Fiche technique
Piratage d'une machine linux

Sommaire

Objectifs :

- Comprendre les techniques qui permettent de prendre le contrôle d'une machine sous Linux.
- Savoir mettre en place une plateforme de découverte et de test.

Introduction

Dans ce dossier, nous allons voir comment prendre la main sur une machine Linux, sans connaître le mot de passe root ou de n'importe quel utilisateur.
Ces techniques sont utilisées (en temps normal) afin de réinitialiser des mots de passe perdus.
Nous allons chercher à changer le mot de passe de l'administrateur root.

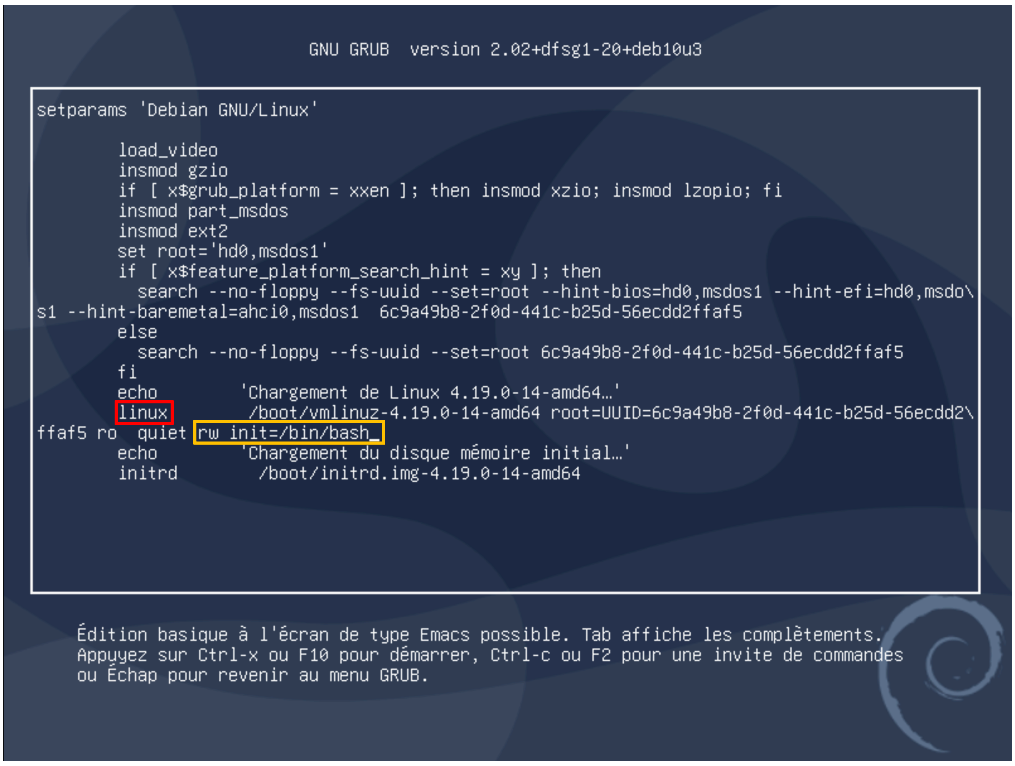
Entrer sans mot de passe avec le loader Grub

Cette première technique consiste à passer par le loader Grub afin de modifier le mot de passe de l'administrateur root.

Grub (**GR**and **U**nified **B**ootloader) est un logiciel permettant de charger un système d'exploitation. Il apparait dès le lancement de la machine et nous laisse le choix du système d'exploitation, mais il peut aussi nous permettre d'ouvrir une console en root sans connaître le mot de passe de ce dernier.

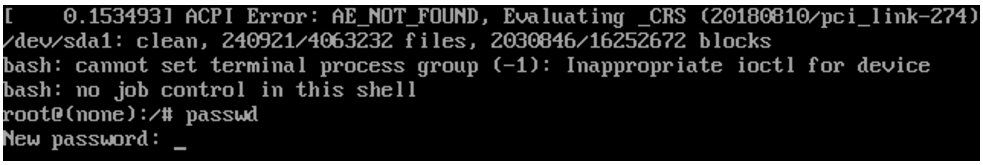
Pour ce faire, nous allons dans un premier temps commencer par démarrer l'ordinateur jusqu'à arriver sur cette fenêtre (le fameux GRUB) :

Dès que cette fenêtre s'affiche, il faut appuyer sur la touche [**e**] du clavier pour arriver sur l'éditeur d'option de démarrage.



