Choses importantes à faire sur le système Debian

Synthèse de bonnes pratiques pour limiter l'exposition des services et renforcer l'accès SSH sur Debian.

Limiter l'accès aux services

Restreindre les services pour qu'ils ne soient accessibles que depuis un endroit bien spécifique peut se faire de plusieurs façons : au niveau du noyau avec un pare-feu, en configurant les services pour écouter uniquement sur une interface définie, ou en utilisant une autre méthode adaptée.

Certains services ne fournissent peut-être pas cette fonctionnalité. Dans ce cas, une solution comme le correctif vserver pour Linux peut, par exemple, forcer les processus à n'utiliser qu'une seule interface réseau.

Sécuriser l'accès SSH

Encourager tous les utilisateurs du système à utiliser SSH au lieu de TELNET. Mieux encore : désinstaller telnet et telnetd.

Il est également recommandé d'éviter de se connecter au système en SSH en tant que superutilisateur. Préférer des méthodes comme su ou sudo pour obtenir les privilèges nécessaires.

Enfin, le fichier **sshd_config**, situé dans **/etc/ssh**, devrait être ajusté afin d'accroître la sécurité.

Recommandations pour sshd_config

- Faire écouter SSH uniquement sur une interface donnée, surtout si la machine possède plusieurs interfaces réseau ou si une nouvelle carte réseau est ajoutée plus tard.
- Éviter autant que possible les connexions directes en tant que superutilisateur. Si quelqu'un veut devenir superutilisateur par SSH, deux étapes sont alors nécessaires, ce qui réduit les risques d'attaque par force brute sur le mot de passe root.
- Changer le port d'écoute, par exemple avec Port 666 ou ListenAddress 192.168.0.1:666. Attention : cela relève surtout de la sécurité par l'obscurité.
- Désactiver les mots de passe vides avec PermitEmptyPasswords no.
- Autoriser uniquement certains utilisateurs à accéder à la machine par SSH. La forme user@host permet aussi de limiter l'accès à un utilisateur donné depuis un hôte donné.

- Autoriser uniquement certains groupes avec AllowGroups. Les directives AllowUsers, DenyUsers et DenyGroups permettent de préciser encore plus finement les accès.
- Privilégier l'accès par clefs SSH placées dans ~/.ssh/authorized_keys lorsque c'est possible. Si c'est le fonctionnement souhaité, désactiver l'authentification par mot de passe.
- Désactiver toute méthode d'autorisation inutile, par exemple RhostsRSAAuthentication, HostbasedAuthentication, KerberosAuthentication ou RhostsAuthentication, même si certaines sont déjà désactivées par défaut.
- Désactiver le protocole SSH version 1, car il comporte des défauts de conception facilitant le piratage de mots de passe.
- Ajouter une bannière d'avertissement pour les utilisateurs qui se connectent au serveur SSH. Dans certains pays, ce type d'avertissement peut contribuer à la protection légale en cas d'accès non autorisé ou de suivi des utilisateurs.