TP4 : Apparmor

Réalisé par Axel BROQUAIRE, B3 - Cybersécurité

Les consignes :

3.1 Installation du systèmes d'exploitations :

Installation d'une VM ubuntu 22.04, sans interface graphique.

```
sudo apt update

sudo apt upgrade -y
```

3.2 Sécurisation de l'administration du serveur :

1. Le serveur sera administré via SSH, aussi vous devrez renforcer la configuration de ce serveur conformément aux recommandations de l'ANSSI 2. L'administrateur système, devra être le seul à pouvoir établir une session distante SSH via son compte utilisateur et une biclef sécurisée.

```
[axel@TP3-Secu-SE ~]$ sudo grep -vE '^\s*#|^\s*$' /etc/ssh/sshd_config
Include /etc/ssh/sshd_config.d/*.conf
StrictModes yes
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com
PermitEmptyPasswords no
MaxAuthTries 3
LoginGraceTime 30
PermitRootLogin no
PrintLastLog yes
AllowUsers axel
PermitUserEnvironment no
AllowTcpForwarding no
X11Forwarding no
PasswordAuthentication no
Port 2222
AuthorizedKeysFile .ssh/authorized_keys
Subsystem sftp /usr/libexec/openssh/sftp-server
```

Explication :

1. StrictModes yes

Active les vérifications strictes des permissions des fichiers et répertoires utilisés par SSH. Cela empêche l'utilisation de clés ou fichiers de configuration avec des permissions trop permissives, réduisant ainsi le risque d'attaques.

2. Ciphers aes256-ctr,aes192-ctr,aes128-ctr

Restreint les algorithmes de chiffrement aux versions AES en mode CTR considérées comme sécurisées et efficaces.

3. MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com

Limite les MAC (Message Authentication Codes) aux versions SHA-2 avec Encrypt-Then-MAC (ETM) garantissant une meilleure intégrité et résistance aux attaques.

4. PermitEmptyPasswords no

Interdit les connexions SSH avec un mot de passe vide, empêchant une grave faille de sécurité.

5. MaxAuthTries 3

Réduit le nombre de tentatives de connexion à 3 avant qu'une session ne soit coupée. Cela limite les attaques par bruteforce.

6. LoginGraceTime 30

Fixe un temps limite de 30 secondes pour s'authentifier. Si l'utilisateur ne s'authentifie pas à temps, la connexion est fermée. Cela réduit la surface d'attaque.

7. PermitRootLogin no

Désactive la connexion SSH directe avec l'utilisateur root. Cela empêche les attaques bruteforce sur le compte administrateur et force l'utilisation d'un compte utilisateur avec élévation de privilèges (`sudo`).

8. PrintLastLog yes

Affiche la date et l'heure de la dernière connexion réussie, permettant à l'utilisateur de détecter une éventuelle intrusion.

9. AllowUsers axel

Restreint les connexions SSH à l'utilisateur axel uniquement, empêchant tout autre utilisateur de tenter une connexion.

10. PermitUserEnvironment no

Empêche l'utilisateur de modifier l'environnement SSH (`~/.ssh/environment`). Cela évite des attaques où un attaquant pourrait injecter des variables nuisibles.

11. AllowTcpForwarding no

Désactive le **TCP forwarding**, empêchant SSH d'être utilisé comme proxy ou tunnel pour rediriger du trafic réseau non autorisé.

12. X11Forwarding no

Désactive le transfert X11, évitant ainsi que des applications graphiques soient exécutées à distance via SSH, ce qui pourrait représenter un risque de sécurité.

13. PasswordAuthentication no

Désactive l'authentification par mot de passe, obligeant l'utilisation de clés SSH. Cela protège contre les attaques par bruteforce sur les mots de passe.

14. Port 2222

Change le port SSH de 22 à 2222, réduisant ainsi les attaques automatisées cherchant à se connecter sur le port standard.

2. Les flux réseaux entrants et sortant du serveur devront être strictement filtrés, et seul le trafic utile devra être autorisé.

```
[axel@TP3-Secu-SE ~]$ sudo firewall-cmd --list-all
public (active)
  target: DROP
  icmp-block-inversion: no
  interfaces: enp0s3 enp0s8
  sources:
  services:
  ports: 2222/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

3.3 Installation d'un serveur Web

1. Dans un premier temps, installer un serveur web apache avec sa configuration par défaut.

Installation :

```
sudo apt install apache2
```

Lancement :

```
sudo systemctl enable apache2
sudo systemctl start apache2
```

2. Installer ensuite Apparmor si celui si n'est pas présent par défaut sur la machine.

