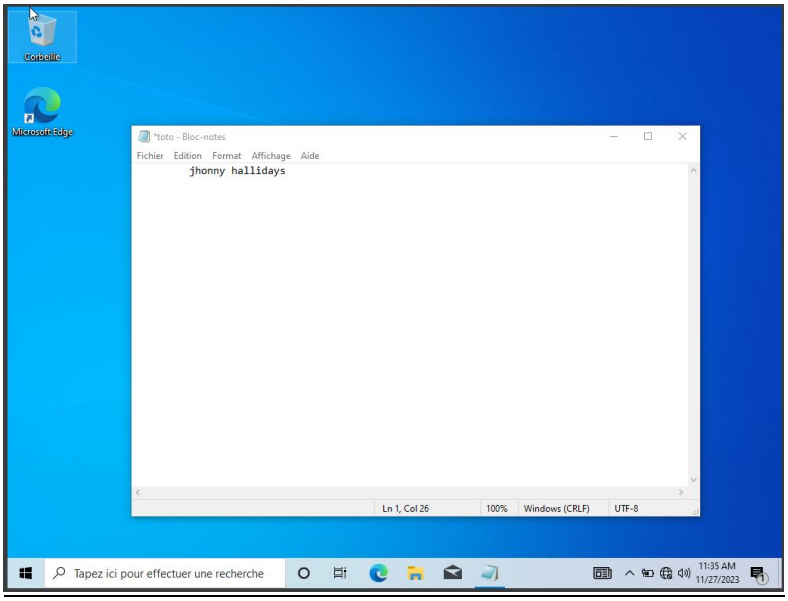
TP-Intrusion1 (Compte-rendu) :

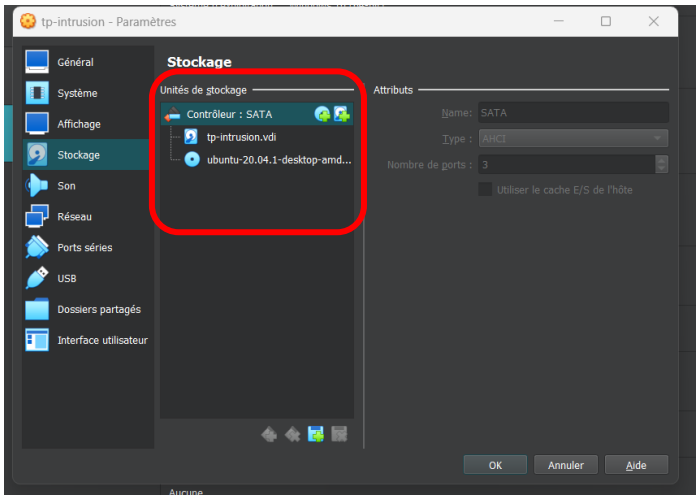
Pour commencer ce TP, nous allons installer une machine virtuelle sous Windows 10.

Astuces : ne mettez d'internet lors de l'installation de Windows

Comme indiqué sur le TP nous créons un fichier .txt dans lequel nous mettons notre chanteur préfère.



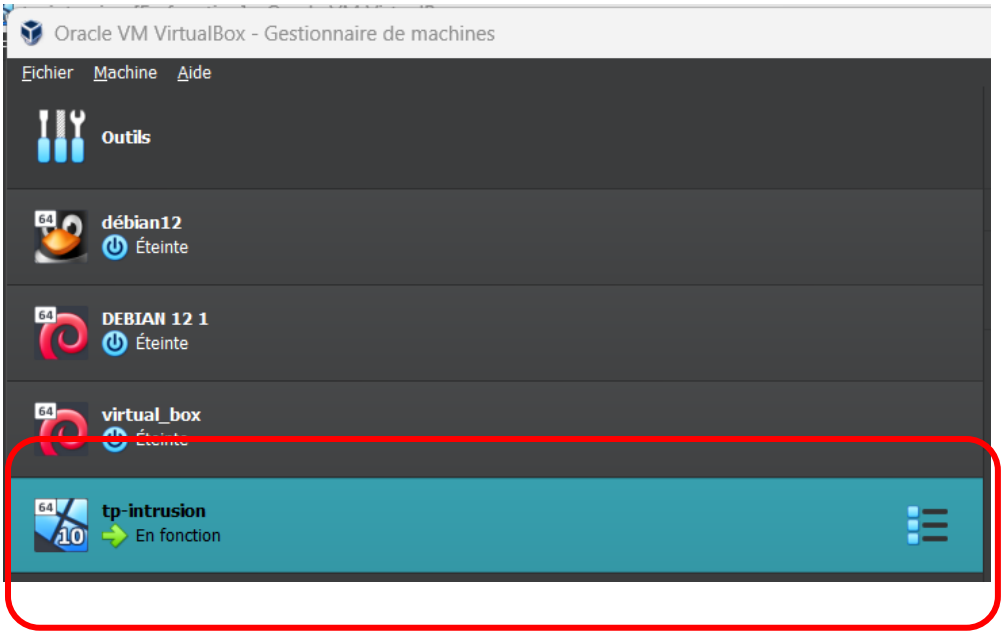
Une fois le fichier créer fermer votre VM a l'aide du bouton Windows en bas à gauche puis alimentation et arrêter.



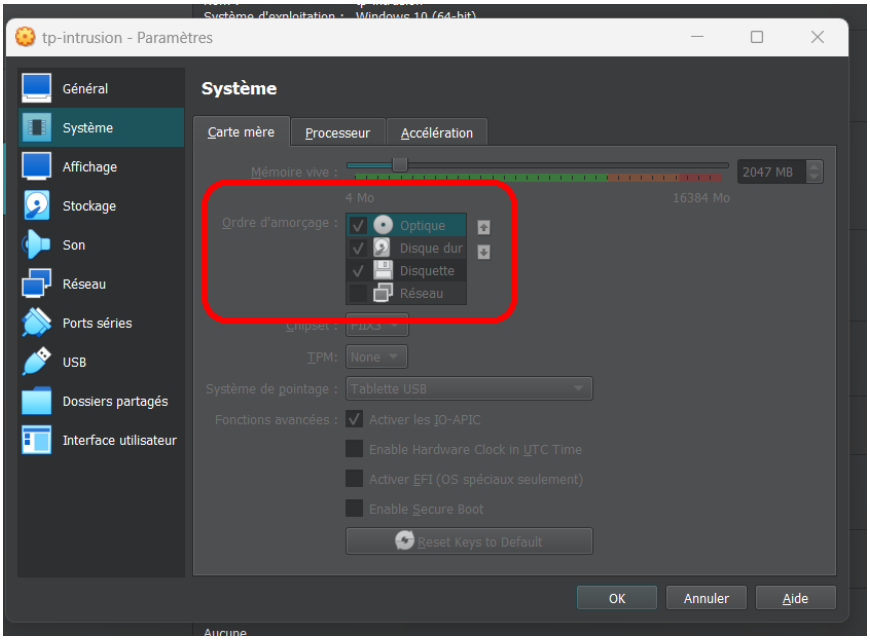
Ensuite, lorsqu'elle est éteinte bootez la VM en utilisant l'ISO (Ubuntu Desktop) pour ce faire : remplacer le disque SATA de Windows avec l'iso Ubuntu.

