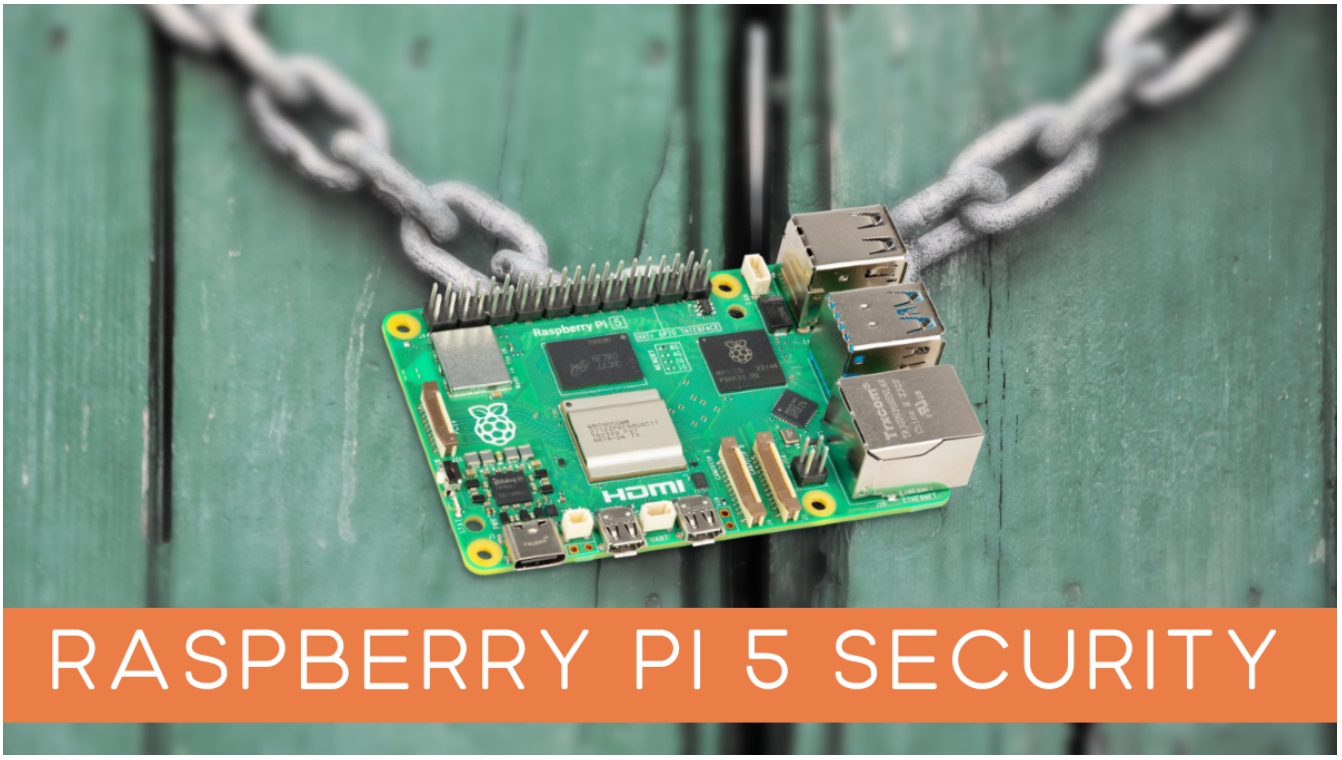
6 façons d'assurer la sécurité de votre Raspberry Pi 5

Par Adam | 20 octobre 2023



Que faire pour sécuriser votre Raspberry Pi 5 ? Dans cet article, je vais passer en revue quelques-uns des moyens les plus rapides et les plus efficaces pour garantir la sécurité de votre Raspberry Pi 5.

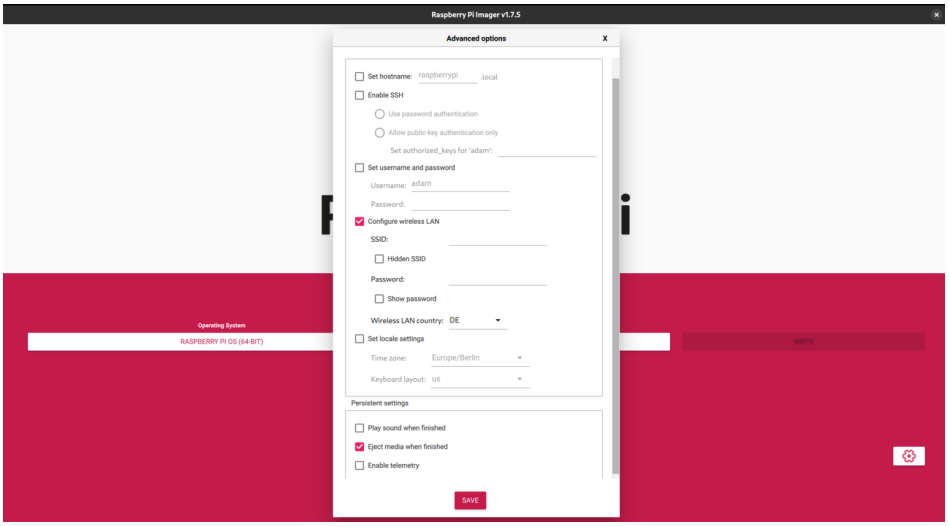
Avant (ou pendant) que vous installez votre Raspberry Pi 5, lisez d'abord cet article !

