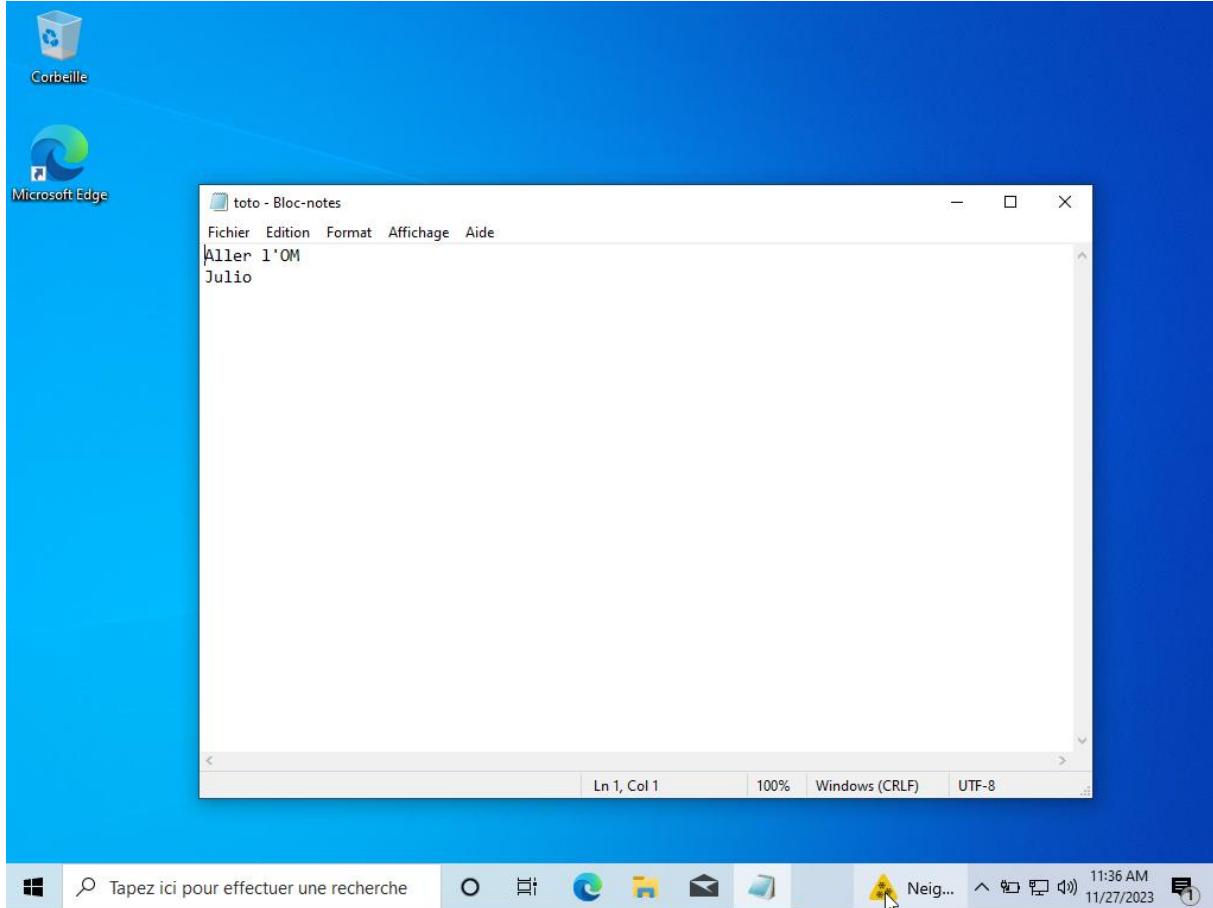


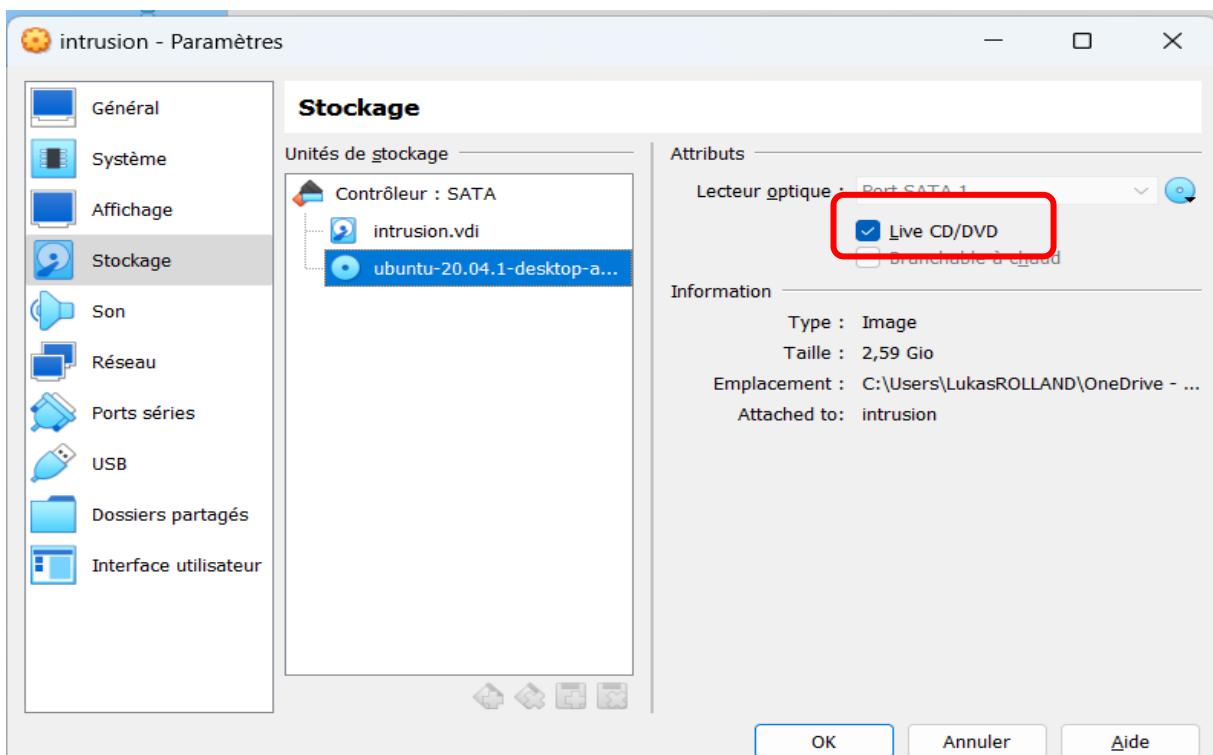
## TP2 : Intrusions

Tout d'abord, nous avons installée l'ISO de Windows 10, puis nous avons donc créeé une Machine Virtuel sous Windows 10.

