TP 11
Renforcement de la sécurité des serveurs

Objectif :

• utiliser les stratégies de groupe pour sécuriser les serveurs membres ;
• effectuer l'audit de l'accès au système de fichiers ;
• effectuer l'audit des connexions au domaine.

Besoins :

Pour réaliser ce TP on aura besoin de trois machines :

- Une machine Windows 2012 server **DC1** qui va jouer le rôle du contrôleur de domaine et du serveur DNS
- Deux machines : **CL1 :** cliente Windows 7 et **SRV1** : serveur membre 2012.

Exercice 1: Utilisation des stratégies de groupe pour sécuriser les serveurs membres

Tâche 1 : Créer une unité d'organisation de serveurs membres et y placer les serveurs

1. Sur DC1, ouvrez **Utilisateurs et ordinateurs Active Directory**.
2. Créez une nouvelle unité d'organisation appelée **Unité d'organisation Serveurs membres**.
3. Placez le serveur **SVR1** dans **Unité d'organisation Serveurs membres**.

Tâche 2 : Créer un groupe Administrateurs de serveur

• Sur DC1, dans **Unité d'organisation Serveurs membres**, créez un nouveau groupe de sécurité global appelé **Administrateurs de serveur**.

Tâche 3 : Créer un objet de stratégie de groupe des paramètres de sécurité des serveurs membres et le lier à l'unité d'organisation Serveurs membres

1. Sur DC1, ouvrez la **console de gestion des stratégies de groupe**.
2. Dans la console de gestion des stratégies de groupe (GPMC), dans le conteneur Objets de stratégie de groupe, créez un nouvel **objet de**

stratégie de groupe avec un nom **Paramètres de sécurité des serveurs membres**.

3. Dans la console de gestion des stratégies de groupe, liez l'objet **Paramètres de sécurité des serveurs membres** à l'**unité d'organisation Serveurs membres**.

Tâche 4 : Configurer l'appartenance aux groupes pour les administrateurs locaux afin d'inclure les groupes Administrateurs de serveur et Administrateurs de domaine

1. Sur DC1, ouvrez la **console de gestion des stratégies de groupe**.
2. Modifiez **Default Domain Policy**.
3. Accédez à **Configuration ordinateur**, cliquez sur **Stratégies**, sur **Paramètres Windows**, sur **Paramètres de sécurité**, puis sur **Groupes restreints**.
4. Ajoutez les groupes **Administrateurs de serveur** et **OFPPT\Admins du domaine** au groupe **Administrateurs**.
5. Fermez l'Éditeur de gestion des stratégies de groupe.

Tâche 5 : Vérifier que les administrateurs d'ordinateur ont été ajoutés au groupe Administrateurs local

1. Basculez vers **SVR1**, puis connectez-vous en tant qu'**Administrateur**
2. Ouvrez une fenêtre Windows PowerShell, et à l'invite de commande Windows PowerShell, tapez la commande suivante : Gpupdate /force
3. Ouvrez le **Gestionnaire de serveur**, ouvrez la console **Gestion de l'ordinateur**, puis développez **Utilisateurs et groupes locaux**.
4. Confirmez que le groupe **Administrateurs** contient à la fois **OFPPT\ Admins du domaine** et **OFPPT\Administrateurs de serveur** comme membres.
5. Fermez la console **Gestion de l'ordinateur**.

Tâche 6 : Modifier l'objet GPO Paramètres de sécurité des serveurs membres pour supprimer des utilisateurs de l'autorisation Permettre l'ouverture d'une session locale

1. Basculez vers **DC1**.
2. Sur DC1, dans GPMC, modifiez l'objet GPO **Paramètres de sécurité des serveurs membres**.
3. Dans la fenêtre Éditeur de gestion des stratégies de groupe, accédez à **Configuration ordinateur\ Stratégies\Paramètres Windows\ Paramètres de sécurité\Stratégies locales\Attribution des droits utilisateur** et configurez **Permettre l'ouverture d'une session locale** pour les groupes de sécurité **Admins du domaine** et **Administrateurs**.

Tâche 7 : Modifier l'objet GPO Paramètres de sécurité des serveurs membres pour activer Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur intégré

1. Sur DC1, dans la fenêtre Éditeur de gestion des stratégies de groupe, accédez à **Configuration de l'ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\ Options de sécurité**.
2. Activez **Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur intégré**.
3. Fermez l'Éditeur de gestion des stratégies de groupe.

Tâche 8 : Vérifier qu'un utilisateur ne disposant pas de droits d'administration ne peut pas se connecter à un serveur membre

1. Basculez vers SVR1.
2. Ouvrez une fenêtre Windows PowerShell et à l'invite de commande Windows PowerShell, tapez la commande suivante : Gpupdate /force
3. Déconnectez-vous de SVR1.
4. Essayez de vous connecter à **SVR1** en tant qu'**OFPPT\Ali**. (Ali un compte utilisateur de domaine)
5. Vérifiez que vous ne pouvez pas vous connecter à SVR1.

Exercice 2 : Audit de l'accès au système de fichiers

Tâche 1 : Modifier l'objet GPO Paramètres de sécurité des serveurs membres pour activer l'audit de l'accès aux objets

1. Basculez vers **DC1**.
2. Connectez-vous à **DC1** en tant qu'**OFPPT\Administrateur**
3. Dans la console GPMC, modifiez l'objet GPO **Paramètres de sécurité des serveurs membres**.
4. Dans la fenêtre Éditeur de gestion des stratégies de groupe, accédez à **Configuration ordinateur\ Stratégies\Paramètres Windows\ Paramètres de sécurité\Stratégies locales\Stratégie d'audit**.
5. Activez **Auditer l'accès aux objets** avec les deux paramètres **Réussite** et **Échec**.
6. Déconnectez-vous de DC1.