#1 : Mettre en place des mots de passe sécurisés, *sérieusement*

Pour de nombreuses personnes, la méthode standard d'installation du Raspberry Pi 5 commence par ceci : l'imageur Raspberry Pi.

Heureusement, au cours des dernières années, le Raspberry Pi Imager a vraiment évolué. Aujourd'hui, il est très facile de démarrer et de mettre en place rapidement des protocoles de sécurité sur votre Pi.

Donc, premièrement, si vous n'avez pas besoin d'une interface de communication, ne la mettez pas en place. Si vous prévoyez de configurer votre Raspberry Pi 5 pour quelque chose sans WiFi, alors ne configurez pas le WiFi. Si vous n'avez pas l'intention de vous connecter en SSH à votre Pi, ne le configurez pas.



Bien sûr, vous pouvez changer d'avis plus tard et activer ces interfaces après avoir déjà configuré votre Pi. Mais si vous comptez utiliser ces interfaces, vous devez utiliser des mots de passe forts.

Les mots de passe forts sont longs et comprennent des lettres minuscules et majuscules, des chiffres et des caractères spéciaux. Mais en réalité, les meilleurs mots de passe ressemblent davantage à *phrases de passe*.

Ne me croyez pas sur parole. Écoutez Edward Snowden :

Aujourd'hui, le Raspberry Pi Imager ne propose pas de nom d'utilisateur et de mot de passe par défaut. Historiquement, cependant, comme nous l'avons déjà écritLes noms d'utilisateur et les mots de passe par défaut sur les Raspberry Pis étaient les suivants :

nom d'utilisateur : pi

mot de passe : framboise

Par conséquent, de nombreux Raspberry Pis dans le monde ont encore ce nom d'utilisateur et ce mot de passe. Il s'agit d'une combinaison facile à retenir, mais qui n'est pas très sûre.

Les mots de passe doivent être utilisés avec discernement, car ils constituent souvent votre première ligne de défense. Bien entendu, les clés SSH sont encore plus efficaces que les mots de passe, mais nous y reviendrons plus tard.

#2 : Mise à jour && Mise à niveau

Une fois que votre nouveau Raspberry Pi OS a été flashé sur la carte SD, vous devez vous assurer que tout est conforme aux normes.

Ce que vous devez faire ici est tout simplement du style Debian classique.

Ouvrez le terminal et exécutez :

```
sudo apt update && sudo apt upgrade
```

Si vous êtes déjà un utilisateur de Debian, vous avez probablement l'habitude de lancer ce programme en permanence. Vous devez le faire avant d'installer un nouveau programme, avant de faire des changements, ou simplement tous les quelques jours.

Si vous n'êtes pas un utilisateur de Debian, cela peut sembler inutile, mais vous devriez absolument l'intégrer dans vos tâches informatiques quotidiennes. Si le logiciel de votre Pi est à jour, il est plus sûr.

#3 : Déterminer qui peut accéder à SSH

Comme je l'ai mentionné ci-dessus, si vous n'avez pas l'intention d'utiliser SSH sur votre Pi, vous pouvez simplement désactiver SSH en tant qu'interface. Cependant, si vous prévoyez d'utiliser SSH, vous devez vous assurer qu'il est aussi sécurisé que possible.

Il existe en fait plusieurs façons de s'assurer que votre SSH est sécurisé, je vais donc en présenter quelques-unes.

L'une d'entre elles consiste à limiter les utilisateurs qui peuvent accéder au Pi via SSH.

Pour ce faire, vous devez modifier votre fichier de configuration SSH Daemon. Vous allez donc dans le terminal et vous tapez :

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

Faites ensuite défiler la page jusqu'en bas et ajoutez `AllowUsers` suivi des noms d'utilisateur que vous souhaitez autoriser. Appuyez sur Ctrl-X et exécutez :

```
sudo service ssh restart
```

Vous avez maintenant un accès limité au SSH de votre Raspberry Pi.

#4 : Modifier le numéro de port SSH

Une autre façon de sécuriser votre SSH est de changer le numéro de port SSH.

Le numéro de port SSH par défaut est 22.

Devinez qui le sait ? Tous ceux qui cherchent des ports SSH ouverts.

