Université FERHAT ABBAS SETIF I
Faculté des sciences
Département d'informatique
Sécurité des Applications Web
1ère année Master GL, IDTW

TP n°2

Objectif

L'objectif de ce TP est :

- d'apprendre à utiliser l'outil de virtualisation VirtualBox ainsi que la machine virtuelle Kali Linux.
- d'étudier et de manipuler les droits d'accès aux fichiers sur un système Linux.
- de s'initier à l'administration des utilisateurs et des groupes sous linux et à l'attribution de privilèges aux utilisateurs.

Travail à réaliser

1. Se connecter en tant que l'utilisateur **kali** ayant pour mot de passe **kali** (il faut taper **kqli** en cas d'utilisation d'un clavier AZERTY).
2. Si le clavier utilisé est en AZERTY :
    a. aller dans les paramètres système et choisir un clavier français AZERTY.
    b. Éditer le fichier **/etc/default/keyboard** et changer le modèle de clavier et la langue

    XKBMODEL="pc102"
    XKBLAYOUT ="fr"
3. Ouvrir un terminal.
4. Quel est le répertoire courant (répertoire de travail) ?
5. Créer un fichier ***test*** dans le répertoire d'accueil.
6. Quels sont les droits d'accès sur ce nouveau fichier ?
7. Qui est le propriétaire du fichier ? Quel est le groupe d'utilisateurs auquel appartient le fichier ?
8. Donner tous les droits d'accès sur ce fichier au propriétaire du fichier, le droit de lecture et d'exécution au groupe d'utilisateurs du fichier, et le droit d'exécution seulement pour les autres.
9. Enlever le droit de lecture au groupe d'utilisateurs du fichier.
10. Donner le droit de lecture à tous les utilisateurs.
11. Créer un répertoire ***dossier*** dans votre répertoire courant. Créer deux nouveaux fichiers ***test1*** et ***test2*** dans le répertoire ***dossier***.

12. Enlever les droits de lecture sur le répertoire ***dossier*** à tous les utilisateurs.

13. Que signifie le droit de lecture pour un répertoire ?

14. Enlever les droits d'exécution sur le répertoire **dossier** au propriétaire du répertoire.

15. Que signifie le droit d'exécution sur un répertoire ?

16. Donner tous les droits à tous les utilisateurs sur le répertoire ***dossier*** et tout son contenu (***test1*** et ***test2***).

17. Enlever le droit d'exécution sur **test1** à tous les utilisateurs, et sur **test2,** au groupe et aux autres. Donner le droit **X** au **groupe** sur dossier et tout son contenu. Pourquoi le droit d'exécution est attribué au groupe sur **test2** et pas sur **test1**.

18. Quels sont les droits d'accès attribués par défaut à la création d'un fichier ?

19. Comment sont définis les droits d'accès par défaut ?

20. Modifier le masque pour la session en cours à 0027.

21. Créer un répertoire ***dossier2*** et un fichier ***test4*** dans le répertoire d'accueil. Quelle différence remarque-t-on entre les droits d'accès par défaut qui leurs sont attribués ?

22. Créer un utilisateur **saw1** ayant pour mot de passe **saw1** et un utilisateur saw2 ayant pour mot de passe **saw2**.

23. Créer le groupe **master**.

24. Affecter au groupe **master** les utilisateurs **saw1** et **saw2**.

25. Changer le groupe du fichier **test** et l'affecter au groupe **master**. Changer le propriétaire du fichier **test** et l'affecter à l'utilisateur **saw1**.

26. Ouvrir une session dans le terminal en tant que l'utilisateur **saw1**.

27. Exécuter la commande **newgrp master**. Créer un fichier **test2**. Quelle est la particularité de ce fichier par rapport à ceux déjà créés.

28. Fermer la session de l'utilisateur **saw1**.

29. Qu'affiche la commande **groups** ? Qu'affiche la commande **groups saw1** ? Qu'affiche la commande **groups saw2** ?

30. Analyser le contenu du fichier **/etc/passwd**. Que contient-il (utiliser la commande **man 5 passwd** pour connaître la signification de chaque champ du fichier) ?

31. Analyser le contenu du fichier **/etc/shadow**. Que contient-il de plus que le fichier **/etc/passwd** (utiliser la commande **man shadow** pour connaître la signification de chaque champ du fichier) ?

32. Analyser le contenu du fichier **/etc/group**. Que contient-il (Utiliser la commande **man group** pour connaître la signification de chaque champ du fichier) ?

33. Ouvrir le fichier **/etc/sudoers** en exécutant la commande **visudo**. (Pour sauvegarder le fichier modifié, appuyer sur CTRL+X puis sur SHIFT+O). **SI LE FICHIER MODIFIE CONTIENT UNE ERREUR, IL NE FAUT SURTOUT PAS LE SAUVEGARDER ET REVENIR A LA VERSION PRECEDENTE !!! SI UNE ERREUR EST SIGNALEE APPUYER SUR E ou X.**

34. Remplacer la ligne **Defaults env_reset** par **Defaults env_reset, timestamp_timeout = 0** Que remarque-t-on de changer dans l'utilisation de **sudo** ?

35. Autoriser l'utilisateur **saw2** à créer et supprimer des utilisateurs (commande **adduser** et **deluser** droits de l'utilisateur **root**). Vérifier que cela fonctionne.

36. Autoriser le groupe master, à démarrer, arrêter et redémarrer les services **apache2**. Vérifier que cela fonctionne.

37. Autoriser le groupe **master** à redémarrer la machine (commande **reboot** avec les droits de l'utilisateur **root**). Vérifier que cela fonctionne.

38. A quel groupe doit appartenir un utilisateur pour avoir automatiquement tous les droits d'administration ?

39. Effacer toutes les modifications apportées précédemment au fichier **/etc/sudoers**.

40. Supprimer les utilisateurs **saw1, saw2** et le groupe **master**. Supprimer les répertoire home de **saw1** et **saw2**.

41. Consulter le contenu du fichier **/var/log/auth.log** (ne prendre en compte que les dernières lignes commençant par la date du jour). Quelles sont toutes les informations journalisées suites à l'exécution d'une commande avec **sudo**.

Utiliser le manuel utilisateur Linux (commande man) pour connaitre le fonctionnement des commandes utilisées (touch, ls, chmod, mkdir, umask, sudo, adduser, addgroup, chown, chgrp, newgrp, su).