

La sécurité Physique

Objectifs de cette section

Menaces physiques concernant la sécurité.

Actions à mener lorsqu'on a un accès physique à l'équipement.

Actions à mener lorsqu'on héberge notre système à distance.

Sécurisation du cloud.

Stratégies permettant d'atténuer les risques de sécurité physique.

Chiffrement des données ++

Concepts de sécurité physique

Sécurité physique = Sécurité de Linux

Si un attaquant a un accès physique à votre équipement (qu'il peut mettre les mains dessus) alors il pourra contourner la plupart des types de sécurité mis en place.

Possibilité d'accéder au « single user mode » au démarrage du système :

- Autorise tous les accès de manière non restreinte.

N'autoriser les accès physiques, uniquement lorsque c'est nécessaire.

Bonnes pratiques

Garder votre système le plus loin possible des attaquants.

Garder le datacenter et les ordinateurs dans des pièces verrouillées tout le temps.

- Actions potentiellement malveillantes
- Personnes non autorisées qui peuvent mettre sur power off les équipements

Garder la main sur les contrôles d'accès :

- Actualiser les droits du personnel en fonction des changements de postes et de responsabilités.
- Supprimer les comptes des personnes qui ont quitté l'entreprise.

Visiteurs

N'autoriser les accès que lorsqu'ils sont nécessaires.

Escorter toujours les visiteurs lorsqu'ils obtiennent un accès.

Garder un journal avec le nom de toutes les personnes qui ont accédé à la pièce contenant les serveurs.

VISITOR LOG

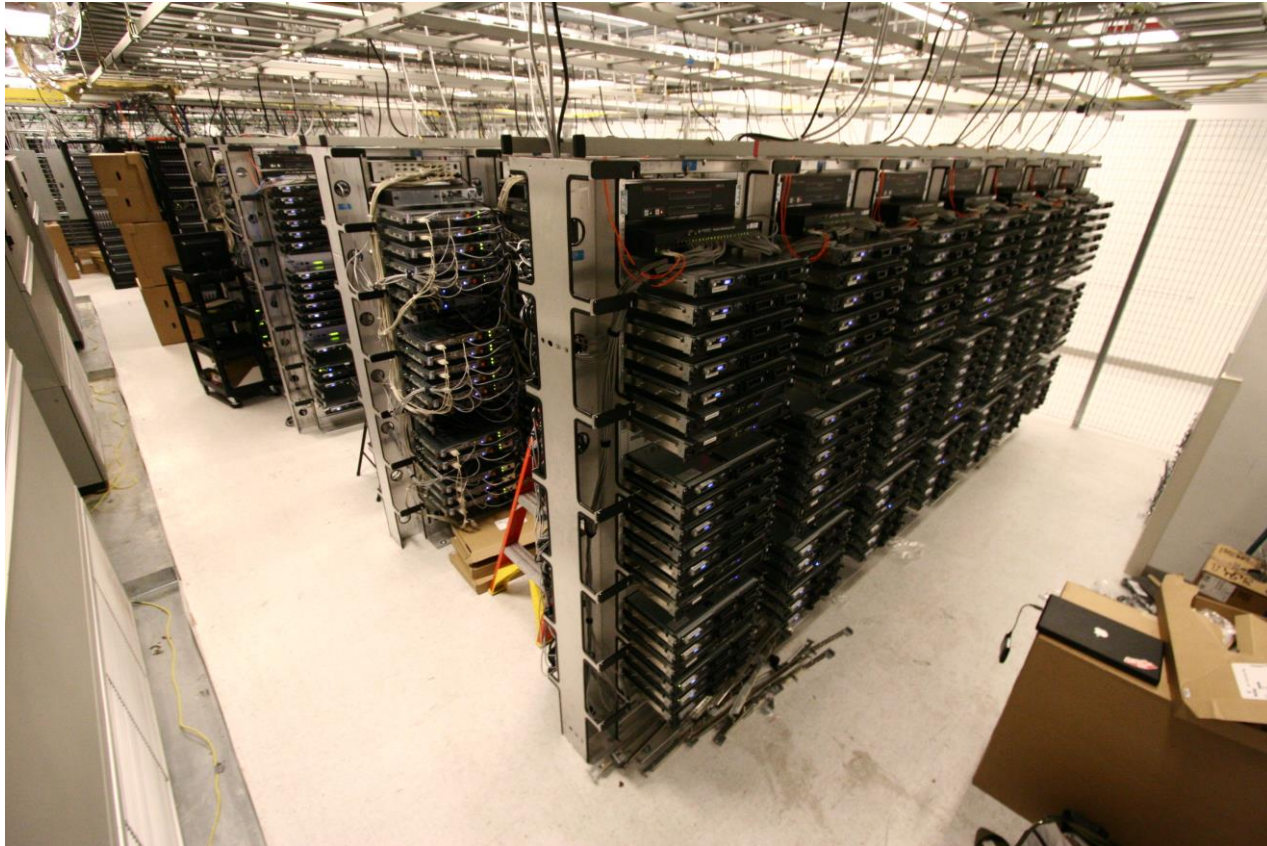
[illegible]

Sécurité d'un datacenter

Voici quelques règles de bonnes pratiques pour le contrôle d'accès au datacenter :

- Garde, portes et checkpoints.
- Système de vidéosurveillance.
- Système d'alarme.
- Système d'authentification par plusieurs facteurs.
- Badges.
- Vérification préalable des employés.

Sécurité d'un datacenter



Protéger Linux contre les attaques physiques

Obtenir l'accès à un système Linux

Démarrer le système en : « Single User Mode »

- Redémarrer l'équipement
- Taper « e » dans le grub
- Ecrire les lignes :
 - ro rescue
 - ro s
 - ro S
 - ro 1
 - ro systemd.unit=rescue.target

Mode Single User

Les nouvelles distributions Linux demandent tout de même un mot de passe pour l'utilisateur root, y compris en mode Single User.

Démonstration

Vidéo 11

Sécuriser le boot-loader

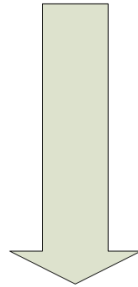
Vidéo 12

Chiffrement du disque

Pourquoi faire ?

Si vous ne voulez pas que quelqu'un puisse facilement lire ou altérer vos données sur votre système.

Bonjour je m'appelle Jordan



Fonction de Hash MD5

e2c8aa7930ba8e06078a9545492e0020

Le système d'exploitation nécessite des accès

Il faut faire en sorte qu'après avoir chiffré vos données, le système d'exploitation puisse toujours y accéder.

Déchiffrer les données avec un mot de passe ou un fichier contenant une clé (pouvant être protégé par un mot de passe).

Chiffrement du disque sur Linux

La commande : « **dm-crypt – device mapper crypt** » fournit un chiffrement transparent du disque.

- Vous pouvez y spécifier les fichiers que vous souhaitez chiffrer.
- Certains systèmes autorisent le chiffrement de fichiers racines.

LUKS (Linux Unified Key Setup)

Front-end pour la fonction dm-crypt.

Permet de chiffrer l'intégralité du disque.

Supporte les mots de passe multiples (si on a plusieurs utilisateurs)

Intéressant également pour le chiffrement des supports amovibles.

Utilisation de LUKS sur un nouvel équipement

Utiliser LUKS sur un nouvel équipement

Utiliser ce processus pour chiffrer des nouveaux blocks de données.

- Clé USB
- Partitions sur votre système

Suivre la procédure ci-après va supprimer l'ensemble des données sur la partition (ou la clé USB par exemple) que vous souhaitez chiffrer.

