



EXPLOITER UN SERVEUR WINDOWS



Exploiter un Serveur Windows

Table des matières

Questions de positionnement :	2
Introduction.....	4
Activité 1 – Pare-feu et ICMP (PSSI-ACL1)	4
Activité 2 – GPO de sécurisation des sessions	5
Activité 3 – Politique de mot de passe (PSSI-AUTH1)	7
Activité 4 – Script Batch de sauvegarde et tâche planifiée (PSSI-BCUP2)	8
Conclusion	10

Questions de positionnement :

Q1. Qu'est-ce qu'une GPO ?

Une GPO (Group Policy Object) est un objet de stratégie de groupe permettant de centraliser et d'appliquer automatiquement des paramètres de configuration et de sécurité sur les utilisateurs et/ou ordinateurs d'un domaine Active Directory.

Q2. Pourquoi utiliser des GPO ?

Les GPO permettent d'appliquer de manière homogène des règles de sécurité et de configuration à grande échelle, sans intervention manuelle sur chaque poste, ce qui réduit les erreurs humaines et facilite l'administration.

Q3. Comment configurer une GPO en 4 étapes ?

1. Créer la GPO dans la console *Group Policy Management* (*gpmc.msc*).
2. Configurer les paramètres souhaités dans l'édition de la stratégie.
3. Lier la GPO à l'OU (unité d'organisation) contenant les comptes visés.
4. Tester l'application de la GPO sur un poste (*gpupdate /force*, puis vérification du résultat).

Q4. Qu'est-ce qu'un fichier Batch ? Intérêt.

Un fichier Batch est un script texte (.bat ou .cmd) contenant une suite de commandes Windows exécutées automatiquement par l'interpréteur de commandes. Il est simple à écrire, ne nécessite pas de compilateur et permet d'automatiser rapidement des tâches d'administration courantes (copies de fichiers, création de dossiers, exécution de programmes, etc.).

Q5. Quel outil permet d'exécuter automatiquement un script Batch à fréquence programmée ?

L'outil utilisé est le Planificateur de tâches Windows (*taskschd.msc*), qui permet de lancer un script ou programme selon un calendrier ou un événement.

Q6. En quoi une tâche planifiée peut-elle améliorer la sécurité ?

Une tâche planifiée peut automatiser des actions de sécurité régulières (sauvegardes, nettoyage de fichiers temporaires, désactivation de comptes inactifs, exécutions de scripts de conformité), ce qui garantit qu'elles sont réalisées systématiquement, même en l'absence d'intervention humaine.

Q7. Pourquoi une PSSI est-elle nécessaire dans une entreprise ?

La PSSI définit un cadre clair et partagé pour la protection du SI : elle formalise les règles, responsabilités et bonnes pratiques de sécurité, permet d'harmoniser les comportements et sert de référence en cas d'incident ou d'audit.

Q8. Quels sont les décideurs de la PSSI ?

En général, les décideurs sont :

- La direction générale.
- Le RSSI (Responsable de la Sécurité des SI).
- Les responsables métiers et informatiques (DSI, chefs de service), en concertation avec la direction.

Q9. Trois endroits où l'on trouve des ACL dans un SI.

- Sur les systèmes de fichiers (NTFS sur les dossiers/fichiers).
- Sur les équipements réseau (pare-feu, routeurs, switchs).
- Dans certaines applications ou services (partages réseau, base de données, règles de pare-feu Windows, etc

Introduction

Dans le cadre du TP, l'infrastructure de notre projet a été utiliser avec un contrôleur de domaine SRV1--AD (10.16.140.10/24) et un poste client CLT01 (10.16.140.146/24) joint au domaine AMMNS.local.