Une fois arriver à cette étape, si vous démarrer maintenant la VM vous arriverez encore sur l'écran de verrouillage Windows.

Pour ce faire :

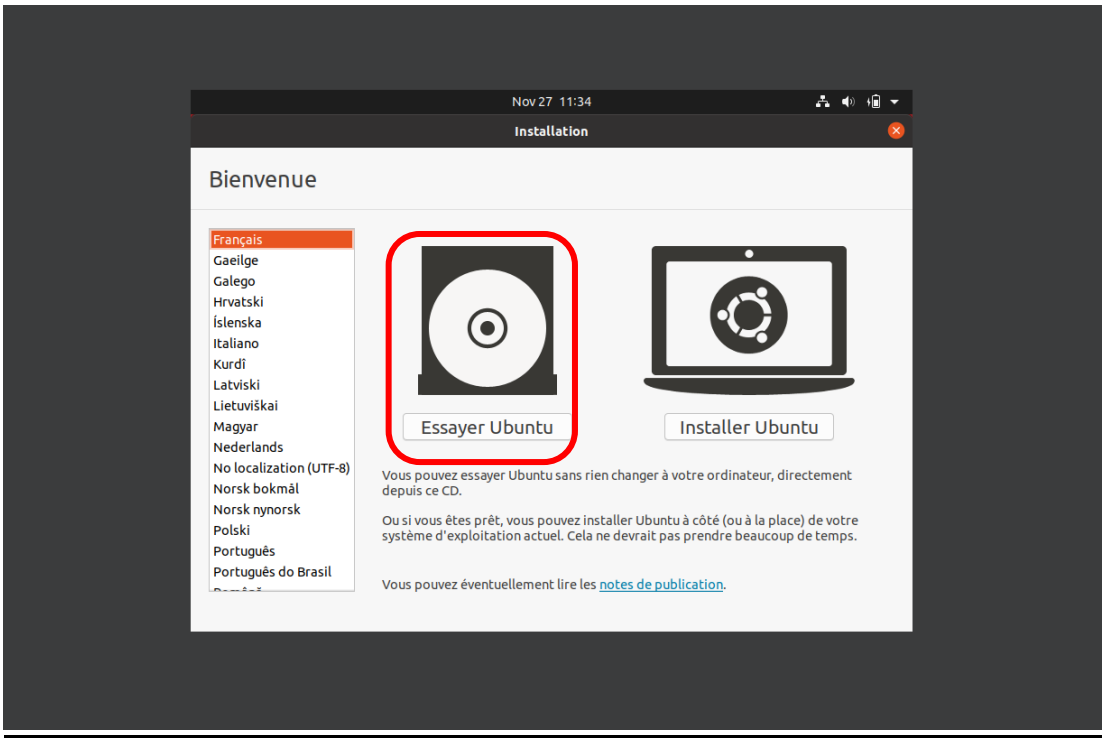


Arrivez sur l'écran d'accueil de Virtual box, vous cliquez sur les 3 traits à côté de votre machine qui correspond au paramètre de celle-ci.



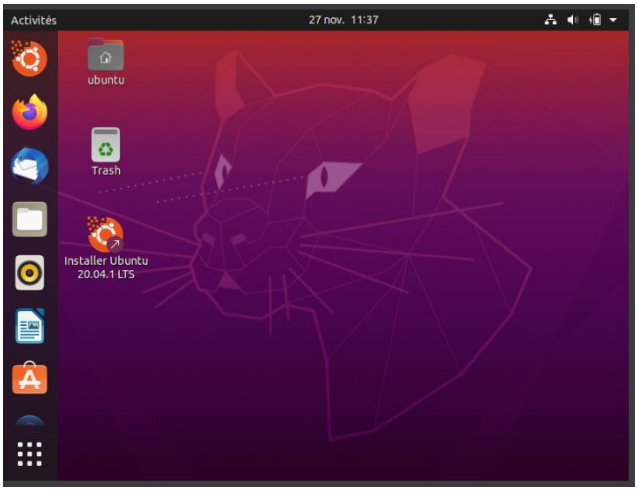
Ensuite, Vous vous rendez dans l'onglet système puis ordre d'amorçage pour faire en sorte que le disque SATA se lance avant le disque dur ou Windows est rangé.

Ce qui permettra d’arriver ici :



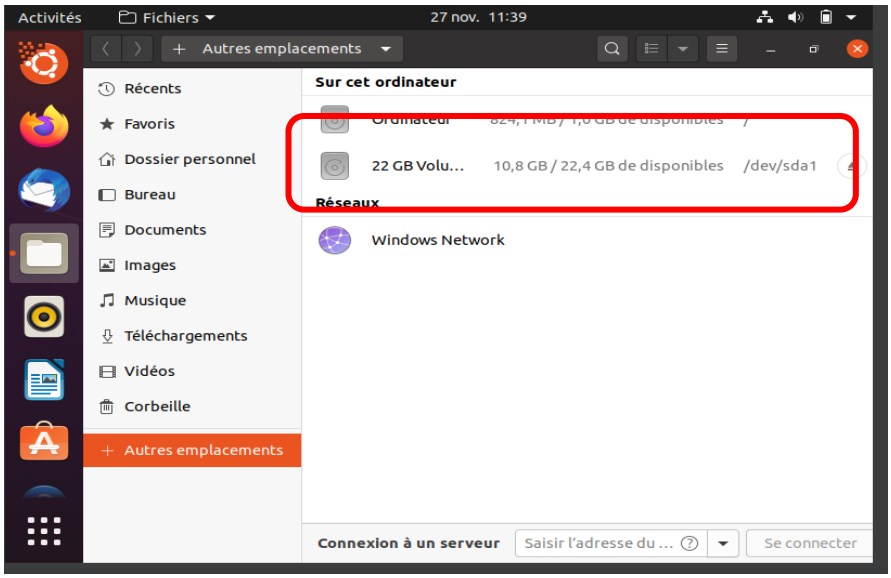
Vous cliquez sur « Try Ubuntu » pour accéder au données mise dans Windows comme le fichier « toto.txt » créer au paravant.

Warning : si au contraire vous cliquez sur Installer Ubuntu, toutes les données seront écrasées puisque Ubuntu se téléchargera sur l’espace alloué à Windows.