Il faut alors chercher la ligne qui débute par **Linux**
Dans son état initial le paramètre de montage de la racine est ro = lecture seule (read only).
Nous allons alors ajouter un paramètre à la fin de cette ligne afin d'ajouter le paramètre **rw init=/bin/bash**
Grâce à ce paramètre, le paramètre de montage de la racine est passé en mode lecture et écriture (read and write).

Enfin, on appui sur les touches **ctrl+x** afin d'enregistrer et ouvrir une console en root, sans demander de mot de passe :



On peut maintenant modifier le mot de passe de root avec la commande **passwd**
(Ou **passwd <utilisateur>** pour changer le mot de passe de l'utilisateur).

A noter que la méthode la plus discrète reste de modifier le mot de passe d'un utilisateur de l'ordinateur et de l'ajouter dans la liste des sudoers.

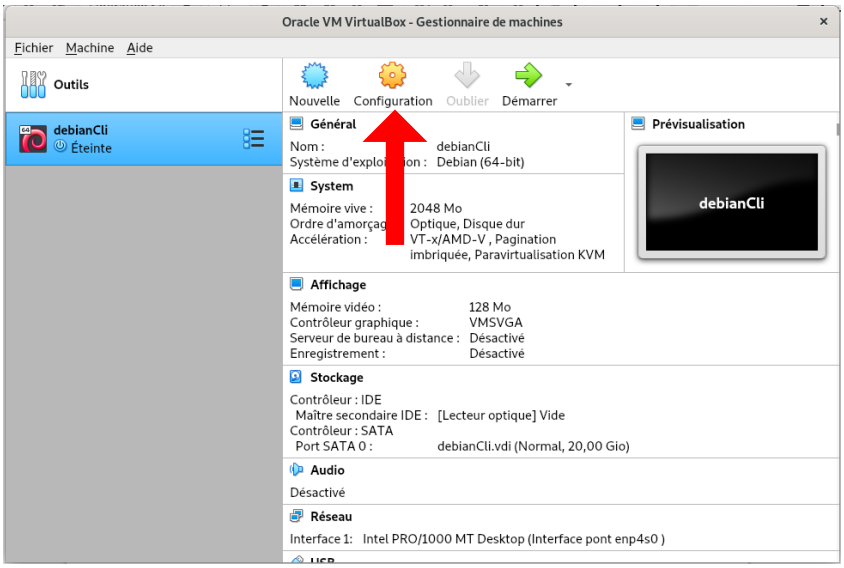
Entrer sans mot de passe avec le disque (ISO) d'installation

Cette deuxième méthode consiste à passer par le disque d'installation du système d'exploitation.

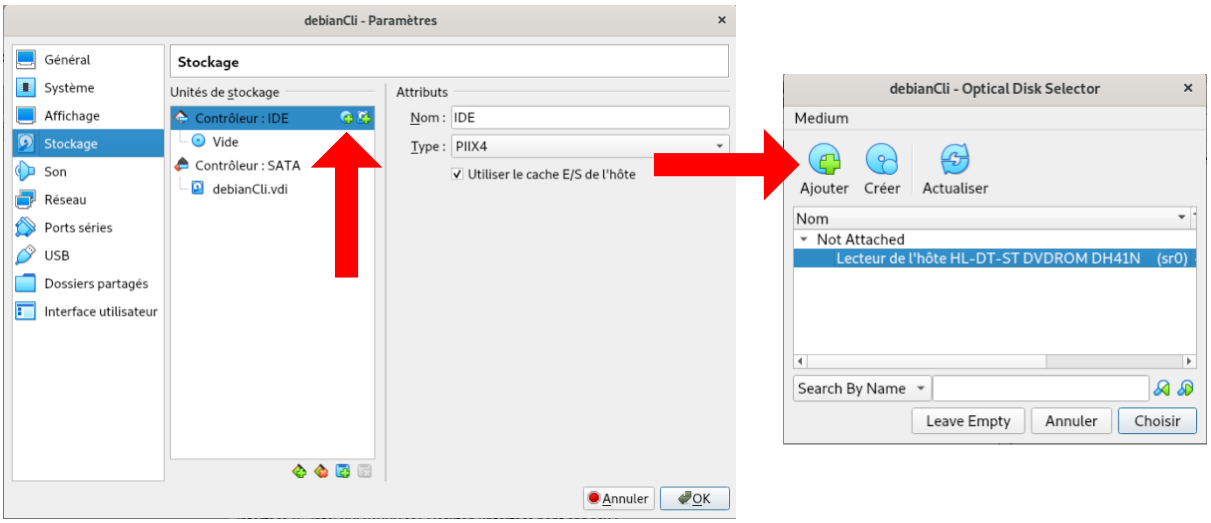
Pour ce faire, il faut configurer insérer le disque d'installation dans l'ordinateur et booter (démarrer) dessus.
Ici, nous allons voir comment booter sur l'image disque (ISO) avec VirtualBox.