Activité 1 – Pare-feu et ICMP (PSSI-ACL1)

3.1. Mise en place

- Sur SRV1--AD, ouverture du Pare-feu Windows Defender avec fonctions avancées.
 - Création d'une règle de trafic entrant ICMPv4 autorisant uniquement le sous-réseau local 10.16.140.0/24 en profils Domaine et Privé, conformément à la règle PSSI-ACL1.
 - Vérification que la règle est bien activée.

```
Partage de fichiers et d'imprimantes (Demande d'écho - Trafic entrant ICMPv4)
Partage de fichiers et d'imprimantes (LIMNR=1IDP-In)
Partage d' Invité de commandes
Partage d' Microsoft Windows [version 10.0.26100.7462]
Partage d' (c) Microsoft Corporation. Tous droits réservés.
Partage d' C:\Users\mathieu.maisonneuve>ping 10.16.140.10
Partage d' Envoi d'une requête 'Ping' 10.16.140.10 avec 32 octets de données :
Partage d' Protocole Réponse de 10.16.140.10 : octets=32 temps=1 ms TTL=128
Partage d' Découvert Réponse de 10.16.140.10 : octets=32 temps=2 ms TTL=128
Partage d' Découvert Réponse de 10.16.140.10 : octets=32 temps=2 ms TTL=128
Partage d' Découvert Réponse de 10.16.140.10 : octets=32 temps=2 ms TTL=128
Partage d' Découvert Statistiques Ping pour 10.16.140.10:
Partage d' Découvert Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Partage d' Découvert Durée approximative des boucles en millisecondes :
Partage d' Découvert Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
Partage d' Découvert C:\Users\mathieu.maisonneuve>
```

3.2. Tests

- Depuis le client CLT01, exécution de ping 10.16.140.146 et obtention de réponses (0% de perte).
 - Test inverse depuis le serveur vers le client pour vérifier la connectivité.

Diagnostics de réseau de base - Demande d'écho ICMP (ICMPv4-Sortant)	Diagnostics de réseau de base	Privé, ...	Non	Autoriser	Non	System	Tout	Sous-réseau local	ICMPv4	T
Diagnostics de réseau de base - Demande d'écho ICMP (ICMPv4-Sortant)	Diagnostics de réseau de base	Dom...	Non	Autoriser	Non	System	Tout	Tout	ICMPv4	T
Diagnostics de réseau de base - Demande d'écho ICMP (ICMPv6-Sortant)	Diagnostics de réseau de base	Dom...	Non	Autoriser	Non	System	Tout	Tout	ICMPv6	T
Diagnostics de réseau de base - Demande d'écho ICMP (ICMPv6-Sortant)	Diagnostics de réseau de base	Dom...	Non	Autoriser	Non	System	Tout	Sous-réseau local	ICMPv6	T
Diagnostic								Tout	TCP	T
Expérience	invite de commandes							Tout	Tous	T
Écran de veille	Microsoft Windows [version 10.0.20348.4529]							Tout	Tous	T
E-mail et calendrier	(c) Microsoft Corporation. Tous droits réservés.							Tout	Tous	T
Expérience	C:\Users\adm.m.maisonneuve>ping 10.16.140.146							Tout	Tous	T
Expérience	Envoyé d'une requête 'Ping' à 10.16.140.146 avec 32 octets de données :							Tout	Tous	T
Flux du port	Réponse de 10.16.140.146 : octets=32 temps=2 ms TTL=128							Tout	Tous	T
Fonction	Réponse de 10.16.140.146 : octets=32 temps=2 ms TTL=128							Convertisseurs Li...	TCP	T
Fonction	Réponse de 10.16.140.146 : octets=32 temps=1 ms TTL=128							Convertisseurs Li...	UDP	T
Fonction	Réponse de 10.16.140.146 : octets=32 temps=1 ms TTL=128							Convertisseurs Li...	UDP	T
Serveur de	Statistiques Ping pour 10.16.140.146:							Tout	UDP	T
Serveur de	Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),							Sous-réseau local	UDP	T
Gestion de	Durée approximative des boucles en millisecondes :							Sous-réseau local	TCP	T
Gestion de	Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms							Tout	TCP	T
Client de								Tout	TCP	T
Outil d'ins								Tout	TCP	T
Programm								Tout	TCP	T
Service d'inf								Tout	TCP	T

Analyse :

La configuration respecte la PSSI en autorisant le ping uniquement depuis le réseau local de confiance, ce qui facilite le diagnostic sans exposer le serveur à un déni de service ICMP extérieur.

