**Procédure audit utilisateurs**

1. Tout d’abord rendez-vous « Gestionnaire des stratégies de groupe » :

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

1. Ensuite, allez dans « Domaines » puis faite un clic droit sur « learn.local » et faite « Créer un objet GPO dans ce domaine, et le lier ici… » :

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

1. Choisissez le nom que vous voulez et valider :

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

1. En suite refaite un clic droit sur « learn.local » et faite « Lier un objet de stratégie de groupe existant » :

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

1. Choisissez la stratégie que nous venons de créer, nous faisons ca pour vérifier que la stratégie est bien lier :

Une image contenant texte, Appareils électroniques, capture d’écran, affichage

Description générée automatiquement

1. En suite faite clique droit sur la stratégie que nous venons de créer, et faite modifier :

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

1. Maintenant rendez-vous dans « Configuration ordinateur » puis « Paramètres Windows » puis « Paramètres de sécurité » puis « Configuration avancé de la stratégie d’audit » puis « Stratégies d’audit » puis « gestion de compte ». Maintenant faites un clic droit sur « Auditer la gestion des comptes d’utilisateurs ».

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

1. Maintenant cocher « Configurer les événements d’audit suivants » et en suite « Succès »

Une image contenant texte, capture d’écran, affichage, logiciel

Description générée automatiquement

1. Ensuite nous créons un compte pour voir si cela apparait dans l’observateur d’événements :

Une image contenant texte, capture d’écran, nombre, logiciel

Description générée automatiquement

1. Nous voyons bien un évènement, le 4720 qui nous dis qu’un utilisateur a été créé :

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

1. Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

   Description générée automatiquementMaintenant nous allons modifier le mot de passe d’un utilisateur pour voir si un événement s’affiche. Pour commencer, rendez-vous sur un utilisateur depuis le « Centre d’administration Active Directory », et faite un clic droit sur l’utilisateur, puis « Réinitialiser le mot de passe… » :
2. Maintenant changez le mot de passe :

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

1. Nous pouvons maintenant allez voir dans l’observateur d’événements :

Nous avons l’évènement 4724 qui nous dit qu’il y a eu une tentative de réinitialisation de mot de passe, suivi du 4738 qui nous dit qu’un utilisateur a été modifié :

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquementUne image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement