CONFIG - Secure SHell

Configuration SSH

Arrêter de suivre le troupeau

Jusqu'à présent, vous avez utilisé ssh-keygen sans réfléchir. C'est mignon, mais dangereux. Un administrateur système compétent contrôle chaque aspect de sa cryptographie.

Les paramètres vitaux de ssh-keygen

- **-t (Type) :** L'algorithme. Par défaut, c'est souvent RSA. C'est robuste, mais lent et les clés sont énormes.
    - *La recommandation moderne :* **Ed25519**. C'est de la cryptographie à courbe elliptique. C'est plus rapide, plus sécurisé, et la clé est minuscule.
- **-b (Bits) :** La taille de la clé.
    - *Pour RSA :* C'est crucial. Une clé de 2048 bits est le minimum syndical. Une clé de **4096** bits est recommandée pour résister au temps (et à la NSA, peut-être).
    - *Pour Ed25519 :* La taille est fixe. Pas besoin de spécifier -b.
- **-f (File) :** L'emplacement. Si vous gérez 50 serveurs, vous n'allez pas tout écraser dans id_rsa. Vous devez nommer vos clés (srv-bdd, srv-web, etc.).
- **-N (New Passphrase) :** Permet de définir la passphrase directement dans la commande. Utile pour les scripts, ou pour avoir l'air d'un pro qui n'a pas le temps d'attendre le prompt interactif.

La Sécurité par l'Obscurité : Changer le Port

Le port 22 est le port par défaut. 99% des attaques automatisées (bots) tapent sur le port 22. Changer ce port (ex: 2222) ne rend pas votre serveur "invulnérable", mais cela réduit le bruit dans vos logs de 90%. C'est de l'hygiène numérique.

TD (Travaux Dirigés) : Chirurgie de précision

Objectif : Créer une clé moderne dédiée et déplacer le service SSH.

Étape 1 : Génération "Mode Expert"

Oubliez RSA. Nous passons sur Ed25519. Nous allons tout faire en une seule ligne de commande.

Sur votre machine **locale** :

-t : Algo Ed25519

-f : On range ça proprement avec un nom explicite

-N : On met une passphrase solide immédiatement

```
ssh-keygen -t ed25519 -f ~/.ssh/lab-srv-01 -N "MaSuperPassPhrase123"
```

```
Generating public/private ed25519 key pair.
Your identification has been saved in /home/user/.ssh/lab-srv-01
Your public key has been saved in /home/user/.ssh/lab-srv-01.pub
The key fingerprint is:
SHA256:HdYilMem++pJj721UWceKuCW3GNb9vvVVvyfKniNaRg user@desktop
The key's randomart image is:
+--[ED25519 256]--+
|        .o       |
|       .. +.     |
|        .++ .    |
|        .+ o   . |
|        So.   ..=|
|        +E+  ..+=|
|        .*+=*+  *|
|       ..BoB*+..+|
|       .=.*oo..+=|
+----[SHA256]-----+
```

Notez que nous n'utilisons pas -b ici car Ed25519 a une taille fixe. Si vous étiez forcé d'utiliser RSA, la commande aurait été : ssh-keygen -t rsa -b 4096 …

Étape 2 : Déploiement de la nouvelle clé

Envoyez cette clé spécifique sur le serveur (qui écoute encore sur le port 22 pour l'instant).

L'option -i indique quelle clé publique envoyer

```
ssh-copy-id -i ~/.ssh/lab-srv-01.pub root@192.168.200.252
```

```
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/user/.ssh/lab-srv-01.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already
installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new
keys
root@192.168.200.252's password:  # <-- ENTRER LE PASSWORD de l'utilsateur distant (ici ROOT)

Number of key(s) added: 1

Now try logging into the machine, with: "ssh -i /home/tuto/.ssh/srv-config 'root@192.168.200.252'"
and check to make sure that only the key(s) you wanted were added.
```

Étape 3 : Changement du Port (Côté Serveur)

Connectez-vous au serveur et éditez la configuration du démon SSH. **Attention :** Une erreur ici et vous vous enfermez dehors. Ne tremblez pas.

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

Cherchez la ligne #Port 22. Décommentez-la (enlevez le #) et changez la valeur.

```
Port 2222
```

Sauvegardez (Ctrl+O, Entrée, Ctrl+X).

Étape 4 : Redémarrage et Test

Redémarrez le service pour appliquer les changements.

```
sudo systemctl restart ssh
```

Sur RedHat/CentOS, c'est souvent 'sshd'

NE FERMEZ PAS VOTRE SESSION ACTUELLE ! Ouvrez un *nouveau* terminal local pour tester. Si ça rate, vous avez encore la session ouverte pour corriger.

Étape 5 : Mise à jour du client (~/.ssh/config)

Votre alias ne fonctionne plus car il tape sur le port 22. Mettez-le à jour.

```
nano ~/.ssh/config
```

```
Host srv-config
    HostName 192.168.1.50
    User user
    Port 2222
    IdentityFile ~/.ssh/srv-config
```

Tester

```
ssh srv-config
```