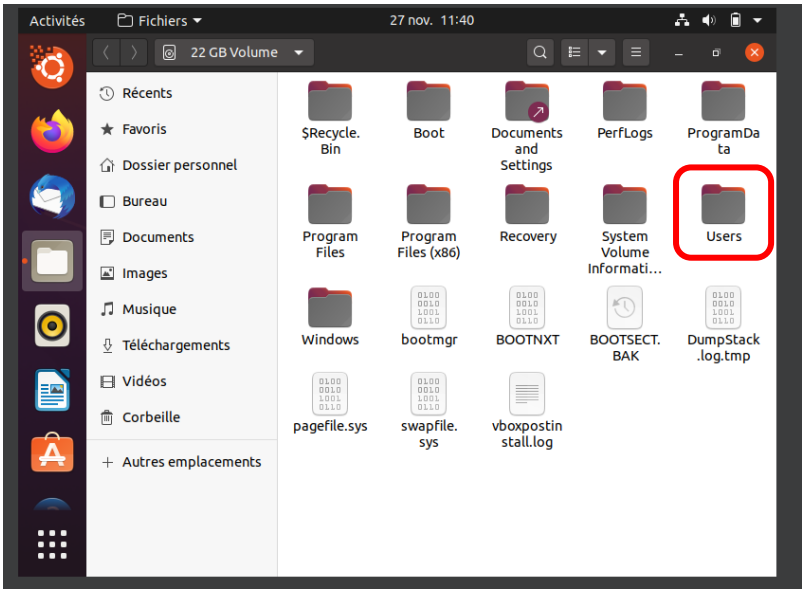


Cela étant fait vous arriver sur le bureau de Ubuntu. Une fois ici sélectionné « fichier » dans le menu déroulant à gauche de l’écran.

Après sélectionné « autres emplacement » puisque le dossier recherché est dans le volume alloué.



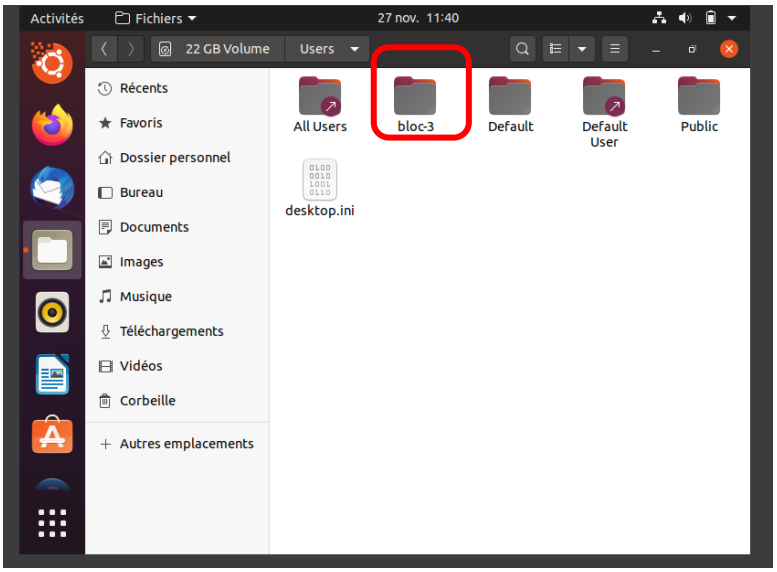
Donc sélectionné « 22 GB volume »

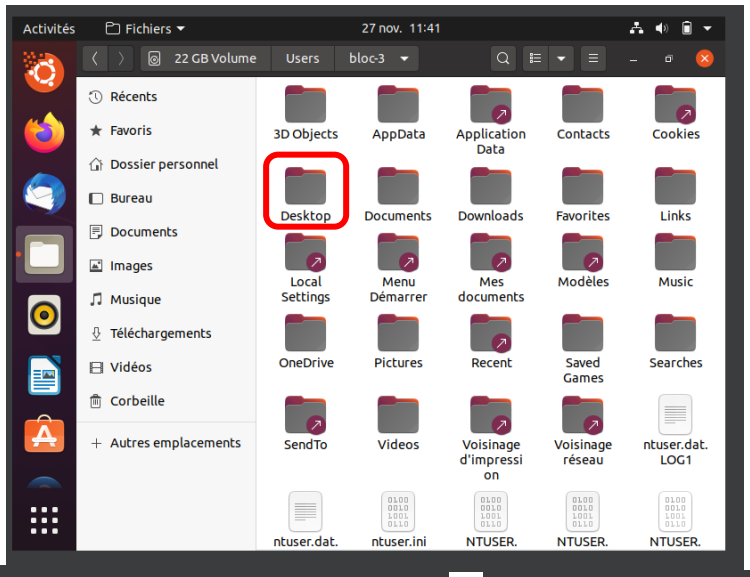


Voici tous les fichiers dont a besoin Windows et sélectionné « Users » puisqu'encore une fois le fichier qu'on recherche dans un utilisateur.

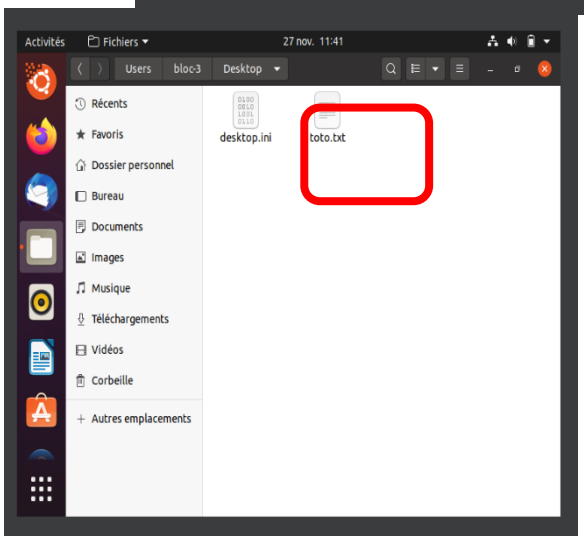
Une fois dans « users », sélectionné

Le fichier qui correspond au nom de la session ou est le fichier recherché.

