TP SELinux : confinement du service mini-httpd

L'objectif est de se familiariser avec le fonctionnement de SELinux. Il est difficile de bien comprendre l'ensemble du fonctionnement dans le cadre d'un TP, mais il est possible de se faire une idée de l'apport en termes de sécurité, ainsi que de la difficulté de configuration.

Consignes

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

Dans ce TP, nous allons étudier l'apport de SELinux pour le confinement d'un programme de type service réseau. Nous allons créer un profil de configuration pour le serveur HTTP mini-httpd.

Installation de SELinux

Debian

Référence : `https://wiki.debian.org/SELinux`

Tout comme AppArmor, SELinux est compilé dans le noyau de Debian, mais il est désactivé par défaut en faveur de AppArmor.

On commence par installer les packages nécessaires au fonctionnement :

```
# aptitude -R install selinux-basics selinux-policy-default auditd \
    selinux-policy-dev newrole
```

Ensuite Debian fournit une commande pour configurer le système pour SELinux :

```
# selinux-activate
```

Vérifier le contenu du fichier /etc/default/grub, surtout si vous passez de AppArmor à SELinux :

```
--------
...
GRUB_CMDLINE_LINUX=" security=selinux"
...
--------
```

Ensuite vous devez redémarrer, le boot suivant sera long car SELinux doit configurer les contextes de sécurité de tous les fichiers existants. Après redémarrage, vous avez plusieurs commandes pour vérifier l'activation de SELinux :

```
# sestatus
# mount |grep selinuxfs
# id -a
# ps axZ
# check-selinux-installation
```

La dernière est spécifique à Debian.

Ubuntu

A priori, l'activation de SELinux se fait de la même façon que pour Debian.

Création d'une configuration pour mini-httpd

Téléchargez les fichiers de démarrage `mini_httpd.fc` et `mini_httpd.te`, et placez-les dans un dossier de travail (par exemple nommé selinux-mini_httpd).

Création de la configuration

Placez-vous dans le dossier de travail, et compilez le module de configuration avec cette commande :

```
# make -f /usr/share/selinux/devel/Makefile
```

Si tout se passe bien, ceci produit un fichier mini_httpd.pp. Vous pouvez le charger dans la configuration SELinux globale ainsi :

```
# semodule -i mini_httpd.pp
```

Ensuite vous pouvez vérifier la liste des modules de configuration chargés :

```
# semodule -l
```

Enfin, avant de commencer à travailler sur l'ajout de règles, vous devez configurer le contexte de sécurité de mini-httpd (redéfini dans le fichier mini_httpd.fc) :

```
# sudo restorecon -R /usr/sbin/mini_httpd /var/log/mini_httpd.log /var/www/wwwroot
```

Ensuite vous devez démarrer le serveur mini-httpd et interagir avec. Pour démarrer mini-httpd dans le contexte d'un service système, on va utiliser systemd.

Démarrage avec systemd

Il existe déjà un service mini-httpd défini dans systemd, mais on va en modifier la ligne de commande :

```
# systemctl edit mini-httpd
```

Il faut ajouter les lignes suivantes :

```
[Service]
ExecStart=
ExecStart=/usr/sbin/mini_httpd -u root -d /var/www/wwwroot -c 'index.sh' -l /var/log/
    mini_httpd.log
ExecStop=
ExecStop=pkill mini_httpd
```

Ensuite vous utilisez systemctl pour démarrer ou arrêter le service mini-httpd.

Démarrage manuel

On peut également lancer la commande depuis un terminal, mais il faut attribuer le contexte de sécurité explicitement :

```
# runcon system_u:system_r:mini_httpd_t <ligne de commande de mini-httpd>
```

Analyse des logs

Les logs produits par SELinux sont, comme pour AppArmor, dans /var/log/audit/audit.log. Vous pouvez les consulter avec cette commande :

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

Ensuite, SELinux fournit une commande pour créer des règles de politiques à partir des logs :

```
# audit2allow -al
```

N'hésitez pas à vous référer à la page de man pour la signification des options.

Contrairement au cas de AppArmor, ici nous n'allons pas tenter de créer une configuration de façon manuelle, nous allons nous baser sur la génération automatique.

Adaptation pour les scripts CGI

Comme pour le TP AppArmor, nous allons maintenant tenter d'exécuter des scripts CGI avec mini-httpd, et adapter le module de configuration SELinux en conséquence.

Une fois que le module de politique est terminé, on peut passer la configuration en mode "enforcing". Attention ! Ce réglage est global pour SELinux, tout le système sera en mode "enforcing".

Passage en mode enforcing :

```
# setenforce 1
```

Retour en mode permissif :

```
# setenforce 0
```

Notez qu'il est possible de configurer un type SELinux en mode permissif, en laissant le réglage global en enforcing :

```
# semanage permissive -a mini_httpd_t
```

L'objectif est d'autoriser l'exécution du script CGI tout en interdisant qu'il affiche des fichiers en dehors de la racine du site web.

Conclusion

Pensez-vous qu'on obtient un niveau de confinement équivalent à celui fournit par AppArmor ? Lequel des 2 mécanismes est le plus simple à configurer ?