Activité 2 – GPO de sécurisation des sessions

4.1. GPO « PSSI-Session »

Étapes :

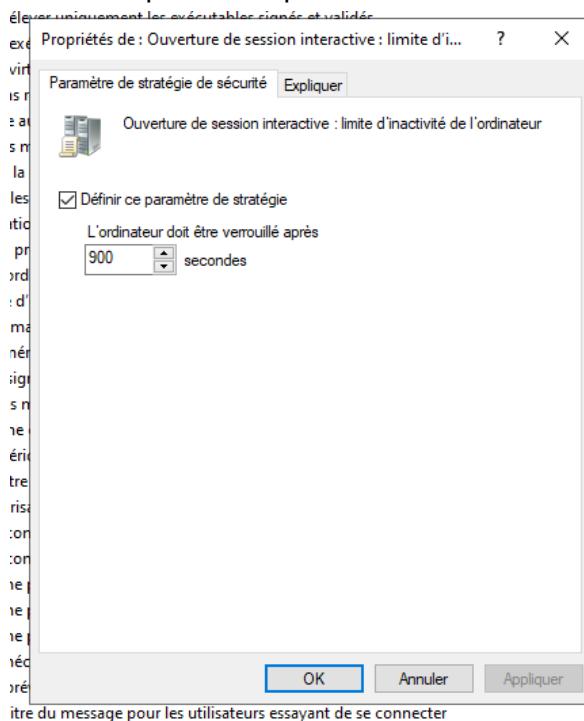
- Ouverture de gpmc.msc sur SRV1--AD.
- Création de la GPO « PSSI-Session ».
- Lien de cette GPO sur l'OU contenant les utilisateurs du domaine.

Paramètres configurés :

1. Verrouillage de session (PSSI-AUTH3)

- Stratégie : *Ouverture de session interactive : limite d'inactivité de l'ordinateur.*

- Valeur : 900 secondes (15 minutes) afin que la session se verrouille automatiquement après inactivité.



2. Restriction du Panneau de configuration (PSSI-HARD1)

- Stratégie : *Interdire l'accès au Panneau de configuration et aux Paramètres.*
- État : Activé pour les utilisateurs standards.

Intervalle d'application	Non configuré	Non
Interdire l'accès au Panneau de configuration et à l'application	Activé	Non

4.2. Tests et résultats

- Lancement d'un gpupdate /force sur le poste client puis reconnexion.
- Après 15 minutes d'inactivité, l'écran se verrouille automatiquement, retour à la fenêtre de connexion.
- Lorsqu'un utilisateur ouvre le Panneau de configuration, un message indique que cette action est restreinte par l'administrateur.

Analyse :

La GPO « PSSI-Session » applique correctement les exigences de la PSSI : protection contre l'accès non autorisé à une session laissée ouverte et limitation des possibilités de modification système par les utilisateurs non privilégiés.

Activité 3 – Politique de mot de passe (PSSI-AUTH1)

5.1. Configuration de la Default Domain Policy

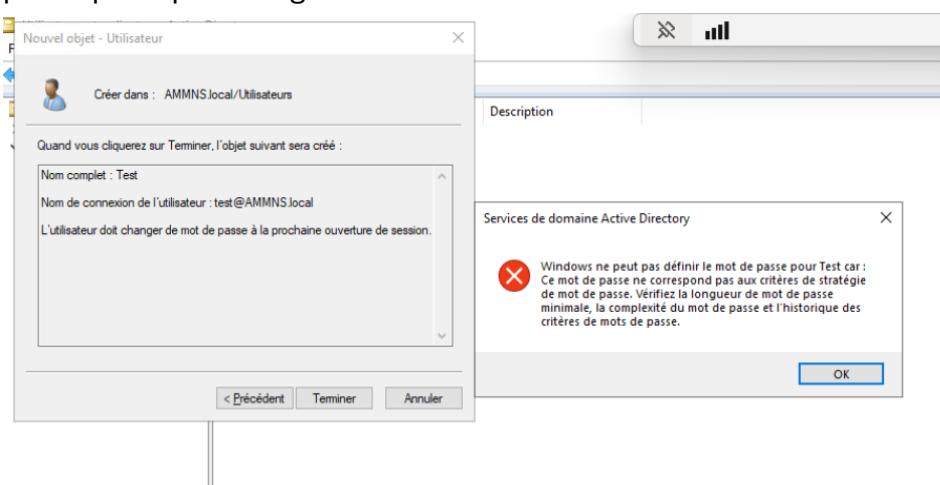
Dans Default Domain Policy, les paramètres de mot de passe ont été définis comme suit, conformément à PSSI-AUTH1 :

- Longueur minimale : 12 caractères.
- Complexité : activée (majuscules, minuscules, chiffres, caractères spéciaux).
- Durée de vie maximale : 90 jours.
- Historique des mots de passe : 5 derniers mots de passe mémorisés.

