

Q&A - Hardening OS

1. Quelle est la première étape recommandée pour commencer le processus de hardening d'un système d'exploitation ?

- **Réponse : b) Auditer les configurations actuelles et les vulnérabilités du système.**
 - **Explication :** Avant de commencer le processus de hardening, il est essentiel d'évaluer l'état actuel du système. Cela permet d'identifier les failles et de prioriser les actions de sécurisation.
-

2. Lors du hardening d'un système, quel est l'objectif principal de la segmentation réseau ?

- **Réponse : b) Isoler les différents services pour limiter la propagation des menaces.**
 - **Explication :** La segmentation réseau divise le réseau en segments distincts, empêchant une menace ou un attaquant de se propager facilement d'une partie du réseau à une autre.
-

3. Quelle est la meilleure pratique pour gérer les mises à jour de sécurité sur un système critique en production ?

- **Réponse : c) Tester les mises à jour sur un environnement de test avant de les déployer en production.**
 - **Explication :** Tester les mises à jour dans un environnement de test permet de vérifier qu'elles n'introduisent pas de nouveaux problèmes avant de les appliquer aux systèmes critiques en production.
-

4. Pourquoi est-il important de minimiser les services en cours d'exécution sur un serveur ?

- **Réponse : b) Pour réduire la surface d'attaque et limiter les vulnérabilités exploitables.**
 - **Explication :** Moins il y a de services actifs, moins il y a de points d'entrée potentiels pour les attaquants. Cela réduit la probabilité qu'un service vulnérable soit exploité.
-

5. Quel est l'objectif principal de l'utilisation de listes de contrôle d'accès (ACL) dans le hardening ?

- **Réponse : a) Restreindre les accès aux fichiers et aux ressources en fonction de rôles définis.**
 - **Explication :** Les ACL permettent de contrôler finement qui a accès à quoi, en définissant des permissions précises basées sur les rôles des utilisateurs.
-

6. Comment le principe du moindre privilège contribue-t-il à la sécurité d'un système d'exploitation ?

- **Réponse : b) Il garantit que chaque utilisateur n'a accès qu'aux ressources nécessaires pour ses tâches spécifiques.**
 - **Explication :** En limitant les privilèges des utilisateurs, on minimise les risques en cas de compromission d'un compte, car l'attaquant ne pourra pas accéder à des ressources au-delà de ce qui est strictement nécessaire pour l'utilisateur.
-

7. Quelle est la meilleure pratique pour sécuriser les configurations par défaut d'un système nouvellement installé ?

- **Réponse : b) Modifier les configurations par défaut pour réduire les vulnérabilités courantes.**
 - **Explication :** Les configurations par défaut peuvent contenir des paramètres peu sécurisés. Les modifier est crucial pour éviter l'exploitation de vulnérabilités connues.
-

8. Lors de la configuration d'un pare-feu, quelle règle devrait être appliquée en premier pour sécuriser un réseau ?

- **Réponse : b) Bloquer tout le trafic et autoriser uniquement les services et ports nécessaires.**
 - **Explication :** Cette approche "deny by default" est la plus sécurisée car elle garantit que seuls les services explicitement autorisés peuvent fonctionner, réduisant ainsi le risque d'accès non autorisé.
-

9. Comment le chiffrement des données contribue-t-il au hardening d'un système ?

- **Réponse : a) Il empêche les utilisateurs non autorisés d'accéder aux données, même s'ils accèdent physiquement au support de stockage.**
 - **Explication :** Le chiffrement protège les données en rendant leur lecture impossible sans les clés de déchiffrement appropriées, même si l'attaquant a un accès physique au matériel.
-

10. Pourquoi est-il crucial de surveiller les journaux d'événements sur un système sécurisé ?

- **Réponse : a) Pour identifier les tentatives d'accès non autorisé et détecter les incidents de sécurité.**
 - **Explication :** La surveillance des journaux permet de repérer rapidement les anomalies et les incidents, ce qui est essentiel pour réagir rapidement en cas de compromission.
-

11. Quelle est l'importance d'utiliser des outils d'analyse de vulnérabilité dans le cadre du hardening ?

- **Réponse : a) Ils permettent d'identifier les failles de sécurité avant qu'elles ne soient exploitées.**
 - **Explication :** Ces outils scannent le système à la recherche de vulnérabilités connues, permettant ainsi de les corriger avant qu'elles ne soient exploitées par des attaquants.
-

12. Quelle approche est recommandée pour sécuriser les environnements multi-utilisateurs ?

- **Réponse : b) Mettre en place une séparation stricte des privilèges et des rôles pour chaque utilisateur.**
 - **Explication :** En séparant strictement les privilèges, on s'assure que chaque utilisateur ne peut accéder qu'aux ressources qui lui sont nécessaires, limitant ainsi les risques de compromission.
-

13. Pourquoi est-il essentiel d'utiliser des environnements de test pour les nouvelles configurations de sécurité avant leur déploiement en production ?

- **Réponse : a) Pour garantir que les nouvelles configurations n'affecteront pas négativement les systèmes critiques.**
 - **Explication :** Tester les configurations en amont permet de s'assurer qu'elles n'introduisent pas de problèmes qui pourraient impacter les systèmes de production.
-

14. Quel est le rôle du contrôle d'accès basé sur les rôles (RBAC) dans le hardening d'un système ?

- **Réponse : a) Limiter l'accès des utilisateurs à seulement ce qui est nécessaire à leur rôle.**
 - **Explication :** Le RBAC assure que les utilisateurs n'ont accès qu'aux ressources nécessaires à leur rôle, minimisant les risques d'accès non autorisé.
-

15. Comment les correctifs de sécurité contribuent-ils à la robustesse d'un système d'exploitation ?

- **Réponse : a) Ils corrigent les failles de sécurité connues et améliorent la résilience contre les attaques.**

- **Explication** : Les correctifs de sécurité comblent les vulnérabilités connues, réduisant ainsi la surface d'attaque du système et le protégeant contre des menaces spécifiques.
-

Revision #2

Created 3 September 2024 20:59:13 by Alek

Updated 6 September 2024 08:19:49 by Alek