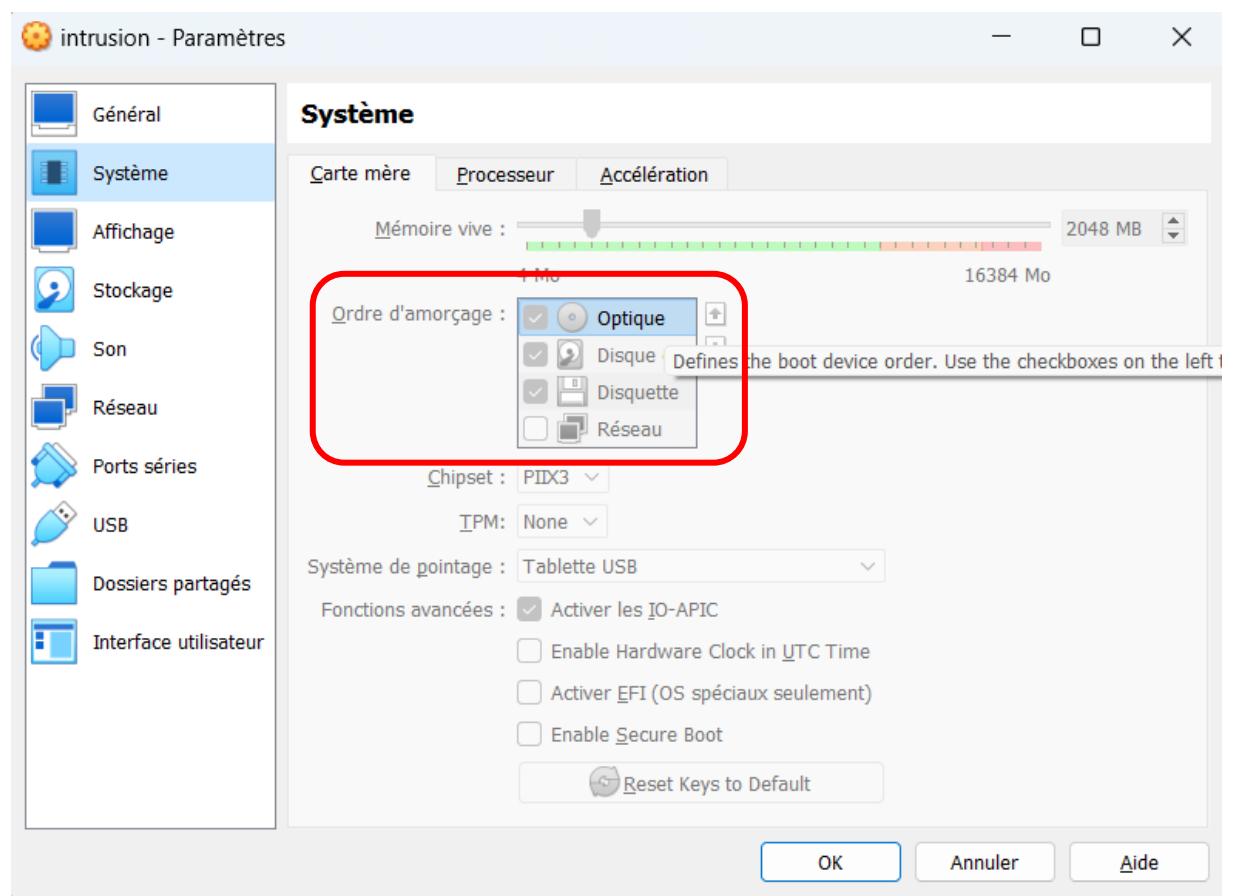
Une fois la VM crée, j'ai créé un document toto.txt



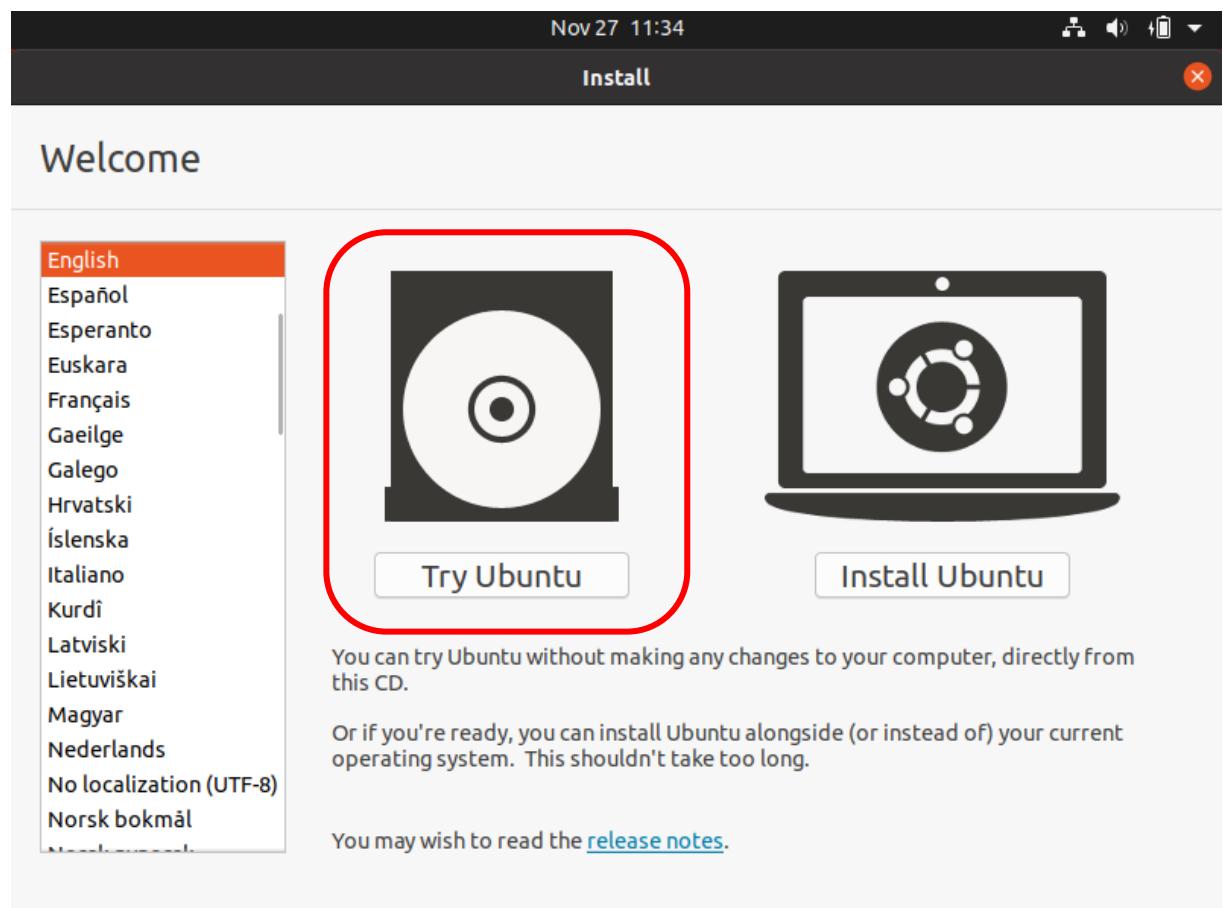
Après cela, j'ai éteint la VM pour ensuite la booter avec une ISO Ubuntu Desktop, et j'ai cocher « Live CD/DVD »