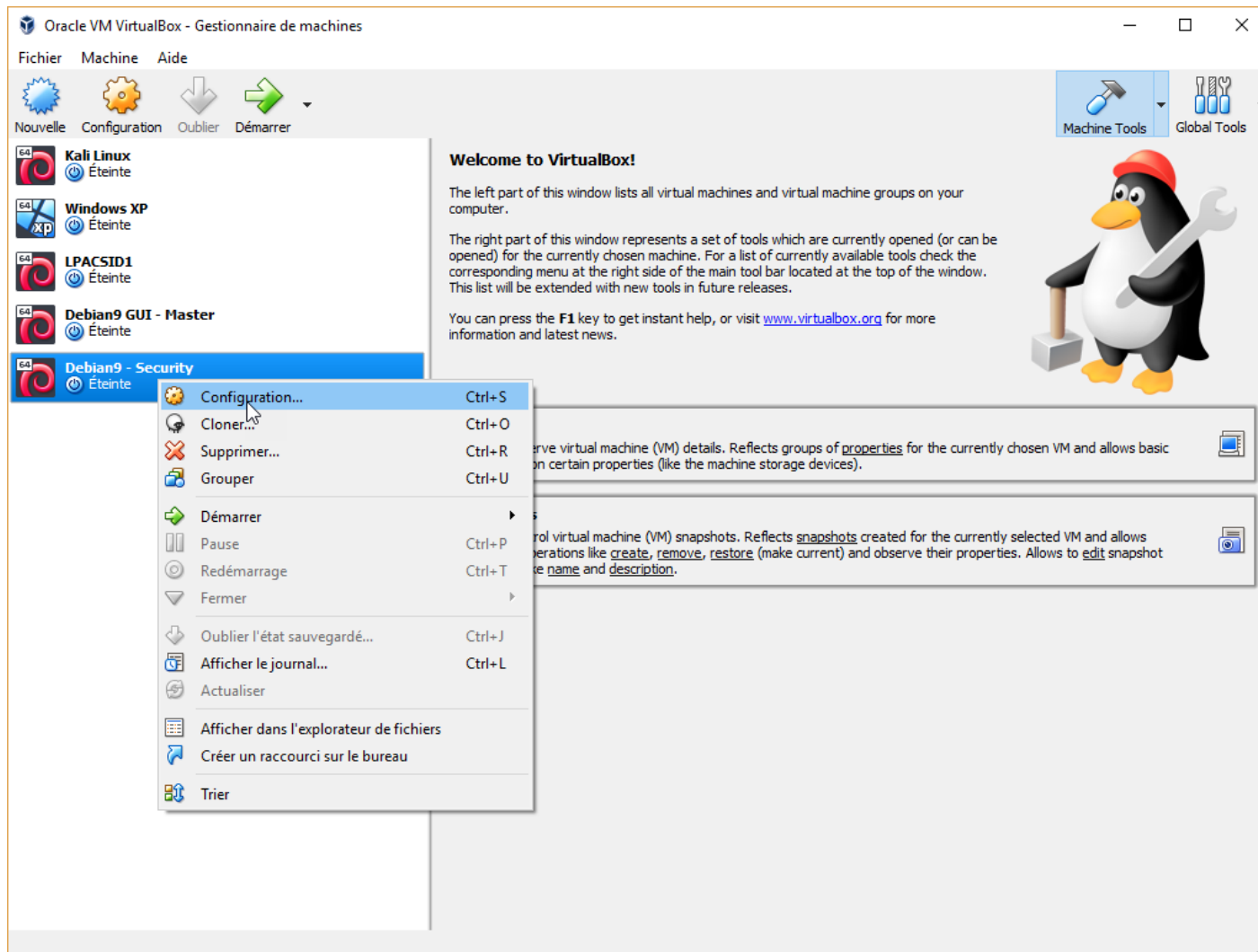
Procédure pour le TP

Section 3 – vidéo 14

Créer ou utiliser une machine virtuelle existante.

Ajouter un nouveau disque sur la VM.

Sur centos : `sudo fdisk -l | less`



- Général
- Système
- Affichage
- Stockage**
- Son
- Réseau
- Ports séries
- USB
- Dossiers partagés
- Interface utilisateur

Stockage

Storage Devices

- Contrôleur : IDE
 - Vide
- Contrôleur : SATA**
 - Debian9 - Security.vdi

Attributs

Nom : SATA

Type : AHCI

Nombre de ports : 1

☐ Utiliser le cache E/S de l'hôte

Ajoute un disque dur.

OK

Annuler

- Général
- Système
- Affichage
- Stockage**
- Son
- Réseau
- Ports séries
- USB
- Dossiers partagés
- Interface utilisateur

Stockage

Storage Devices

Contrôleur : IDE

Vide

Contrôleur : SATA

Disque dur virtuel

Attributs

Nom : SATA

Type : AHCI

VirtualBox - Question



Vous êtes sur le point d'ajouter un nouveau disque dur virtuel au contrôleur **SATA**.

Voulez-vous créer un nouveau fichier vide pour le contenu du disque ou bien en choisir un existant?

Créer un nouveau disque

Choisir un disque existant

Annuler



OK

Annuler



← Créer un disque dur virtuel

Type de fichier de disque dur

Choisissez le type de fichier que vous désirez utiliser pour le nouveau disque virtuel. Si vous n'avez pas besoin de l'utiliser avec d'autres logiciels de virtualisation vous pouvez laisser ce paramètre inchangé.

- ☒ VDI (Image Disque VirtualBox)
- ☐ VHD (Disque dur Virtuel)
- ☐ VMDK (Disque Virtual Machine)

Mode expert

Suivant >

Annuler

?×

← Créer un disque dur virtuel

Stockage sur disque dur physique

Veillez choisir si le nouveau fichier de disque dur virtuel doit croître au fur et à mesure (allocation dynamique) ou bien s'il doit être créé à sa taille maximale (taille fixe).

Un fichier de disque dur **alloué dynamiquement** n'utilisera d'espace sur votre disque dur physique qu'au fur et à mesure qu'il se remplira (jusqu'à une **taille fixe maximale**), **cependant il ne se réduira pas automatiquement lorsque de l'espace sur celui-ci sera libéré.**

Un fichier de disque dur à **taille fixe** sera plus long à créer sur certains systèmes mais sera souvent plus rapide à utiliser.