Tâche 2 : Créer et partager un dossier

1. Basculez vers **SVR1**.
2. Connectez-vous à **SVR1** en tant qu'**OFPPT\Administrateur**

3. Sur SVR1, sur le lecteur C, créez un nouveau dossier avec le nom **Marketing**.

4. Configurez le dossier **Marketing** avec les autorisations de partage **Lecture/écriture** pour l'utilisateur **Ali**.

Tâche 3 : Activer l'audit sur le dossier Marketing pour les utilisateurs du domaine

1. Sur SVR1, dans la fenêtre Disque local (C:), configurez l'audit sur le dossier **Marketing**, avec les paramètres suivants :

o Sélectionnez un principal : **Utilisateurs du domaine**

o Type : **Tout**

o Autorisation : **Lecture et exécution, Affichage du contenu du dossier, Lecture, Écriture**

o Conservez les valeurs par défaut des autres paramètres.

2. Actualisez la stratégie de groupe en tapant la commande suivante dans une fenêtre PowerShell : gpupdate /force

Tâche 4 : Créer un nouveau fichier dans le partage de fichiers à partir de CL1

1. Basculez vers **CL1**.

2. Connectez-vous à **CL1** en tant qu'**OFPPT\Administrateur**.

3. Ouvrez une fenêtre d'invite de commandes et tapez la commande suivante :
gpupdate /force
4. Fermez la fenêtre d'invite de commandes.

5. Déconnectez-vous de CL1, puis connectez-vous de nouveau en tant qu'**OFPPT\Ali**.

6. Ouvrez le dossier **Marketing** sur SVR1 en utilisant le chemin d'accès UNC suivant : **\\SVR1\Marketing**.

7. Créez un document texte nommé **Employés**.

8. Déconnectez-vous de CL1.

Tâche 5 : Visualiser les résultats dans le journal de sécurité sur le contrôleur de domaine

1. Basculez vers **SVR1**, et démarrez l'**observateur d'événements**.

2. Dans la fenêtre de l'observateur d'événements, développez **Journaux Windows**, puis ouvrez **Sécurité**.

3. Vérifiez que l'événement et les informations suivants s'affichent :

o Source : **Microsoft Windows Security Auditing**

o ID d'événement : **4663**

o Catégorie de la tâche : **Système de fichiers**

o Une tentative d'accès à un objet a été effectuée.

Exercice 3 : Audit des connexions au domaine

ॐ Tâche 1 : Modifier l'objet GPO Stratégie de domaine par défaut

1. Basculez vers **DC1**.

2. Connectez-vous à **DC1** en tant qu'**OFPPT\Administrateur**.

3. Sur DC1, démarrez le **Gestionnaire de serveur**, puis, dans le Gestionnaire de serveur, démarrez la console **GPMC**.

4. Sur DC1, dans la console GPMC, modifiez l'objet GPO **Default Domain Policy**.

5. Dans la fenêtre Éditeur de gestion des stratégies de groupe, accédez à **Configuration ordinateur\ Stratégies\Paramètres Windows\ Paramètres de sécurité\Stratégies locales\Stratégie d'audit**.

6. Activez **Auditer les événements de connexion aux comptes** avec les deux paramètres **Réussite** et **Échec**.

7. Mettez à jour la stratégie de groupe en utilisant la commande **gpupdate /force**.

Tâche 2 : Exécuter GPUpdate

1. Basculez vers **CL1**.

2. Connectez-vous à **CL1** en tant qu'**OFPPT\Administrateur**

3. Ouvrez une fenêtre d'invite de commandes et tapez la commande suivante :

gpupdate /force

4. Fermez la fenêtre d'invite de commandes et déconnectez-vous de CL1.

Tâche 3 : Se connecter à CL1 avec un mot de passe incorrect

• Connectez-vous à CL1 en tant qu'**OFPPT\Ali**.

Remarque : Ce mot de passe est intentionnellement incorrect afin de générer une entrée de journal de sécurité indiquant qu'une tentative de connexion infructueuse a été effectuée.

ॐ Tâche 4 : Examiner les journaux des événements sur DC1

1. Sur DC1, démarrez l'**observateur d'événements**.

2. Dans la fenêtre de l'**observateur d'événements**, développez **Journaux Windows**, puis cliquez sur **Sécurité**.

3. Examinez les journaux des événements pour rechercher le message suivant : « **ID d'événement 4771 La pré-authentification Kerberos a échoué. Informations sur le compte : ID de sécurité : OFPPT\Ali**. »

Tâche 5 : Se connecter à CL1 avec le mot de passe correct

• Connectez-vous à **CL1** en tant qu'**OFPPT\Ali**

Tâche 6 : Examiner les journaux des événements sur DC1

1. Sur DC1, démarrez l'**observateur d'événements**.

2. Dans la fenêtre de l'**observateur d'événements**, développez **Journaux Windows**, puis cliquez sur **Sécurité**.

3. Examinez les journaux des événements pour rechercher le message suivant : « **ID d'événement 4624 L'ouverture de session d'un compte s'est correctement déroulée. Nouvelle connexion : ID de sécurité : OFPPT\Ali**. »