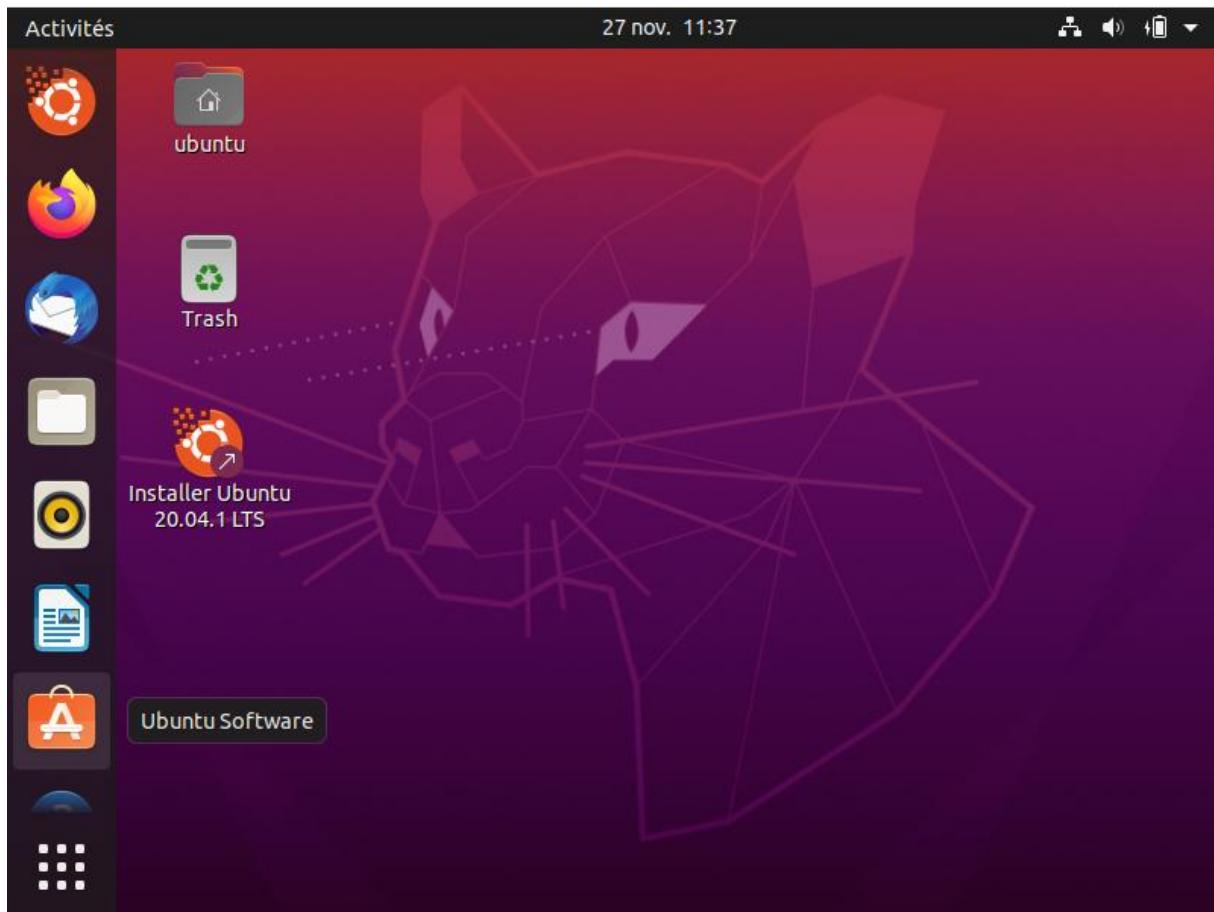
Ensuite j'ai dû forcer l'ordre de démarrage des disques pour que l'ISO Ubuntu se lance en premier.



Une fois Ubuntu lancé, il faut lancer et non installer.



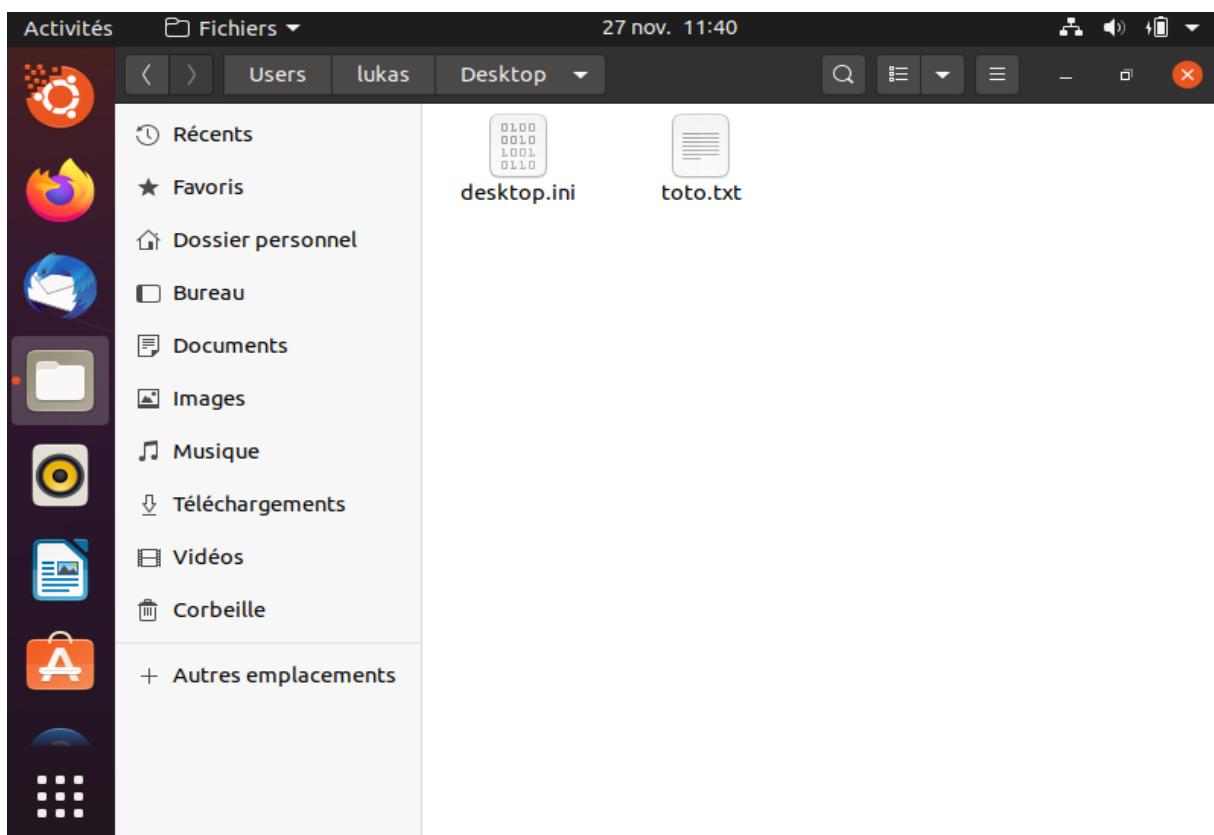
Après, il faut chercher le fichier toto.txt



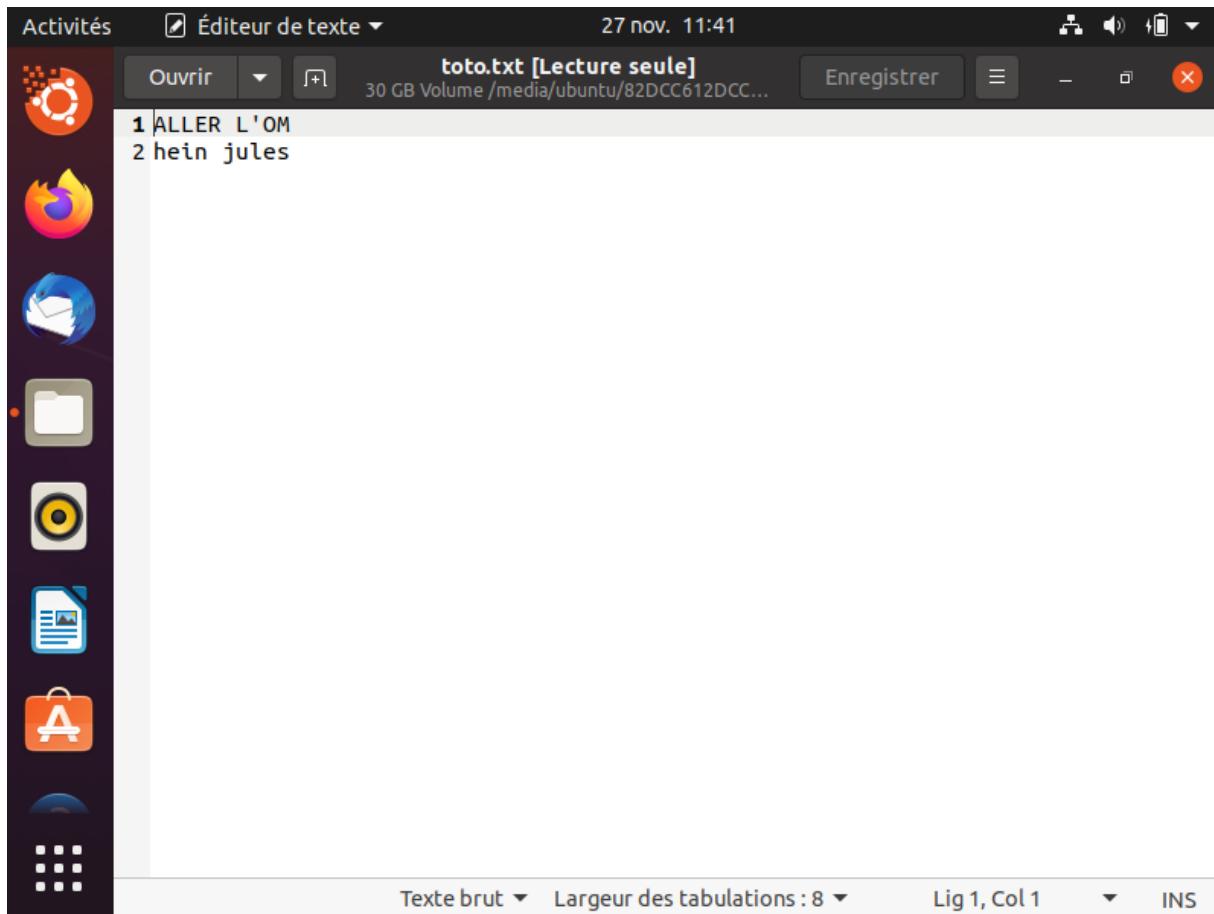
Pour trouver le fichier j'ai suivi le chemin suivant :

