Master 2 SeCReTS

TP SELinux

Première partie
Généralités

1 Objectif du TP

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.

2 Consignes

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

On suppose que le binaire thttpd est installé en `/chroot-thttpd/usr/bin/thttpd`, si ce n'est pas le bon chemin, adaptez-le en fonction de votre installation. Pensez à modifier ce chemin dans le fichier `thttpd.fc`.

Dans ce TP nous travaillerons sur la machine virtuelle `client1`.

3 Installation de SELinux

Tout comme AppArmor, SELinux est compilé dans le noyau d'ubuntu bionic mais il est désactivé par défaut.

On commence par installer les packages nécessaires s'ils ne sont pas déjà présents :

```
# apt install selinux-basics selinux-policy-default auditd selinux-policy-dev
```

Si vous n'avez pas accès à internet, les packages correspondant sont disponible sur une iso dans le répertoire tp-selinux/deb :

```
# dpkg -i selinux*.deb auditd*.deb
```

Ensuite Ubuntu 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=" selinux=1 security=selinux"
...
--------
```

Si besoin, modifiez le fichier de configuration puis regénérer le menu de boot grub.cfg (commande update-grub). Vous pouvez également éditez manuellement le fichier /boot/grub/menu.cfg en ajoutant les options à la ligne correspondant au chargement du noyau.

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

```
# sestatus
# mount |grep selinuxfs
# id -a
# ps axZ
# ls -laZ
# (check-selinux-installation)
```

Deuxième partie

Création d'une configuration pour thttpd

1 chroot

Avant toutes choses, mettez en place tous les fichiers que vous aurez besoin afin de lancer thttpd dans un chroot. Vous construirez l'arborescence nécessaire dans le répertoire `/chroot-thttpd`.

Aidez-vous des commandes `ldd` et `strace` et validez que vous arrivez à éxécuter le cgi linux.sh ainsi qu'a lire n'importe quel fichier présent dans l'arborescence du chroot.

La ligne de commande permettant de démarrer thttpd dans un chroot est la suivante :

```
# chroot  /chroot-thttpd/ /usr/bin/thttpd -dd /var/wwwroot/
    -nor -p 80  -u root -c '**.sh' -l - -D
```

2 selinux

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

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

```
# make -f /usr/share/doc/selinux-policy-dev/examples/Makefile
```

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

```
# semodule -i thttpd.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 thttpd (redéfini dans le fichier thttpd.fc) :

```
# restorecon -R /chroot-thttpd
```

Ensuite vous devez démarrer le serveur thttpd et interagir avec. 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.

3 Utilisation de macros

Il est possible de factoriser la plupart des règles SELinux en utilisant des macros.

Télécharger la politique de reférence sur le github de Tresys. Si vous n'avez pas accès à internet, une cope se trouve dans le répertoire tp-selinux de l'iso du tp.

Prenez exemple des fichiers `refpolicy-master/policy/support/*`, en particulier `file_patterns.spt` et `obj_perm_sets.spt`.

Simplifier votre fichier de politique thttpd.te en utilisant ces macros.

4 Adaptation pour les scripts CGI

Comme pour le TP AppArmor, nous allons maintenant tenter d'exécuter des scripts CGI avec thttpd, 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
```

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 (appelée wwwroot dans le tp sur chroot).