TP Intrusion simple Windows – Bloc 3 – CHADHOULI EL-Anrif – 2023/2024 – Mewo

Objectif : découvrir l'intérêt de sécuriser correctement une machine sous Windows et savoir se protéger en se mettant à la place de l'attaquant.

Créer une VM Windows 10 avec VMware

1. **Lancer VMware** et cliquer sur *Create a New Virtual Machine*.
2. **Sélectionner l'ISO Windows 10**.
3. **Nommer la VM** et choisir l'emplacement.
4. **Configurer les ressources** : allouer 4 Go de RAM, 2 cœurs CPU, 60 Go de disque et choisir *NAT* ou *Bridged* pour le réseau.
5. **Finaliser** et démarrer la VM pour installer Windows 10.

J'ai créé un fichier texte « toto.txt » avec une parole d'une chanson une fois Windows 10 configurer

Boot Ubuntu sur la VM Windows

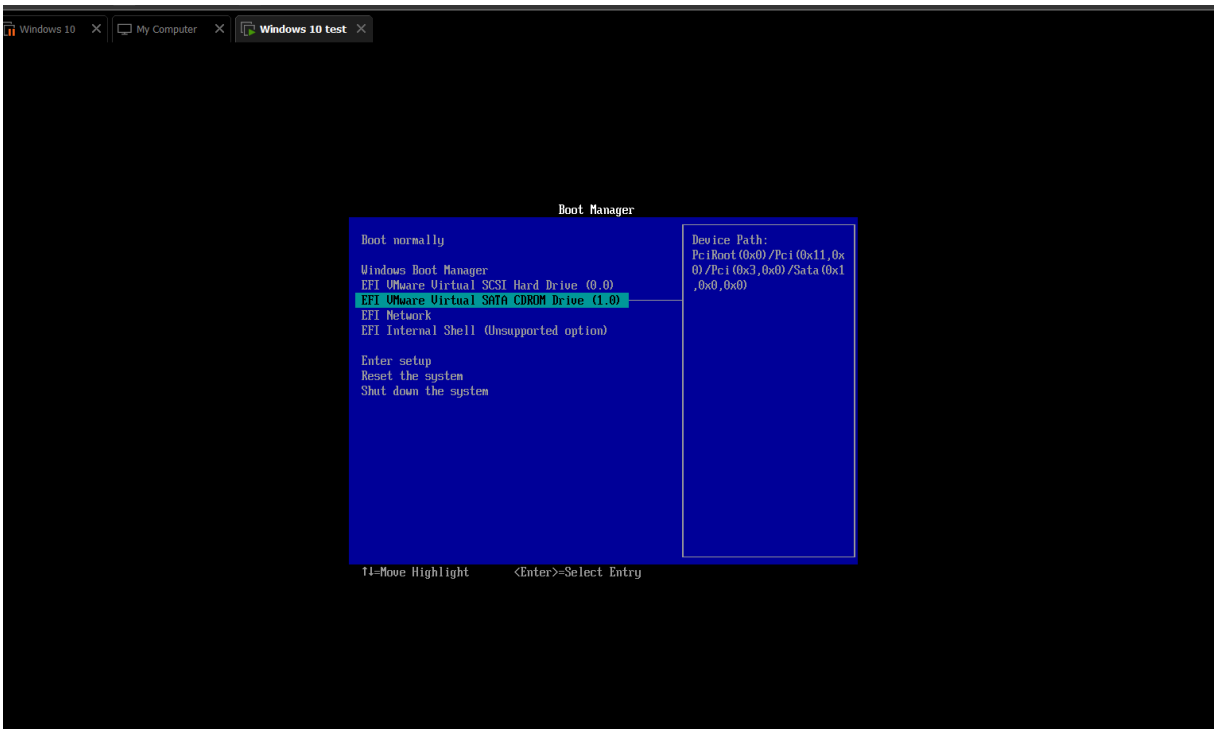
1. Ouvrez VMware, sélectionnez la VM, puis allez dans Edit Virtual Machine Settings.

