TP : Gestion des vulnérabilités et configurations sécurisées

Contexte du problème

Vous êtes ingénieur(e) en cybersécurité au sein d'une entreprise ayant une infrastructure informatique hétérogène comprenant des serveurs Linux et Windows. Récemment, l'entreprise a été avertie de plusieurs vulnérabilités critiques découvertes sur certains logiciels et systèmes utilisés dans son infrastructure. En tant que responsable sécurité, votre tâche est d'évaluer précisément ces vulnérabilités, d'identifier les risques encourus, de recommander les actions correctives nécessaires et enfin de vérifier leur mise en conformité selon les standards reconnus (notamment les CIS Benchmarks).

Objectifs du problème

En résolvant ce problème, vous devez démontrer que vous êtes capable de :

- Identifier avec précision les vulnérabilités présentes sur les systèmes.
- Évaluer la gravité et l'impact potentiel des vulnérabilités en utilisant la base CVE.
- Recommander et tester des correctifs appropriés avant leur déploiement.
- Proposer des configurations sécurisées conformes aux bonnes pratiques (CIS Benchmarks).
- Vérifier la sécurité effective après application des correctifs et des configurations.

Description détaillée du problème à résoudre

Votre équipe de sécurité vient de terminer un scan automatisé de vulnérabilités sur deux systèmes critiques :

- Un serveur **Linux Ubuntu 22.04 LTS** exposé à Internet, hébergeant une application web basée sur Apache.
- Un serveur **Windows Server 2022** qui héberge une base de données MS SQL critique à l'interne.

Le scan automatisé (via Nessus ou OpenVAS) a généré les alertes suivantes :

Vulnérabilités détectées :

1. **Serveur Linux Ubuntu :**
   a. CVE-2022-22720 : Vulnérabilité critique dans Apache HTTP Server (CVSS : 9.8).
   b. Configuration non sécurisée : Plusieurs services inutiles activés, tels que FTP et Telnet, et ports ouverts non justifiés (21 et 23).
2. **Serveur Windows Server :**
   a. CVE-2023-23384 : Vulnérabilité critique dans Microsoft SQL Server permettant l'élévation de privilèges à distance (CVSS : 9.0).
   b. Configuration non sécurisée : Comptes administratifs obsolètes non supprimés et politique de mots de passe faible.

Missions à réaliser :

Afin d'apporter une solution structurée et complète au problème soulevé par ce rapport, veuillez répondre méthodiquement aux points suivants :

Partie 1 : Identification et analyse des vulnérabilités

- Décrivez précisément chaque vulnérabilité en consultant la base CVE/NVD :
  - Quelles sont les conditions techniques d'exploitation ?
  - Quels sont les impacts potentiels pour l'organisation en cas d'exploitation réussie ?

Partie 2 : Proposition de gestion des correctifs

- Identifiez les correctifs spécifiques disponibles pour chaque vulnérabilité :
  - Où les télécharger ? Quelle est leur procédure d'application ?
  - Quelle stratégie recommandez-vous pour leur application (automatique ou manuelle) et pourquoi ?
- Décrivez comment vous testerez ces correctifs dans un environnement de préproduction :
  - Quels critères devez-vous vérifier avant leur déploiement en production ?

Partie 3 : Proposition de configurations sécurisées

- À partir des CIS Benchmarks appropriés (Ubuntu Linux et Windows Server), indiquez précisément les configurations sécurisées recommandées pour :
  - Désactiver les services inutiles (ex : FTP, Telnet).
  - Fermer les ports ouverts non nécessaires.
  - Renforcer la gestion des comptes administratifs et la politique de mots de passe.

- Décrivez précisément comment vous mettrez en œuvre ces configurations sécurisées à l'aide d'outils automatisés (Ansible, Puppet, Chef).

Partie 4 : Vérification finale et audit de sécurité

- Proposez une méthode complète pour vérifier après correction :
  - Que les correctifs ont bien été installés et fonctionnent correctement.
  - Que les configurations sécurisées sont appliquées conformément aux CIS Benchmarks.
- Indiquez précisément quels outils ou quelles techniques vous utiliserez pour cet audit final.

Livrables attendus

À l'issue de votre analyse et de vos recherches, vous devez présenter :

- Un rapport structuré répondant précisément aux questions posées ci-dessus.
- Un plan détaillé (procédure technique) décrivant comment appliquer les correctifs et les configurations sécurisées recommandées.
- Une méthodologie précise d'audit et de vérification finale de la sécurité des systèmes.