Compléments sur les capacités Linux

1. Préambule

L'objectif de ce TP est de d'approfondir la compréhension des capacités Linux.

2. Prérequis

Une machine virtuelle au format VirtualBox est utilisée pour ce TP :

- SES_TP2_Debian : système Debian 9 utilisé lors des TP 2 et 3 (pour mémoire, le compte utilisateur est *tp* et les mots de passes sont également *tp*), en fonction de ce qui a été fait au TP2, il peut être préférable de repartir d'un état zéro (snapshot ou redéploiement de la machine virtuelle) ;

3. Capacités Linux

Exercice 3-1

Objectif : manipuler les capacités dans un programme écrit en C

La VM à utiliser pour cet exercice est la VM Debian. Afin de pouvoir compiler le programme use_cap.c, il est nécessaire d'installer le paquet libcap-dev_2.25-1_amd64 :

```
sudo apt-get install libcap-dev
```

ou, à partir de l'archive fournie

```
sudo dpkg -i libcap-dev_2.25-1_amd64.deb
```

Lors de la génération du binaire, il ne faut pas oublier de lier la bibliothèque libcap.

```
gcc -o use_cap -lcap use_cap.c
```

Exécuter le binaire généré et analyser la trace d'exécution. Les étapes (a) à (e) sont-elles réussies ? Expliquer le résultat renvoyé pour chacune des étapes.

Il est possible d'analyser les capacités détenues par le processus à différentes étapes de son

exécution. Plusieurs méthodes simples existent, en voici au moins 2 qui ne nécessite pas l'utilisation d'un *debugger*.

La première méthode consiste à insérer des lignes de code `getchar() ;` pour interrompre le déroulement du processus et identifier les capacités du processus sur la base de son PID.

```
/sbin/getpcaps PID
```

ou

```
grep ^Cap /proc/PID/status
```

La deuxième méthode consiste à insérer la ligne de code suivante :

```
printf("Capacités détenues %s\n\n", cap_to_text(cap_get_proc(), NULL));
```

Que faut-il faire pour que seule l'étape (c) réussisse ?

_____
_____

Que faut-il faire pour que les étapes (a) et (c) réussissent ?

_____
_____

Lorsque vous regénérer le binaire, que se passe-t-il pour les capacités qui ont été attribuées avec la commande setcap ? Ce résultat peut-il se produire dans d'autres situations ?

_____
_____
_____
_____