Stratégie	Paramètres de stratégie
Assouplir les limites de longueur minimale du mot de passe	Non défini
Audit de la longueur minimale du mot de passe	Non défini
Conserver l'historique des mots de passe	5 mots de passe mémorisés
Durée de vie maximale du mot de passe	90 jours
Durée de vie minimale du mot de passe	1 jours
Enregistrer les mots de passe en utilisant un chiffrement rév...	Désactivé
Le mot de passe doit respecter des exigences de complexité	Activé
Longueur minimale du mot de passe	12 caractère(s)

5.2. Test

- Création d'un nouvel utilisateur avec un mot de passe volontairement trop court ou sans complexité.
- Windows affiche un message d'erreur indiquant que le mot de passe ne respecte pas la politique configurée



Analyse :

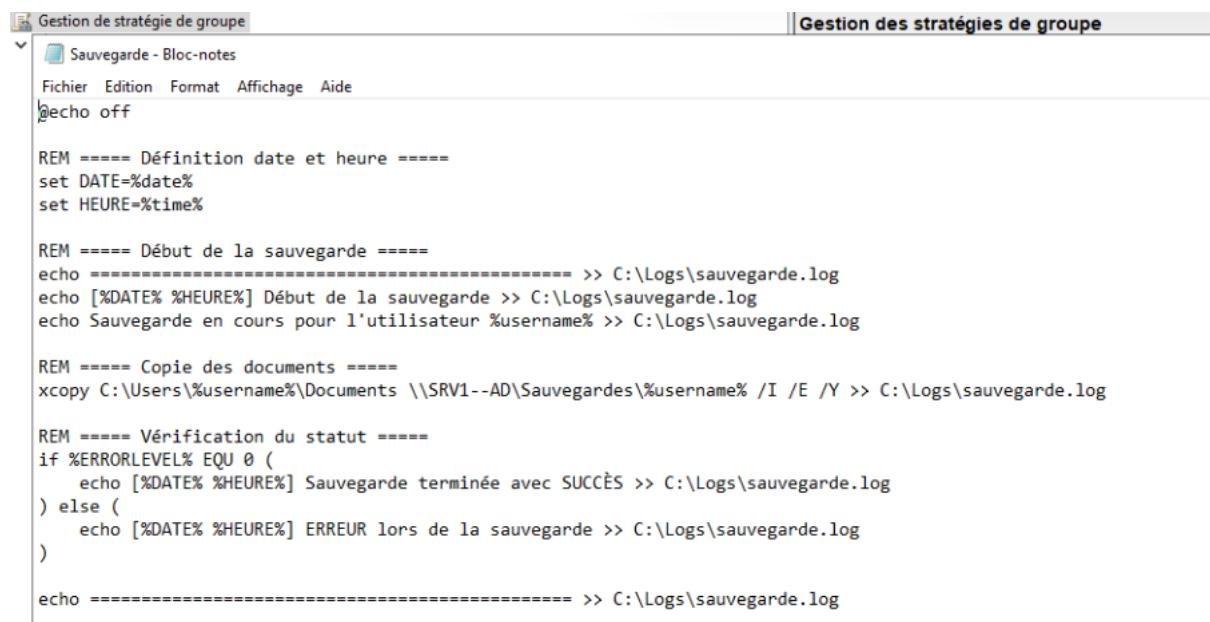
La politique de mot de passe assure un niveau de robustesse conforme aux recommandations de la PSSI et de l'ANSSI, rendant plus difficiles les attaques par force brute ou par devinette.