1. Prérequis : ajout de l'ISO dans la machine virtuelle

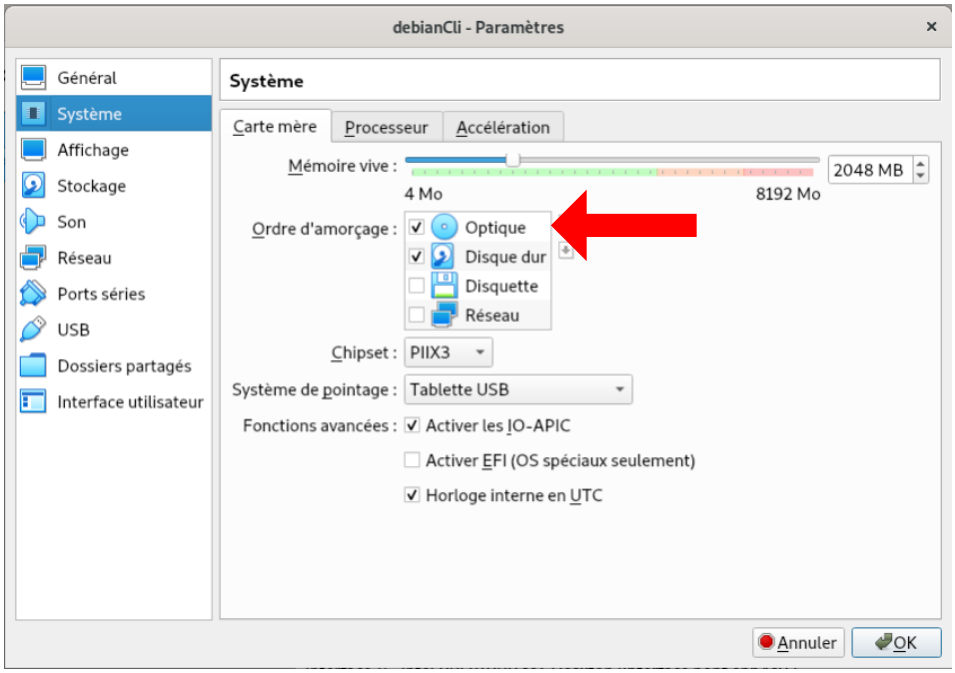
On commence par aller dans le menu de configuration de la machine virtuelle :



Dans le menu **stockage**, on ajoute l'image disque dans le contrôleur IDE (qui simule un lecteur de CD/DVD).



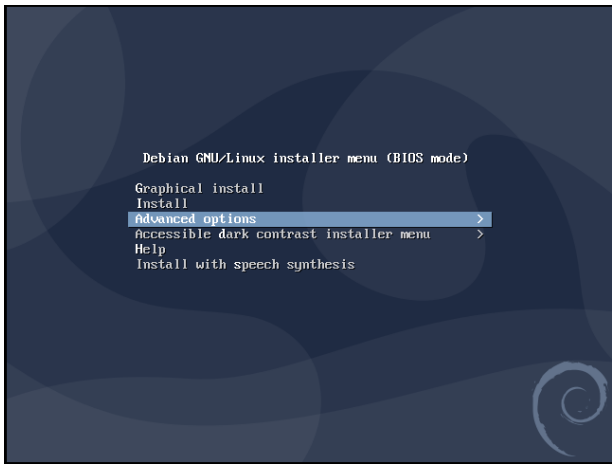
Dans le menu système, on s’assure que le lecteur de disque optique est premier dans l’ordre d’amorçage (ordre de démarrage).

