Procédure de durcissement et sécurisation des accès distants (SSH) sur Debian 13

Table des matières / Sommaire

1. Cahier des charges – Expression des besoins

Descriptif de l'existant

Le serveur Debian 13 est actuellement accessible via le protocole SSH sur son port par défaut (22). De plus, l'accès direct avec le compte "root" est autorisé. Cette configuration de base expose le serveur à des attaques par force brute automatisées provenant d'Internet.

Besoin(s)

L'objectif est de renforcer la sécurité des accès distants au serveur. Il est nécessaire de :

- Dissuader les scans automatiques en modifiant le port d'écoute.
- Restreindre les privilèges en interdisant la connexion directe au compte super-utilisateur (root).
- Garantir que seuls les administrateurs connaissant la configuration spécifique puissent tenter une connexion.

Contrainte(s)

Type	Description
Technique	Modification du service **sshd** sur Debian 13.
Sécurité	Application des bonnes pratiques de durcissement (Hardening).
Temps	Mise en place immédiate (moins de 30 minutes).

2. Ressources

Ressources mises à disposition

- **Serveur :** Une Machine Virtuelle (VM) sous **Debian 13** installée sur un hyperviseur.
- **Réseau :** Une connexion réseau fonctionnelle entre l'hôte et la VM.
- **Accès :** Un compte utilisateur standard avec les droits **sudo** ou l'accès au compte **root** pour la configuration initiale.

Ressources dont vous avez besoin pour la réalisation

- **Matériel d'administration :** d'un PC sous **Windows 11 Pro**.
- **Logiciels :** Un terminal (PowerShell/Putty sur Windows) pour tester la connexion distante.
- **Éditeur de texte :** L'outil **Nano** intégré à Debian pour modifier les fichiers de configuration.

Façon dont vous allez gérer ses ressources

L'administration se fait exclusivement en ligne de commande pour garantir la légèreté et la rapidité d'exécution. Les modifications sont effectuées directement dans les fichiers de configuration du système, suivies d'un redémarrage du service pour appliquer les nouveaux paramètres de sécurité.

3. Analyse

Descriptifs des solutions

La solution consiste à modifier la configuration du démon **SSHD** (Secure Shell Daemon). Le protocole SSH est l'outil standard pour l'administration à distance, mais sa configuration d'origine sur Debian 13 privilégie l'accessibilité au détriment de la sécurité maximale.

Comparaison des solutions

Méthode	Avantage	Inconvénient
Port 22 (Défaut)	Facile à retenir, pas de config client.	Cible prioritaire des bots et scans.
Port Personnalisé	Stoppe 99% des scans automatisés.	Nécessite de préciser le port à la connexion.
Authentification Root	Pratique pour l'admin direct.	Risque critique en cas de vol de mot de passe.

Choix d'une solution

Le choix du "Hardening" (durcissement) est retenu pour minimiser la surface d'attaque. Changer le port d'écoute et interdire le login root direct force un attaquant à d'abord trouver le bon port, puis à deviner un nom d'utilisateur standard avant de tenter une élévation de privilèges. C'est une stratégie de **défense en profondeur**.