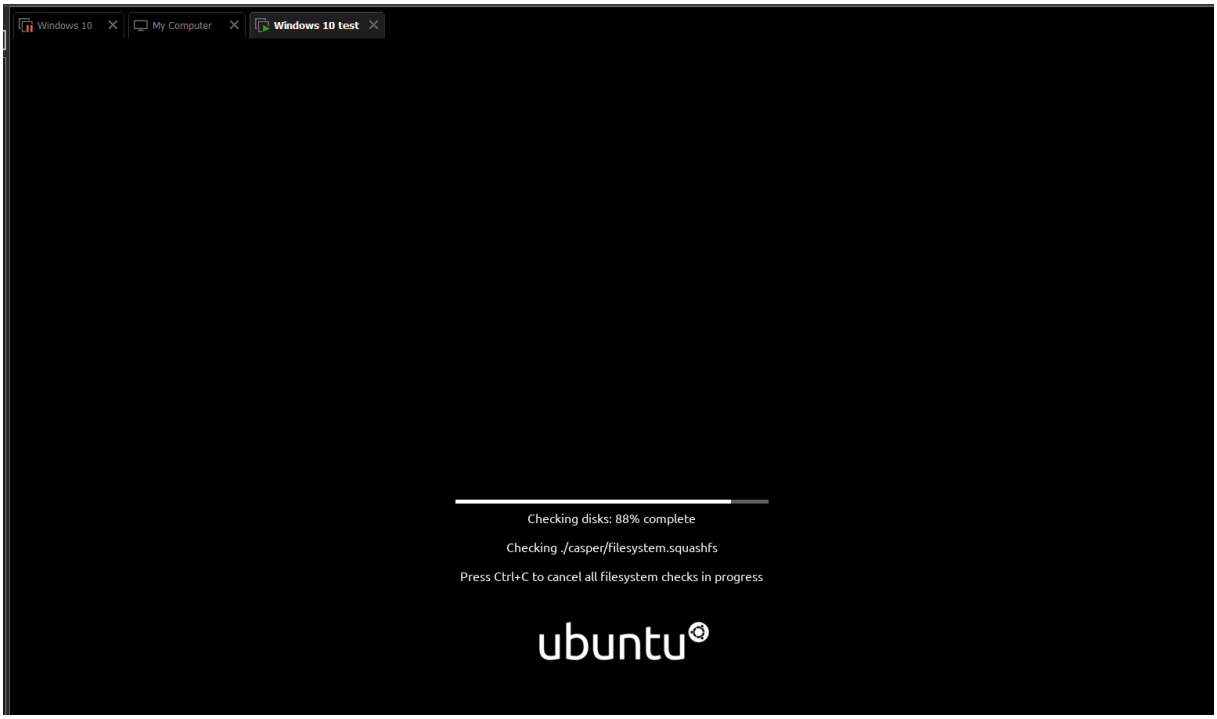
2. Dans CD/DVD (SATA), cochez Use ISO image file, cliquez sur Browse et sélectionnez l'ISO d'Ubuntu.