☒ Dynamiquement alloué

☐ Taille fixe

Suivant >

Annuler

?×

← Créer un disque dur virtuel

Emplacement du fichier et taille

Veuillez saisir un nom pour le nouveau fichier de disque dur virtuel dans la boîte ci-dessous ou cliquez sur l'icône dossier pour choisir un autre dossier dans lequel le créer.



Choisissez la taille du disque dur virtuel en mégaoctets. Cette taille est la limite de la quantité de données de fichiers qu'une machine virtuelle sera capable de stocker sur le disque dur.

4,00 Mio

2,00 Tio

8,00 Gio

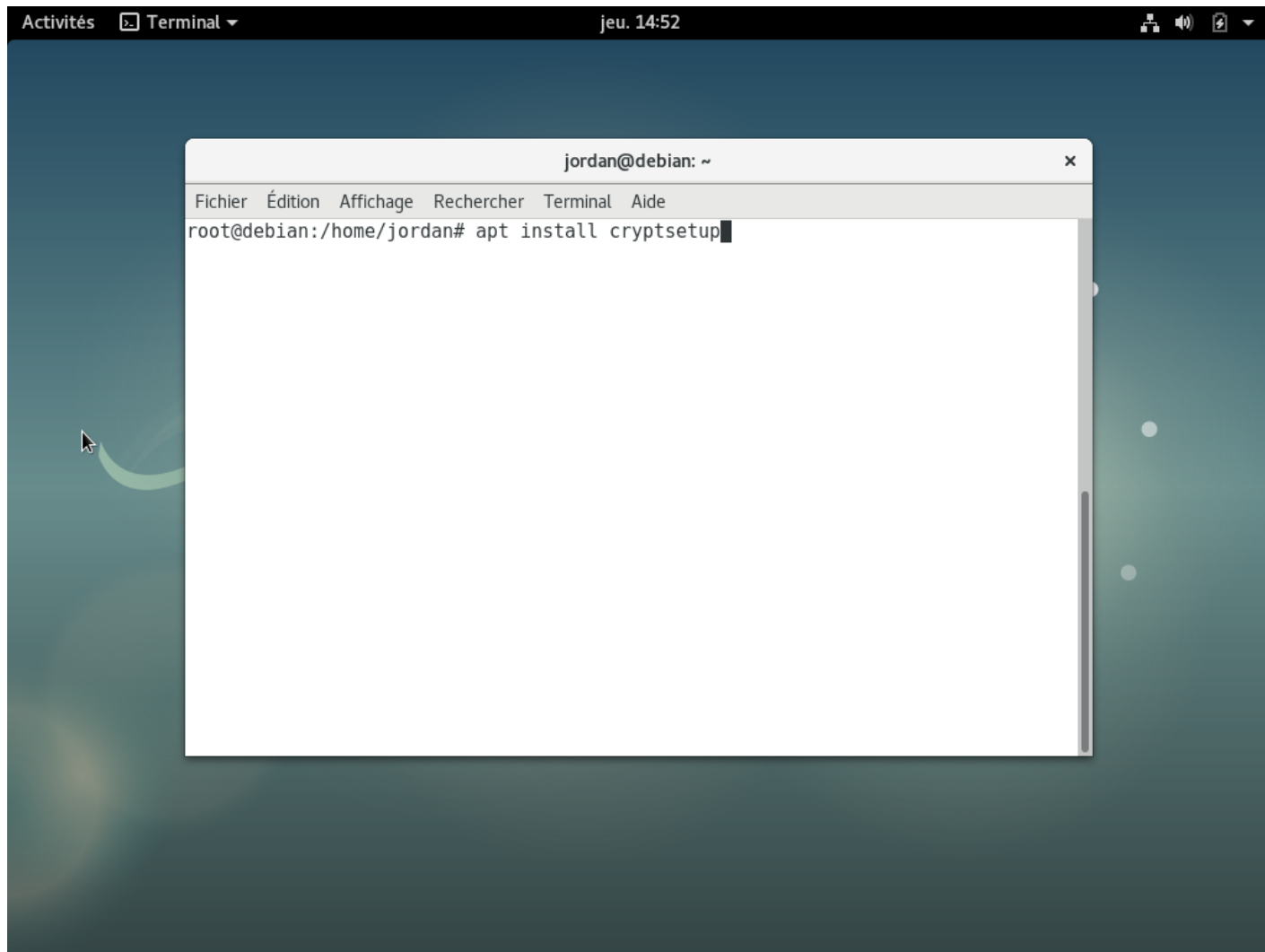
Créer

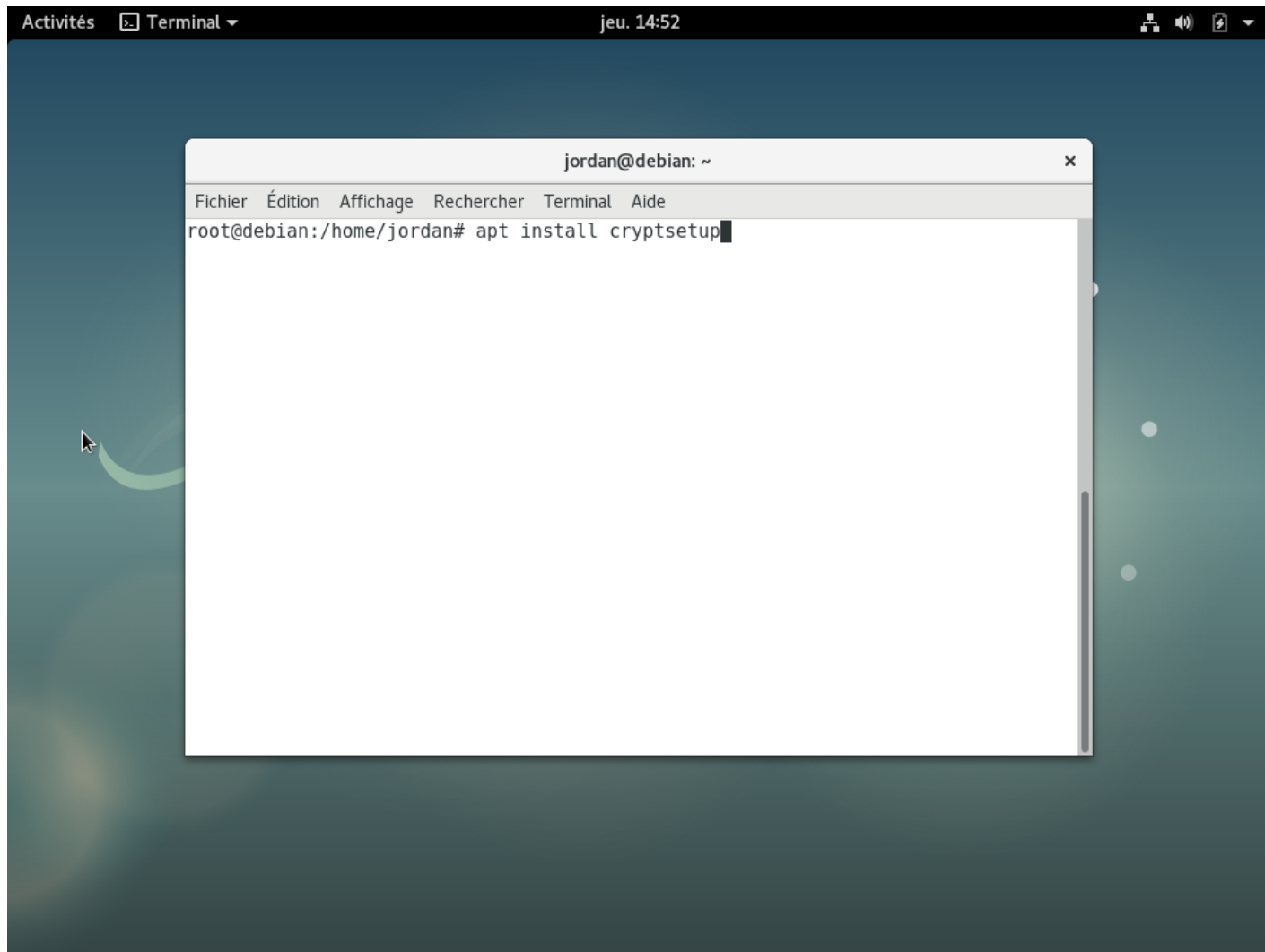
Annuler

```
jordan@debian: ~  
Fichier  Édition  Affichage  Rechercher  Terminal  Aide  
jordan@debian:~$ su  
Mot de passe :  
root@debian:/home/jordan#  
root@debian:/home/jordan# fdisk -l  
Disque /dev/sdb : 8 GiB, 8589934592 octets, 16777216 secteurs  
Unités : secteur de 1 × 512 = 512 octets  
Taille de secteur (logique / physique) : 512 octets / 512 octets  
taille d'E/S (minimale / optimale) : 512 octets / 512 octets  
  
Disque /dev/sda : 8 GiB, 8589934592 octets, 16777216 secteurs  
Unités : secteur de 1 × 512 = 512 octets  
Taille de secteur (logique / physique) : 512 octets / 512 octets  
taille d'E/S (minimale / optimale) : 512 octets / 512 octets  
Type d'étiquette de disque : dos  
Identifiant de disque : 0xc4c01bb3  
  


| Périphérique | Amorçage | Début    | Fin      | Secteurs | Taille | Id | Type                  |
|--------------|----------|----------|----------|----------|--------|----|-----------------------|
| /dev/sda1    | *        | 2048     | 12582911 | 12580864 | 6G     | 83 | Linux                 |
| /dev/sda2    |          | 12584958 | 16775167 | 4190210  | 2G     | 5  | Étendue               |
| /dev/sda5    |          | 12584960 | 16775167 | 4190208  | 2G     | 82 | partition d'échange L |

  
root@debian:/home/jordan#
```