```
axel@TP4-Secu-SE:~$ sudo apt install apparmor apparmor-utils
```

3. Apparmor dispose de différent mode, quels sont il ? Est a quoi sert chaque mode ?

Il existe 2 modes :

- Complain qui fait que les violations de la politique sont enregistrés et écrits dans les logs mais aucune action n'est bloquée
- Enforce qui bloque les opérations qui violent la politique de sécurité

4. Que se passe t'il si un profiles Apparmor est configurer en mode « enforce » et qu'il ne convient pas parfaitement au binaire associé ?

L'éxécution sera bloquée et l'erreur loggée. Le programme risque de mal fonctionner ou ne pas fonctionner du tout.

3.4 Configuration d'un profil Apparmor

1. Créer un profile squelette Apparmor pour le binaire « ls » et rédigez une procédure.

D'abord retirer ls de ce fichier de conf

```
sudo vim /etc/apparmor/logprof.conf
```

Puis :

```
sudo aa-genprof /bin/ls
```

2. Qu'elle commande permet de vérifier le fonctionnement d'un profile Apparmor ?

```
sudo aa-status
```

3. En utilisant cette commande sur votre profile squelette que constaté vous ?

Je constate que le profil pour ls est passé par défaut en enforce.

4. Modifier le profile créer précédemment pour qu'il soit adapté a l'utilisation normal du binaire « ls ».

```
axel@TP4-Secu-SE:~$ sudo cat /etc/apparmor.d/usr.bin.ls
# Last Modified: Wed Apr  9 23:56:35 2025
abi <abi/3.0>,

include <tunables/global>

/usr/bin/ls {
  include <abstractions/base>
  include <abstractions/opencl-pocl>

  capability dac_override,
  capability dac_read_search,

  /home/ r,
  /usr/bin/ls mr,
  owner /home/*/ r,

}
```

5. Vérifier de nouveau sont utilisation en mode « complain », remarquer vous de nouveau des limitation ?

Tout fonctionne correctement !

3.5 Durcissement de la configuration d'Apparmor

Je vais donc suivre les recommandations du CIS, plus particulièrement la partie 1.3.1 Configure Apparmor.

1.3.1.1 Ensure AppArmor is installed

```
axel@TP4-Secu-SE:~$ dpkg-query -s apparmor &>/dev/null && echo "apparmor is installed"
apparmor is installed
```

Apparmor est bien installé.

1.3.1.2 Ensure AppArmor is enabled in the bootloader configuration

```
axel@TP4-Secu-SE:~$ grep "^\s*linux" /boot/grub/grub.cfg | grep -v "apparmor=1"
    linux /boot/vmlinuz-6.8.0-57-generic
root=UUID=e2f8d7a2-94d7-4c01-b24a-d8ecefe7c78c ro  quiet splash $vt_handoff
        linux /boot/vmlinuz-6.8.0-57-generic
root=UUID=e2f8d7a2-94d7-4c01-b24a-d8ecefe7c78c ro  quiet splash $vt_handoff
        linux /boot/vmlinuz-6.8.0-57-generic
root=UUID=e2f8d7a2-94d7-4c01-b24a-d8ecefe7c78c ro recovery nomodeset dis_ucode_ldr
        linux /boot/vmlinuz-6.8.0-40-generic
root=UUID=e2f8d7a2-94d7-4c01-b24a-d8ecefe7c78c ro  quiet splash $vt_handoff
        linux /boot/vmlinuz-6.8.0-40-generic
root=UUID=e2f8d7a2-94d7-4c01-b24a-d8ecefe7c78c ro recovery nomodeset dis_ucode_ldr
    linux16 /boot/memtest86+.bin console=ttyS0,115200n8
```

Remédiation : Modification de `/etc/default/grub` et ajout de "apparmor=1 security=apparmor" dans GRUB_CMDLINE_LINUX

Mise à jour :

```
axel@TP4-Secu-SE:~$ sudo update-grub
```

Vérification :

```
axel@TP4-Secu-SE:~$ grep "^\s*linux" /boot/grub/grub.cfg | grep -v "apparmor=1"
    linux16 /boot/memtest86+.bin console=ttyS0,115200n8
```

C'est mieux !

1.3.1.3 Ensure all AppArmor Profiles are in enforce or complain mode

```
axel@TP4-Secu-SE:~$ sudo apparmor_status | grep profiles
52 profiles are loaded.
52 profiles are in enforce mode.
0 profiles are in complain mode.
0 profiles are in kill mode.
0 profiles are in unconfined mode.
5 processes have profiles defined.
```

Tous les profiles sont en mode enforce.

1.3.1.4 Ensure all AppArmor Profiles are enforcing

```
axel@TP4-Secu-SE:~$ sudo apparmor_status | grep profiles
52 profiles are loaded.
52 profiles are in enforce mode.
0 profiles are in complain mode.
0 profiles are in kill mode.
0 profiles are in unconfined mode.
5 processes have profiles defined.
```

Même chose qu'avant, tous les profiles sont en mode enforce.