
Sécurité des Réseaux - TP3

Contrôle d'Accès

Monroe Samuel

30 décembre 2015

1 Préambule

Ce tp est réalisé avec CentOS Security virtualisé de l'EPHEC avec VMWare.

2 Contrôle d'accès aux fichiers Unix

2.1 Utilisation du contrôle d'accès

2.1.1 Création des users et groupes

La création des utilisateurs se fait via la commande **adduser nom_du_user**

La création des groupes se fait via la commande **groupadd nom_du_groupe**

La commande **usermod** permet d'ajouter un utilisateur existant à un groupe, ici utilisée de la manière suivante : **usermod -a -G grp1 userX**

2.1.2 /etc/group

Le fichier contient des entrées du type : **kek :x :502 :user1,user2**

Ces entrées ont donc les champs suivants :

- Le nom du groupe
- Un mot de passe, souvent non utilisé et laissé blank (x)
- Le GID, group id
- La liste des users appartenant à ce groupe

2.1.3 Différences entre /etc/passwd, /etc/shadow

La fichier **passwd** associe à chaque entrée, qui correspond un user, le nom complet du User et le chemin absolu vers son **home** terminé par son compte shell.

Le fichier **shadow** quant à lui, contient :

- Le nom du user
- Le mot de passe codé
- Des nombres de jours à propos des modifications de mots de passes (update, validité, expiration,)

2.1.4 Accès au répertoire

Le répertoire de userX a tout les droits au niveau user et groupe, les autres ont le droit à X et R mais pas en écriture.

Un test avec userZ, appartenant au groupe 2, n'est pas possible étant donné que le répertoire Home ne propose des droits qu'au propriétaire !

2.1.5 Cascade des droits

Afin de propager les droits, le bits SGID doit être positionné afin que les fichiers et répertoires suivants héritent de ces mêmes droits.

chmod 2xxxx dir

2.1.6 Suppression des fichiers personnels

Ceci est effectué en positionnant le sticky bit, de sorte qu'un user ne puisse supprimer que les fichiers qui lui appartiennent dans ce répertoire.

chmod 1xxx dir

2.1.7 Droits d'accès fichiers spéciaux

- /dev/sda : brw-rw—
- /dev/tty : crw-rw-rw
- /dev/lp : crw-rw—

2.1.8 Droits défaut dans home

Les droits par défaut sont RWX pour le propriétaire uniquement.