Autre Emplacements/30GB volumes/User/Lukas/Desktop

Nous avons donc accès au fichier créé depuis Windows au début.



Et il est aussi possible de l'ouvrir pour voir son contenu.



Maintenant essayons de changer le mot de passe du compte :

Une fois dans l'invite de commande, je suis aller dans le lecteur C : en faisant « C : » puis j'ai fait un « dire » pour voir si c'était le bon lecteur, et comme vous pouvez le voir c'était le bon puisqu'il y a les répertoires Windows.

```
C:\>dir
Le volume dans le lecteur C n'a pas de nom.
Le numéro de série du volume est DCC6-0081

Répertoire de C:\

07/12/2019  10:14    <DIR>          PerfLogs
27/11/2023  12:07    <DIR>          Program Files
06/10/2021  14:34    <DIR>          Program Files (x86)
27/11/2023      0        Recovery.txt
27/11/2023  12:08    <DIR>          Users
27/11/2023  12:08           1 539  vboxpostinstall.log
27/11/2023  12:08    <DIR>          Windows
              2 fichier(s)           1 539 octets
              5 Rép(s)   10 261 651 456 octets libres
```

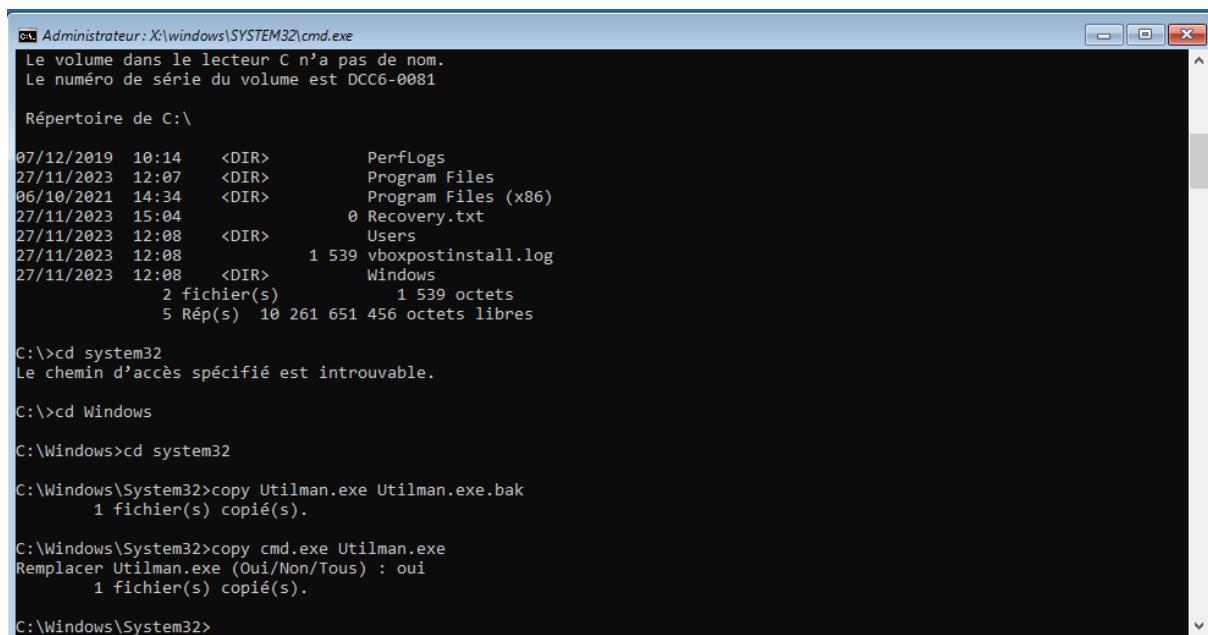
En suite j'ai fait les commandes donner dans le site internet lecrabinfo :

Cd system32 (sert à se rendre dans le fichier system32)

Cd Windows (sert à se rendre dans le fichier Windows)

Copy Utilman.exe Utilman.exe.bak (crée une sauvegarde du fichier Utilman.exe)

