

TP3 : SELinux

Réalisé par Axel BROQUAIRE, B3 - Cybersécurité

Les consignes :

3.1 Installation du systèmes d'exploitations :

Installation d'une VM rocky 9 minimal, sans interface graphique.

Mise à jour :

```
sudo dnf update -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. Puis Tentez d'y accéder via votre navigateur web.

```
sudo dnf install httpd -y
sudo systemctl start httpd
sudo systemctl enable httpd
sudo firewall-cmd --add-port=80/tcp --permanent
sudo firewall-cmd --reload
```

Preuve :

```

axel@Dell-G15:~$ curl http://10.1.1.13
<!doctype html>
<html>
  <head>
    <meta charset='utf-8'>
    <meta name='viewport' content='width=device-width, initial-scale=1'>
    <title>HTTP Server Test Page powered by: Rocky Linux</title>
    <style type="text/css">
      /**]
...
</pre>
</div>
<div data-bbox="75 256 483 269" data-label="Section-Header">
<h2>2. Installer ensuite SELinux si celui-ci n'est pas déjà présent sur la machine</h2>
</div>
<div data-bbox="62 285 380 439" data-label="Text">
<pre>
[axel@TP3-Secu-SE ~]$ sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:      /etc/selinux
Loaded policy name:           targeted
Current mode:                 permissive
Mode from config file:       permissive
Policy MLS status:           enabled
Policy deny_unknown status:   allowed
Memory protection checking:   actual (secure)
Max kernel policy version:    33
</pre>
</div>
<div data-bbox="75 457 547 470" data-label="Section-Header">
<h2>3. SELinux dispose de différents modes, quels sont-ils ? Est à quoi sert chaque mode ?</h2>
</div>
<div data-bbox="52 477 154 489" data-label="Text">
<p>Il existe 3 modes :</p>
</div>
<div data-bbox="75 495 952 551" data-label="List-Group">
<ul>
<li>• Enforcing qui est le mode actif par défaut, les règles de sécurité sont strictement définies dans la politique, en cas de non respect de ces dernières, les actions sont bloquées et loggées.</li>
<li>• Permissive qui est généralement utilisé pour du test ou debug, ce mode fonctionne comme <i>enforcing</i> mais les actions ne sont pas bloquées, seulement loggées.</li>
<li>• Disabled qui est lorsque SELinux est désactivé, les actions ne sont ni loggées ni bloquées.</li>
</ul>
</div>
<div data-bbox="75 558 778 571" data-label="Section-Header">
<h2>4. Que se passe-t-il si un profil Selinux est configuré en mode « enforce » et qu'il ne convient pas parfaitement au binaire associé ?</h2>
</div>
<div data-bbox="52 576 670 589" data-label="Text">
<p>L'exécution sera bloquée et l'erreur loggée. Le programme risque de mal fonctionner ou ne pas fonctionner du tout.</p>
</div>
<div data-bbox="52 603 304 619" data-label="Section-Header">
<h2>3.4 Modification d'un profil Selinux</h2>
</div>
<div data-bbox="75 629 460 642" data-label="Section-Header">
<h3>1. Quel est le contexte des différents fichiers du serveur web Apache ?</h3>
</div>
<div data-bbox="62 659 479 728" data-label="Text">
<pre>
[axel@TP3-Secu-SE ~]$ ls -d -Z /var/www/html
system_u:object_r:httpd_sys_content_t:s0 /var/www/html

[axel@TP3-Secu-SE ~]$ ls -d -Z /var/www/cgi-bin/
system_u:object_r:httpd_sys_script_exec_t:s0 /var/www/cgi-bin/
</pre>
</div>
<div data-bbox="52 746 423 759" data-label="Text">
<p>Contextes : httpd_sys_content_t &amp; httpd_sys_script_exec_t</p>
</div>
<div data-bbox="75 766 313 779" data-label="Section-Header">
<h3>2. Quel est le contexte du service Apache ?</h3>
</div>
<div data-bbox="62 795 487 879" data-label="Text">
<pre>
[axel@TP3-Secu-SE ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0      787 ?      00:00:00 httpd
system_u:system_r:httpd_t:s0      813 ?      00:00:00 httpd
system_u:system_r:httpd_t:s0      815 ?      00:00:01 httpd
system_u:system_r:httpd_t:s0      816 ?      00:00:01 httpd
system_u:system_r:httpd_t:s0      817 ?      00:00:01 httpd
</pre>
</div>
<div data-bbox="52 895 164 910" data-label="Text">
<p>Contexte : httpd_t</p>
</div>
<div data-bbox="75 916 518 930" data-label="Section-Header">
<h3>3. Activez le mode « enforce » sur le profil apache, le serveur web fonctionne-t-il ?</h3>
</div>
<div data-bbox="52 935 666 949" data-label="Text">
<p>Modification de <code>/etc/sysconfig/selinux</code> pour passer SELinux en enforcing de manière permanente, y ajouter :</p>
</div>
```

```
SELINUX=enforcing
```

Est-ce que le serveur web fonctionne toujours ?

