

Épreuve intégrée – Audit d'un poste Windows via PowerShell (Manoah Sw)

Vous êtes technicien informatique et vous devez collecter des informations essentielles sur un poste Windows afin de les transmettre à un serveur de surveillance du parc.

 niveau

Ce document présente l'énoncé personnalisé de l'épreuve intégrée et précise les informations à collecter pour ce poste.

Contraintes

- Travail en PowerShell, utilisation du pipeline attendue
- Script dans un fichier `.ps1` lisible, structuré et commenté
- `Get-CimInstance` est autorisée et recommandée
- Chaque bloc doit être réalisé dans sa propre fonction
- Aucun accès direct au registre
- Export final d'un objet au format JSON à l'aide de `ConvertTo-Json`
- Respectez **EXACTEMENT** les valeurs qui vous sont demandées

Blocs à réaliser

Informations générales du poste

Objectif : Identifier de manière fiable la machine auditée dans un parc informatique.

A Faire : Récupérer les informations générales permettant d'identifier un poste Windows.

Commandes autorisées / recommandées : `$env:COMPUTERNAME`, `Get-CimInstance Win32_ComputerSystem`

Clé dans le json: `device`

Informations à récupérer

- **Nom de la machine**: Nom local du poste.
- **Constructeur du poste**: Fabricant (ex. Dell, HP, Lenovo).

- **Modèle du poste:** Référence du modèle matériel.
- **RAM totale:** Quantité totale de mémoire vive.
- **Utilisateur connecté:** Compte utilisateur actif au moment de l'exécution.
- **Présence d'un hyperviseur:** Indique si le système tourne dans un environnement virtualisé.
- **Processeurs logiques:** Nombre de threads visibles par l'OS.

Traitements à appliquer

- La quantité de RAM doit être affichée en MB.

Processeur (CPU)

Objectif : Décrire les capacités CPU du poste.

A Faire : Récupérer les informations essentielles du processeur.

Commandes autorisées / recommandées : `Get-CimInstance Win32_Processor`

Clé dans le json: `cpu`

Informations à récupérer

Pour tous les objets retournés:

- **Modèle du processeur:** Nom complet du processeur.
- **Nombre de cœurs:** Nombre de cœurs physiques.
- **Nombre de threads:** Nombre de processeurs logiques du CPU.
- **Désignation courte:** Nom court (si disponible).
- **Socket:** Désignation du socket (si disponible).
- **Identifiant CPU:** Identifiant système du CPU.

Système d'exploitation

Objectif : Identifier précisément le Windows installé.

A Faire : Récupérer les informations essentielles du système d'exploitation.

Commandes autorisées / recommandées : `Get-CimInstance Win32_OperatingSystem`

Clé dans le json: `os`

Informations à récupérer

- **Nom du système:** Nom complet du système d'exploitation Windows installé.
- **Version:** Version principale du système d'exploitation.

- **Numéro de build:** Numéro de build précis de Windows.
- **Utilisateur enregistré:** Nom de l'utilisateur enregistré lors de l'installation.
- **Nom de la machine:** Nom de l'ordinateur tel que reconnu par le système.
- **Date d'installation:** Date à laquelle Windows a été installé.

Sécurité – Pare-feu

Objectif : Vérifier l'état du pare-feu Windows.

A Faire : Lister les profils de pare-feu et leur activation.

Commandes autorisées / recommandées : `Get-NetFirewallProfile`

Clé dans le json: `firewallProfiles`

Informations à récupérer

Pour tous les objets retournés:

- **Nom du profil:** Profil (Domain/Private/Public).
- **Activé:** Indique si le pare-feu est activé.
- **Action entrante par défaut:** Action par défaut (Allow/Block).
- **Fichier de log:** Chemin de log (si disponible).
- **Action sortante par défaut:** Action sortante (Allow/Block).
- **Notification:** Notification sur écoute (si disponible).

Processus gourmands

Objectif : Identifier des processus consommant beaucoup de ressources.

A Faire : Lister les Top N processus par CPU et par mémoire (Working Set).

Commandes autorisées / recommandées : `Get-Process`

Clé dans le json: `performance`

Informations à récupérer

- **Nom du processus:** Nom du processus.
- **CPU:** Temps CPU (si disponible).
- **Mémoire (Working Set 64):** Mémoire utilisée en octets.
- **Heure de démarrage:** Heure de lancement (si disponible).
- **PID:** Identifiant du processus.

- **Chemin exécutable:** Chemin de l'exécutable (si disponible).

Traitements à appliquer

- Afficher les 5 processus les plus gourmands en CPU.
- Afficher les 8 processus les plus gourmands en mémoire (Working Set).

Résultat attendu

Votre script doit produire un **objet** structuré contenant les informations demandées dans les blocs ci-dessus et l'exporter au format JSON.

Votre script **DOIT fonctionner correctement** et fournir les informations demandées.

Présentation orale

Vous devrez être capable d'expliquer :

- comment vous avez identifié les bonnes informations
- pourquoi vous avez choisi certaines commandes
- comment vous avez appliqué les tris / filtres / seuils
- comment vous avez structuré les données
- Vous devrez être en mesure de modifier le script pour ajouter des informations supplémentaires ou corriger des erreurs.