Copy cmd.exe Utilman.exe.bank (remplace les options d'ergonomie utilman.exe par l'invite de commandes cmd.exe)



```
c:\ Administrator:X:\windows\SYSTEM32\cmd.exe
Le volume dans le lecteur C n'a pas de nom.
Le numéro de série du volume est DCC6-0081

Répertoire de C:\

07/12/2019 10:14    <DIR>      PerfLogs
27/11/2023 12:07    <DIR>      Program Files
06/10/2021 14:34    <DIR>      Program Files (x86)
27/11/2023 15:04          0 Recovery.txt
27/11/2023 12:08    <DIR>      Users
27/11/2023 12:08          1 539 vboxpostinstall.log
27/11/2023 12:08    <DIR>      Windows
      2 fichier(s)           1 539 octets
      5 Rép(s)   10 261 651 456 octets libres

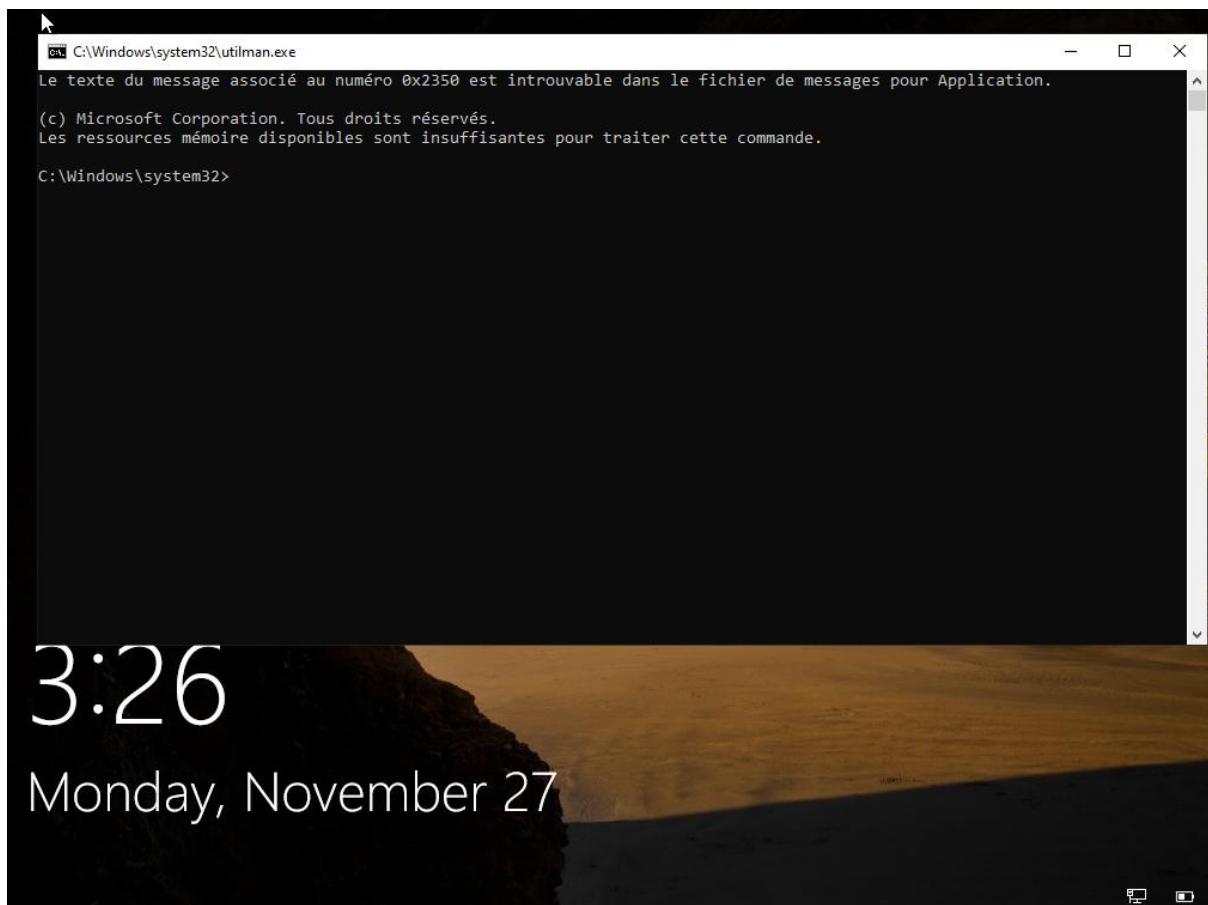
C:\>cd system32
Le chemin d'accès spécifié est introuvable.

C:\>cd Windows
C:\Windows>cd system32
C:\Windows\System32>copy Utilman.exe Utilman.exe.bak
      1 fichier(s) copié(s).

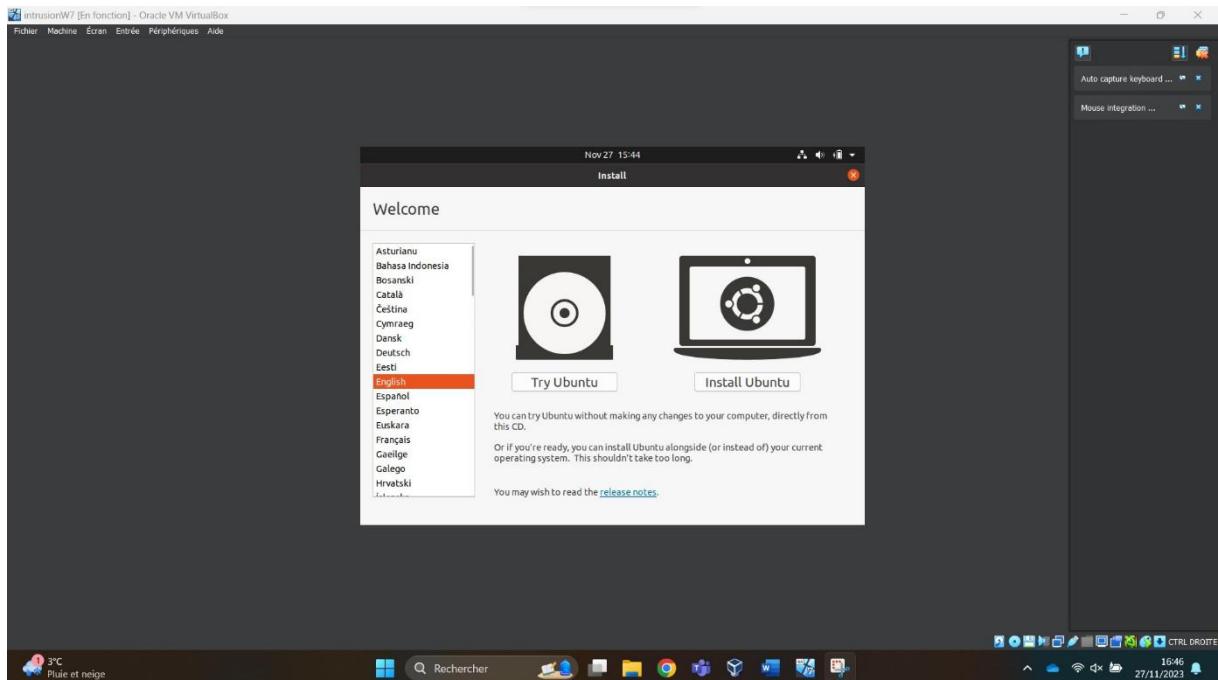
C:\Windows\System32>copy cmd.exe Utilman.exe
Remplacer Utilman.exe (Oui/Non/Tous) : oui
      1 fichier(s) copié(s).

C:\Windows\System32>
```

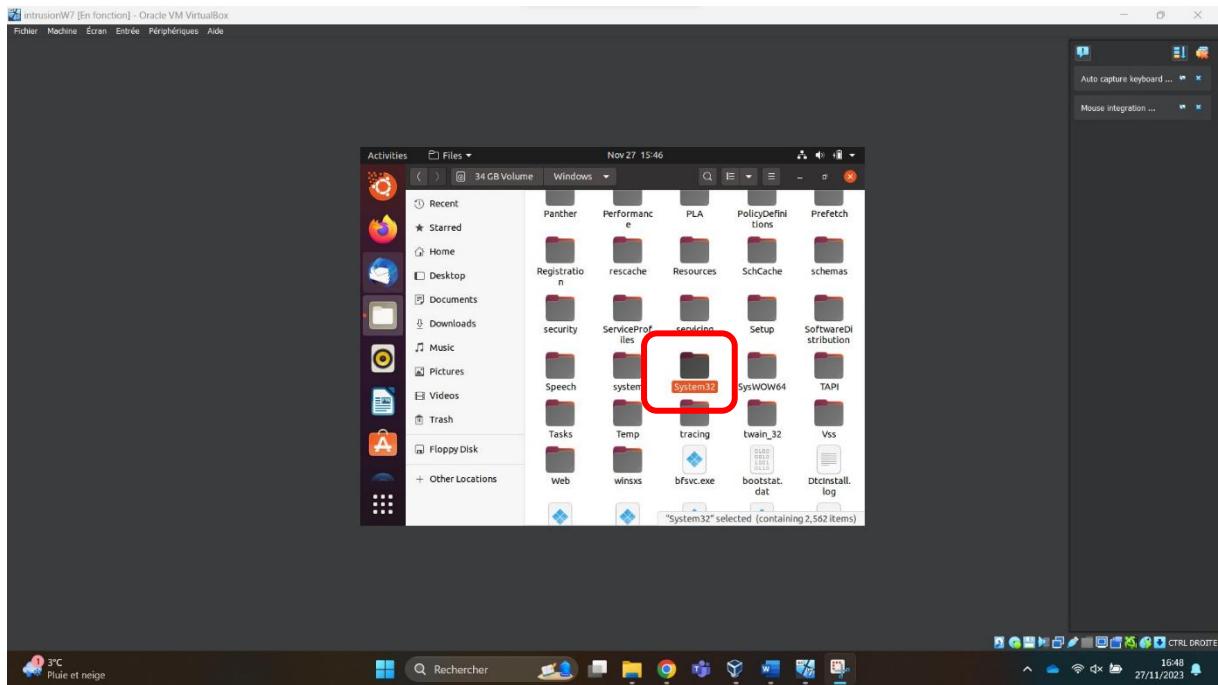
En suite j'ai dû redémarrer ma VM plusieurs fois pour pouvoir accès à l'invit de commande en faisant WIN+U



