TP AppArmor : confinement du service mini-httpd

L'objectif de ce TP est d'observer comment on peut confiner un programme à l'aide de AppArmor, et de comparer à d'autres mécanismes avec des objectifs similaires, en particulier chroot.

Consignes

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

Nous allons travailler avec le programme mini-httpd qui est packagé pour Debian, à installer si ce n'est pas encore fait.

Installation de mini-httpd

Installez mini-httpd, et arrêtez le service s'il est démarré automatiquement. Nous allons ensuite le démarrer manuellement.

```
# apt install mini-httpd
# systemctl status mini-httpd
# systemctl stop mini-httpd
# systemctl disable mini-httpd
```

Nous allons aussi utiliser un script spécifique à faire exécuter comme service par mini-httpd. Récupérez et extrayez l'archive wwwroot.tgz.

```
# tar xzf wwwroot.tgz -C /var/www
```

Installation de AppArmor

Sous Ubuntu et Debian

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

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

Passez à la partie suivante.

Confinement du serveur mini-httpd

Vérifiez que le programme mini-httpd est bien installé et fonctionnel.

```
# mini_httpd
# ps aux |grep httpd
# pgrep httpd
```

Vérifiez que le serveur Web est utilisable avec un navigateur comme Firefox, en pointant sur l'URL `http://127.0.0.1/`.

Et enfin, arrêtez-le :

```
# pkill mini_httpd
```

La ligne de commande à utiliser par la suite pour lancer le serveur mini-httpd sera la suivante (pensez à adapter le nom du répertoire) :

```
# /usr/sbin/mini_httpd -u root -d /var/www/wwwroot -c 'index.sh' -l /var/log/mini_httpd.log
```

Créez dans votre répertoire utilisateur un nouveau fichier nommé usr.sbin.mini_httpd (c'est la façon standard de nommer un fichier contenant un profil AppArmor).

Mettez le contenu suivant dans ce fichier :

```
# Profil AppArmor pour le service mini-httpd

/usr/sbin/mini_httpd flags=(complain) {

}
```

Chargez ce profil AppArmor (vide) dans le système avec la commande suivante :

```
# apparmor_parser -a usr.sbin.mini_httpd
```

Le profil est chargé en mode ”complain” (toutes les actions sont autorisées et enregistrées). Vous pouvez le vérifier avec la commande aa-status.

Relancez le serveur mini-httpd. Avec la commande suivante, vous allez afficher la liste des log consécutifs au lancement du serveur mini-httpd :

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

Le fichier audit.log est en fait le journal du daemon auditd, il enregistre tous les événements relatifs à la sécurité niveau noyau.

A partir d’ici, l’objectif est de compléter le profil AppArmor du serveur mini-httpd jusqu’à ce qu’il soit complet, et qu’on puisse le placer en mode ”enforce”. Vous devez donc ajouter des actions autorisées dans le fichier usr.sbin.mini_httpd. Le langage à utiliser est décrit sur la page suivante : `https://gitlab.com/apparmor/apparmor/-/wikis/QuickProfileLanguage`

Par exemple, vous pouvez ajouter cette ligne pour l’accès au bibliothèques dynamiques :

```
/usr/lib{,64}/**/lib*.so* mr,
```

———

Vous pouvez vous inspirer des autres profils présents dans le dossier /etc/apparmor.d.

Quand vous ajoutez des lignes au profil, vous devez le recharger avec cette commande :

```
# apparmor_parser -r usr.sbin.mini_httpd
```

On utilise ici l’option `--replace` pour indiquer que l’on souhaite remplacer un profil déjà chargé.

Laissez un terminal ouvert avec la commande suivante :

```
# tail -f /var/log/audit/audit.log
```

Lorsque vous lancez mini-httpd, de nouvelles lignes vont apparaître dans ce terminal. Une fois que vous aurez un profil complet, plus aucune ligne ne devrait apparaître.

Enfin, lorsque vous avez terminé d’écrire le profil pour AppArmor, vous pouvez le supprimer avec :

```
# apparmor_parser -R usr.sbin.mini_httpd
```

Génération automatique de profil

Un outil fournit par AppArmor vous permet de générer automatiquement un profil pour une nouvelle application. Voici la commande à lancer :

```
# aa-genprof /usr/sbin/mini_httpd
```

Ensuite vous devrez démarrer le serveur mini-httpd, interagir avec, et enfin l’arrêter. Puis vous devez presser la touche ’s’ pour demander que aa-genprof scanne les journaux d’événements à la recherche des logs de AppArmor. Enfin pour chaque ligne trouvée, on vous demande si vous souhaitez ajouter la modification au profil.

Le profil généré est automatiquement chargé, et le fichier correspondant est `/etc/apparmor.d/usr.sbin.mini_httpd`. Regardez le contenu de ce fichier. Est-ce qu’il correspond à ce que vous avez défini manuellement ? Pensez-vous qu’il est préférable d’avoir une génération automatique ou manuelle ?

Faites le ménage en retirant les profils générés de façon automatique :

```
# pkill mini_httpd
# aa-remove-unknown
# apparmor_parser -R /etc/apparmor.d/usr.sbin.mini_httpd
```

Adaptation au lancement de scripts CGI

———————————

Pour la suite, rechargez le profil AppArmor que vous avez écrit, ou demandez-moi un profil complet à charger.

Relancez le service mini-httpd si ce n’est pas le cas, et utilisez le script index.sh au travers du serveur Web. Pour que le script soit fonctionnel, vous allez devoir compléter le profil AppArmor.

Essayez de lire des fichiers réservés à root comme `/etc/shadow`. Ces attaques sont-elles bloquées par AppArmor ?

Comparaison avec *chroot*

Maintenant, nous allons comparer la protection AppArmor avec la protection offerte par chroot. Commencez par décharger le profil AppArmor pour mini-httpd.

Ensuite, vous allez démarrer mini-httpd avec l'option `-r`.

```
# /usr/sbin/mini_httpd -r -u root -d /var/www -dd wwwroot -c 'index.sh' -l /var/log/
    mini_httpd.log
```

Si vous utilisez le script index.sh au travers du serveur Web, vous devriez constater qu'il n'est plus fonctionnel. Pouvez-vous expliquer pourquoi ?

Essayer de faire en sorte que le script index.sh fonctionne dans le dossier utilisé pour le chroot (votre dossier courant).

Tentez à nouveau d'accéder à des fichiers lisibles uniquement par root au travers du serveur Web, et normalement cela devrait être bloqué.

Conclusion

_____

Dans ce TP, on a mis en évidence les possibilités de confinement offertes par AppArmor. Pouvez-vous comparer avec chroot ?