3. Assurez-vous que Connected at power on est coché, puis validez.

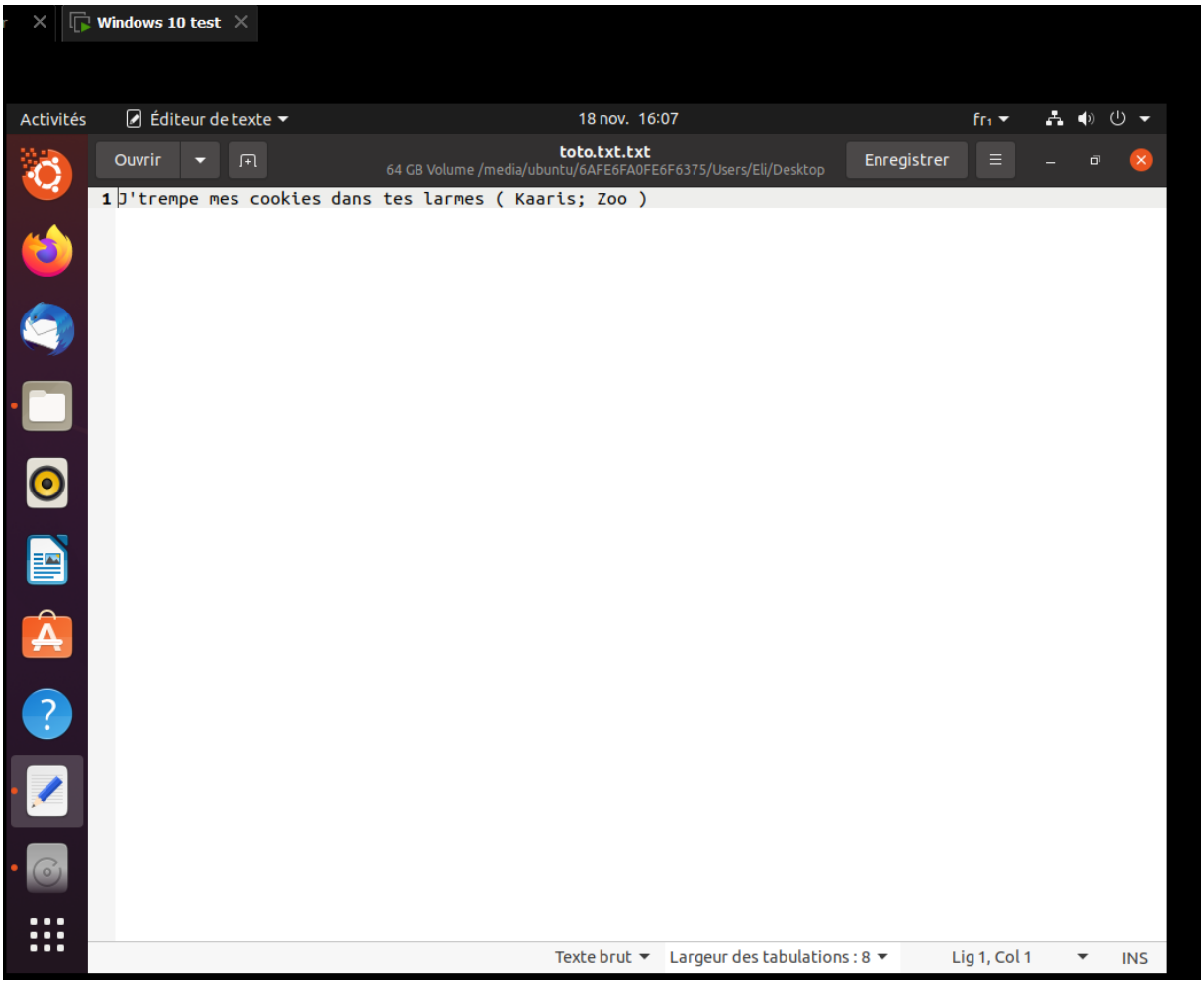
4. Démarrez la VM et appuyez sur Échap ou F2pour accéder au menu de démarrage.

5. Choisissez CD-ROM pour démarrer sur l'ISO.





Une fois sur Ubuntu, allez dans **Fichiers**, puis dans **Autres emplacements**. Vous verrez le disque dur de Windows 10 accessible. Il ne reste plus qu'à chercher directement le fichier *toto.txt*.



Conditions tout à fait possibles de lire et de modifier le fichier *toto.txt* depuis Ubuntu, à condition d'avoir les permissions nécessaires sur le disque Windows 10. Ubuntu permet d'accéder et de manipuler les fichiers stockés sur les partitions Windows (NTFS) grâce à son support intégré.

Réinitialisation d'un mot de passe Windows en Local

J'ai choisi la méthode numéro 2 : Utilman.exe

La méthode va modifier les outils d'accessibilité par l'invite de commande.

Pour ce faire voici les étapes :

- Démarrez Windows et accédez au BIOS/UEFI.
- Configurez le démarrage sur SATA ROM.
- Une fois dans l'outil de démarrage avancé, cliquez sur Continuer.
- En bas à gauche, cliquez sur Réparer l'ordinateur.
- Sélectionnez Options avancées, puis Invite de commandes.

Une fois dans l’invité de commandes :

Vérifiez que vous êtes dans le bon lecteur (C : dans mon cas).

