Atelier No6 -2 :

☞ **Sécurisation et dépannage de l'authentification (compte utilisateur)**

Sécurisation et dépannage de l'authentification.(30 minutes)

Dans cet exercice vous allez configurer des stratégies d'audit de domaine. Vous générerez des événements de connexion, vous examinerez et dépannerez les résultats de ces connexions:

A. Configuration des stratégies:

1- Ouvrez utilisateurs et ordinateurs d'Active Directory.
2- Sélectionnez le nœud du domaine (exemple Keglg.net)
3- Dans le menu Action, choisir Propriétés
4- Dans l'onglet Stratégie de groupe, choisissez Default Domain Policy puis cliquer sur Modifier
5- Cliquez sur Configuration de l'ordinateur, puis sur Paramètres Windows, Paramètres de sécurité, Stratégies de comptes et enfin Stratégie de verrouillage du compte.
6- Double cliquez sur durée de verrouillage des comptes
7- Cochez la case Définir ce paramètre de stratégie.
8- Dans la zone Le compte verrouillé pour, tapez **0,** puis cliquez sur Appliquer

Le système vous prévient qu'il va configurer les stratégies correspondant au seuil de verrouillage du compte et à la réinitialisation du compte de verrouillage. Cliquez sur OK

9- Cliquez sur Ok pour confirmer ces paramètres.
10- Confirmez que la durée de verrouillage des comptes est zéro, que le seuil est défini à 5 et que la réinitialisation du compte est fixée à 30 minutes.
11- Fermez la fenêtre Éditeurs d'objets de stratégies de groupe.
12- Dans la boite de dialogue Propriétés du domaine Keglg.net , Cliquez sur Ok
13- Sélectionnez le conteneur Domain Controllers situé sous le nœud du domaine
14- Dans le menu Action, choisir Propriétés
15- Dans l'onglet Stratégie de Groupe, sélectionnez Default Domain Controllers Policy et cliquer sur Modifier
16- Cliquez sur Configuration de l'ordinateur, puis sur Paramètres Windows, Paramètres de sécurité, Stratégies locales et enfin Stratégie d'audit.
17- Double-cliquez sur la stratégie Auditer les événements de connexion aux comptes
18- Cochez la case Définir ces paramètres de stratégie, cocher les cases Réussite et Échec. Puis Cliquer sur OK
19- Double-cliquez sur la stratégie Auditer les événements de connexion
20- Cochez la case Définir ces paramètres de stratégie, cocher les cases Réussite et Échec
21- Double-cliquez sur la stratégie Auditer la gestion des comptes.
22- Cochez la case Définir ces paramètres de stratégie, cochez la case Réussite puis Cliquez sur OK
23- Fermez la fenêtre Éditeur d'objets de stratégie de groupe.
24- Cliquez sur OK pour fermer la boite de dialogue Propriétés de Domain Controllers.

B. Génération d'événements de connexion

(au préalable sbishop doit être membre du groupe opérateurs d'impression du conteneur Builtin, si vous n'avez pas de station XP)

1. Déconnectez-vous de votre serveur
2. Générez deux événements d'échec d'ouverture de session en vous connectant avec le nom d'utilisateur sbishop et un mot de passe non valide.
3. Connectez-vous correctement en tant que sbishop
4. Déconnectez-vous.

C. Génération d'événements de gestion de comptes

1. Connectez-vous comme Administrateur
2. Ouvrez utilisateurs et ordinateurs dans Active Directory
3. sélectionnez dans l'arborescence l'OU Eleves
4. Dans le volet de droite, sélectionner l'utilisateur Scott Bishop, puis cliquez sur le menu Action
5. Cliquez sur la commande Réinitialisez le mot de passe
6. Saisissez et confirmer un nouveau mot de passe pour Scott Bishop puis Cliquez OK

D. Examiner les messages d'authentification des événements de sécurité.

1. Dans les outils d'Administration, ouvrez la console Gestion de l'ordinateur
2. Développer l'Observateur d'événements et sélectionner Sécurité
3. Explorez les événements qui ont été générés par une activité récente. Relevez les échecs de connexion, les réussites de connexion et la réinitialisation du mot de passe de Scott Bishop. Élargir la colonne catégorie pour pouvoir identifier les types d'événements.