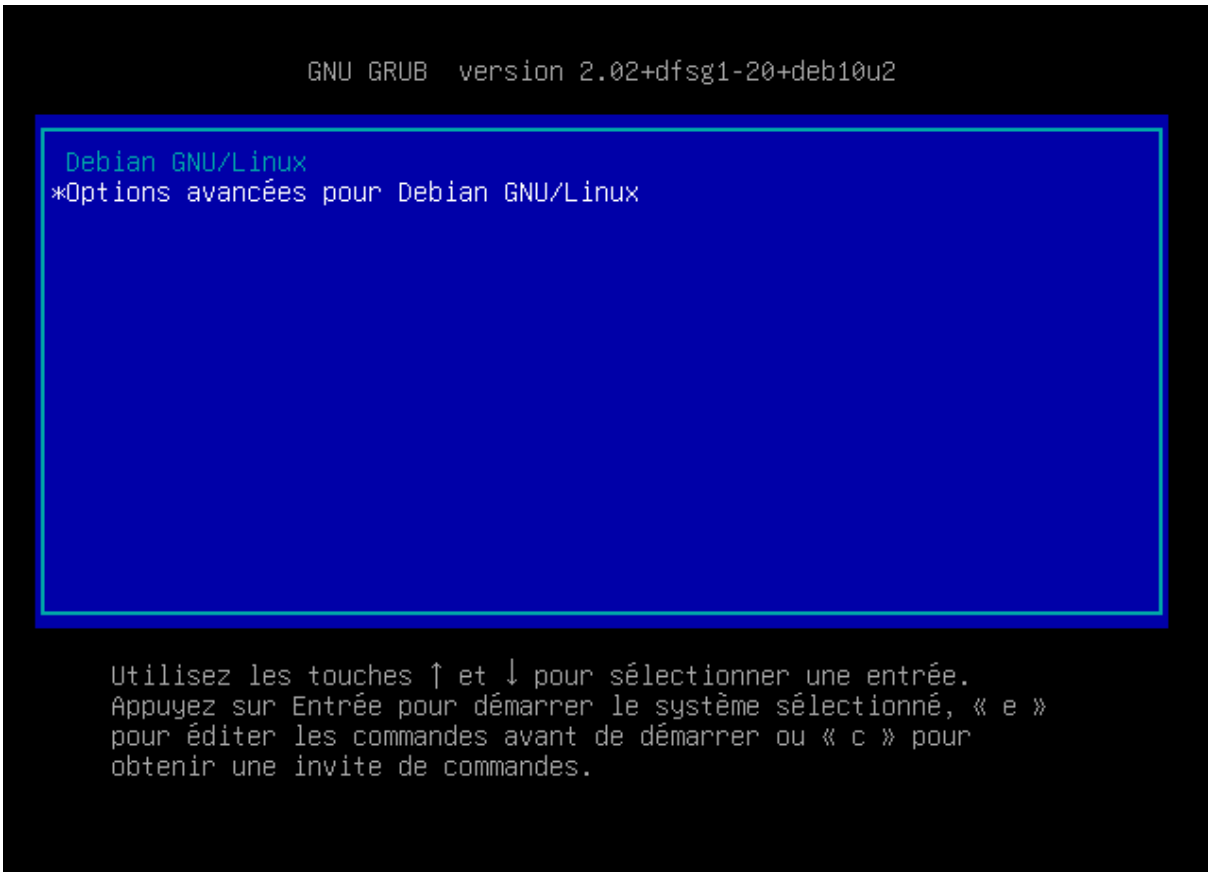
Bypass du mot de passe root

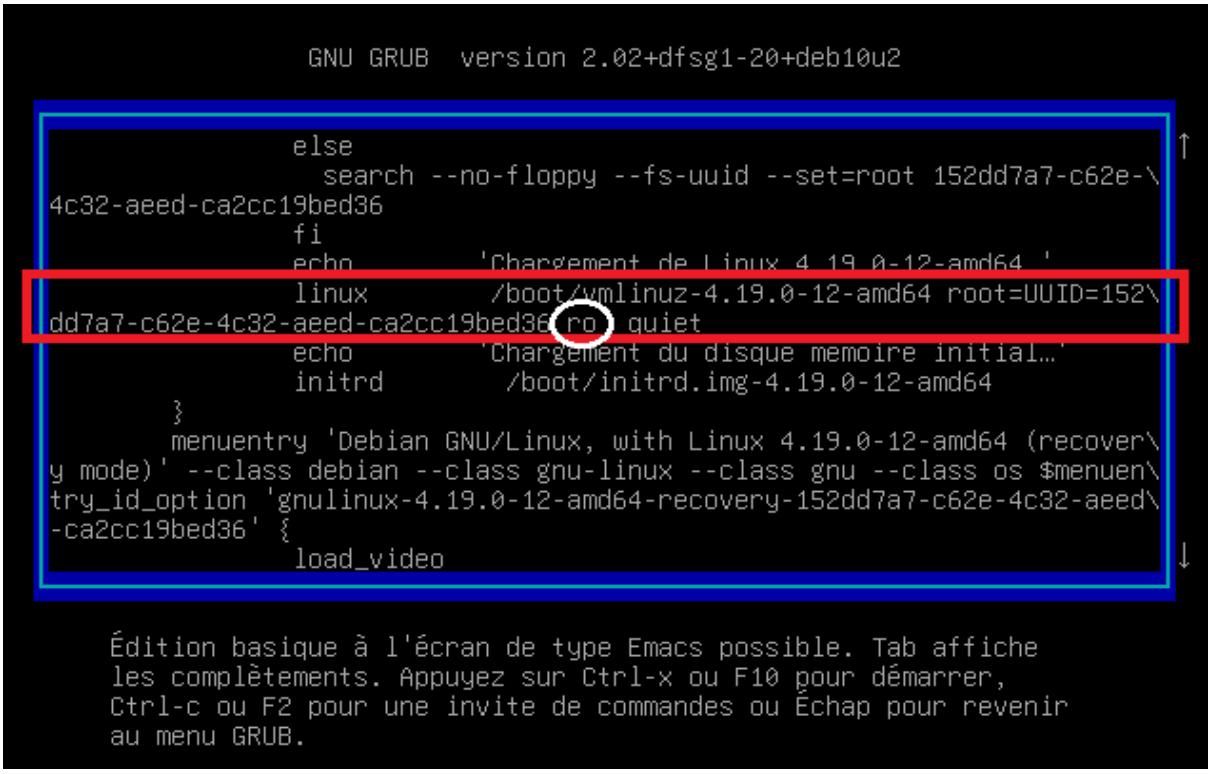
1. Réinitialisation par Grub.

Pour cela il faut passer par Grub, au démarrage de celui-ci, au lieu de charger la distribution, on va appuyer sur la touche ‘e’ pour éditer les commandes avant de démarrer.



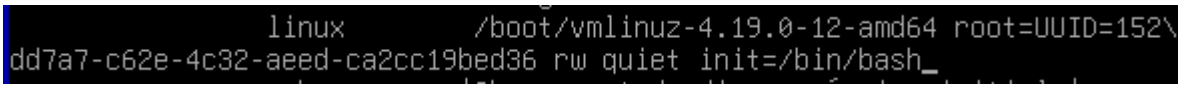
Une fois l’éditeur d’option de démarrage ouvert, il faut trouver la première ligne commençant par **linux**.

!! **A ce stade le clavier est en qwerty.**



Dans son état initial le paramètre de montage de la racine est **ro** = lecture seule (read only). Pour enregistrer un nouveau mot de passe, il faut un montage en lecture/écriture, on le remplace donc par **rw** (read and write).
On va ensuite ajouter **init=/bin/bash** à la fin de la ligne pour monter une console.
(Les paramètres reviendront à leur état initial au prochain démarrage)

Cela nous donne :



On appuie maintenant sur **Ctrl+x** ou **F10** pour démarrer avec les nouveaux paramètres.

On se retrouve dans une console loggé en root, on peut donc modifier son mot de passe.

```
passwd
```

Une fois le mot de passe modifié, on lance le processus **init** qui va prendre le PID 1 (ici utilisé par le processus qui génère la console (shell) en cours d'usage). Afin d'accéder aux commandes système classiques (reboot, shutdown ...).

Pour cela, on exécute la commande suivante :

```
exec /sbin/init
```

Une fois exécuté, on peut se logger en root avec le nouveau mot de passe et redémarrer la machine pour éviter toutes erreurs.