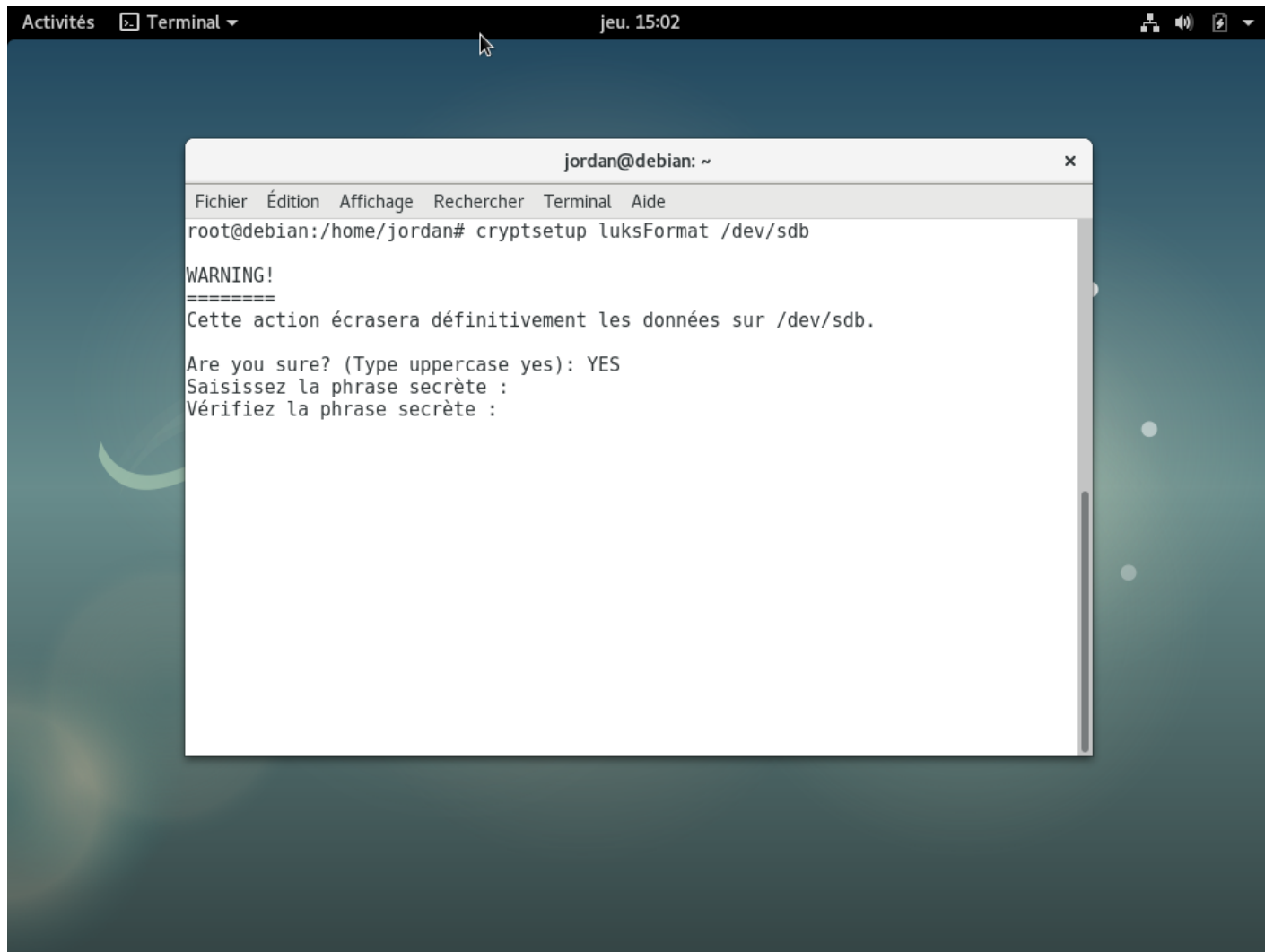


jordan@debian: ~

✕

Fichier Édition Affichage Rechercher Terminal Aide

```
root@debian:/home/jordan# shred -v -n 1 /dev/sdb
shred: /dev/sdb : passe 1/1 (random)...
shred: /dev/sdb : passe 1/1 (random)...1003MiB/8,0GiB 12 %
shred: /dev/sdb : passe 1/1 (random)...2,0GiB/8,0GiB 25 %
shred: /dev/sdb : passe 1/1 (random)...2,9GiB/8,0GiB 37 %
shred: /dev/sdb : passe 1/1 (random)...4,0GiB/8,0GiB 50 %
shred: /dev/sdb : passe 1/1 (random)...5,0GiB/8,0GiB 63 %
shred: /dev/sdb : passe 1/1 (random)...6,0GiB/8,0GiB 75 %
shred: /dev/sdb : passe 1/1 (random)...6,9GiB/8,0GiB 87 %
shred: /dev/sdb : passe 1/1 (random)...7,8GiB/8,0GiB 97 %
shred: /dev/sdb : passe 1/1 (random)...8,0GiB/8,0GiB 100 %
root@debian:/home/jordan#
```



```
Activités Terminal ▾ jeu. 15:02
```

```
jordan@debian: ~
```

```
Fichier Édition Affichage Rechercher Terminal Aide
```

```
root@debian:/home/jordan# cryptsetup luksFormat /dev/sdb
```

```
WARNING!
```

```
=====
```

```
Cette action écrasera définitivement les données sur /dev/sdb.
```

```
Are you sure? (Type uppercase yes): YES
```

```
Saisissez la phrase secrète :
```

```
Vérifiez la phrase secrète :
```

