🛠️ TD : Automatisation et Persistance via la Base de Registre

🎯 Objectif

Maîtriser le fournisseur `Registry::` pour lire, créer et modifier des configurations système. Vous allez apprendre à marquer le système avec vos propres données d'audit et à automatiser des réglages d'interface et de confidentialité.

📚 Étape 1 : Exploration et Lecture

En PowerShell, le registre se manipule comme un lecteur logique (lecteurs `HKCU:` et `HKLM:`).

Votre mission :

1. Identifiez la clé qui gère le nom réseau de l'ordinateur : `HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName`.
2. Utilisez la commande `Get-ItemProperty` pour extraire uniquement la valeur de la propriété `ComputerName`.

⚙️ Étape 2 : Création d'une "Empreinte d'Audit"

Pour garder une trace de vos scripts de santé, vous devez créer votre propre structure dans le registre pour stocker des métadonnées.

Consignes :

1. Créez une nouvelle clé nommée `AuditSante` dans le chemin suivant : `HKCU:\Software\`.
2. À l'intérieur de cette clé, créez deux entrées (Valeurs) :

- **DernierCheck** (Type String) : Doit contenir la date et l'heure actuelle via `(Get-Date).ToString()`.
- **VersionScript** (Type Dword) : La valeur `1`.

> 💡 **Indices :** Utilisez `New-Item` pour créer la clé (le "dossier") et `New-ItemProperty` pour créer les valeurs à l'intérieur.

🌙 Étape 3 : Personnalisation de l'interface (Mode Sombre)

Windows stocke la préférence de thème dans la ruche de l'utilisateur.

Votre mission : Écrire une fonction `Set-DarkMode` qui bascule Windows en mode sombre.

1. **Chemin :** `HKCU:\Software\Microsoft\Windows\CurrentVersion\Themes\Personalize`
2. **Propriété :** `AppsUseLightTheme` (Type DWORD).
3. **Logique :** La valeur `0` active le mode sombre, la valeur `1` le mode clair.

Défi "Toggle" : Faites en sorte que la fonction lise la valeur actuelle : si c'est `0`, elle met `1`, et inversement.

📊 Étape 4 : Sécurisation (Désactivation Télémétrie)

L'un des usages les plus fréquents en entreprise est la mise en conformité (Hardening).

Défi : Écrivez une fonction `Set-PrivacyMode` qui :

1. Vérifie si la clé `HKLM:\SOFTWARE\Policies\Microsoft\Windows\DataCollection` existe (si non, la créer).
2. Définit la valeur `AllowTelemetry` à `0` (Dword) pour bloquer les rapports automatiques.

🧪 Défi Final : Intégration Totale

Modifiez votre fonction `Get-DashBoard` (du TD précédent) pour qu'à la fin de son exécution, elle mette automatiquement à jour la valeur **DernierCheck** dans `HKCU:\Software\AuditSante\` avec l'horodatage actuel.

📋 Aide-mémoire des commandes clés

Action	Commande PowerShell
Lister les sous-clés	`Get-ChildItem`
Lire une valeur	`(Get-ItemProperty -Path ...).NomValeur`
Créer une clé	`New-Item -Path ...`
Créer/Forcer une valeur	`Set-ItemProperty -Path ... -Name ... -Value ...`
Supprimer	`Remove-Item` / `Remove-ItemProperty`
