrow \land \uparrow $=$ > Ce	Affichage Out PC >	Cuvrir Ouvrir Ouvrir dans une nouvelle fenêtre Épingler à Accès rapide Activer BitLocker	at > Installer Annule	er			
I → ← ↑ → ← ↑ → ← Ce	Affichage Out PC > V Dossiers (7)	 < Précédent Suivar Ouvrir Ouvrir dans une nouvelle fenêtre Épingler à Accès rapide Activer BitLocker Accorder l'accès à 	it > Installer Annule	er			
Image: Image	Affichage Out PC > V Dossiers (7) Bure	 < Précédent Suivar Ouvrir Ouvrir dans une nouvelle fenêtre Épingler à Accès rapide Activer BitLocker Accorder l'accès à Configurer les clichés instantanés 	it > Installer Annule	er			
Image: Image	Affichage Out PC > V Dossiers (7) Bure	 < Précédent Suivar Ouvrir Ouvrir dans une nouvelle fenêtre Épingler à Accès rapide Activer BitLocker Accorder l'accès à Configurer les clichés instantanés Restaurer les versions précédentes 	it > Installer Annule	er			
Image: Second state in the image. Image: Second state in	Affichage Out PC > V Dossiers (7) Bure Musi	 < Précédent Suivar Ouvrir Ouvrir dans une nouvelle fenêtre Épingler à Accès rapide Activer BitLocker Accorder l'accès à Configurer les clichés instantanés Restaurer les versions précédentes Épingler à l'écran de démarrage 	it > Installer Annule	er			
Image Image	Affichage Out PC > Dossiers (7) Bure Musi	 < Précédent Suivar Ouvrir Ouvrir dans une nouvelle fenêtre Épingler à Accès rapide Activer BitLocker Accorder l'accès à Configurer les clichés instantanés Restaurer les versions précédentes Épingler à l'écran de démarrage Formater 	At > Installer Annule	er			
Image → → → Image Image Image Image Image Image Image	Affichage Out PC > C Dossiers (7) Bure Musi Vidé	 < Précédent Suivar Ouvrir Ouvrir dans une nouvelle fenêtre Épingler à Accès rapide Activer BitLocker Accorder l'accès à Configurer les clichés instantanés Restaurer les versions précédentes Épingler à l'écran de démarrage Formater Copier 	it > Installer Annule	er			
 chier Ordinateur chier Or	Affichage Out PC > C Dossiers (7) Bure Musi Vidé	 < Précédent Suivar Ouvrir Ouvrir dans une nouvelle fenêtre Épingler à Accès rapide Activer BitLocker Accorder l'accès à Configurer les clichés instantanés Restaurer les versions précédentes Épingler à l'écran de démarrage Formater Copier Créer un raccourci 	it > Installer Annule	er			
 chier Ordinateur chier Or	Affichage Out PC > C Dossiers (7) Bure Musi Vidé C Périphériau	 < Précédent Suivar Ouvrir Ouvrir dans une nouvelle fenêtre Épingler à Accès rapide Activer BitLocker Accorder l'accès à Configurer les clichés instantanés Restaurer les versions précédentes Épingler à l'écran de démarrage Formater Copier Créer un raccourci Renommer 	it > Installer Annule	2r			
 thier Ordinateur → ~ ↑ □ > Ce Accès rapide Bureau Téléchargement: Documents Images Soft System32 Ce PC Réseau 	Affichage Out PC > > Dossiers (7) Bure Bure Vidé > Périphériqu	 < Précédent Suivar Suivar Ouvrir Ouvrir dans une nouvelle fenêtre Épingler à Accès rapide Activer BitLocker Accorder l'accès à Configurer les clichés instantanés Restaurer les versions précédentes Épingler à l'écran de démarrage Formater Copier Créer un raccourci Renommer Propriétés 	nt > Installer Annule	er			
Images Images Images Images <t< td=""><td>Affichage Out PC > > Dossiers (7) Bure Bure Vidé > Périphériqu Uisq 27.8 Go</td><td> < Précédent Suivar Ouvrir Ouvrir dans une nouvelle fenêtre Épingler à Accès rapide Activer BitLocker Accorder l'accès à Configurer les clichés instantanés Restaurer les versions précédentes Épingler à l'écran de démarrage Formater Copier Créer un raccourci Renommer Propriétés </td><td>nt > Installer Annule</td><td>2 F</td></t<>	Affichage Out PC > > Dossiers (7) Bure Bure Vidé > Périphériqu Uisq 27.8 Go	 < Précédent Suivar Ouvrir Ouvrir dans une nouvelle fenêtre Épingler à Accès rapide Activer BitLocker Accorder l'accès à Configurer les clichés instantanés Restaurer les versions précédentes Épingler à l'écran de démarrage Formater Copier Créer un raccourci Renommer Propriétés 	nt > Installer Annule	2 F			

Il suffit ensuite de suivre les étape et surtout de bien conserver la clé de récupération dans un endroit sur.

