tutoriel

Sécuriser votre Raspberry Pi

La sécurité de votre Raspberry Pi est importante. Les failles de sécurité laissent votre Raspberry Pi ouvert aux pirates qui peuvent ensuite l'utiliser sans votre permission.

Le niveau de sécurité dont vous avez besoin dépend de votre utilisation du Raspberry Pi. Par exemple, si vous utilisez votre Raspberry Pi sur votre réseau domestique, derrière un routeur avec un pare-feu, alors il est déjà assez sécurisé par défaut.

Mais si vous exposez votre Raspberry Pi directement à Internet, que ce soit avec une connexion directe ou en laissant certains protocoles (par exemple SSH) traverser le pare-feu de votre routeur, vous devrez renforcer la sécurité de base.

Même si vous êtes caché derrière un pare-feu, prenez la sécurité au sérieux.

Cette documentation décrit quelques moyens d'améliorer la sécurité de votre Raspberry Pi.

Pré-requis

Première étape : Changer votre mot de passe par défaut

Le nom d'utilisateur (**pi**) et le mot de passe (**raspberry**) par défaut sont utilisés pour tout Raspberry Pi exécutant le système d'exploitation Raspberry Pi. Donc, si vous avez accès à un Raspberry Pi et que ces paramètres n'ont pas été modifiés, vous avez un accès root à ce Raspberry Pi.

La première chose à faire est donc de changer le mot de passe. Cela peut être fait via l'application raspi-config :

```
pi@framboise:~ $ sudo raspi-config
```

Sélectionnez l'option 2 et suivez les instructions pour modifier le mot de passe.

Autres étapes

Faire en sorte que sudo nécessite un mot de passe : Placer sudo devant une commande l'exécute en tant que superutilisateur, et par défaut, cela n'a pas besoin d'un mot de passe.
Ce n'est généralement pas un problème.
Mais si votre raspberry Pi est ouvert à Internet, un attaquant pourra modifier ce qui nécessite des permissions de superutilisateur.
Pour forcer sudo à exiger un mot de passe, éditez avec les droits d'administration le fichier **/etc/sudoers.d/010_pi-nopasswd** et changez l'entrée pi en :

/etc/sudoers.d/010_pi-nopasswd

```
pi ALL=(ALL) PASSWD: ALL
```

Disposer des derniers correctifs de sécurité :

- Assurez-vous que votre version du système d'exploitation Raspberry Pi est à jour.
- Si vous utilisez SSH pour vous connecter à votre Raspberry Pi, il peut être intéressant d'ajouter une tâche cron qui met à jour le serveur ssh.
  La commande suivante, placée en tant que tâche cron quotidienne, vous assurera de disposer rapidement des derniers correctifs de sécurité SSH :

```
pi@framboise:~ $ sudo apt install openssh-server
```

3. **Installer Ufw sur Raspberry Pi : Installer un pare-feu**
4. **Installer fail2ban** Fail2ban : Bannir des IP

Conclusion

Problèmes connus

Voir aussi

- **(en)** https://www.raspberrypi.org/documentation/configuration/security.md

---

Basé sur « Securing your Raspberry Pi » par Raspberry Pi Foundation.