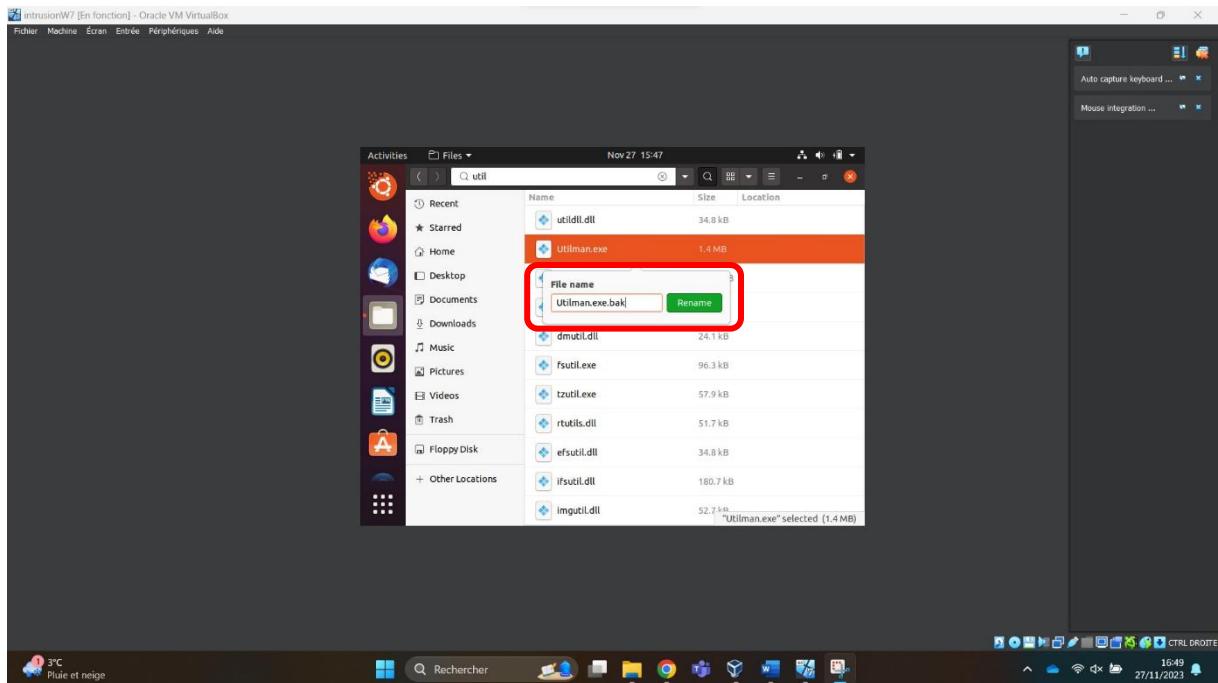
A chaque fois que le cmd se lance, il se referme directement après dû à Windows defender. Donc nous allons re essayer avec Windows 7. Donc j'ai installé une ISO pour Windows 7, j'ai créé une VM. Pour cette version de Windows, il faut mettre un ISO ubuntu et le lancer :



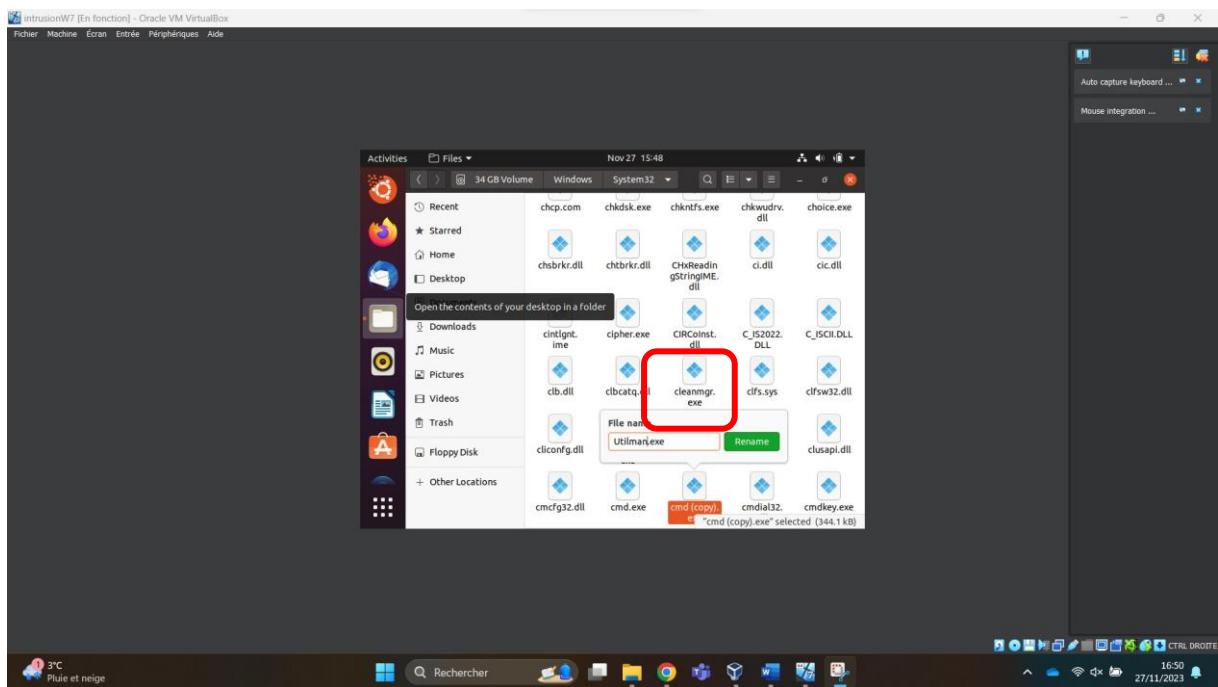
En suite aller dans le fichier « Windows » puis « system32 »



