TP contrôle - Conception, Déploiement et Administration d'un Réseau d'Entreprise

Contexte

Vous êtes responsable IT d'une entreprise fictive appelée **TechSecure**. Cette entreprise gère une infrastructure hybride composée de serveurs Windows et Linux, protégée par un firewall centralisé. Afin de garantir la sécurité et l'efficacité des opérations, l'entreprise souhaite automatiser la gestion, le déploiement et la sécurisation de son infrastructure à l'aide d'Ansible.

Votre mission consiste à mettre en place une solution complète qui permet :

1. La configuration et l'administration des serveurs Windows et Linux.
2. Le déploiement de règles de firewall pour sécuriser les flux réseau.
3. Le déploiement et la gestion d'un serveur Web
4. L'application des mesures de hardening sur les systèmes pour améliorer leur sécurité.

Objectifs du projet

- Comprendre comment structurer un projet Ansible pour gérer une infrastructure hybride.
- Automatiser des tâches d'administration courante (création d'utilisateurs, gestion des services, etc.).
- Déployer et configurer des règles de firewall en respectant les bonnes pratiques de sécurité.
- Implémenter des stratégies de hardening pour les systèmes Windows et Linux.

Livrables

. • Les fichiers Ansible :

- Inventaire (`hosts`).
- Playbooks.
- Templates Jinja2 si nécessaire.

• Une documentation utilisateur décrivant :

- La structure du projet Ansible.
- Les commandes pour exécuter les playbooks.

Sujet

Étape 1 : Préparation

1. Analysez l'infrastructure actuelle (un schéma simplifié peut être fourni avec l'étude de cas).
2. Identifiez les tâches à automatiser, par exemple :
    - Gestion des utilisateurs.
    - Activation ou désactivation de services.
    - Configuration réseau (DNS, IP statique).

Étape 2 : Configuration de l'environnement

1. Créez un inventaire Ansible pour représenter l'infrastructure (fichiers `inventory`).
    - Catégorisez les machines par type (Linux, Windows, firewall).

Étape 3 : Automatisation des tâches

1. Administration Linux :
    - Créez un playbook qui installe des paquets nécessaires (ex : `htop`, `fail2ban`, etc.).
    - Configurez SSH pour renforcer la sécurité (désactiver root login, key-based auth).
2. Administration Windows :
    - Créez un playbook qui installe des outils (DNS, DHCP, etc) via powershell
    - Appliquez une stratégie de mot de passe sécurisée.
    - Créer des entrées DNS dans la zone DNS
    - Créer une étendue DHCP
3. Administration Web:

- Créez un playbook qui installe le serveur nginx
- Héberger l'application web
- Certificat SSL/TLS

4. Firewall :
    - Créez un playbook qui déploie des règles de firewall (ex : IPTables, UFW).
    - Ouvrez uniquement les ports nécessaires (SSH, HTTP/HTTPS).

Étape 4 : Hardening

1. Implémentez les mesures de hardening pour chaque type de système :
    - Linux : Configuration des permissions, désactivation des services inutiles.
    - Windows : Paramètres de registre pour limiter les attaques (SMBv1, RDP).

Étape 5 : Tests et validation

1. Testez vos playbooks sur des machines virtuelles.
2. Corrigez les erreurs éventuelles.
3. Fournissez un rapport avec :
    - Les résultats des tâches exécutées.
    - Une évaluation des mesures de sécurité appliquées.