2. <u>Sécurisation d'un contrôleur de domaine Active Directory</u>

Activer la corbeille AD

La première étape consiste à activer la corbeille AD. Cette fonctionnalité permet de restaurer facilement les objets supprimés, tels que les utilisateurs, groupes ou ordinateurs, sans avoir besoin de restaurer l'ensemble de la base de données AD.

Centre d'ac	dministration Active D	irectory			- 🗆 X	_
	Centre	d'administration Acti	ive Directory • Vue d'ensemble		🕶 🗭 Gérer Aide	
Centre	d'adminis <				CONTENU 🔻	
E 15-		BIENVENUE DANS LE CEN	TRE D'ADMINISTRATION ACTIVE DIRECTORY		۲	
Vue d'enser	mble	En say	oir plus sur le Centre d'administration	Active Directory		
Contrôle	Modifier le contrô	leur de domaine	le Centre d'administration Active Directory pour	dérer des tâches informatiques		
Authent						
Q Recherc	Activer la Corbeille	e	le module Active Directory pour Windows Powe	erShell		
-	Nouveau	,	des réponses sur le forum Active Directory			
	Rechercher sous c Propriétés	e nœud	er le contrôle d'accès dynamique			
		AZURE ACTIVE DIRECTORY	er les silos et les stratégies d'authentification	er a conligurer le controle d'acces dynamique		
		RÉINITIALISER LE MOT DE	PASSE 🛞 🔊	RECHERCHE GLOBALE	×	
		Nom d'utilisateur :	Domaine\Nom d'utilisateur	Rechercher	P	
		Mot de passe : Confirmation :		Étendue : miami (local)		
		Changer le mot de passe i Déverrouiller le compte	à la prochaine session Appliquer Effacer			
HISTORIQUE	DE WINDOWS PO	OWERSHELL			e	•
م 📲	ii 🧿	📄 🔮 🛷 💷			覧 4 _{8 02/12/2024} 〇	

Centre d'administration Active	Directory		- 0 ×
Centre	d'administration Acti	ive Directory + miami (local) +	- 🗊 Gérer Aide
Centre d'adminis <	miami (local) (15)		Tâches
Uue d'ensemble	Filtrer		le Builtin
🖬 miami (local)	Nom Tj	ype Description	Nouveau
Deleted Objects	🛍 Builtin bu	uiltinDom	Supprimer
Contrôle d'accès dynamique	Computers Co	onteneur Default container for upgr	Rechercher sous ce nœud
Authentification	Deleted Objects Co	onteneur Default container for delet	Propriétés
Recherche globale	Domain Controllers U	nité d'org Default container for dom	miami (local)
- Necherche globale	ForeignSecurityPrincipals Co	onteneur Default container for secur	Modifier le contrôleur de dom
	Infrastructure in	frastructu	Augmenter le niveau fonction
	Keys Co	onteneur Default container for key o	Augmenter le niveau fonction
	LostAndFound Io	sstAndFou Default container for orph	Activer la Corbeille
	Managed Service Accounts Co	onteneur Default container for man	Nouveau
	NITES Quetar	nite a org	Rechercher sous ce nœud
	Program Data	onteneur Default location for storag	Propriétés
	-	sentence benauchetation for storages	1
	Builtin	v	
	Classe d'objets : builtinDomain Description :	Modifié le : 28/08/2024 15:06	
	Résumé		
	OWERSHELL		6

Modifier le quota d'utilisateur dans ADSI

La deuxième étape consiste à modifier le quota d'utilisateur qui ont le droit d'entrer dans ordinateur au domaine dans modificateur ADSI de 10 (par défaut) à 0. Cela permet de limiter les permissions par défaut et empêche les utilisateurs non autorisés d'ajouter des machines au domaine, renforçant ainsi la sécurité globale du réseau.