Listez les fichiers pour confirmer que vous êtes bien à la racine du lecteur.

Accédez au dossier Windows puis au dossier System32.

Créez une copie de sauvegarde de Utilman.exe en le renommant en Utilman.exe.bak.

Tapez la commande pour remplacer Utilman.exe par cmd.exe :

C :

Dir

Cd Windows

Cd System32

Copy Utilman.exe Utilman.exe.bak

Sélectionné non

copy cmd.exe Utilman.exe

Remplacer le fichier

Cette commande copie cmd.exe et le renomme en Utilman.exe. Cela permet d'utiliser l'outil Invite de commandes à la place de l'outil d'accessibilité Utilman lors du démarrage de Windows.

Confirmez l'action en appuyant sur Oui lorsque vous y êtes invité.

Une fois la commande exécutée, redémarrez votre ordinateur.

Une fois arrive celui redémarrer appuyez sur la touche Windows + U pour afficher l’invité de commande :

Avec la commande suivante : Net user “Nom de la session“ nouveau mot de passe. Cliquez sur entrer et le mot de passe est modifié

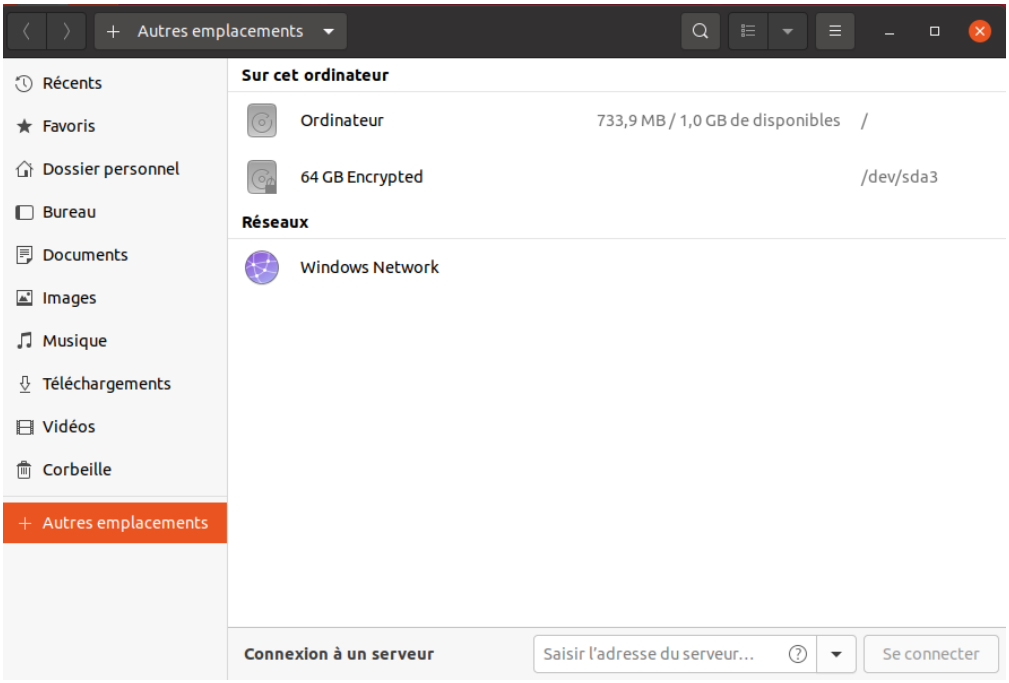
```
C:\Windows\system32>net user "eli" 12345
La commande s'est terminée correctement.


C:\Windows\system32>
```

En résumé, Windows n'est pas suffisamment sécurisé avec un simple mot de passe surtout avec un compte local. Il est facile de contourner ses protections, comme le montre l'exploitation de **utilman.exe**, ce qui permet à un attaquant de voler des données. Pour une véritable sécurité, il est essentiel de mettre en place des mesures supplémentaires, comme le chiffrement, l'authentification multifactorielle, et une gestion stricte des permissions.