Activité 4 – Script Batch de sauvegarde et tâche planifiée (PSSI-BCUP2)

6.1. Script de sauvegarde

Sur le poste CLT01 :

- Création du dossier caché C:\Scripts et du dossier C:\Logs.
- Rédaction du script C:\Scripts\Sauvegarde.bat qui :
 - Ajoute une ligne horodatée dans C:\Logs\sauvegarde.log.
 - Copie le contenu de C:\Users\%username%\Documents vers \\SRV-DC\Sauvegardes\%username%.
 - Indique dans le log si la sauvegarde s'est bien terminée.



```
Notepad window titled "Sauvegarde - Bloc-notes" showing a batch script. The script starts with @echo off, then defines variables REM ===== Définition date et heure ===== set DATE=%date% set HEURE=%time%. It then logs the start of the backup with echo messages. REM ===== Début de la sauvegarde ===== echo =====>> C:\Logs\sauvegarde.log echo [%DATE% %HEURE%] Début de la sauvegarde >> C:\Logs\sauvegarde.log echo Sauvegarde en cours pour l'utilisateur %username% >> C:\Logs\sauvegarde.log. It then copies user documents to a network location with xcopy C:\Users\%username%\Documents \\SRV1--AD\Sauvegardes\%username% /I /E /Y >> C:\Logs\sauvegarde.log. Finally, it checks the error level with if %ERRORLEVEL% EQU 0 ( and logs success or error based on the result.
```

Test manuel : exécution du script → création du répertoire utilisateur sur le serveur et remplissage du fichier sauvegarde.log avec la date, l'heure et le statut.

6.2. Tâche planifiée « SauvegardeUtilisateur »

- Ouverture du Planificateur de tâches.
- Création de la tâche :
 - Nom : SauvegardeUtilisateur.
 - Déclencheur : tous les jours à 22h00.
 - Action : exécuter C:\Scripts\Sauvegarde.bat.
 - Options :
 - « Exécuter même si l'utilisateur n'est pas connecté ».
 - « Exécuter avec les autorisations les plus élevées ».
 - Compte d'exécution : compte admin de domaine ou compte de service.

6.3. Validation et traçabilité

Preuve 1 :

- Lancement manuel de la tâche via « Exécuter ».
- Vérification de C:\Logs\sauvegarde.log contenant les lignes « Sauvegarde en cours » et « Sauvegarde terminée avec succès ».
- Vérification du partage \\SRV1--AD\Sauvegardes\%username% contenant les fichiers du dossier Documents.

Preuve 2 :

- Consultation de l'Observateur d'événements :
 - Journaux des applications et des services → Microsoft → Windows → TaskScheduler → Operational.
 - Vérification des événements ID 100/101/102 (démarrage, réussite, fin) ou 103 si échec.

Prise-papiers	Image	Créé	Formes	Couleurs
Information		16/12/2025 13:32:12	TaskScheduler	100 Task Started
Information		16/12/2025 13:33:00	TaskScheduler	100 Task Started
Erreur		05/12/2025 08:29:56	TaskScheduler	101 Task Start Failed
Erreur		05/12/2025 08:29:55	TaskScheduler	101 Task Start Failed

Prise-papiers	Image	Créé	Formes	Couleurs
Information		16/12/2025 13:32:12	TaskScheduler	100 Task Started
Information		16/12/2025 13:33:00	TaskScheduler	100 Task Started
Erreur		05/12/2025 08:29:56	TaskScheduler	101 Task Start Failed
Erreur		05/12/2025 08:29:55	TaskScheduler	101 Task Start Failed

Analyse :

La solution met en œuvre la règle PSSI-BCUP2 en assurant une sauvegarde quotidienne automatique des documents utilisateurs vers le serveur, avec des preuves de bon fonctionnement grâce aux logs et aux journaux Windows.

Conclusion

L'ensemble des actions réalisées (GPO, pare-feu, politique de mot de passe, script Batch et tâche planifiée) montre comment administrer et sécuriser un environnement Windows en appliquant une PSSI d'entreprise. Les postes clients sont durcis, les sessions sont protégées, les mots de passe sont robustes et les données utilisateurs sont sauvegardées automatiquement, avec une traçabilité permettant d'auditer le bon fonctionnement du système.