Bypass d'authentification depuis le GRUB

Présentée par Pwnwithlove lors du SteakOverflow 2022

>whoami ?

- Étudiante en BTS SIO à l'ESNA.

- Passionnée de cybersécurité, player ctf

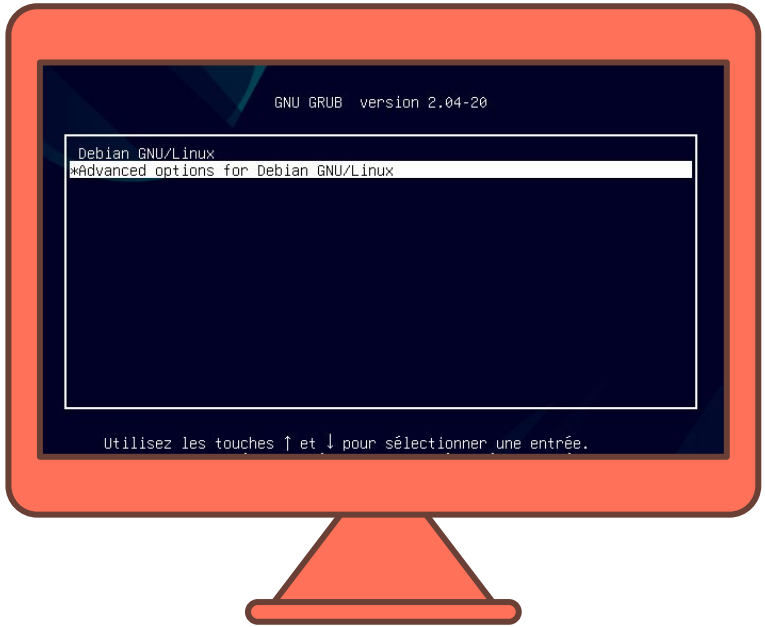
- Intéressée par la forensic, le web (server) & le boot2root.

01

Rappels

Qu’est-ce que le GRUB ?

Qu'est-ce que le GRUB ?



-**S'exécute** dès lors de la mise sous tension de votre machine **GNU/Linux**
-**Sélection** du système d'exploitation/noyau
-Transmission d'informations au **kernel** load.
-Généralement situé en **clear** sur une **partition annexe** à votre système == aucun accès si **chiffrement** (voir conditions..)

ESN'HACK

02

Elévation de privilège / Privesc

Priv-quoi ?

steakoverflow by ESN'HACK

Priv-quoi ?

Un privilège ?

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

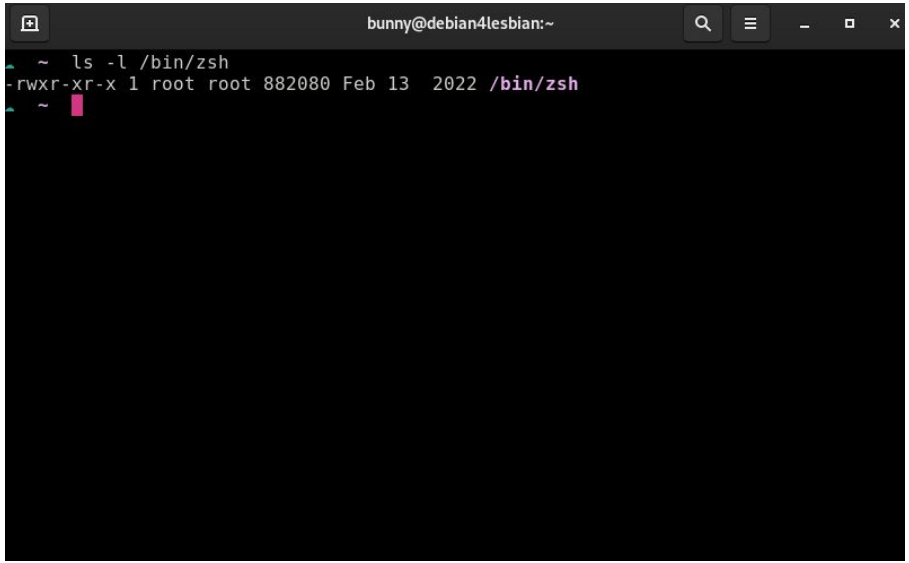
C'est quoi une privesc ?