Il y'a plusieurs solutions possibles :

BitLocker :

BitLocker chiffre votre disque dur de façon que son contenu reste protégé, même si vous tentez d'y accéder depuis un autre système d'exploitation. Par exemple, en démarrant sur une ISO d'Ubuntu, le disque dur restera chiffré et illisible, car BitLocker empêche tout accès non autorisé depuis un environnement externe. Cette sécurité garantit que seules les personnes disposant des clés de déchiffrement peuvent accéder aux données.



Une seconde option, Le **Secure boot** :

Qu'est-ce que le Secure Boot ?

Le Secure Boot est une fonctionnalité de sécurité qui empêche les logiciels malveillants (comme les rootkits) de s’exécuter au démarrage en autorisant uniquement les logiciels signés et approuvés.

Activer Secure Boot sur VMware :

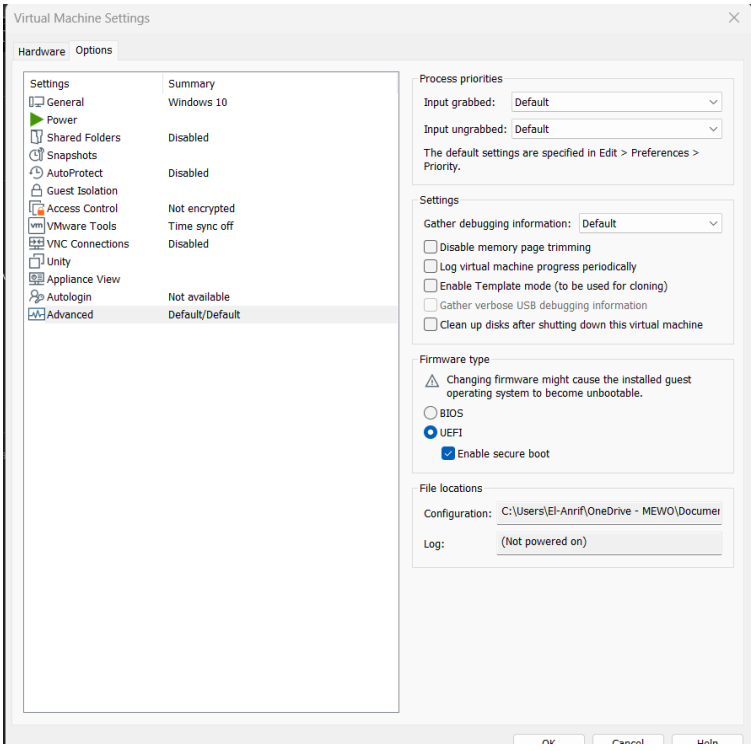
Éteignez la VM.

Dans VMware Workstation, allez dans les paramètres de la VM.

Sous Options > Firmware, sélectionnez UEFI (obligatoire).

Cochez Enable Secure Boot.

Redémarrez la VM pour appliquer les changements.

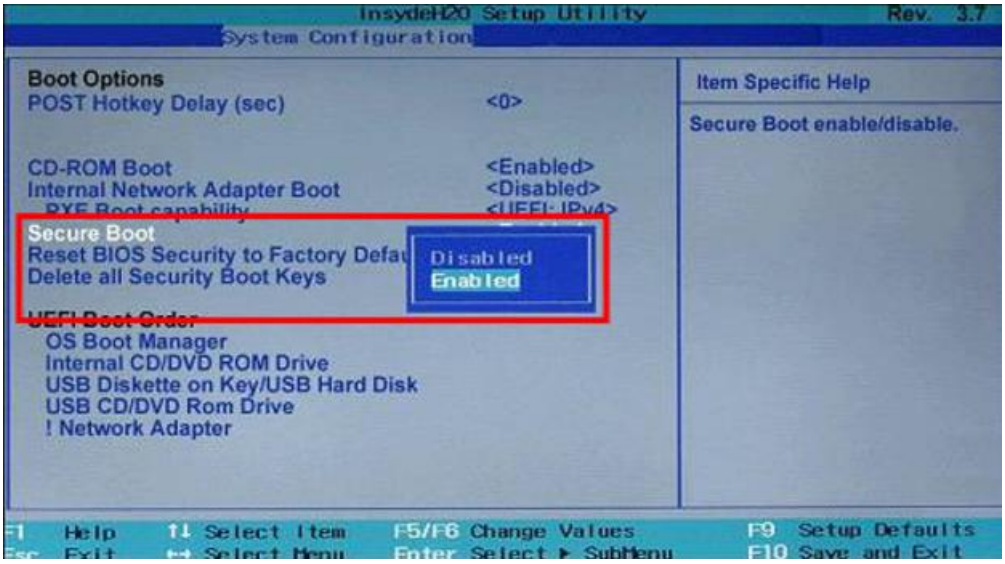


Activer Secure Boot sur une machine physique :