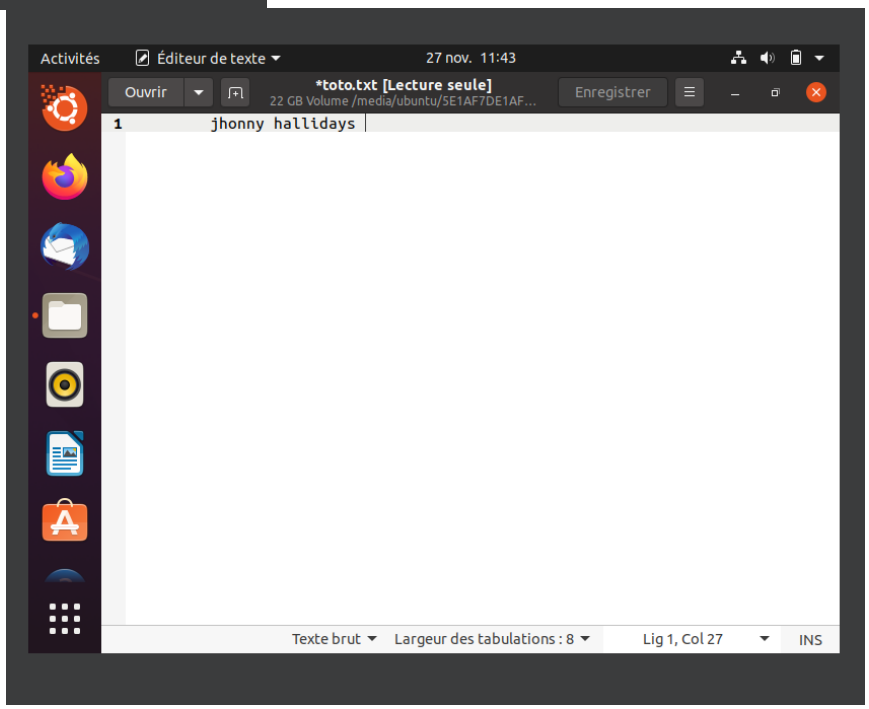




Une fois rentrée dans la session cherche la ou est rangé le fichier que vous cherchez. Pour ma part, il est dans le bureau donc dans le « desktop ».
Ce qui nous fait arriver la ou le fichier est rangé, nous pouvons l'ouvrir et regardé ce qui est marque dedans

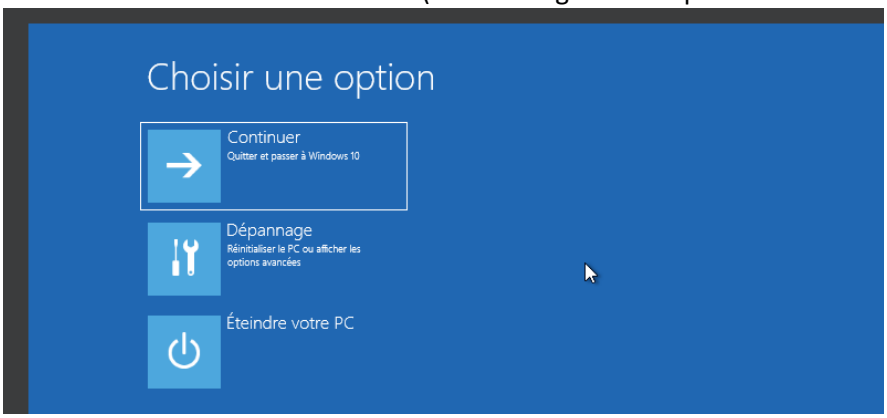


Je n'ai pas fait cette méthode mais pour moi la méthode qui se rapproche le plus de la vidéo d'introduction est la méthode 1 avec la clé USB.



Maintenant essayons une méthode pour changer le mot de passe :

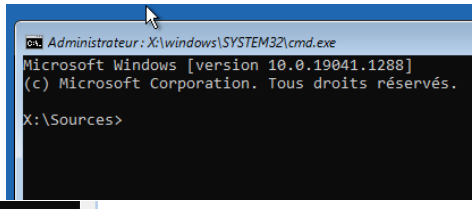
Revenons sur l'interface Windows. (en rechangeant l'iso par l'iso Windows)

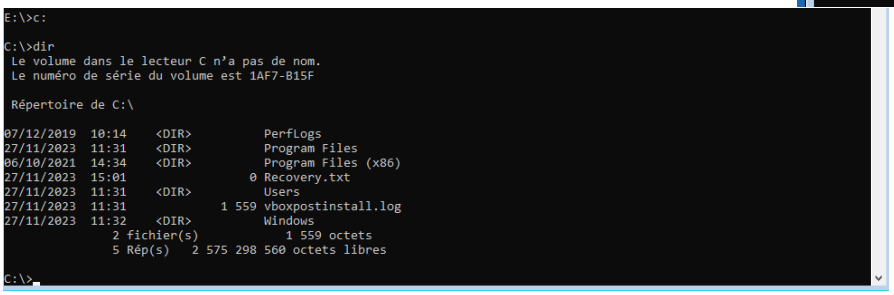


pour continuer , il faut lancer l'invite de commande là où j'ai rencontré quelque difficulté a le lancé puisqu'un mot de passe était demande (mot de passe que ne sommes censé ne pas connaitre)

(Refaire des captures intermédiaires).

Une fois dans l'invite de commande comme sur la photo ci-contre :



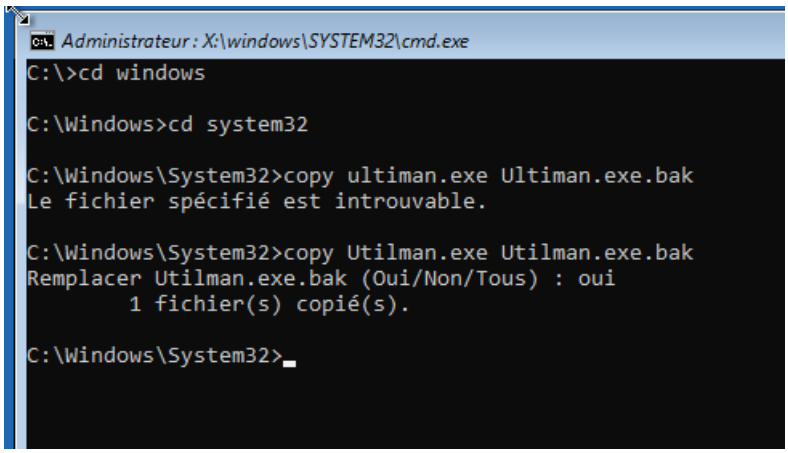


-Rendez-vous dans le lecteur de lettre grâce à la commande **c :**

-Utilisez la commande **cd Windows** et **cd system32**

(Qui servent à se déplacer dans les fichiers.)

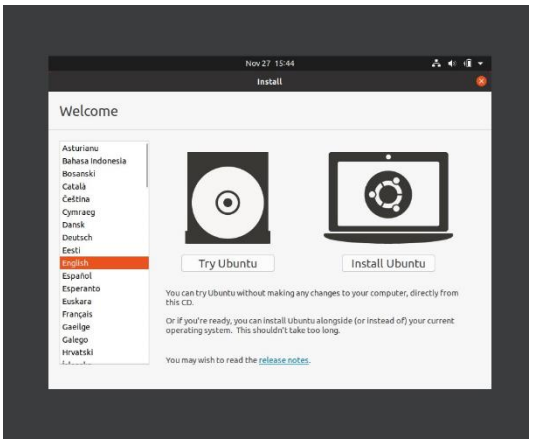
-Ensuite nous créons une sauvegarde de fichier **Utilman.exe** que l'on restaurera après la réinitialisation du mot de passe.

