

Q&A - Hardening Windows

1. Dans un environnement Windows, pourquoi est-il essentiel d'isoler les comptes et systèmes de niveau 0 dans un modèle en niveaux (Tiered Model), et comment cela renforce-t-il la sécurité globale ?

- **Réponse : a) Les comptes et systèmes de niveau 0 ont des droits sur tous les niveaux inférieurs ; les isoler réduit le risque de compromission totale de l'infrastructure en cas de brèche.**
 - **Explication :** Les comptes et systèmes de niveau 0 contrôlent les actifs critiques (comme les contrôleurs de domaine). Les isoler des autres niveaux empêche qu'une compromission à un niveau inférieur n'affecte ces actifs vitaux, limitant ainsi les dégâts potentiels.
-

2. Comment configurez-vous un serveur Windows pour qu'il applique automatiquement les correctifs de sécurité sans intervention manuelle, tout en minimisant les risques de redémarrage imprévu en production ?

- **Réponse : a) En activant l'installation automatique des mises à jour avec planification via WSUS et en configurant des heures de maintenance.**
 - **Explication :** Utiliser WSUS permet de contrôler quand et comment les mises à jour sont déployées. Configurer des fenêtres de maintenance permet de minimiser les interruptions en production en programmant les redémarrages en dehors des heures critiques.
-

3. Quelle stratégie de groupe (GPO) doit être mise en place pour restreindre l'accès aux ports USB sur les postes de travail Windows, tout en permettant leur utilisation pour des périphériques spécifiques autorisés ?

- **Réponse : b) Configurer une GPO pour bloquer l'installation de périphériques non autorisés et utiliser une liste de périphériques approuvés.**
 - **Explication :** Cette méthode permet de restreindre l'accès aux ports USB tout en permettant l'utilisation de périphériques spécifiques nécessaires aux opérations, réduisant ainsi le risque d'insertion de dispositifs malveillants.
-

4. Dans quel cas utiliseriez-vous BitLocker avec TPM et PIN, et quel est l'avantage de cette configuration ?

- **Réponse :** a) Pour protéger les systèmes contre les vols physiques ; cela ajoute une couche de sécurité supplémentaire en nécessitant une authentification lors du démarrage.
 - **Explication :** L'ajout d'une couche d'authentification via un PIN en plus du TPM assure que même si un appareil est volé, les données restent protégées, car le démarrage du système nécessite une authentification supplémentaire.
-

5. Quel est l'objectif principal de la séparation des comptes administratifs et standards sous Windows, et comment cette pratique renforce-t-elle la sécurité du système ?

- **Réponse :** a) Minimiser l'impact d'une compromission de compte en limitant les droits administratifs ; les utilisateurs standards ne peuvent effectuer que des tâches de base.
 - **Explication :** En séparant les comptes administratifs des comptes standards, on limite les possibilités d'abus ou de compromission. Si un compte standard est compromis, les dommages potentiels sont minimisés.
-

6. Pourquoi est-il important de désactiver les comptes d'administrateur local par défaut sur les machines Windows, et comment cette action contribue-t-elle à la sécurité globale ?

- **Réponse :** a) Pour empêcher les utilisateurs non autorisés d'accéder au système via des mots de passe par défaut ; cela réduit les risques d'attaques.
 - **Explication :** Les comptes administratifs locaux par défaut sont souvent la cible d'attaques, car ils utilisent des mots de passe prédictibles. Désactiver ces comptes ou changer les mots de passe par défaut réduit considérablement ce risque.
-

7. Lors de la configuration de Windows Defender Application Control (WDAC), quel est le principal avantage de la création d'une politique en mode "Audit" avant de la mettre en application en mode "Enforcement" ?

- **Réponse :** a) Tester l'impact de la politique sur les applications et services avant de bloquer les actions, afin de ne pas perturber les opérations en production.
- **Explication :** Le mode "Audit" permet de voir comment la politique affecte les systèmes sans bloquer immédiatement les applications non conformes, ce qui aide à affiner les règles avant leur application stricte.

8. Comment pouvez-vous configurer une stratégie de gestion des mises à jour pour éviter que les serveurs critiques ne redémarrent de manière inattendue après l'installation de mises à jour de sécurité ?

- **Réponse :** a) Configurer les fenêtres de maintenance et utiliser les "Options de redémarrage contrôlé" pour planifier les redémarrages en dehors des heures de production.
- **Explication :** Cette approche permet de garantir que les serveurs ne redémarrent pas de manière imprévue après l'application des mises à jour, minimisant ainsi les interruptions en production.

9. Quel est le rôle de l'outil "Security Compliance Toolkit" (SCT) de Microsoft dans le processus de hardening des systèmes Windows ?

- **Réponse :** a) Fournir des configurations de sécurité recommandées par Microsoft que vous pouvez personnaliser et appliquer pour durcir les systèmes.
- **Explication :** Le Security Compliance Toolkit offre des modèles de configurations de sécurité basées sur les meilleures pratiques de Microsoft, ce qui facilite le processus de durcissement tout en assurant la conformité aux normes de sécurité.

10. Lors de la mise en œuvre d'une solution de gestion des accès privilégiés (PAM) sous Windows, pourquoi est-il recommandé d'utiliser l'accès "just-in-time" et comment cela réduit-il les risques de sécurité ?

- **Réponse :** a) L'accès "just-in-time" limite la durée pendant laquelle les privilèges administratifs sont actifs, réduisant ainsi la fenêtre de vulnérabilité en cas de compromission d'un compte.
- **Explication :** En limitant la durée des privilèges administratifs, l'accès "just-in-time" réduit le risque d'exploitation prolongée en cas de compromission d'un compte privilégié, rendant le système plus sécurisé.