TP - ASR5 système d'exploitation

Un peu de système

9 avril 2018

Pour ce TP, nous avons créé plusieurs machines virtuelles sur lesquelles vous allez vous connecter. Votre charger de TP vous indiquera l'adresse de celle que vous devez utiliser. Ces machine sont connues par leur adresse IP, dans le sujet, celle-ci est nomée `IP_VM`. Ces machines sont reliées à l'anuaire de l'université, pour vous connecter vous allez donc utiliser votre login de l'université et votre mot de passe. Dans la suite du TP, votre login sera noté `UTILISATEUR`.

Contrairement à ce qui était anoncé, il n'y aura plus de TP noté. cette séance et la suivante portera sur l'utilisation du sytème linux. Mais prenez des notes, lors du dernier contrôle, certaines questions porteront sur l'utilisation des commandes vues aujourd'hui.

I Gestion des utilisateur

Connectez-vous sur la machine fournie. Vous devez être administrateur pour faire cette exercice. Si vous n'êtes pas parvenu à le faire via les commandes du TP précédant, ne vous inquiétez pas, nous avons modifié la configuration générale.

Q.I.1) - Créez un utilisateur dont le login est `votreprenom.votrenom` via la commande `adduser`. Pouvez-vous directement utiliser la commande `adduser` ? Et via `sudo` ?

Q.I.2) - Regardez les fichiers de configuration `/etc/sudoers` et `/etc/sudoers.d/*`. Qu'est-ce qui vous permet d'utiliser la commande sudo ?

Q.I.3) - Que signifie au niveau du système la création d'un utilisateur ? Regardez dans les fichiers `/etc/group`, `/etc/passwd`, `/etc/shadow`. Quelles lignes correspondent à l'utilisateur que vous avez créé.

Q.I.4) - Ajoutez l'utilisateur au groupe admin (`usermod -aG admin LOGINUSER`). Qu'est-ce que cela change ?

Q.I.5) - **Attention ne faite pas cet exercice sur votre propre ordinateur** Votre chargé.ée de TP va interdire la lecture du fichier `/etc/passwd`. Que se passe-t-il ? Essayez de changer l'utilisateur courant vers celui que vous avez créé :

5(a) - Cela fonctionne-t-il en utilisant la commande `sudo su - VOTREPREONOM.VOTRENOM` ?

5(b) - Cela fonctionne-t-il en utilisant la commande `su - VOTREPREONOM.VOTRENOM` ?

I.1 Si vous êtes en avance

Q.I.6) - La manipulation précédente ne change pas le fonctionnement de votre compte universitaire. Où la machine va-t-elle chercher les informations correspondant à ce compte ? Regardez dans le fichier `/etc/nsswich.conf`.

Q.I.7) - Que signifie l'empreinte du mot de passe stockée dans `/etc/shadow` ? Le mot de passe stocké ressemble à cela :
`$6$3N1ccgt8$jJy4k4p7SmAMUhvK1J0bSqIIq3HI7JBxkCZ5xbv/X4Gq4fdR/F4L/EWercjmfYRKXoc4zuRbKFJE3OTM4H0`
Il se décompose en 3 morceau (séparé par des $). Que signifie ces morceaux (voir le manuel de `crypt(3)`.

Q.I.8) - Grâce à la commande `mkpasswd` pouvez-vous regénérer l'empreinte ?

II Utilisation des logs

Les fichiers de logs du système sont dans le répertoire `/var/log`. Aujourd'hui nous allons nous intéresser au fichier `/var/log/auth.log`

Q.II.1) - Qui a le droit de le lire d'y écrire et pourquoi ?

Q.II.2) - Que contient-il ?

Q.II.3) - Grâce à la la commande `grep` retrouvez les ligne correspondant à chaque fois où la commande `sudo` a été utilisée. Affichez les lignes mentionnant préciséement la commande qui a été exécutée.

Q.II.4) - Grâce à la commande `sed` retrouvez dans le résultat précédent chaque utilisateur et chaque commande utilisée sous la forme de 2 colonne "UTILISATEUR COMMANDE" [1].

Q.II.5) - Grâce aux commandes `sort` et `uniq` triez par utilisateur et commande identiques puis compter le nombre d'ocurence de chaque commande.

III Informations sur les processus

Copiez le fichier `code1.c` sur la machine virtuelle. Ils se compilent avec la commande
`gcc -g -Wall -O0 code1.c -o code1.exx`

Dans un `screen`, lancez le programme `./code1.exx`, retrouvez son `pid` et explorez le répertoire `/proc/PID/`.

Q.III.1) - Que contiennent les fichiers `cmdline`, `environ`, `loginuid`, `cwd`, `maps`

Q.III.2) - Regardez le contenu du répertoire `fd`, que contient-il ?

Q.III.3) - Comment retrouver les processus qui utilisent un fichier présent dans le répertoire `/home/` ?

Q.III.4) - Regardez le contenu du fichier `maps`. Que signifient les lignes de ce fichier ?

1. Pensez au expréssion régulières de sed : sed −e `'s/sudo:(.*)/\1/'` remplace chaque ligne contenant `sudo: truc` par `truc`