Chapitre 1

Audit de configuration

1.1 Système d'exploitation

1.1.1 GNU/Linux

1.1.2 Microsoft Windows

Politique des comptes utilisateurs

La gestion des comptes utilisateurs est un point important de tout système d'exploitation. La gestion des comptes passe d'abord par la gestion de leurs mots de passe. Il est recommandé de forcer l'utilisateur à choisir un mot de passe fort, étant différent des précédant mots de passe et dont l'usage doit être limité à une période de temps. Ces contraintes minimisent le risque qu'un attaquant réussisse à découvrir le mot de passe par attaque par brute-force. La politique de blocage des comptes est un autre point important de la gestion des comptes. Il faut notamment configurer le temps d'inactivité avant verrouillage de session, le nombre de tentatives de connexions autorisées et le temps de verrouillage d'un compte utilisateur. Si la machine fait partie d'un domaine **Active Directory**, ces poliques peuvent être distribuées par **GPO**.
Localement elles peuvent aussi être configurées avec l'outil **Stratégie de sécurité locale** dans **Paramètres de sécurité** puis **Stratégies de comptes**.
La configuration peut être récupérée avec l'outil `PS > secedit.exe` en utilisant la commande suivante : `PS > secedit /export /CFG secedit.txt`.
On peut aussi récupérer la configuration en accèdant à la clé de registre correspondante :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters

Attribution des droits d'utilisateur

Les droits accordés aux utilisateurs doivent être restreint au maximum, pour minimiser la capacité d'un attaquant à faire une élévation de privilèges lors d'une compromission d'un compte ou d'une machine. L'accès distant depuis le réseau ou la connection via des services comme **Remote Desktop Service** doit être réservée au compte **Administrateur**. De même pour les fonctionnalité du système, par exemple le changement d'heure du système affecte la journalisation et doit donc aussi être restreint à l'administrateur. L'utilisateur **Guests** même si il n'est pas activé par défaut, doit avoir les droits les plus

restreints possible. Toutes ces configurations sont distribuables par **GPO**. Localement cette politique peut être modifié avec l'outil **Stratégie de sécurité locale** dans **Paramètres de sécurité** puis **Stratégies de comptes**.

Les configurations sur la politique des comptes utilisateurs sont accessibles avec l'outil **secedit.exe** en utilisant la commande suivante :
`PS > secedit /export /areas USER_RIGHTS /cfg policies.txt` .

Pare-feu

Gestion des logs

Composants Windows