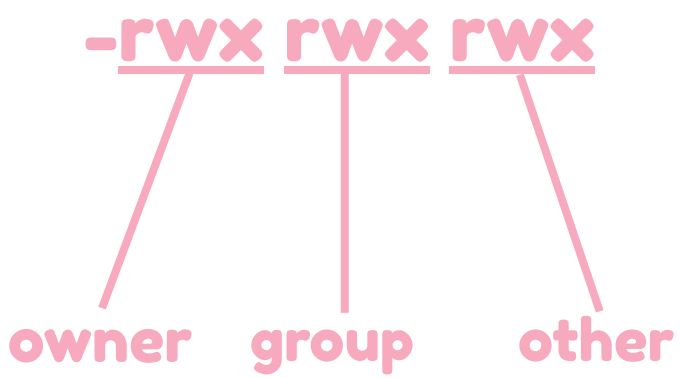
C'est un mécanisme permettant à un utilisateur d'obtenir des droits supérieurs à ceux qu'il a.

Pour faire quoi ?

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

Priv-quoi ?

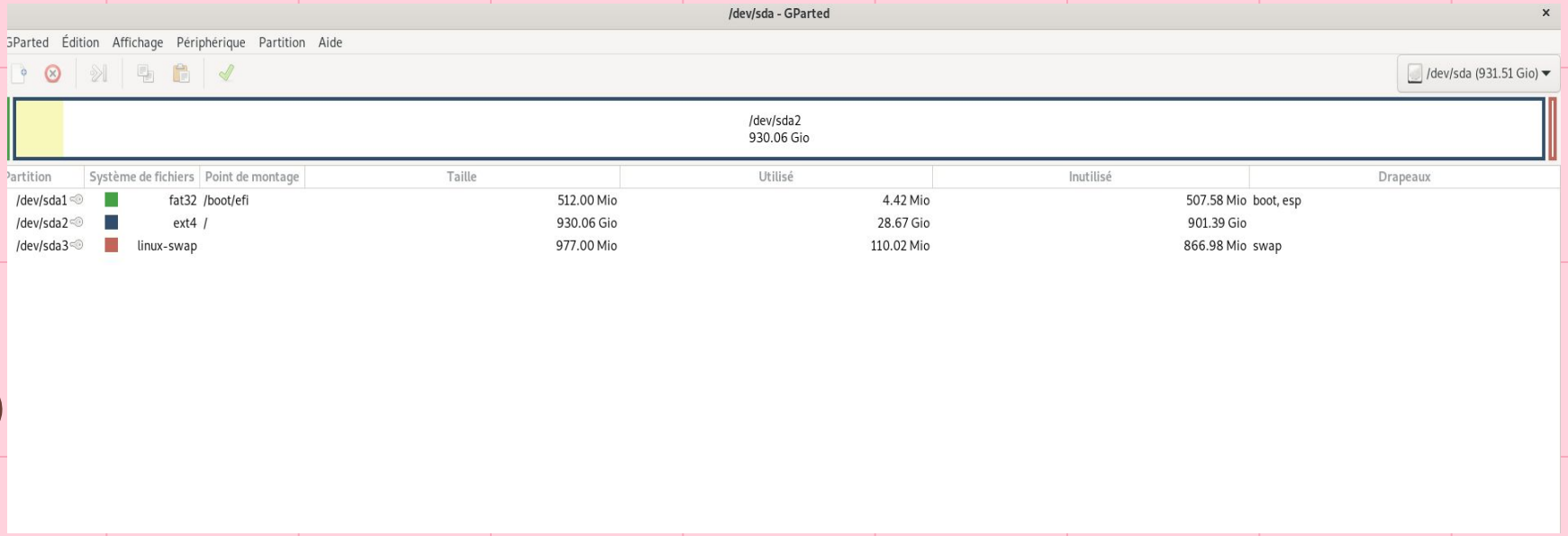




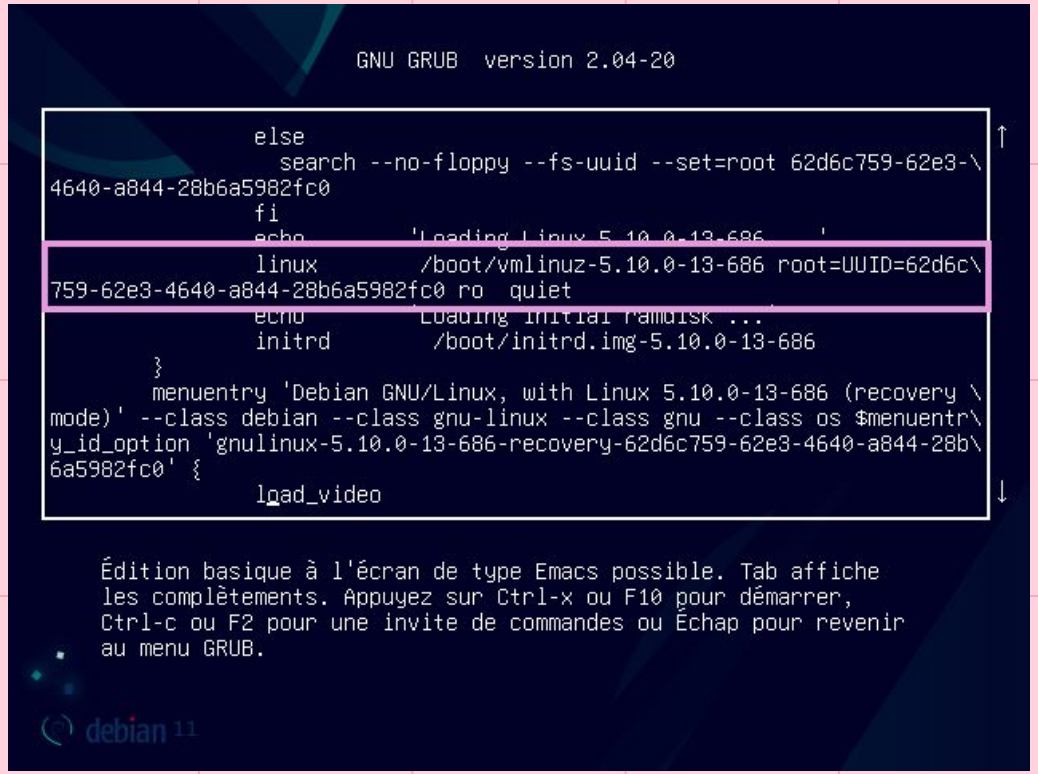
- : fichier classique

03 Privesc local depuis le GRUB

Comment faire pop un shell root en quelques secondes



Exemple de partitionnement



Modification de “ro” par “rw”