2. Bloquer cette entrée.

Désactiver l'affichage de grub.

Une option pour empêcher l'entrée dans l'éditeur de démarrage de grub est de désactiver l'attente d'affichage de celui-ci.

Dans le fichier /etc/default/grub

```
#nano /etc/default/grub
```

Modifier la ligne

```
GRUB_TIMEOUT=5
```

Passer la valeur 5 à 0.

L'inconvénient de cette technique est que plus rien n'est accessible.

Ajouter un mot de passe à l'option [e] éditer de grub.

Une autre méthode est d'ajouter un login et mot de passe pour accéder à grub (mode de récupération, édition, ...) sauf pour accéder aux distributions.

Tout d'abord, on ajoute un super utilisateur à grub.
Pour cela, on ajoute les lignes suivantes au fichier /etc/grub.d/40_custom

```
set superusers="grub"
      password_pbkdf2 grub grub.pbkdf2.sha512.10000.6731............
#           |           |        |
#   Methode(chiffré)  user    mot de passe chiffré
```

Pour chiffrer le mot de passe, on utilise la commande :

```
#grub-mkpasswd-pbkdf2
```

On copie le résultat de la commande.

Pour empêcher l'identification à chaque démarrage, on désactive l'authentification pour les distributions.
Pour cela, on ajout **--unrestricted** aux deux **echo "menuentry '$...** du fichier /etc/grub/10_linux

```
[...]
      echo "menuentry '$(echo "$title" | grub_quote)' --unrestricted
....
  else
      echo "menuentry '$(echo "$os" | grub_quote)' --unrestricted .....
[...]
```

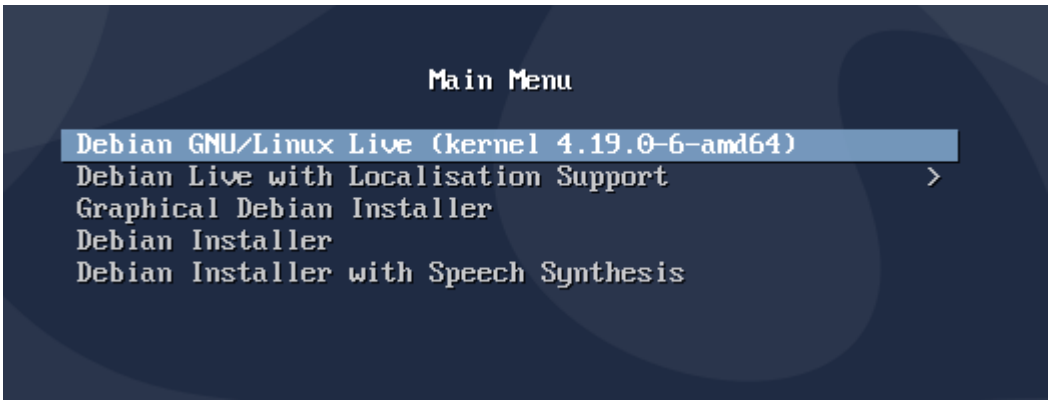
Il faut ensuite appliquer les changement avec la commande :

```
#update-grub
```

3. Entrer par une autre porte.

On peut encore réinitialiser le mot de passe root en passant par un live cd.
Par ce biais, nous allons utiliser le logiciel chroot afin de détourner la racine du system.

Pour cela, on lance un live cd de debian :



Se loger dans un terminal en root. (user/live $sudo su -)

Monter la racine du système de la machine ici sda1 en tant que /mnt

```
#mount /dev/sda1 /mnt
```

On monte ensuite les dossiers spéciaux nécessaires au fonctionnement du système :

```
#mount --bind /dev /mnt/dev
#mount -t proc /proc /mnt/proc
#mount -t sysfs /sys /mnt/sys
```

Enfin, on bascule vers le nouveau système avec la commande **chroot** :

```
#chroot /mnt /bin/bash
```

On est maintenant sur le système installé sur le disque dur, on peut donc changer le mot de passe.

```
#passwd
```

On peut maintenant sortir du chroot et démonter les systèmes de fichiers.

```
#exit
#umount /mnt/dev
#umount /mnt/proc
#umount /mnt/sys
#umount /mnt
```

On peut enfin redémarrer la machine avec un nouveau mot de passe root.