La solution classique de l'administrateur système consiste donc à modifier ce numéro. Sur votre Raspberry Pi, tout ce que vous avez à faire est d'aller dans le terminal et de changer à nouveau le fichier de configuration du SSH Daemon.

Alors, courez :

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

Vous devez faire défiler l'écran vers le bas et modifier la ligne qui indique `#Port 22` à quelque chose comme `Port 2222`. Vous devrez également supprimer le # au début de la ligne.

Je dois préciser que vous pouvez également choisir un autre numéro si vous le souhaitez. Le 2222 est un changement typique.

Mais ensuite, une fois de plus, vous devez redémarrer SSH (n'oubliez pas cette étape !):

```
sudo service ssh restart
```

Maintenant, lorsque vous voulez vous connecter en SSH à votre Raspberry Pi, vous devez ajouter `-p 2222` à la commande SSH dans le terminal.

Mais c'est tout pour le SSH. Passons maintenant à d'autres protections de base.

#5 : Installer Fail2Ban

Fail2Ban est un merveilleux logiciel qui bloque les adresses IP lorsqu'elles tentent de se connecter trop souvent. Il met automatiquement à jour le pare-feu du Raspberry Pi pour bloquer les adresses IP potentiellement malveillantes.

Il est donc très utile pour sécuriser votre Raspberry Pi. Il est également très léger, puisqu'il ne pèse qu'environ 3 000 Ko.

Après avoir utilisé des mots de passe forts, configuré votre interface SSH et mis à jour votre Raspberry Pi, je vous recommande d'installer Fail2Ban.

Vous devez à nouveau mettre à jour :

```
sudo apt update && sudo apt upgrade
```

Et puis courir :

```
sudo apt install fail2ban
```

Fail2Ban peut faire beaucoup de choses et je n'entrerai pas dans les détails ici. Si cela vous intéresse, vous pouvez consulter les fichiers de configuration en vous rendant à l'adresse suivante `/etc/fail2ban`.

La configuration par défaut prévoit 5 tentatives infructueuses avant d'interdire l'adresse IP, puis l'adresse IP est interdite pendant 10 minutes.

C'est un excellent petit programme pour se protéger contre quelqu'un qui essaye de forcer votre mot de passe. Maintenant que vous avez configuré cela, il vous reste une dernière chose à faire avec votre Raspberry Pi 5.

#6 : Sauvegardez vos données, *sérieusement*

Cette étape est tout aussi importante que l'utilisation de bons mots de passe et, malheureusement, tout aussi souvent ignorée.

Votre carte SD peut tomber en panne et je ne suis pas le seul à en avoir fait l'expérience.

L'une de mes amies gardait beaucoup de choses importantes sur sa carte SD et celle-ci lui a fait lamentablement défaut.

Ne faites pas comme Anna. Sauvegardez vos données !

Par ailleurs, si vous souhaitez en savoir plus sur les cartes SD, sur celles que vous devriez acheter et sur les raisons de leur défaillance, consultez les articles suivants :

- Vitesse de la carte Micro SD du Raspberry Pi 5
- Classification des cartes SD
- Comment fonctionne la mémoire flash ?
- Qu'est-ce qu'une carte SD ?
- Tout sur la santé des cartes SD sur le Raspberry Pi

Procurez-vous une clé USB sympa, utilisez Google Drive, utilisez Dropbox. Ok, n'utilisez pas les deux derniers si vous vous souciez vraiment de la sécurité, mais vous voyez ce que je veux dire !

Vous devez conserver vos données en toute sécurité et les sauvegarder. Faites-moi confiance.

Conclusion

Voilà, vous l'avez compris. Ce sont les 6 choses que vous devez faire immédiatement avec votre Raspberry Pi 5 afin de le sécuriser.

Bien sûr, ces conseils ne couvrent que les bases. Mais une fois que vous les avez faits, vous avez au moins assuré un mur de sécurité minimal pour votre Pi 5.

Avez-vous d'autres moyens de garder votre Pi en sécurité ? Faites-le nous savoir dans les commentaires !

← Projet Paragon : Terminal portable Linux Projet Paragon : Blackberry Pi Cyberdeck →

1 commentaire

Chris sur novembre 9, 2023 à 5:40 pm

Quelle est la meilleure façon de sauvegarder la carte SD, autre que de l'enlever pour la copier ? Garder le Pi en ligne.

Réponse

Laissez un commentaire

Commentaire

Nom (obligatoire)

Email (ne sera pas publié) (obligatoire)

Site Web

Enregistrer mon nom, mon e-mail et mon site dans le navigateur pour mon prochain commentaire.

Envoyer le commentaire

Consultez nos autres articles !

Maîtriser l'électricité avec un oscilloscope Raspberry Pi Pico

Par Adam | 27 novembre 2023

Tout sur le Raspberry Pi en 10 minutes

Par Adam | 25 novembre 2023