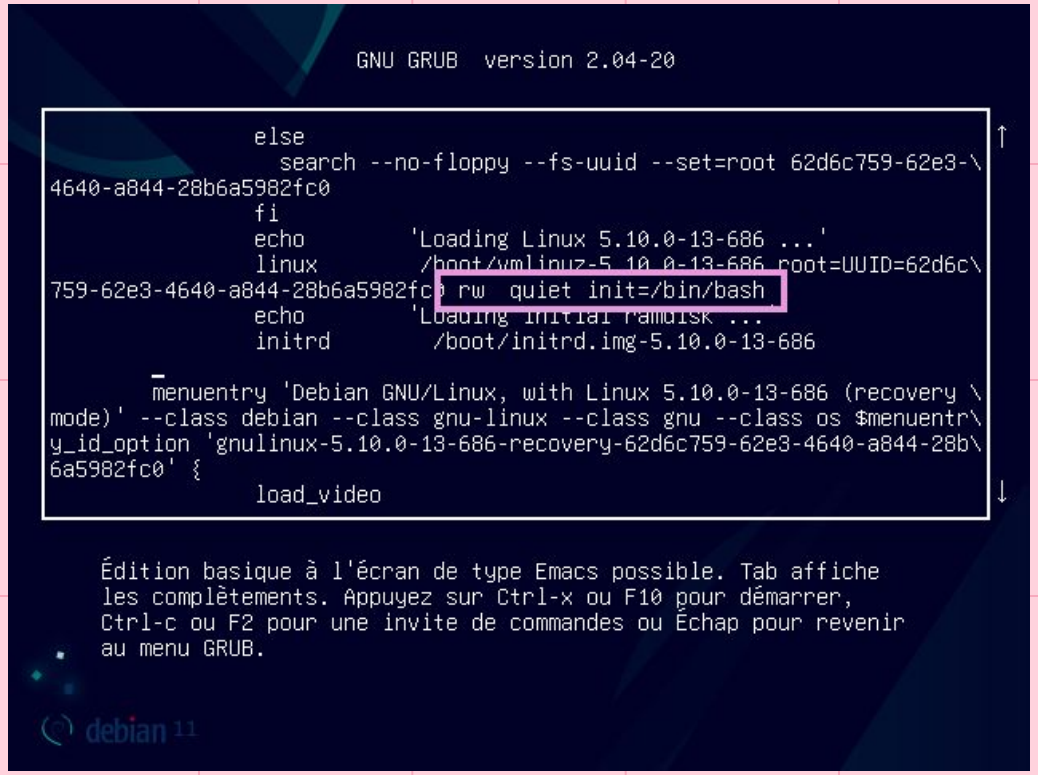
Read-Only & Read-Write

Read-Only

(Autorise seulement la lecture)

Read-Write

(Autorise l'écriture et la lecture)



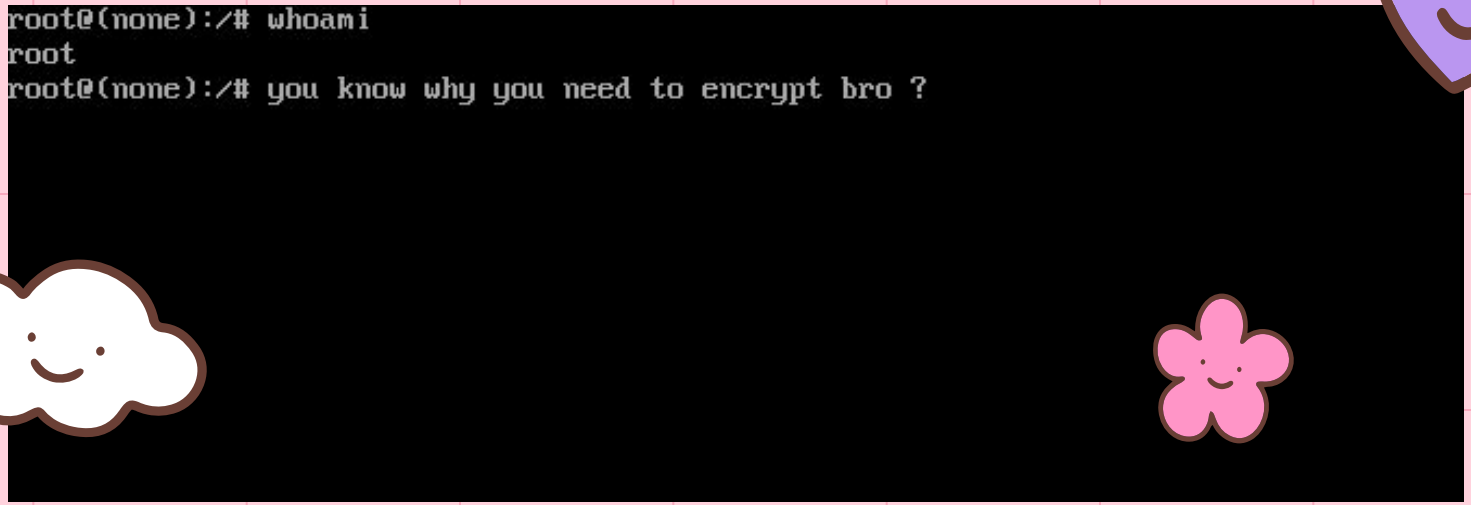
Ajout paramètre init

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 !



Nous voilà sur un shell root !

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.

Conclusion ! 04

Pourquoi et comment chiffrer ?

Pourquoi et comment chiffrer ?

- Garantir la sécurité de vos données personnelles
- Vous pouvez utiliser LVM & LUKS lors de votre partitionnement
- Pour une installation déjà faite: chiffrement d'un path avec encryptfs
- Assister à ma prochaine rump !

Merci de votre attention ! (づ◕‿◕)づ♡

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

Et sur twitter: @pwnwithlove

steakoverflow by ESN'HACK