1. Redémarrez le PC et accédez au BIOS (touche comme **F2**, **Del** ou **F10** au démarrage).
2. Dans le BIOS, activez le **mode UEFI** dans les paramètres de démarrage.

3. Recherchez l'option **Secure Boot** dans les menus **Boot** ou **Security** et activez-la.
4. Sauvegardez et redémarrez.

Cela sécurise le démarrage en bloquant les logiciels non signés.



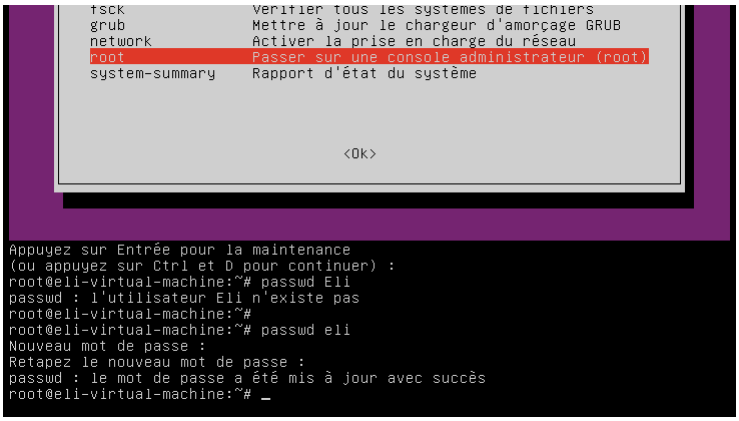
Source : https://lecrabeinfo.net/app/uploads/2021/09/secure-boot-enabled-pc-dell-uefi-6139ffc7ef619.png

Création une machine sous Noyau Linux pour essayer tester la sécurité.

Je vais utiliser l'environnement de production Ubuntu pour réaliser ce test :

Méthode 1 : Accéder via le Recovery Mode

1. **Redémarrez l'ordinateur** et maintenez **Shift** ou **Esc** pour afficher le menu GRUB.
2. Sélectionnez **Advanced options for Ubuntu**, puis une entrée avec **(recovery mode)**.
3. Choisissez **Root - Drop to root shell prompt** dans le menu.
4. Tapez la commande « passwd « nom d'utilisateur »
5. Tapez votre nouveau mot de passe



Conclusion :

Bien que Linux soit considéré comme un système très sécurisé, des configurations par défaut peuvent parfois permettre l'accès non autorisé en cas de besoin d'administrateur. Le mode de récupération permet d'accéder au système sans mot de passe, ce qui peut constituer une faille de sécurité si des mesures de protection ne sont pas en place

