# Grand Unified NoobLoader

Auteur: bWlrYQ

# 1. Recon

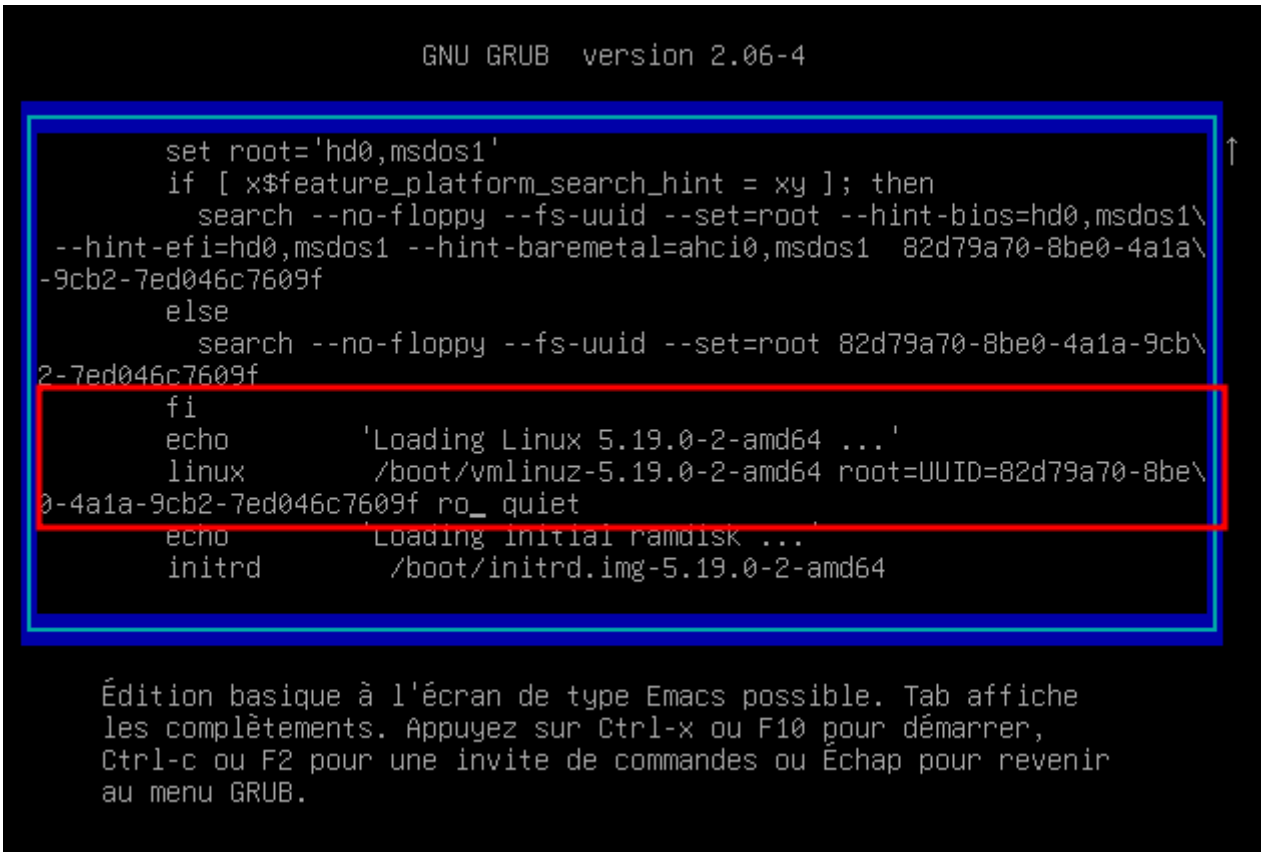
Nous sommes face à un ordinateur dont nous n'avons aucun accès au disque. Nous pouvons juste le démarrer et l'éteindre, sans avoir le mot de passe (qui est un mot de passe fort), la seule possibilité pour obtenir un shell sur la machine est d'utiliser GRUB, le bootloader installé.

Le disque dur n'est pas chiffré, on peut donc changer les options de démarrage dans le bootloader pour avoir un shell en tant que root.