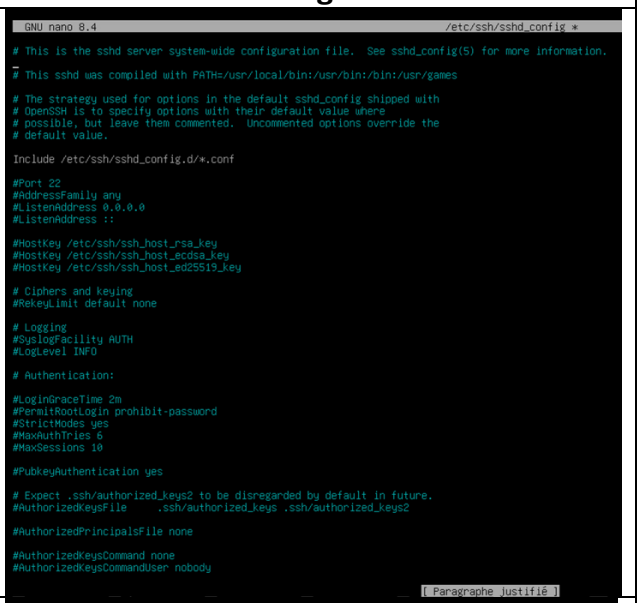
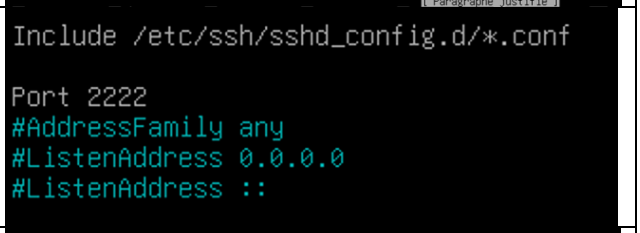
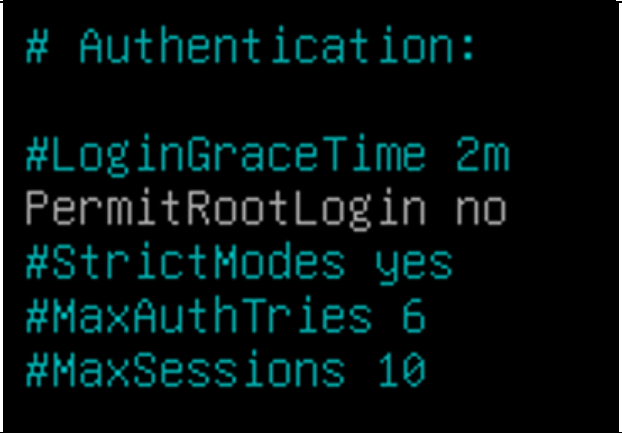
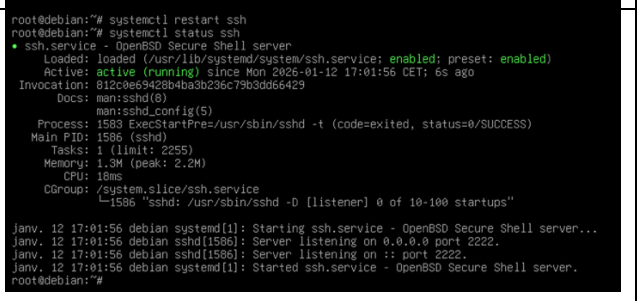
Plan d'adressage

- **IP du serveur :** IP du Serveur Debian (ex: 192.168.x.x).
- **Ancien Port :** 22 (TCP).
- **Nouveau Port :** 2222 (TCP).
- **Accès :** Interdiction stricte du compte root en SSH.

Etude de l'impact sur le SI existant

- **Sécurité :** Réduction drastique des logs de tentatives de connexion échouées (brute force).
- **Performance :** Aucun impact notable sur les ressources du serveur.
- **Ergonomie :** L'administrateur devra désormais utiliser la commande **ssh -p 2222 utilisateur@ip** depuis son terminal

4. Mise en place

Étape	Description	Images
1	**Accès à la configuration** : Ouverture du fichier de configuration du service avec l'éditeur Nano. **sudo nano /etc/ssh/sshd_config**	
2	**Changement du port** : Modification de la directive "Port" pour passer du port 22 par défaut à un port personnalisé (ex: 2222).	
3	**Interdiction du Root :** Modification de la ligne "**PermitRootLogin**" à "**no**" pour empêcher la connexion directe en super-utilisateur.	
4	**Redémarrage du service** : Sortie de l'éditeur (Ctrl+X) et application des nouveaux paramètres en relançant le démon SSH. **systemctl restart ssh**	

5	**Test de connectivité** : Vérification de l'accès au serveur en précisant le nouveau port depuis le client. **ssh -p 2222 utilisateur@ip_serveur**	

Rapport de tests

Test de sécurité	Commande testée	Résultat attendu	Résultat obtenu
Tentative port 22	ssh utilisateur@IP	Connexion refusée (Connection refused)	OK
Tentative port 2222	ssh -p 2222 utilisateur@IP	Demande de mot de passe / Accès autorisé	OK
Tentative Root 2222	ssh -p 2222 root@IP	Permission refusée (Permission denied)	OK

5. Bilan

Conclusion

La sécurisation du service SSH sur le serveur Debian 13 est une étape fondamentale dans le durcissement (hardening) du système d'information. En changeant le port d'écoute et en interdisant l'accès direct au compte "root", on élimine la quasi-totalité des attaques automatisées (scripts et bots). Cette procédure simple à mettre en œuvre augmente considérablement le niveau de sécurité global sans impacter les performances du serveur.

Auto-évaluation sur la qualité du travail réalisé

Le travail a été réalisé de manière efficace. Les tests de connexion ont validé que les nouvelles règles de sécurité sont bien appliquées (accès refusé sur le port 22 et en root, accès autorisé sur le port 2222 pour l'utilisateur standard).

Compétence SISR mobilisée	Description du travail réalisé
Gérer le patrimoine informatique	Maintenance et configuration sécurisée des accès distants aux serveurs de l'infrastructure.
Mettre en œuvre la sécurité du SI	Application des bonnes pratiques de sécurisation pour protéger les flux d'administration contre les intrusions.