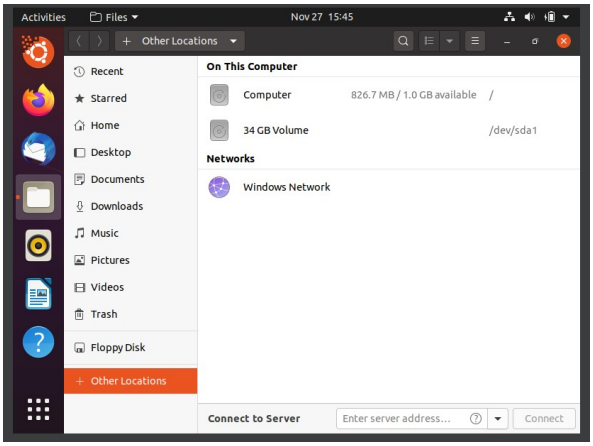


Ensuite il faut redémarrer le pc. Il faut en théorie ouvrir l'invite de commande avec Windows + u mais en réalité car Windows defender nous à chopper et à bloquer le pseudo virus donc la suite du tp se feras sous Windows 7.

Maintenant avec Windows 7 :

Mettez un ISO Ubuntu comme tout à l'heure pour aller voir le fichier « toto.exe »

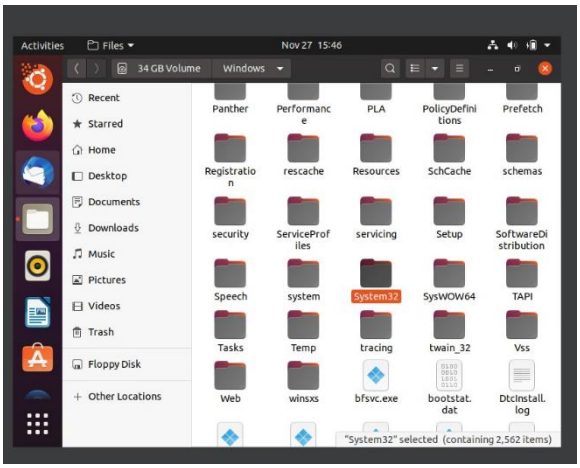




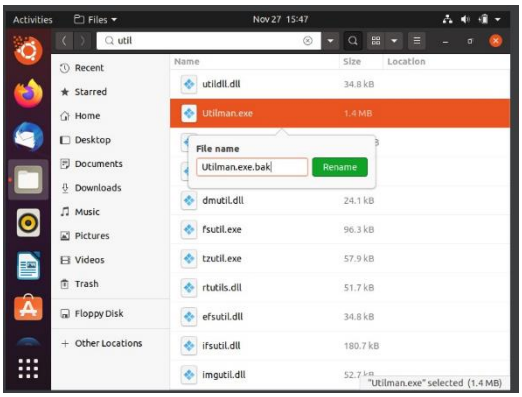
Comme avant appuyer sur « Try Ubuntu ».

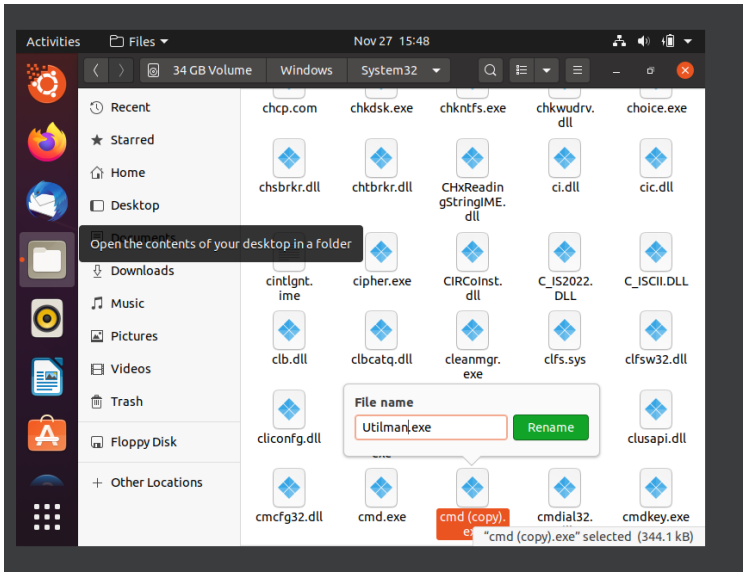
Recherche de fichier

Ensuite : rendons-nous dans le fichier « Windows », ensuite chercher le fichier « system 32 »

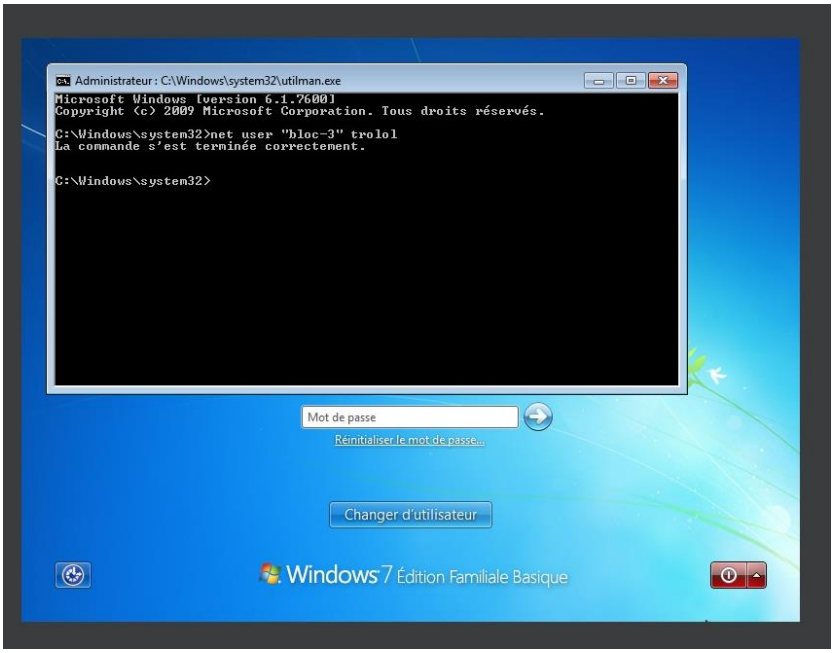


Une fois dans le fichier « system32 » on cherche le fichier on renomme le fichier « utilman.exe » par « utilman.exe.bak »



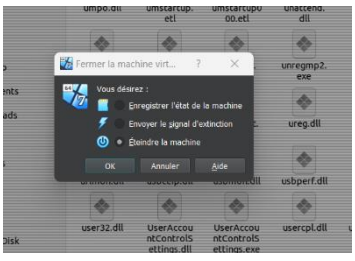


On copie le cmd pour avoir les droits administrateurs et le renomme en « utilman.exe »



Après ouvrez le terminal utiliser la commande : **net users « nom_de_votre_utilisateurs » avec le nouveau mot de passe après**

Ensuite on redémarre la VM sous Windows



Et on rentre le nouveau mot de passe. Une fois accéder à la session nous voyons que la manipulation à fonctionner.