🏝 i 🛃 🔜 🖛 i			Gérer	Outils d'ad	ministration			
Fichier Accueil	Partag	e Affichage	Outils de raccourci					
← → ~ ↑ 檔	> Panr	neau de configurati	on > Système et sécuri	té → Outils	d'administratio	on		ٽ ~
A coùo conida		Nom	^	Modi	fié le	Туре	Taille	
Bureau	*	Terminal Serv Analyseur de	ices performances	15/09 15/09	/2018 09:19 /2018 09:12	Dossier de fichiers Raccourci	2 Ko	
Téléchargemer Documents	nt:∦ ∦	Centre d'adm	inistration Active Directo du système	ory 15/09	/2018 09:13 /2018 09:12	Raccourci Raccourci	2 Ko 2 Ko	
Soft	*	Défragmenter	et optimiser les lecteurs	15/09	/2018 09:12	Raccourci Raccourci	2 Ko	
System32		Diagnostic de	mémoire Windows	15/09	/2018 09:13	Raccourci	2 Ko 2 Ko	
Ce PC		Domaines et a	approbations Active Dire	ctory 15/09	/2018 09:14	Raccourci	2 Ko	
💣 Réseau		Gestion de l'in	npression	15/09	/2018 09:13	Raccourci	2 Ko	
		Gestion des st	ratégies de groupe	15/09	/2018 09:12	Raccourci	2 Ko 2 Ko	
		Informations	système	15/09	/2018 09:13	Raccourci	2 Ko	
		Initiateur iSCS Lecteur de réd	upération	15/09	/2018 09:12 /2018 09:12	Raccourci Raccourci	2 Ko 2 Ko	
		Modification Module Activ	ADSI e Directory pour Windov	15/09 vs 15/09	/2018 09:13 /2018 09:13	Raccourci Raccourci	2 Ko 2 Ko	
		Moniteur de r Moniteur de r Mettoyage de	essources disque	15/09 15/09	/2018 09:12 /2018 09:12	Raccourci Raccourci	2 Ko 2 Ko	
		B Observateur of Solar S	l'événements ources (32-bit)	15/09 15/09	/2018 09:12 /2018 09:12	Raccourci Raccourci	2 Ko 2 Ko	
33 élément(s) 1 élé	ment se	electionné 1,14 Ko						



Supprimer "Utilisateur authentifié du groupe Accès compatible pré-Windows 2000

En réduisant les permissions par défaut, nous pouvons limiter l'accès aux ressources du réseau.



Supprimer "Administrateur" du groupe "Administrateur du schéma"

Cela va permettre de limiter les privilèges des comptes administrateur. En bloquant l'accès aux modifications du schéma, nous réduisons les risques de modifications qui pourraient compromettre la sécurité du Controleur de Domaine.

2 SIO - SRV-V-AD2-AT sur N-14	-G-2 - Connexion à un ordinateur virtuel						
Eichier Action Média Affi	charas Aide						
Fichier Action Media Attic	chage Alde						
	8 D 🚼 🛍						
Utilisateurs et ordinateurs Active	Directory						
Fichier Action Affichage ?							
l 🗢 🔿 🖄 🛅 🔏 🖾 🛛 🗶 🛙	🖹 Q 📑 🛛 🗊 🗏 🐮 🛅 🍸 💆 🍇						
Utilisateurs et ordinateurs Active	Nom		Туре		Description		
> 📔 Requêtes enregistrées	& Administrateur	Propriéte	s de : Adm	inistrateurs	du schéma		? X
miami.local	Administrateurs clés	riophen			du senemu		
	Administrateurs clés Enterprise	Général	Membres	Membre de	Géré par		
> Domain Controllers	Administrateurs de l'entreprise	Membr	es ·				
> i ForeignSecurityPrincipal:	Administrateurs DHCP	Nem			Dession Convises de d	ampine Active Dimetery	
> Managed Service Accourt	Administrateurs du schéma	2 D	desiratest ou u		miami logal /l logm	ornaine Active Directory	
🗸 📴 Miami	Admins du domaine	•	aministrateur	-	miami.jocai/ Users		
Groupes	Controleurs de domaine						
Ordinateurs	Controleurs de domaine cionables						
RUS	Contrôleurs de domaine d'entreprise en lecture seule						
Users	Des Admins						
Osers	Diskumins Diskumins						
	Éditeurs de certificats						
	Groupe de réplication dont le mot de passe RODC est autorisé						
	Groupe de réplication dont le mot de passe RODC est refusé						
	🖁 Invité						
	A Invités du domaine						
	A Ordinateurs du domaine	<					>
	Ropriétaires créateurs de la stratégie de groupe	Aio	ter	Supprimer	1		
	Reprotected Users	130		oupprinter	1		
	A Serveurs RAS et IAS						
	A Utilisateurs DHCP				OK	Annuler	Appliquer
	🚜 Utilisateurs du domaine						- hite de se

Ajouter "Administrateur" au groupe "Protected Users"

Les membres de ce groupe ont des protections supplémentaires contre les attaques, telles que l'impossibilité d'utiliser des protocoles d'authentification faibles et le fait qu'aucune machine ne garde en cache les hachages des mots de passes des comptes administrateur de notre domaine.



GPO pour désactiver NTLM

La dernière étape va donc être de créer une stratégie de groupe pour désactiver NTLM. NTLM est un protocole obsolète et vulnérable aux attaques. En le désactivant, nous forçons l'utilisation de protocoles plus modernes et sécurisés, tels que Kerberos.

NTLM est considéré comme moins sécurisé que les protocoles modernes comme Kerberos, car il est vulnérable à plusieurs types d'attaques, notamment les attaques par force brute.



