Labos OS

Labo 1 :

Notes :

Tout fichier qui commence par un **point** est un fichier caché (sur Linux).

History affiche l'historique des commandes entrées. Flèches pour parcourir.

Sudo = « laisse-moi faire en tant que super user »

Su - = super user

Useradd crée user

Attention à utiliser *-m* pour bien créer l'user !!!
-c « xxx » = ajouter une chaine de caractère

Louis -> root -> usermod -G sudo -a e190230

Rapport:

Creation des groupes (*groupadd student* | *groupadd whitehat*)
Création des users (*useradd -m -g student -c « Fabrice Bodson » e190230*)

Créer mot de passe user (*passwd e190230*)
Modifier shell (*usermod -s /bin/bash e190230*)

Creation compte hacker (*useradd -m -G student,whitehat -c "hacker" hacker*)
Créer mot de passe user (*passwd hacker*)
Modifier shell (*usermod -s /bin/bash hacker*)

Ajout de e190230 aux groups sudo et whitehat (*usermod -G sudo -a e190230*
usermod -G whitehat -a e190230)

Groupes:

1. fabrice (mdp comme machine labo) → (1) fabrice, (2) sudo
2. e190230 (mdp helmo) → (1) student, (2) sudo, whitehat
3. hacker (mdp hacker) → (1) hacker, (2) whitehat

Labo 2 :

Notes :

Lorsque commande *history* exécutée, je peux taper *!X* où X est le numéro de la commande que je souhaite réexécuter.

Rapport:

Labo 3 :

Notes :

Rapport:

Créer groupe : « set-localgroup ***** »
Créer user : « set-localuser ** »
Trouver les groupes : « get-localgroup ».

Ajouter user dans groupe : *"add-localgroupmember -Group "student" -Member "e190230""*.

Compte admin : mdp HELMo.
Compte e190230 : mdp HELMo.

Labo 4 :

Notes :

Changer groupe (root) : *usermod -g student fabrice*
Changer dans le *home* : *chgrp -R student ./fabrice*
Log out

Après les commandes « cd / » et « ls -lLd * » :

Les fichiers appartiennent à « root »
Les utilsateurs ne peuvent pas écrire des sous répertoires.

« /root » = seul l'user root a tous les accès, les autres n'ont aucun droit dessus.
« /lost+found » = idem
« /tmp » = tout le monde a tous les droits dessus.

J'ai tous les droits sur mon répertoire personnel.
C'est accessible pour hacker en lecture et exécution car ils sont du même groupe mais il peut seulement lire et lister les fichiers, il ne peut pas en créer.
Louis y a accès car les utilisateurs ont le droit de lire et exécuter.

chown [-R] nv-user fichiers → change propriétaire
chown [-R] nv-user fichiers → change groupe propétaire
chown [-R] nv-user :nv-groupe fichiers → change les 2
Le -R permet d'agir sur l'ensemble des sous-répertoires.

Binaire ----- Droit ----- Octal
000 ---------- (---) -------- 0
001 ---------- (--x) -------- 1
010 ---------- (-w-) -------- 2
011 ---------- (-wx) -------- 3
100 ---------- (r--) -------- 4
101 ---------- (r-x) -------- 5
110 ---------- (rw-) -------- 6
111 ---------- (rwx) -------- 7

les 3 manières :
« *e190230@kaliVM:/home$ chmod o+rwx e190230 »*
"*e190230@kaliVM:/home$ chmod 750 e190230*"
"e190230@kaliVM:/home$ chmod u=rwx,g=r-x,o= e190230"

Ou être en root plutôt que « e190230@kaliVM ».

Sudo su – hacker
Chmod 750 hacker

-rw-r--r-- 1 root root 3336 Oct 14 13:57 passwd
-rw-r----- 1 root shadow 1968 Oct 7 11:23 shadow

Impossible d'écrire dedans sauf pour root, mais impossible pour tout le monde d'exécuter.
Shadow est nommé ainsi car seul root et ceux du groupe shadow peuvent lire le contenu. Tout autre utilisateur ne peut rien faire dedans.

Non, à partir du compte hacker, il est impossible de faire quoique ce soit avec le répertoire shadow.

Impossible de copier le dossier shadow mais possible pour passwd.
Impossible de copier le passwd.bak à la place de passwd.

Pour m'accorder le droit de copie, je me donne l'accès complet (777).

La copie est possible pour hacker car il a reçu tous les droits sur le répertoire /home/temp. Il peut donc y écrire ce qu'il veut. Il a également les droits de lecture sur *hosts* et sur *passwd* donc il lui suffit de lire leur contenu et d'aller réécrire ça dans /home/temp.

Umask applique via **XOR** un masque.
Le masque de e190230 est **0022**.
Le droit d'accès par défaut pour un fichier où ce masque est appliqué est **rw-r—r—** (644).
Le droit d'accès par défaut pour un dossier où ce masque est appliqué est **rwxr-xr-x** (755).

Rapport:

Labo 5 :

Notes :

Création des users, groupes et répertoires via interface graphique.

Rapport:

Labo 6 :

1. Les fichiers cachés → (*ls -la*)
2. Depuis /home/fabrice :
    a. ./Network/labo2/TP2-telnet-ssh.pcap → (*find -type f*)
    b. ./Network → (*find -type d*)
    c. ./.config/xfce4/desktop/icons.screen.latest.rc (*find -type l*)
    d.
    e.
    f.
    g.

3. Type de chemin :
    a. A
    b. P
    c. A
    d. R
    e. R
    f. P

4. La commande *cd* – déplace dans le répertoire précédent.
5. Cd ~/Desktop puis cd ~ puis cd -.
6. Ls /usr/local /usr/share
7. Les données sont stockées dans les blocs de données réservés aux répertoires.
8. Convertir en octal :
    a. 664
    b. 775
    c. 002
    d. 744
    e. 440

9. Submask :
    a. 777 – 113 = 664 | 666 – 002 = 664
    b. 777 – 002 = 775 (dès qu'il y a un x activé, c'est un répertoire)
    c. 777 - 775 = 002 | 666 – 664 = 002
    d. 777 – 033 = 744
    e. 777 – 337 = 440 | 666 – 226 = 440

10. UID super user = 0
11.