TP1 : Protection des comptes utilisateurs

Objectifs :

L'objectif de ce TP est de vous introduire certains aspects de base de la sécurité d'un système d'exploitation Linux. Nous allons travailler sur la distribution **CentOS9**.

Nous allons nous intéresser aux aspects suivants :

- Sécurité locale – Gestions comptes utilisateurs ;
- Sécurité des mots de passe ;
- Désactivation des services inutiles

Déroulement du TP :

1. Sécurité locale – Gestion des comptes utilisateurs

Cette première partie décrit certaines tâches qu'un administrateur de système d'exploitation Linux doit effectuer pour approuver ou refuser l'accès au super-utilisateur (root).

1.1 Refus de l'accès à un compte utilisateur

1.1.1 Désactivation du shell d'un utilisateur

Pour empêcher les utilisateurs de se connecter directement en tant que super-utilisateur, les administrateurs système peuvent définir le shell du compte super-utilisateur sur /sbin/nologin dans le fichier /etc/passwd. Cela bloque tout accès au compte super-utilisateur par des commandes qui nécessitent un shell, telles que les commandes su et ssh. N'exécutez les tests qu'avec un compte d'utilisateur normal, pas le compte root. Sinon, votre machine sera bloquée.

- Créer un utilisateur normal (user1 par exemple) et affecter lui un mot de passe. Se loguer avec cet utilisateur.
- Sur un terminal, ouvrir le contenu du fichier «/etc/passwd », essayer de modifier la ligne du ficher concernant l'utilisateur que vous avez créé. Qu'est ce que vous remarquez ?
- Accéder au privilèges du root à l'aide de la commande « su ». Ouvrir le fichier « /etc/passwd » et changer au niveau de la ligne de l'utilisateur « user1 » que vous avez créé, « /bin/bash » par « /sbin/nologin ».

- Se déconnecter du compte root, puis réessayer à nouveau de se connecter (au compte user1) à l'aide de la commande « su ». Qu'est ce que vous constatez ?

1.1.2 Désactivation des connexions SSH super-utilisateur

Une autre mesure de sécurité pour les connexions de super-utilisateur consiste à interdire l'accès à distance par le compte root. Cela empêche l'envoi du mot de passe root sur le réseau.

Il est recommandé d'utiliser le protocole SSL au lieu de Telnet pour ce faire.

A l'aide de l'utilitaire « putty » essayer de vous connecter sur la machine linux à partir de votre machine, en utilisant le protocole SSH.

- Quel port utilise le protocole SSH ?
- Essayer de vous connecter à la machine Linux par le compte de l'utilisateur normal que vous avez créé auparavant, puis par le compte root. Commenter les résultats obtenus.
- Si votre connexion SSH à l'aide du compte root réussie, désactiver-la en suivant l'instruction suivante.
- Afin d'empêcher les connexions super-utilisateur par le biais du protocole SSH, éditer le fichier de configuration du démon SSH (/etc/ssh/sshd_config).

Modifier la ligne stipulant:

#PermitRootLogin yes

Par

PermitRootLogin no

- Tester à nouveau la connexion SSH à l'aide du compte root. Qu'est-ce que vous constatez ?

1.2 Restriction de l'accès root :

Plutôt que de refuser complètement l'accès au super-utilisateur, l'administrateur peut décider d'autoriser l'accès uniquement via des programmes setuid tels que su ou sudo.

La commande sudo :

- Connectez-vous en tant que votre utilisateur normal et redémarrer le service réseau. Quel résultat vous obtenez ?
- Maintenant, faites précéder votre commande par la commande « sudo ». Qu'est ce que vous constatez ? Quelle action devrions-nous faire avant l'utilisation de la commande « sudo » ?
- Vérifier que cette action a été bien reportée au super-utilisateur root.
- Au niveau du fichier /etc/sudoers, ajouter le nom de votre utilisateur et refaire à nouveau le test de tout à l'heure. Qu'est ce que vous constatez ?
- Faites d'autres tests en utilisant la commande « sudo »

2. Sécurité des mots de passe

- Editer le fichier /etc/passwd et analyser la ligne du root de celle de l'utilisateur que vous créé auparavant. Qu'est-ce que vous remarquez concernant le champ « password » ?
- Editer le fichier /etc/shadow et analyser la ligne du root et celle de l'utilisateur que vous avez créé auparavant, et expliquer les différents champs.
- Changer le mot de passe de votre utilisateur et vérifier l'application des changements au niveau du fichier /etc/shadow. Qu'est-ce que vous remarquez ?
- Changer d'autres paramètres de l'utilisateur et faites les vérifications nécessaires au niveau du fichier /etc/shadow.

2.1 Expiration des mots de passe

Pour l'utilisateur que vous avez créé tout à l'heure, spécifier une durée après laquelle il serait contraint de changer son mot de passe. Utiliser pour cela, dans du premier temps la commande :

#chage – M 90 <username>

- Vérifier au niveau du fichier /etc/shadow si ce changement était bien reporté ?
- Taper :
  - #sudo visudo
  - Ajouter la ligne
  - user1 ALL=(ALL) ALL

Quel message est donné par le système avertissant l'utilisateur que son mot de passe est expiré et qu'il doit changer son mot de passe pour pouvoir se connecter ?

2.2 Utilisation de l'utilitaire « John The Ripper »

a. Installer **« John The Ripper »** dans la machine Linux

b. Créer le fichier des mots de passe.

- Nous allons utiliser l'utilitaire « unshadow » de John pour obtenir le format traditionnel d'un fichier de password sous linux :

  # **unshadow** /etc/passwd /etc/shadow > passwds.txt

- Enfin, on exécute John the Ripper pour essayer de retrouver les mots de passe des utilisateurs ciblés, à l'aide de la commande suivante :

  # **john** passwds.txt

- Si vous souhaitez imprimer tous les mots de passe que John a réussi à déchiffrer, vous pouvez exécuter :

  #**john** - - show passwds.txt

3. Désactivation des services inutiles

3.1 **Vérification des services réseaux actifs**

- Identifier Liste des ports TCP/UDP ouverts

    - ss -tuln
- Rechercher la correspondance port/service dans le fichier « /etc/services ».
- Quels sont les ports ouverts sur votre machine et ils correspondent à quels services.

3.2 Vérification des services démarrés

- Afficher la liste des services configurés sur le système :
    - # systemctl list-units --type=service

3.3 Arrêt des services inutiles

- Désactivation du lancement du service au redémarrage du système

  # sudo systemctl disable <service>

- Arrêt du service immédiatement

  # sudo systemctl stop <service>