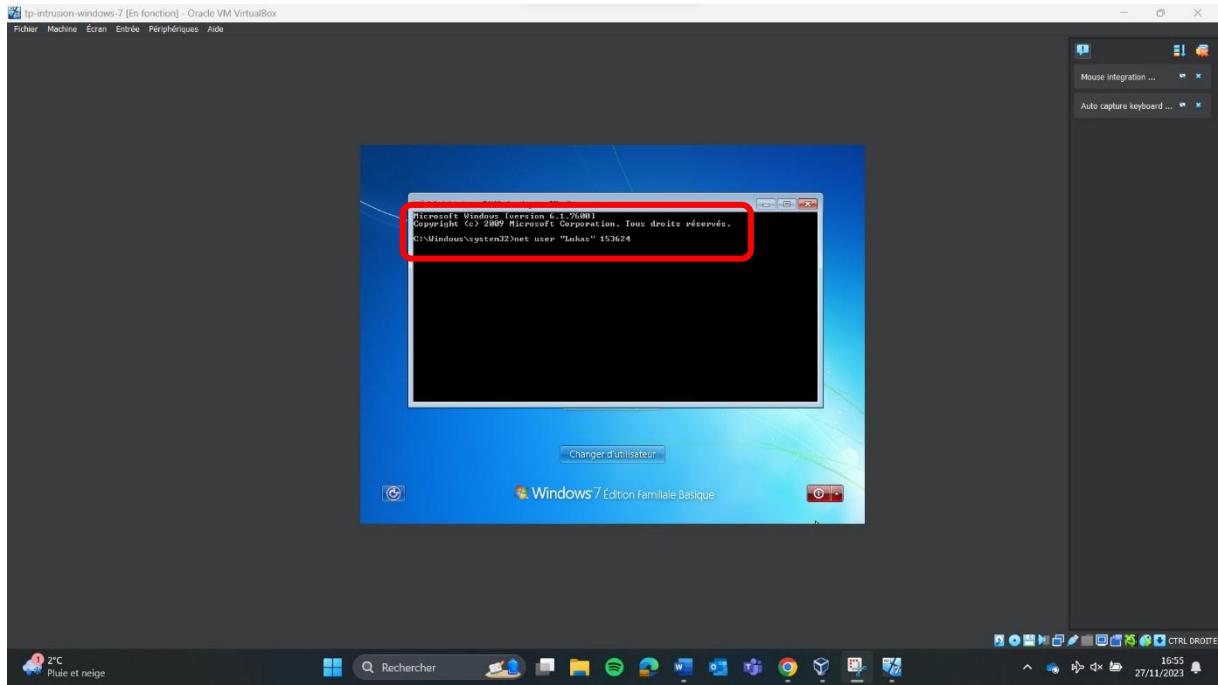
Ensuite chercher le fichier « Utilman.exe » et renommer le « Utilman.exe.bak »



Ensuite il faut renommer « cmd.exe » par « Utilman.exe »



Après cela, retourner sous Windows puis allez dans le terminal et tapez « net user nom d'utilisateur » avec le nouveau mot de passe de l'utilisateur



C'est donc la méthode 1 qui s'approche le plus de la vidéo, mais je n'ai pu la faire car je n'avais pas de machine physique ni de clef USB.

Cette faille consiste à utiliser un fichier nécessaire au lancement de Windows, Utilman.exe est un fichier pour les personnes malvoyantes qui leur permet d'utiliser un ordinateur et qui est donc indispensable pour eux. Cela consiste donc à remplacer Utilman.exe par le cmd pour qu'une fois sur l'écran de veille, il suffit d'ouvrir Utilman et ce sera le cmd qui s'affichera.

Cette faille de sécurité a été résolu sur les versions à partir de Windows 10, mais elle a été simplement décalée puisqu'il est possible de faire la même chose simplement avec un fichier différent. De plus il est possible grâce au Rubber Ducky qui est une clef USB qu'il suffit de brancher, d'outrepasser le mot de passe Windows sans même toucher à l'ordinateur.

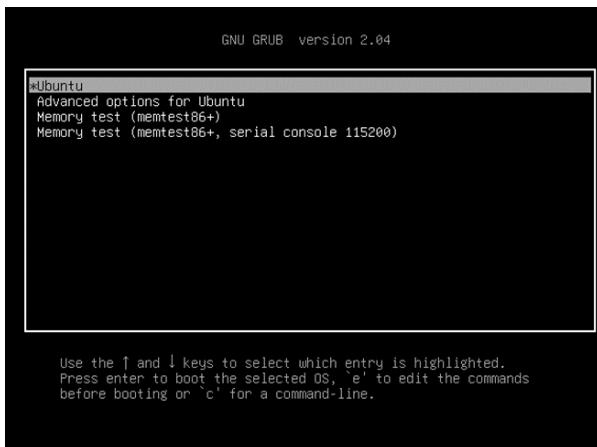
Il y a plusieurs manières pour se protéger de cela :

- Protéger ses répertoires/fichiers en les chiffrant
- Ne pas utiliser le compte administrateur comme compte de tous les jours
- Mettre un mot de passe sur le BIOS

Nous allons maintenant tenter de modifier le mot de passe d'un système linux grâce à la méthode « Bin bash » :

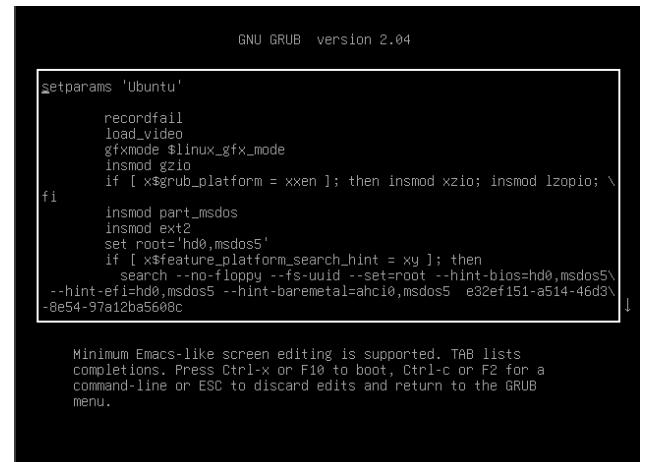
S

Tout d'abord, il faut redémarrer la machine



Appuyez sur maj pendant le redémarrage de votre machine

Maintenant appuyez sur « e » pour avoir ce menu



```

GNU GRUB version 2.04

insmod part_msdos
insmod ext2
set root='hd0,msdos5'
if [ $x$feature_platform_search_hint = xy ]; then
    search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos5\-
-e854-97a12ba5608c
else
    search --no-floppy --fs-uuid --set=root e32ef151-a514-46d3-8e5\
4-97a12ba5608c
fi
linux      /boot/vmlinuz-5.15.0-91-generic root=UUID=e32ef151\
-a514-46d3-8e54-97a12ba5608c no quiet splash $vt_handoff
initrd     /boot/initrd.img-5.15.0-91-generic

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.

```

Descendez sur la ligne ou il y a écrit linux, puis déplacez-vous vers la droite pour trouver « ro quiet »

```

GNU GRUB version 2.04

insmod part_msdos
insmod ext2
set root='hd0,msdos5'
if [ $x$feature_platform_search_hint = xy ]; then
    search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos5\-
-e854-97a12ba5608c
else
    search --no-floppy --fs-uuid --set=root e32ef151-a514-46d3-8e5\
4-97a12ba5608c
fi
linux      /boot/vmlinuz-5.15.0-91-generic root=UUID=e32ef151\
-a514-46d3-8e54-97a12ba5608c rw init=/bin/bash
initrd     /boot/initrd.img-5.15.0-91-generic

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.