La faille que l'on vient de découvrir qui est valable jusque normalement Windows 10 (pas à 100% si Windows Defender détecte que l'on a modifier le fichier « utilman.exe » qui détecté une anomalie et nous bloques) mais en revanche c'est une faille qui est exploite et très dangereuses mais Windows est comme bloque puisque c'est un fichier extrêmement important pour les personnes **mal-voyantes ou en situations de handicap** etc...

Cette faille permet quand même de remplacer le mot de passe d'un pc, donc qui est quand même très gênantes.

Windows a cependant pris les devants avec **Windows 11** en bloquant ce fichier mais malheureusement pour eux des fichiers comme celui-ci existe par **centaines** donc malgré cette faille règle les autres seront toujours exploitable par les mêmes **procédures** (explique au-dessus)

Plusieurs solutions possibles mais seulement pour gagner un peu plus de temps **: ajouter un mot de passe BIOS** (possible à retirer aussi mais fait perdre du temps)

Et en second un peu plus sur est de **chiffre**r les **documents fichiers répertoire** dans l'ensemble plus les choses sont chiffrés mieux seras protèges le PC.

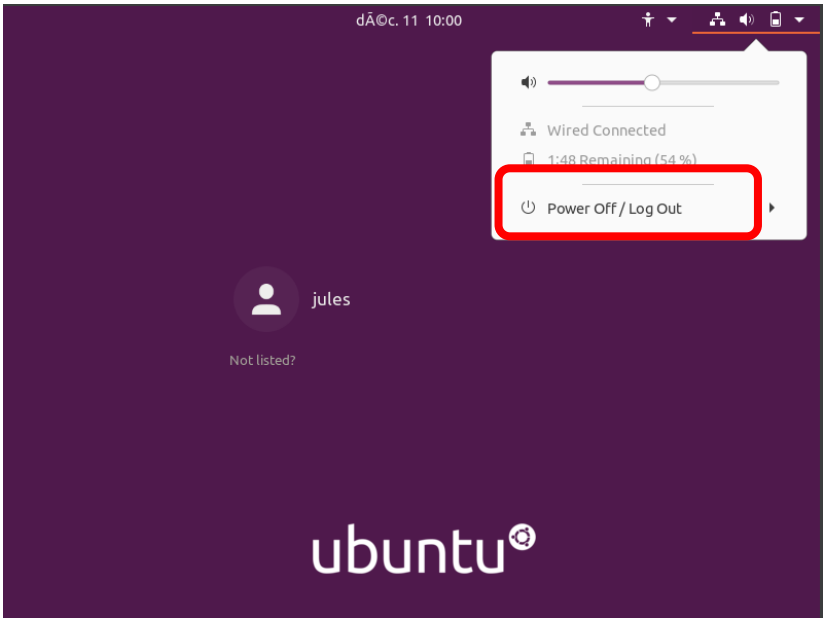
Une autre chose très simple crée un autre **compte** sur le **pc** et ne pas utiliser le **compte administrateur** du pc puisqu'avec un compte administrateur tout est possible sur le pc notamment cette démarche alors qu'avec un **compte standard** cette procédure n'est pas possible.

Dernière solution, utiliser un **bitlogger** pour réduire au maximum l'accès aux fichiers.

Maintenant nous allons voir si cela est possible sur Linux !!

Nous allons essayer avec la méthode Bin Bash :

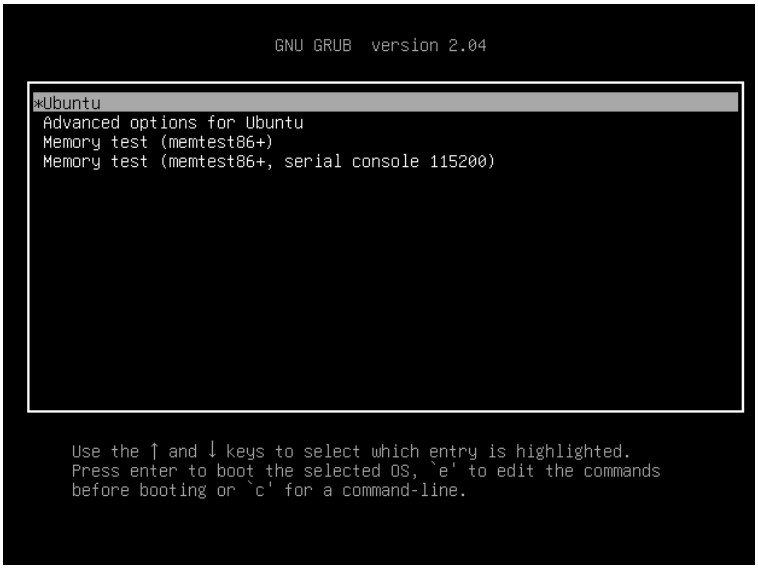
Etape 1 :



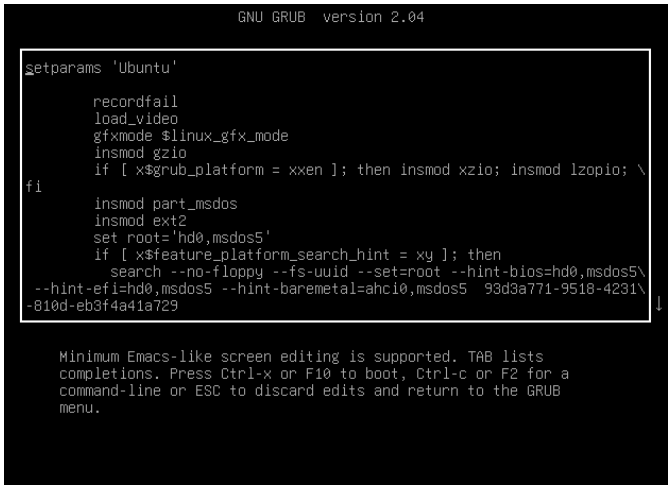
Premièrement redémarrer la VM qui est sous linux