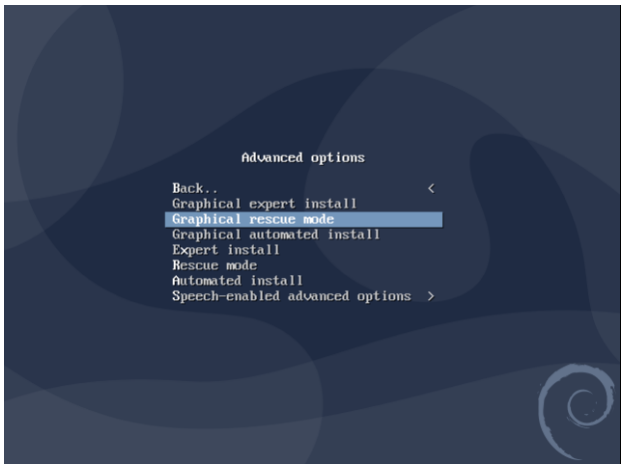


Nous pouvons désormais lancer notre machine virtuelle.

2. Rescue mode

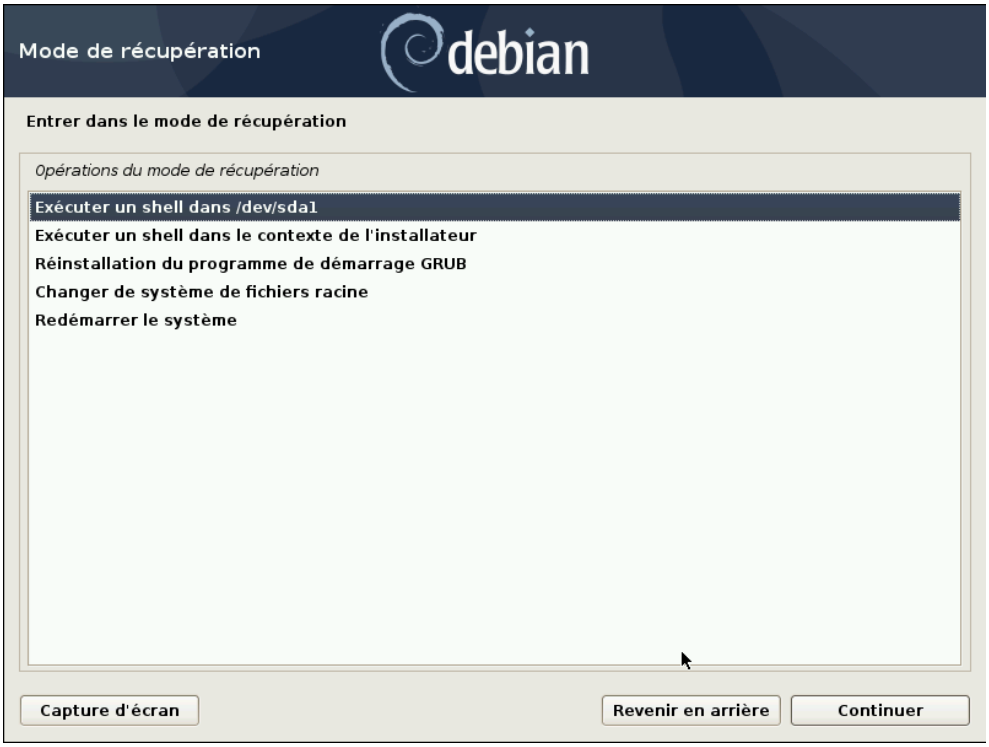
Une fois la machine virtuelle lancée, on va dans les options avancées, puis on lance le mode récupération (rescue mode) en mode graphique.





Après avoir choisi la langue du clavier et de l'interface, on choisit le périphérique **/dev/sda1** qui sera utilisé comme système de fichiers racine.

On exécute un **shell** (console) dans **/dev/sda1**.



Nous voilà dans une console, en root, sans avoir à saisir de mot passe.
Il ne reste qu'à modifier le mot de passe de l'administrateur root avec la commande **passwd** (ou **passwd [utilisateur]** pour changer le mot de passe d'un autre utilisateur).