```

Remplacez « ro quiet... » par  
« rw=/bin/bash »

Ensuite appuyez sur CTRL+X ou F10

pour démarrer.

```

[ 2.761136] usbcore: registered new interface driver usbhid
[ 2.764019] usbhid: USB HID core driver
[ 2.772717] input: VirtualBox USB Tablet as /devices/pci0000:00/0000:00:06.0/
usb2/2-1/2-1:1.0/0003:00EE:0021.0001/input/input6
[ 2.784867] hid-generic 0003:00EE:0021.0001: input,hidraw0: USB HID v1.10 Mouse [VirtualBox USB Tablet] on usb-0000:00:06.0-1/input0
[ 3.065573] e1000 0000:00:03.0 eth0: (PCI:33MHz:32-bit) 00:00:27:e5:82:36
[ 3.068093] e1000 0000:00:03.0 eth0: Intel(R) PRO/1000 Network Connection
[ 3.070619] e1000 0000:00:03.0 enp0s3: renamed from eth0
Begin: Loading essential drivers ... done.
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... done.
Begin: Will now check root file system ... fsck from util-linux 2.34
[/usr/sbin/fsck.ext4 (1) -- /dev/sda5] fsck.ext4 -a -O /dev/sda5
/dev/sda5: clean, 201856/2297456 files, 2305492/9179648 blocks
done.
[ 3.294734] EXT4-fs (sda5): mounted filesystem with ordered data mode. Opts:
(null). Quota mode: none.
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):# 

```

Puis vous vous retrouvez logiquement avec cette écran :

Taper " mount -n -o remount,rw / "

Cela montera le système en lecture et en écriture

(Au lieu de la lecture seule, qui est la valeur par défaut.)

```
[ 3.761136] usbcore: registered new interface driver usbhid
[ 3.764019] usbhid: USB HID core driver
[ 3.772717] input: VirtualBox USB Tablet as /devices/pci0000:00/0000:00:06.0/
usb2/2-1/1.0/0:003:00EE:0021.0001/input/input6
[ 3.784067] hid-generic 0003:00EE:0021.0001: input,hidraw0: USB HID v1.10 Mouse [VirtualBox USB Tablet]
[ 3.065573] e1000 0000:00:03.0 eth0: (PCI:33MHz:32-bit) 08:00:27:e5:82:36
[ 3.068093] e1000 0000:00:03.0 eth0: Intel(R) PRO/1000 Network Connection
[ 3.070619] e1000 0000:00:03.0 enp0s3: renamed from eth0
Begin: Loading essential drivers ... done.
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... done.
Begin: Will now check root file system ... fsck from util-linux 2.34
[/usr/sbin/fsck.ext4 (1) -- /dev/sda5] fsck.ext4 -a -C0 /dev/sda5
/dev/sda5: clean, 201856/2297456 files, 2305492/9179648 blocks
done.
[ 3.294734] EXT4-fs (sda5): mounted filesystem with ordered data mode. Opts: (null). Quota mode: none.
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@none:~# mount -n -o remount,rw /
[ 420.471185] EXT4-fs (sda5): Unrecognized mount option "rz" or missing value
mount: /: mount point not mounted or bad option.
root@none:~# mount -n -o remount,rz/
mount: bad usage
Try 'mount --help' for more information.
root@none:~# passwd lukas
New password:
```

Ensuite tapez « passwd NomUtilisateur »

Si vous avez un message d'erreur similaire, cela veut dire que votre lecteur est déjà monté, passez à la prochaine étape comme si cela avait fonctionné.

```
[ 3.065573] e1000 0000:00:03.0 eth0: (PCI:33MHz:32-bit) 08:00:27:e5:82:36
[ 3.068093] e1000 0000:00:03.0 eth0: Intel(R) PRO/1000 Network Connection
[ 3.070619] e1000 0000:00:03.0 enp0s3: renamed from eth0
Begin: Loading essential drivers ... done.
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... done.
Begin: Will now check root file system ... fsck from util-linux 2.34
[/usr/sbin/fsck.ext4 (1) -- /dev/sda5] fsck.ext4 -a -C0 /dev/sda5
/dev/sda5: clean, 201856/2297456 files, 2305492/9179648 blocks
done.
[ 3.294734] EXT4-fs (sda5): mounted filesystem with ordered data mode. Opts: (null). Quota mode: none.
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@none:~# mount -n -o remount,rw /
[ 420.471185] EXT4-fs (sda5): Unrecognized mount option "rz" or missing value
mount: /: mount point not mounted or bad option.
root@none:~# mount -n -o remount,rz/
mount: bad usage
Try 'mount --help' for more information.
root@none:~# passwd lukas
```

Vous pouvez maintenant définir un nouveau mot de passe

```
[ 3.068093] e1000 0000:00:03.0 eth0: Intel(R) PRO/1000 Network Connection
[ 3.070619] e1000 0000:00:03.0 enp0s3: renamed from eth0
Begin: Loading essential drivers ... done.
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... done.
Begin: Will now check root file system ... fsck from util-linux 2.34
[/usr/sbin/fsck.ext4 (1) -- /dev/sda5] fsck.ext4 -a -C0 /dev/sda5
/dev/sda5: clean, 201856/2297456 files, 2305492/9179648 blocks
done.
[ 3.294734] EXT4-fs (sda5): mounted filesystem with ordered data mode. Opts: (null). Quota mode: none.
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@none:~# mount -n -o remount,rz /
[ 420.471185] EXT4-fs (sda5): Unrecognized mount option "rz" or missing value
mount: /: mount point not mounted or bad option.
root@none:~# mount -n -o remount,rz/
mount: bad usage
Try 'mount --help' for more information.
root@none:~# passwd lukas
New password:
```

Vous avez donc bien changé le mot de passe, vous pouvez maintenant appuyez sur CTRL+D ou CTRL+ALT+SUPPR pour quitter

```
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... done.
Begin: Will now check root file system ... fsck from util-linux 2.34
[/usr/sbin/fsck.ext4 (1) -- /dev/sda5] fsck.ext4 -a -CO /dev/sda5
/dev/sda5: clean, 201856/2297456 files, 2395492/9179648 blocks
done.
[ 3.2947341 EXT4-fs (sda5): mounted filesystem with ordered data mode. Opts:
(null). Quota mode: none.
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@none:# mount -n -o remount,rz
[ 420.4711851 EXT4-fs (sda5): Unrecognized mount option "rz" or missing value
mount: ./ mount point not mounted or bad option.
root@none:# mount -n -o remount,rz/
mount: bad usage
Try 'mount --help' for more information.
root@none:# passwd lukas
New password:
Retype new password:
passwd: password updated successfully
root@none:#
```

```
[ 1026.106256] panic+0x15c/0x1f4
[ 1026.108537] do_cxit_cold+0x52/0xa0
[ 1026.110683] do_group_exit+0x43/0xb0
[ 1026.1126811] __x64_sys_exit_group+0x18/0x20
[ 1026.1157231] do_syscall_64+0x59/0xc0
[ 1026.1179591] ?irqentry_exit+0x1d/0x30
[ 1026.1209371] ?cxg_page_fault+0x89/0x170
[ 1026.1221911] entry_SYSCALL_64_after_hwframe+0x62/0xc
[ 1026.1252081] RIP: 0033:0x0e945cb0100000000
[ 00 45 60 00 0f 05 48 3d 00 f9 ff ff 77 32 f4 09 d7 44 89 e0 0f 05 <48> 3d 00 f9
ff ff 76 e2 f7 d9 64 41 09 01 eb da 66 26 0f ff 04 00
[ 1026.1381881] RSP: 002b:0007fe8d232128 EFLAGS: 00000246 ORIG_RAX: 0000000000000000
900e7
[ 1026.1421761] RAX: ffffffff000000000000000000000000 RBX: 00007fe945db58a0 RCX: 00007fe945cb0146
[ 1026.1460751] RDX: 00000000000000000000000000000003 RD1: 00000000000000000000000000000000
[ 1026.1507681] RBP: 00000000000000000000000000000007 R08: 00000000000000000000000000000007 R09: ffffffffffffbfff80
[ 1026.1545171] R10: 00000000000000000000000000000001 R11: 00000000000000000000000000000246 R12: 00007fe945db58a0
[ 1026.1582151] R13: 00000000000000000000000000000001 R14: 00007fe945bce2e8 R15: 00000000000000000000000000000000
[ 1026.1619431] </TASK>
[ 1026.1649251] Kernel Offset: 0x2300000 from 0xffffffff81000000 (relocation range: 0xffffffff80000000-0xffffffffbf0fffff)
[ 1026.1717591] ---[ end Kernel panic - not syncing: Attempted to kill init! exit code=0x00000000 ]---
```

Ensuite redémarrer avec "Reboot -f"

Rentrez simplement votre nouveau mot de passe et  
Le tour est joué !!