2 Méthodes pour renforcer la sécurité de Linux :

Protéger l'accès au menu GRUB avec un mot de passe

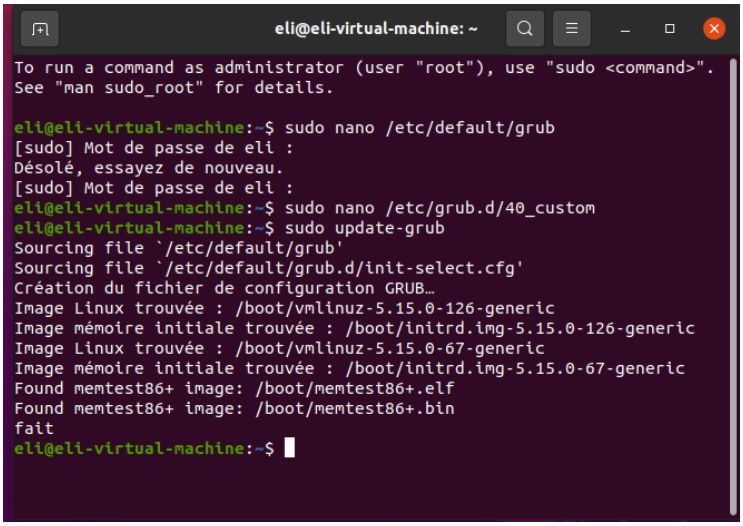
- L'accès au menu GRUB permet de modifier les paramètres de démarrage, y compris l'accès au mode de récupération, ce qui peut être une vulnérabilité si quelqu'un a un accès physique à la machine.
- Il faut ouvrir le Terminal est entre les commande suivante :
  sudo nano /etc/grub.d/40_custom

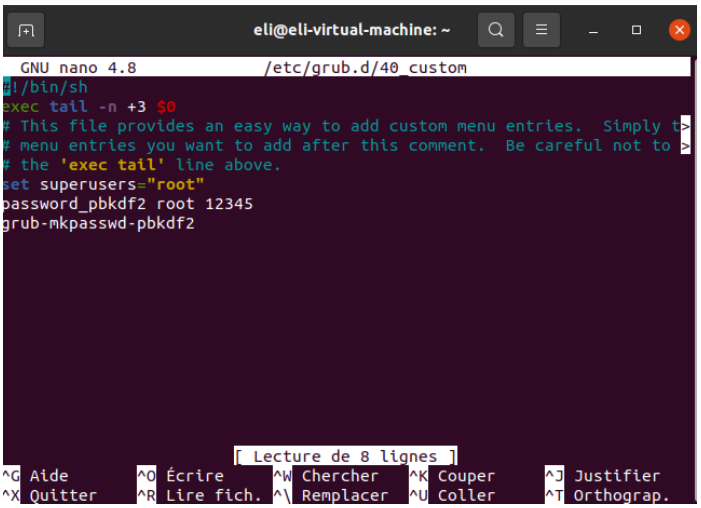
  Dans le nano j'ajoute la commande
  set superusers="root" password_pbkdf2 root <mot_de_passe_hashé>
  grub-mkpasswd-pbkdf2

  Appuyez sur CTRL + O pour enregistrer puis CTRL + x pour quitte le nano

  Tapez la commande suivante pour mettre à jour la GRUB
  sudo update-grub

À chaque démarrage, GRUB demandera un mot de passe avant de permettre l'accès à





l'option de récupération

J'ai rencontré des difficultés à appliquer correctement la méthode GRUB. Dès que j'enregistrais le script et redémarrais Ubuntu, le système me demandait un mot de passe et un identifiant que je ne connaissais pas. Peut-être que je n'ai pas bien compris comment mettre en œuvre cette méthode. Quoi qu'il en soit, je pense que c'est une bonne option pour protéger l'accès à GRUB.

La 2nd méthode est de chiffrer le disque dur

Le chiffrement des données sous Linux permet de protéger les informations en les rendant illisibles sans une clé ou un mot de passe. Avec un outil comme LUKS, on configure une phrase de passe pour sécuriser un disque ou une partition. Les données sont automatiquement chiffrées quand elles sont écrites et déchiffrées quand on les lit, tout cela en arrière-plan.

Ce système demande une authentification avant de pouvoir accéder aux données. On peut l'utiliser pour sécuriser tout le disque, une partition (comme `/home`) ou même des fichiers spécifiques avec des outils comme `gpg`. C'est une solution efficace pour éviter les intrusions et protéger ses données sensibles.

Je n'ai pas pu appliquer la méthode de chiffrement car je ne savais pas quelle partition de mon disque dur devait être chiffrée. Selon moi, cette méthode est une excellente solution pour protéger son environnement Linux contre les intrusions. Elle offre un haut niveau de sécurité en rendant les données inaccessibles sans la clé ou la phrase de passe appropriée.

La méthode utilisée dans la série Mr Robot est la méthode numéro 2 du TP

J'ai utilisé Chatgpt pour rédiger et reformuler mes pensées 😊.