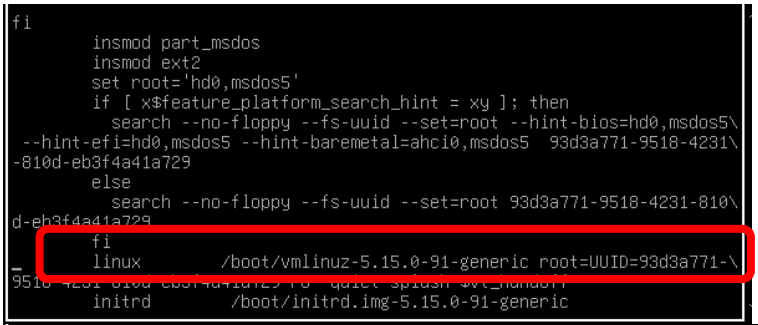
Pour voir le Menu GRUB appuyer sur la touche « MAJ » lors de l'ouverture de la machine

Une fois sur le Menu GRUB cliquez comme ci-dessus sur la touche « e » :

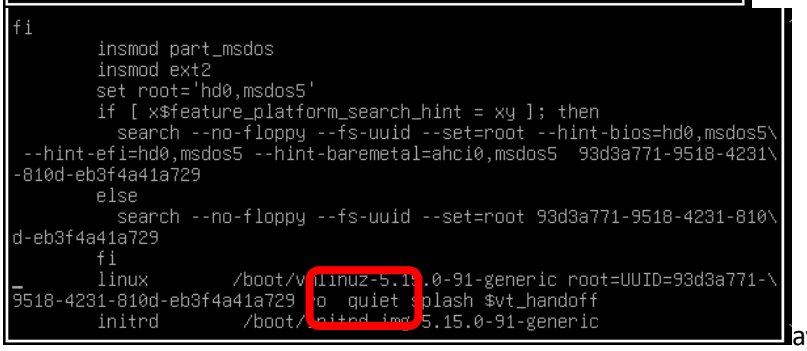


Ce qui nous amène à ce menu-là :

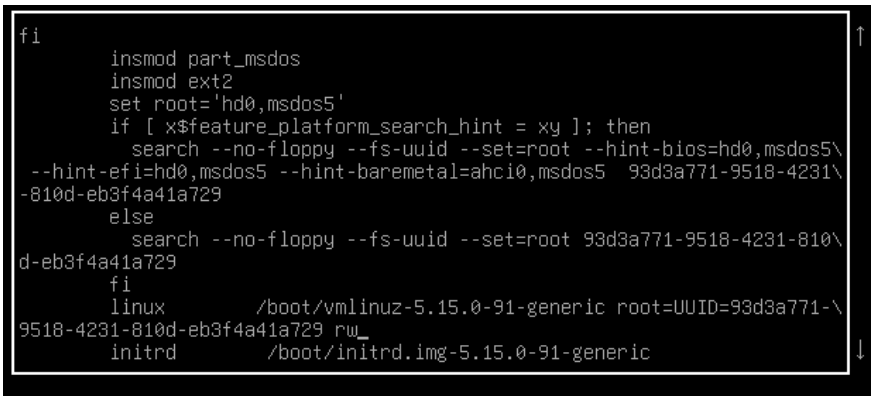




dans ce menu défiler jusque la ligne qui commence par « linux » :



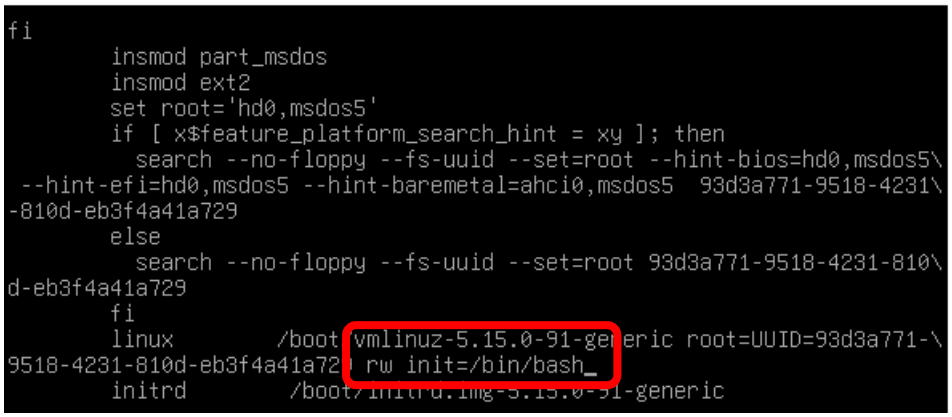
avancez jusque « ro quiet » :



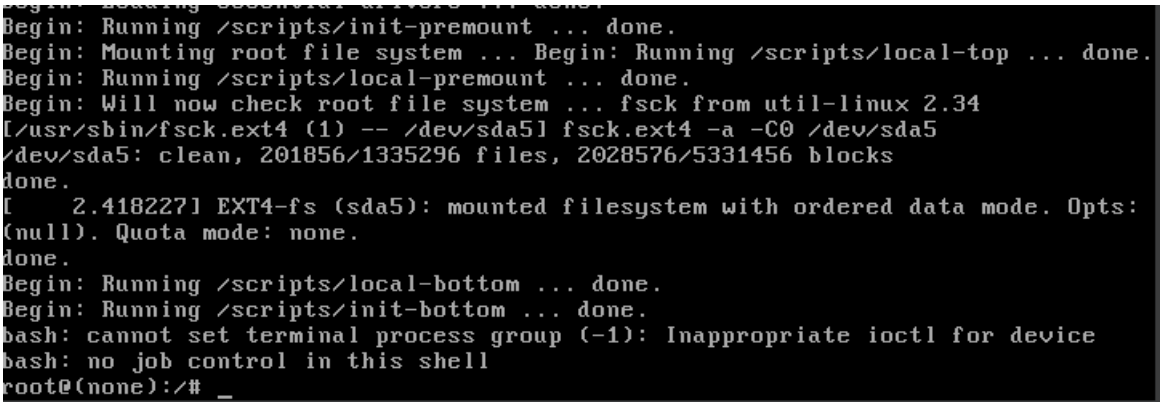
supprimez toute la ligne jusque « ro quiet » et remplacer le « ro » par « rw »

Ajoutez la commande suivante a la suite du « rw » :
« init=/bin/bash »

(Comme sur l'image ci-contre)

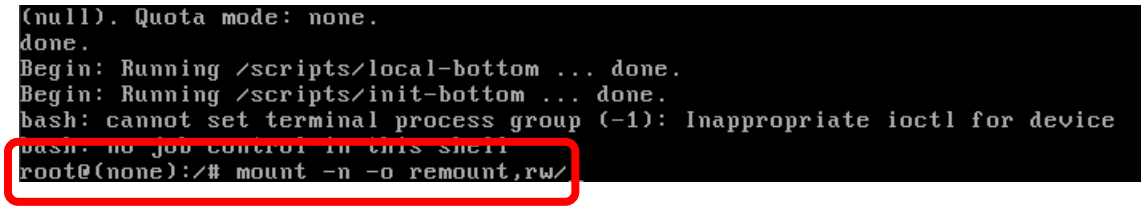


Appuyez ensuite sur « ctrl » + « x » ou « F10 » pour démarrer.