```
axel@Dell-G15:~$ curl http://10.1.1.13
<!doctype html>
<html>
  <head>
    <meta charset='utf-8'>
    <meta name='viewport' content='width=device-width, initial-scale=1'>
    <title>HTTP Server Test Page powered by: Rocky Linux</title>
    <style type="text/css">
      /*<![CDATA[*]

      html {
        height: 100%;
        width: 100%;
      ...
```

Oui, il fonctionne toujours.

4. Désactivez le mode « enforce » puis modifiez la configuration du serveur apache pour placer le path du serveur web dans /srv/srv/srv_1/. Redémarrer ensuite le service apache

Modification de /etc/sysconfig/selinux pour passer SELinux en permissive de manière permanente, y ajouter :

```
SELINUX=permissive
```

Modification de /etc/httpd/conf/httpd.conf pour changer le path du serveur web :

```
[axel@TP3-Secu-SE ~]$ cat /etc/httpd/conf/httpd.conf | grep /srv/srv/srv_1
DocumentRoot "/srv/srv/srv_1"
<Directory "/srv/srv/srv_1">
```

Est-ce que le serveur web fonctionne toujours ?


```
axel@Dell-G15:~$ curl http://10.1.1.13
<!doctype html>
<html>
  <head>
    <meta charset='utf-8'>
    <meta name='viewport' content='width=device-width, initial-scale=1'>
    <title>HTTP Server Test Page powered by: Rocky Linux</title>
    <style type="text/css">
      /*<![CDATA[*]

      html {
        height: 100%;
        width: 100%;
      ...
```

Oui, il fonctionne toujours.

5. Activez de nouveau le mode « enforce » sur le profil Apache. Le serveur web est-il de nouveau accessible ? Pourquoi ?

```
[axel@TP3-Secu-SE ~]$ sudo cat /var/log/httpd/error_log | tail -n 1
[Tue Apr 08 22:59:44.643801 2025] [core:error] [pid 817:tid 926] (13)Permission denied: [client 10.1.1.1:40306] AH00035: access to /
```



Le fichier n'est pas accessible car il est dans un contexte différent je suppose.

```
[axel@TP3-Secu-SE ~]$ ls -ld -Z /srv/srv/srv_1/index.html
unconfined_u:object_r:var_t:s0 /srv/srv/srv_1/index.html
```

6. Ajuster le profil SELinux avec « sealert » pour correspondre à la nouvelle configuration du service Apache. Expliquez brièvement l'utilité et la méthode d'utilisation de « sealert ».

La commande `sudo sealert -a /var/log/audit/audit.log` permet de lire beaucoup plus facilement les logs de SELinux et d'en conclure que :

```
SELinux is preventing /usr/sbin/httpd from getattr access on the file /srv/srv/srv_1/index.html.

**** Plugin catchall_labels (83.8 confidence) suggests ****

If you want to allow httpd to have getattr access on the index.html file
Then you need to change the label on /srv/srv/srv_1/index.html
```

On change le contexte du fichier avec ces commandes :

```
sudo semanage fcontext -a -t httpd_sys_content_t "/srv/srv/srv_1/index.html"

sudo restorecon -v /srv/srv/srv_1/index.html
```

7. Une fois le profil modifié et activé en mode enforce, le service Apache est-il accessible depuis le navigateur ?

Maintenant, ça fonctionne et donne notre `index.html` personnalisé :

```
axel@Dell-G15:~$ curl http://10.1.1.13
<h1>Test</h1>
```

3.5 Durcissement de la configuration de SELinux

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

1.3.1.1 Ensure SELinux is installed

```
[axel@TP3-Secu-SE ~]$ rpm -q libselinux
libselinux-3.6-1.el9.x86_64
```

SELinux installé

1.3.1.2 Ensure SELinux is not disabled in bootloader configuration

```
[axel@TP3-Secu-SE ~]$ sudo grubby --info=ALL | grep -Po '(selinux|enforcing)=0\b'
```

SELinux n'est pas désactivé dans la configuration du bootloader.

1.3.1.3 Ensure SELinux policy is configured

```
[axel@TP3-Secu-SE ~]$ sestatus | grep Loaded
Loaded policy name:          targeted
```

La policy est bien configurée.

1.3.1.4 Ensure the SELinux mode is not disabled

```
[axel@TP3-Secu-SE ~]$ getenforce
Enforcing
```

SELinux n'est pas désactivé.

1.3.1.5 Ensure the SELinux mode is enforcing

```
[axel@TP3-Secu-SE ~]$ getenforce
Enforcing
```

SELinux est bien en enforcing.

1.3.1.6 Ensure no unconfined services exist

```
[axel@TP3-Secu-SE ~]$ ps -eZ | grep unconfined_service_t
[axel@TP3-Secu-SE ~]$
```

Il n'y a pas de "unconfined services".

1.3.1.7 Ensure the MCS Translation Service (mcstrans) is not installed

```
[axel@TP3-Secu-SE ~]$ rpm -q mcstrans  
package mcstrans is not installed
```

Mcstrans n'est pas installé.

1.3.1.8 Ensure SETroubleshoot is not installed

```
[axel@TP3-Secu-SE ~]$ rpm -q setroubleshoot  
setroubleshoot-3.3.32-1.el9.x86_64
```

SETroubleshoot est installé mais il était nécessaire plus haut dans le TP.