HARDEN - Secure SHell

Hardening SSH

Fermer les portes et lâcher les chiens

Avoir une clé SSH, c'est bien. Mais si le serveur accepte encore les mots de passe, un bot chinois finira par trouver votre combinaison "admin/123456".

Nous allons appliquer trois couches de béton armé :

1. **Abolition du mot de passe :** On configure SSH pour ne faire confiance *qu'aux* clés cryptographiques. Plus de devinettes possibles.
2. **Mort au Root direct :** On interdit la connexion directe en root. Si un attaquant veut devenir dieu, il devra d'abord entrer en simple mortel (user), puis escalader ses privilèges (sudo). Ça nous laisse deux fois plus de logs à analyser.
3. **Défense Active (Fail2Ban & Firewall) :**
    - **UFW (Uncomplicated Firewall) :** On ferme tous les ports par défaut. On n'ouvre que le strict nécessaire.
    - **Fail2Ban :** Un script qui lit les logs en temps réel. Si une IP se trompe 3 fois de mot de passe (ou de clé), elle est bannie au niveau du pare-feu. C'est automatique et jouissif.

TD (Travaux Dirigés) : Le Bunker

Prérequis : Avoir réalisé le Module CONFIG (Vous avez une clé Ed25519 fonctionnelle et votre SSH écoute sur le port 2222).

Étape 1 : Modification de sshd_config

Connectez-vous à votre serveur. C'est la dernière fois que vous avez le droit à l'erreur.

```
sudo nano /etc/ssh/sshd_config
```

Cherchez et modifiez (ou ajoutez) ces lignes précises :

```
# Interdit de se loguer en root directement
PermitRootLogin no

# Interdit l'authentification par mot de passe
PasswordAuthentication no

# Sécurité supplémentaire (souvent par défaut, mais on vérifie)
ChallengeResponseAuthentication no
UsePAM yes
```

Note : On garde UsePAM yes pour que Fail2Ban puisse fonctionner correctement, mais l'auth par password est bloquée par la directive précédente.

Redémarrez SSH :

```
sudo systemctl restart ssh
```

***TEST CRITIQUE :** Ouvrez un autre terminal **sans fermer l'actuel**. Essayez de vous connecter. Si ça marche avec la clé : Bravo. Si ça demande un mot de passe : Vous avez raté. Si ça refuse tout : Vous avez coupé la branche sur laquelle vous étiez assis (utilisez votre session ouverte pour corriger).*

Étape 2 : Configuration du Firewall (UFW)

Sur Debian/Ubuntu, UFW est la référence standard.

1. On définit les règles par défaut (tout fermer en entrée)

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
```

2. On autorise NOTRE port SSH personnalisé (Port 2222 du Module 2)

ATTENTION : Si vous oubliez ça, vous êtes mort au prochain reboot.

```
sudo ufw allow 2222/tcp
```

3. On active le pare-feu

```
sudo ufw enable
```

Répondez "y" à la confirmation.

Étape 3 :Installation de Fail2Ban

On va installer le chien de garde.

```
sudo apt update && sudo apt install fail2ban -y
```

Par défaut, Fail2Ban protège le port 22. Comme nous sommes des pros (Module CONFIG), nous utilisons le port 2222. Il faut le dire à Fail2Ban. Créez un fichier de configuration locale (ne touchez jamais au .conf, créez un .local) :

```
sudo nano /etc/fail2ban/jail.d/sshd-custom.local
```

```
[sshd]
enabled = true
port = 2222
maxretry = 3
bantime = 3600
```

(Bantime 3600 = 1 heure de punition. Pour la prod, mettez 1 semaine).

Redémarrez le service :

```
sudo systemctl restart fail2ban
```