

- TP 1 : Inventaire sélectif des disques physiques

TP 2 : Audit de sécurité des comptes locaux

TP 3 : Analyse des performances (Top Processus)

TP 4 : Cartographie des services réseau

TP 5 : Nettoyage automatique des journaux

TP 6 : Surveillance des services critiques

TP 7 : Historique des mises à jour système

TP 8 : Diagnostic matériel rapide (BIOS et Uptime)

TP 9 : Analyse des erreurs critiques du journal d’évènements

TP 10 : Test de rebond réseau (Connectivity)

TP 1 : Inventaire sélectif des disques physiques

- **Objectif** : Isoler les disques système pour un rapport d’inventaire.
- **Énoncé** : Écrivez un script qui liste uniquement les disques dont le nom (`FriendlyName`) contient le mot “Windows” ou “OS”. Affichez sous forme de tableau : le numéro du disque, le nom, et la taille totale convertie en Go.
- **Indices** : `Get-Disk` , `Where-Object -match` , `Select-Object` avec propriété calculée pour les Go.

TP 2 : Audit de sécurité des comptes locaux

- **Objectif** : Identifier les failles de sécurité potentielles sur les mots de passe.
- **Énoncé** : Affichez la liste de tous les utilisateurs locaux qui possèdent la caractéristique “Le mot de passe n’expire jamais”. Le rapport doit afficher le nom de l'utilisateur et la date de sa dernière connexion.
- **Indices** : `Get-LocalUser` , filtre sur `PasswordNeverExpires` , `LastLogon` .

TP 3 : Analyse des performances (Top Processus)

- **Objectif** : Identifier les “consommateurs” de ressources en temps réel.
- **Énoncé** : Créez un script qui identifie les 5 processus utilisant le plus de mémoire vive (RAM) et les 5 utilisant le plus de temps processeur (CPU). Affichez leur nom et leur identifiant (Id).
- **Indices** : `Get-Process` , `Sort-Object -Descending` , `Select-Object -First 5` .

TP 4 : Cartographie des services réseau

- **Objectif** : Lister les “portes d’entrée” ouvertes sur le serveur.
- **Énoncé** : Listez toutes les connexions réseaux dont l’état est “Listen” (en écoute). Pour chaque connexion, affichez le port local et l’identifiant du processus (PID) associé.
- **Indices** : `Get-NetTCPConnection` , paramètre `-State` .

TP 5 : Nettoyage automatique des journaux

- **Objectif** : Gérer l’espace disque en ciblant les vieux fichiers inutiles.
- **Énoncé** : Parcourez le dossier `C:\Windows\Logs` . Pour chaque fichier créé il y a plus de 30 jours, affichez son nom et sa taille. Ajoutez une commande (en mode simulation `-WhatIf`) pour les supprimer.
- **Indices** : `Get-ChildItem -Recurse` , `Where-Object` , `(Get-Date).AddDays(-30)` , `Remove-Item` .

TP 6 : Surveillance des services critiques

- **Objectif** : Vérifier la cohérence entre la configuration et l’état réel.
- **Énoncé** : Trouvez tous les services dont le nom commence par “Win” (ex: WinRM, Windows Update). Affichez uniquement ceux qui sont configurés en démarrage “Automatique” mais qui ne sont pas en cours d’exécution.
- **Indices** : `Get-Service` , filtres combinés sur `StartType` et `Status` .

TP 7 : Historique des mises à jour système

- **Objectif** : Vérifier que le serveur est à jour.
- **Énoncé** : Listez les 10 dernières mises à jour (Hotfix) installées sur la machine. Affichez l’identifiant de la mise à jour (HotFixID), la description et la date d’installation.

- **Indices :** `Get-HotFix` , `Sort-Object InstalledOn` , `Select-Object -First 10` .

TP 8 : Diagnostic matériel rapide (BIOS et Uptime)

- **Objectif :** Obtenir les informations d'identité du serveur.
- **Énoncé :** Récupérez via les classes CIM/WMI le numéro de série de la machine (Tag) et la date du dernier redémarrage. Calculez depuis combien de temps le serveur est allumé.
- **Indices :** `Get-CimInstance -ClassName Win32_BIOS` , `Win32_OperatingSystem` .

TP 9 : Analyse des erreurs critiques du journal d'évènements

- **Objectif :** Anticiper les pannes système.
- **Énoncé :** Interrogez le journal d'évènements "System". Affichez les 5 dernières erreurs (Type: Error) enregistrées, avec l'heure, la source de l'erreur et le message d'explication.
- **Indices :** `Get-EventLog` , `-LogName System` , `-EntryType Error` , `-Newest 5` .

TP 10 : Test de rebond réseau (Connectivity)

- **Objectif :** Tester la communication du serveur vers l'extérieur.
- **Énoncé :** Le script doit vérifier si le serveur distant parvient à joindre `google.com` sur le port 443 (HTTPS) et afficher si le test a réussi ou échoué de manière claire.
- **Indices :** `Test-NetConnection` , `-ComputerName` , `-Port` .