TP AppArmor : shell confiné

L'objectif de ce TP est d'observer comment on peut confiner un programme setuid root à l'aide de AppArmor.

Consignes

Les lignes commençant par '#' désignent des commandes à lancer en root.

Installation de AppArmor

_____

Sous Debian et Ubuntu

Documentation : `https://wiki.debian.org/AppArmor/HowTo`

AppArmor est déjà installé et activé. Il peut être nécessaire d'installer les outils d'administration complémentaires :

```
# apt install apparmor-utils auditd
```

Compilation du shell setuid root

Le but de ce TP est de mettre en évidence les capacités de restriction d'accès aux appels système de AppArmor, en particulier sur les processus exécutés par root. Pour cela, nous allons utiliser un programme qui lance un shell sous l'utilisateur root.

Note : on ne peut pas directement utiliser une copie de bash sur laquelle on positionnerait le bit setuid car bash détecte ces cas d'exécution et restaure l'uid d'origine de l'utilisateur.

```
% gcc -o shell shell.c
% sudo chown root shell
% sudo chmod u+s shell
```

Nous disposons ainsi d'un programme qui lance un processus bash en utilisateur root directement. Vous pouvez le vérifier en exécutant le programme en simple utilisateur, puis en utilisant le programme "id".

```
% ./shell
# id
uid=0(root) gid=0(root) groups=0(root)
```

Confinement avec AppArmor

Partez du squelette fourni dans le dossier du tp, "apparmor.shell".

Observez le contenu du fichier et expliquez chaque ligne présente, afin de vous familiariser avec la syntaxe de AppArmor.

➤ *Essayez d'expliquer les différentes lignes du fichier.*

Chargez le profil avec la commande suivante :

```
# apparmor_parser -a apparmor.shell
```

Ensuite si vous modifiez le profil, vous pourrez le recharger avec :

```
# apparmor_parser -r apparmor.shell
```

Enfin vous pouvez supprimer le profil avec :

```
# apparmor_parser -R apparmor.shell
```

Testez des manipulations réservées au compte root, et mettez en évidence les restrictions imposées par AppArmor.

Vous pouvez vérifier ce qui a été bloqué par AppArmor avec la commande suivante :

```
# grep AVC /var/log/audit/audit.log
```

Le mot-clé AVC est spécifique aux logs des modules de sécurité AppArmor et SELinux.

Pour finir, faites des tests en retirant des lignes du profil de confinement. Après avoir rechargé le profil, est-ce que le programme shell se lance encore ? Est-ce qu'il permet encore d'obtenir le compte root ?

D'après vous, est-ce qu'on pourrait utiliser ce mécanisme pour disposer d'un shell dans lequel on peut exécuter des programmes malveillants ?
