sshd : service ssh

1. Quelques options à modifier

Voici quelques options à modifier dans le fichier `/etc/ssh/ssh_config` afin de sécuriser les accès.

1.1 Interdire root au login

Le paramètre `PermitRootLogin` permet d'interdire l'accès à `root` au programme SSH. Cela permet d'éviter des attaques sur `root`.

Avant de modifier cette valeur, je conseille de faire un test de déconnexion avec votre *user* et de vérifier qui vous puissiez bien basculer sur le compte `root`. Pour passer la valeur à `no` :

```
PermitRootLogin No
```

1.2 Interdire les connexions avec mots de passe

Le paramètre `PasswordAuthentification` permet d'interdire la connexion avec mot de passe.

```
# Authentification par mot de passe interdit
PasswordAuthentification no
```

1.3 Modifier le port de sshd

Une des bonnes pratiques est de changer le port de connexion au service SSH, histoire de brouiller les pistes. N'oubliez pas de le noter précieusement.
Il faut éditer le fichier `/etc/ssh/ssh_config`.

```
Port 11822 # Mettre le numéro de port désiré
```

Une fois les modifications effectuées, il faut redémarrer le service SSH :

```
# sudo systemctl restart ssh
```

A partir de maintenant je vous conseille de vous déconnecter.

```
exit
```

Désormais, pour se **connecter en SSH** via un autre port que le 22 :

```
ssh -p 11822 chloe@cordon.acego.fr
```

Basculer sur le compte `root` :

```
sudo su
```