





Priv-quoi?



Gère les actions attribués aux utilisateurs (lecture, écriture, exécution)

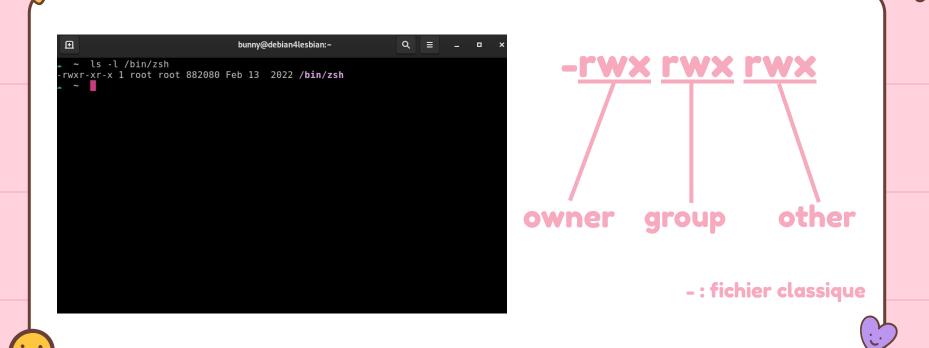
C'est quoi une privesc?

C'est un mécanisme permettant à un utilisateur d'obtenir des droits supérieurs à ceux qu'il a.

Pour faire quoi?

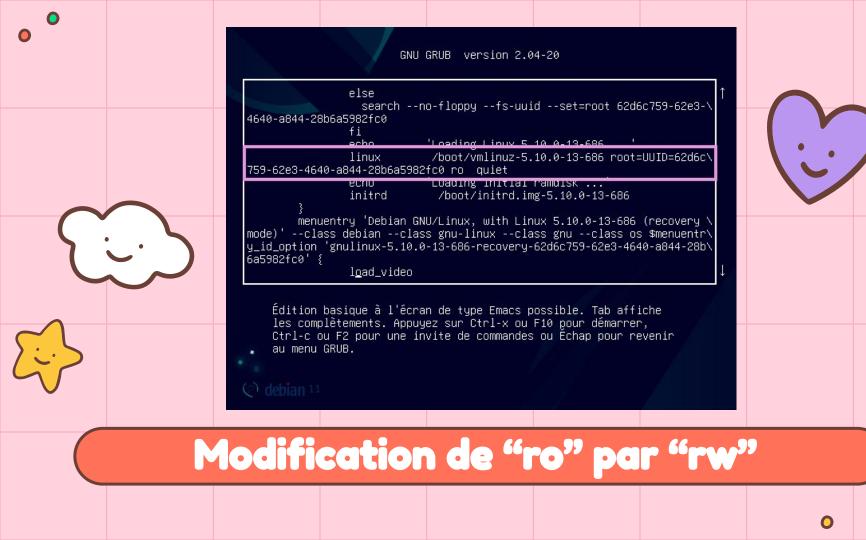
Accéder à la machine sans mot de passe, voler/manipuler des données



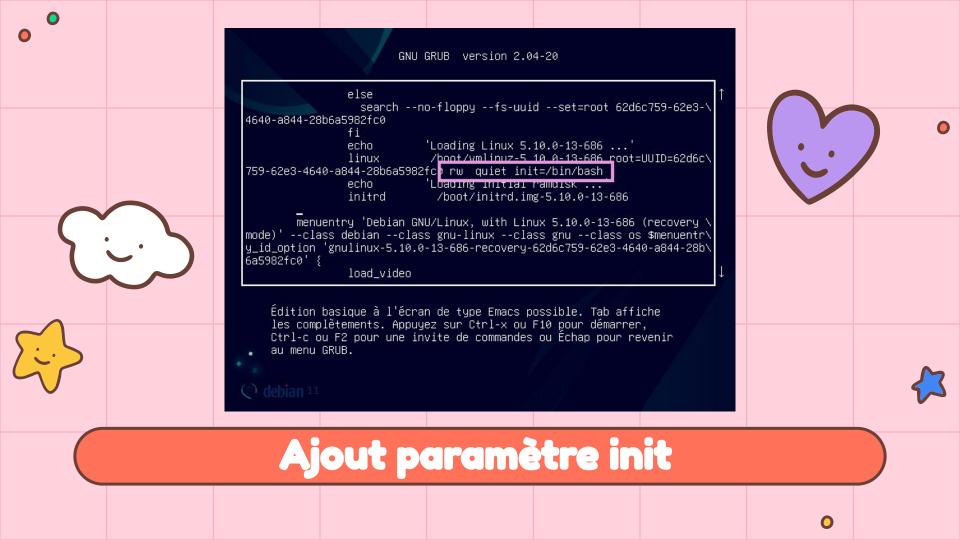














Ajout d'un paramètre kernel

Ici, nous ajoutons init=/bin/bash

- Init = option de start-up kernel, prend n'importe quel exécutable/binaire en paramètre
- /bin/bash = renvoi au shell bash
- Press F10 to boot ! (^~^)/



Documentation kernel ici, scan me!





Quelques commandes avant de partir

adduser [user] & usermod -aG sudo [user]	adduser ajoute un user et usermod -aG l'ajoute dans le groupe sudo.
passwd	change le password pour l'user (root actuellement)
poweroff -f	très important, permet de sortir de cet environnement particulier sans provoquer de kernel panick.







Merci de votre attention!(ブー・・。)づ♡



Vous pouvez me retrouver sur mon site web: pwnwithlove.com











@pwnwithlove

Retrouvez cette rump sur mon github!

@pwnwithlove