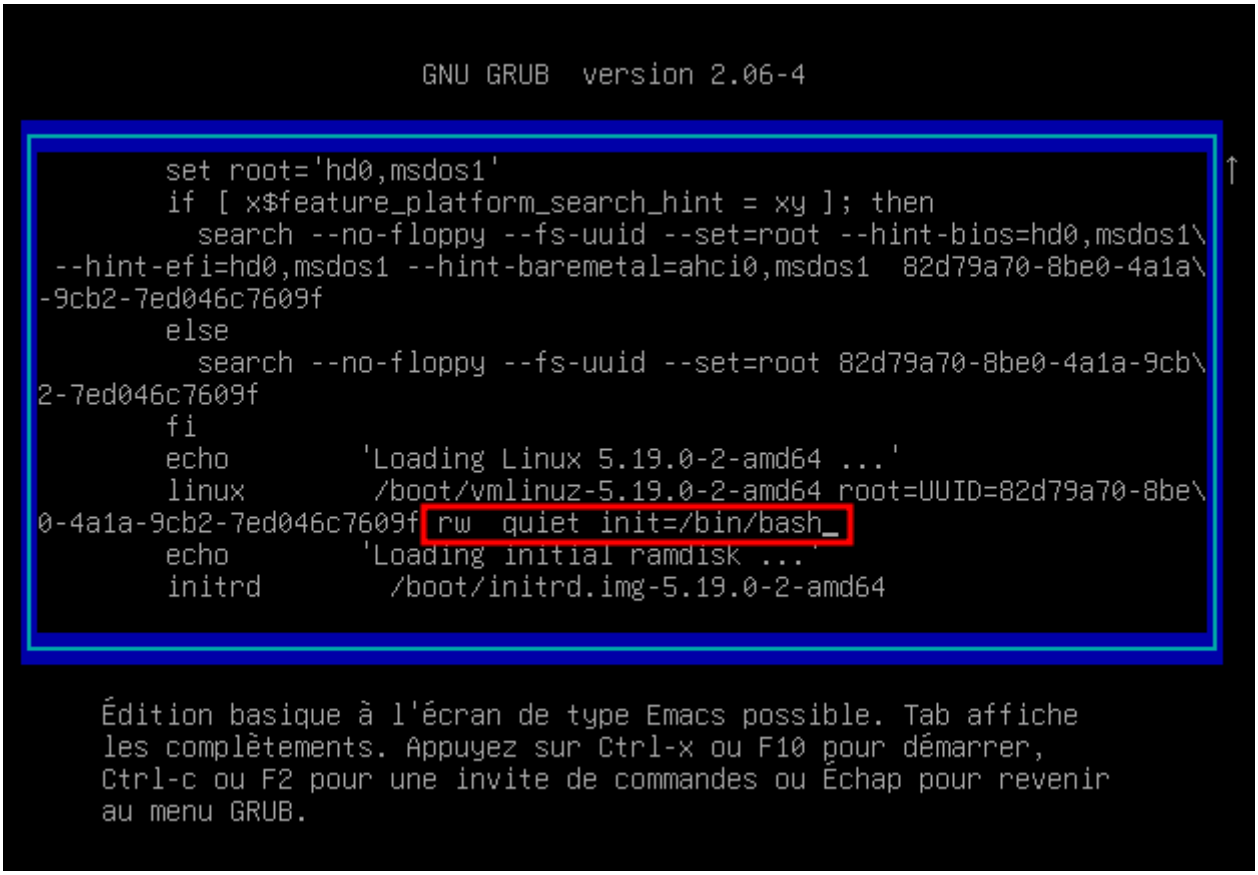
# 2. Application

Une fois sur le bootloader, on peut appuyer sur 'e', pour accéder aux commandes de démarrage.


On peut ensuite éditer ce qui se passe au démarrage du Kernel




Par




Appuyer sur F10

```
[    0.044444] RETBleed: WARNING: Spectre v2 mitigation leaves CPU vulnerable to
 RETBleed attacks, data leaks possible!
/dev/sda1: recovering journal
/dev/sda1: clean, 39634/2035824 files, 633167/8138240 blocks
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# _
```

Et voilà, notre shell !

```
root@(none):/# ls
bin   home            lib32       media  root  sys  vmlinuz
boot  initrd.img      lib64       mnt    run   tmp  vmlinuz.old
dev   initrd.img.old  libx32      opt    sbin  usr
etc   lib             lost+found  proc   srv   var
root@(none):/# cd /root
root@(none):/root# cat flag.txt
FMCTF{EnCrYpT_Y0uR_Fil3System}
root@(none):/root#
```

Plus qu'à récupérer notre flag 😃