Une fois arrive dans l'invite de commande racine :

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



```
se [VirtualBox USB Tablet] on usb-0000:00:06.0-1/input0
[    2.259810] e1000 0000:00:03.0 eth0: (PCI:33MHz:32-bit) 08:00:27:bd:71:9d
[    2.261652] e1000 0000:00:03.0 eth0: Intel(R) PRO/1000 Network Connection
[    2.264563] 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, 201856/1335296 files, 2028576/5331456 blocks
done.
[    2.418227] 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/
mount: bad usage
Try 'mount --help' for more information.
root@(none):/# mount-n-o remount,rw /
mount-n-o: command not found
root@(none):/#  passwd jules
```

Si vous avez ce message d'erreur c'est que le système a déjà pris la décision de le faire (donc cette ligne est optionnelle si le système a déjà pris cette décision.

Tapez ensuite « passwd et votre nom d'utilisateurs »

```
Try 'mount --help' for more information.
root@(none):/# mount-n-o remount,rw /
root@(none):/#  passwd jules
New password:
```

Vous pouvez ensuite décider du nouveau Password pour ce compte utilisateurs

```
New password:
passwd: password updated successfully
root@(none):/#
```

Comme dis sur la capture d'écran : le password a étais changer avec succès.

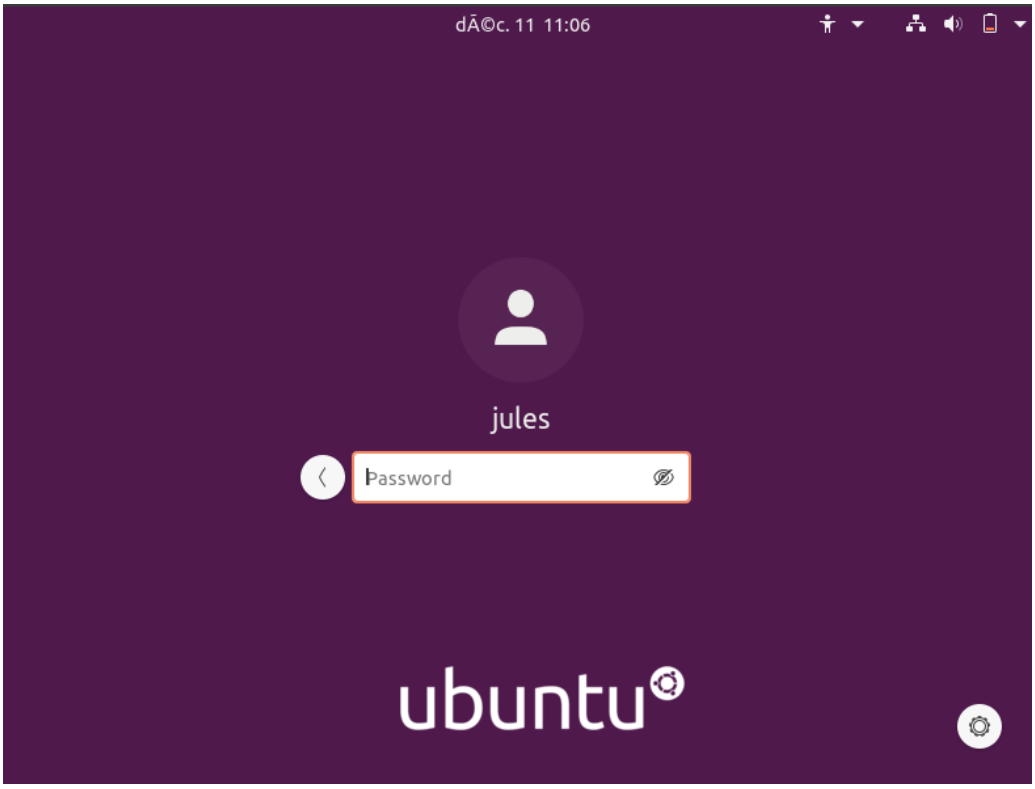
Pour quitter ce menu vous avez plusieurs options :

« Ctrl+D »ou « Ctrl+Alt+Suppr ».

```
[ 1025.115768] RSP: 002b:00007ffc5d438b68 EFLAGS: 00000246 ORIG_RAX: 00000000000
000e7
[ 1025.120597] RAX: ffffffffffffffda RBX: 00007f77910a38a0 RCX: 00007f7790f9e146
[ 1025.124316] RDX: 0000000000000000 RSI: 000000000000003c RDI: 0000000000000000
[ 1025.129155] RBP: 0000000000000000 R08: 00000000000000e7 R09: fffffffffffff80
[ 1025.132694] R10: 0000000000000005 R11: 0000000000000246 R12: 00007f77910a38a0
[ 1025.137341] R13: 0000000000000001 R14: 00007f77910ac2e8 R15: 0000000000000000
[ 1025.141082]  </TASK>
[ 1025.146527] Kernel Offset: 0x38a00000 from 0xffffffff81000000 (relocation ran
ge: 0xffffffff80000000-0xffffffffbfffffff)
[ 1025.152319] ---[ end Kernel panic - not syncing: Attempted to kill init! exit
code=0x00000000 ]---
```

```
[ 1025.115768] RSP: 002b:00007ffc5d438b68 EFLAGS: 00000246 ORIG_RAX: 00000000000
000e7
[ 1025.120597] RAX: ffffffffffffffda RBX: 00007f77910a38a0 RCX: 00007f7790f9e146
[ 1025.124316] RDX: 0000000000000000 RSI: 000000000000003c RDI: 0000000000000000
[ 1025.129155] RBP: 0000000000000000 R08: 00000000000000e7 R09: fffffffffffffff80
[ 1025.132694] R10: 0000000000000005 R11: 0000000000000246 R12: 00007f77910a38a0
[ 1025.137341] R13: 0000000000000001 R14: 00007f77910ac2e8 R15: 0000000000000000
[ 1025.141082]  </TASK>
[ 1025.146527] Kernel Offset: 0x38a00000 from 0xffffffff81000000 (relocation ran
ge: 0xffffffff80000000-0xffffffffbfffffff)
[ 1025.152319] ---[ end Kernel panic - not syncing: Attempted to kill init! exit
code=0x00000000 ]---
```

Ensuite redémarrer avec le code « reboot-f » ou alors redémarrer la machine simplement



Vous pouvez ensuite essayer de rentrer le nouveau password pour savoir si la manipulation marcher.