jordan@debian: ~

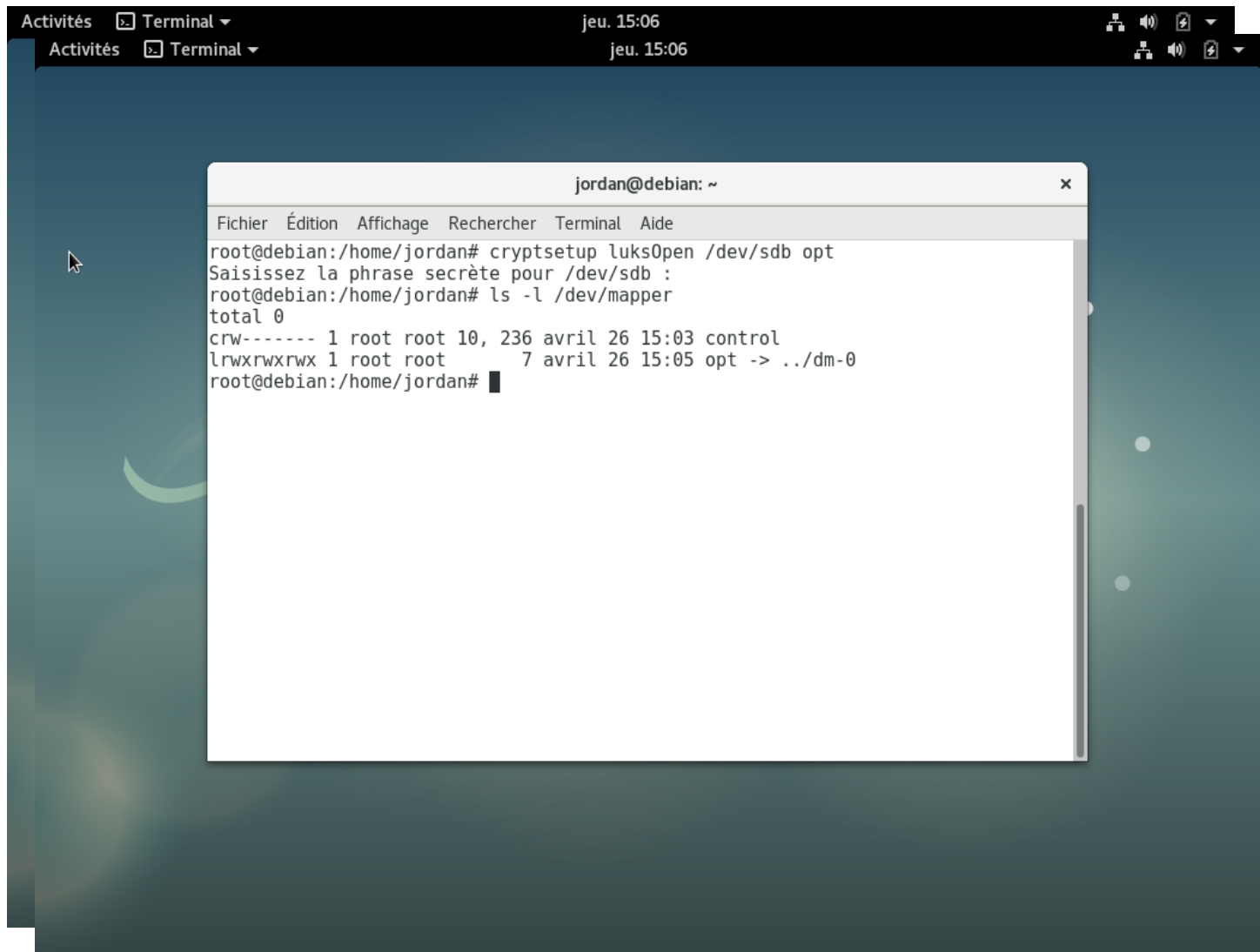
✕

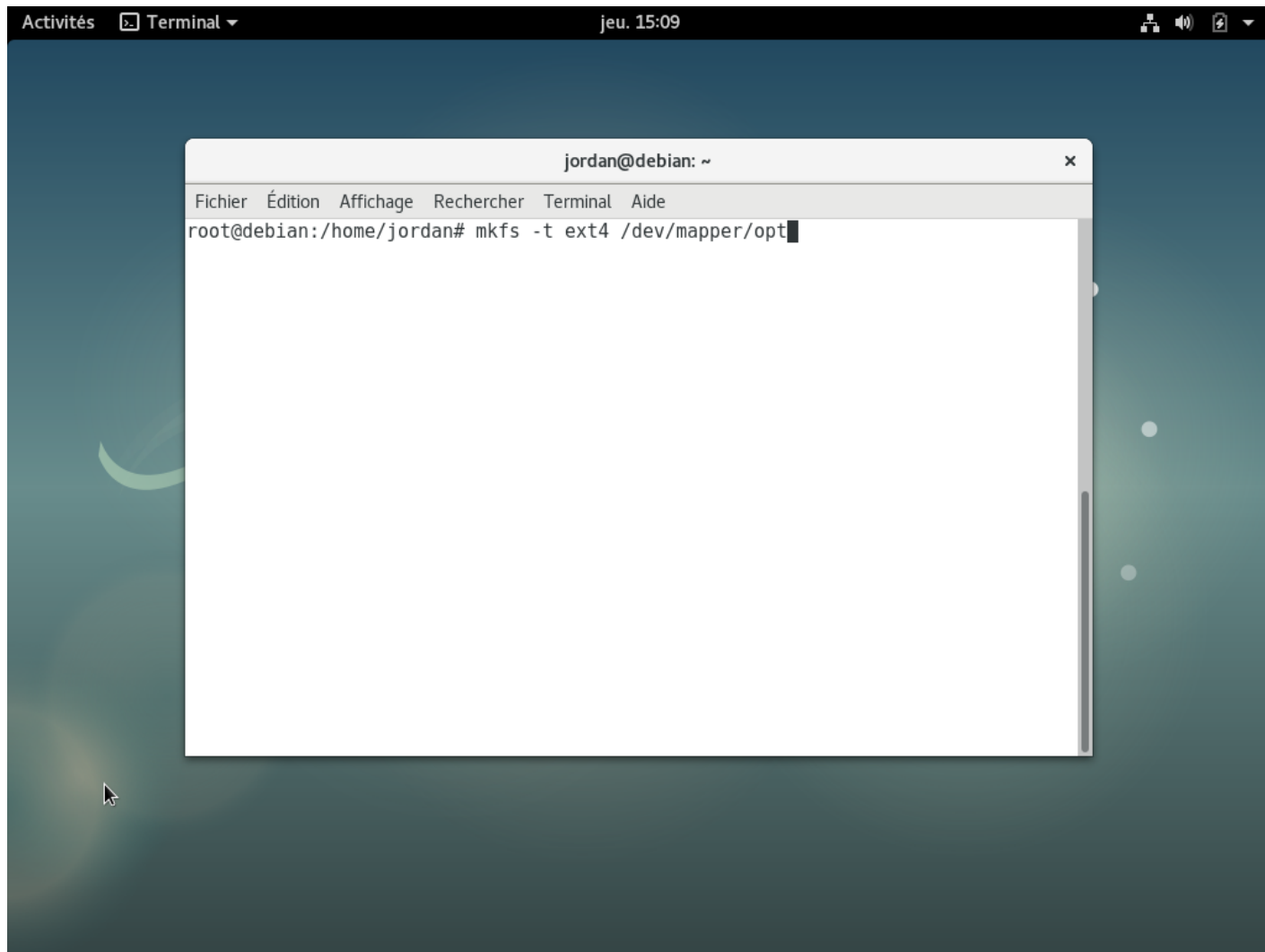
Fichier Édition Affichage Rechercher Terminal Aide

root@debian:/home/jordan# cryptsetup luksOpen /dev/sdb opt

Saisissez la phrase secrète pour /dev/sdb :

root@debian:/home/jordan# █





jordan@debian: ~

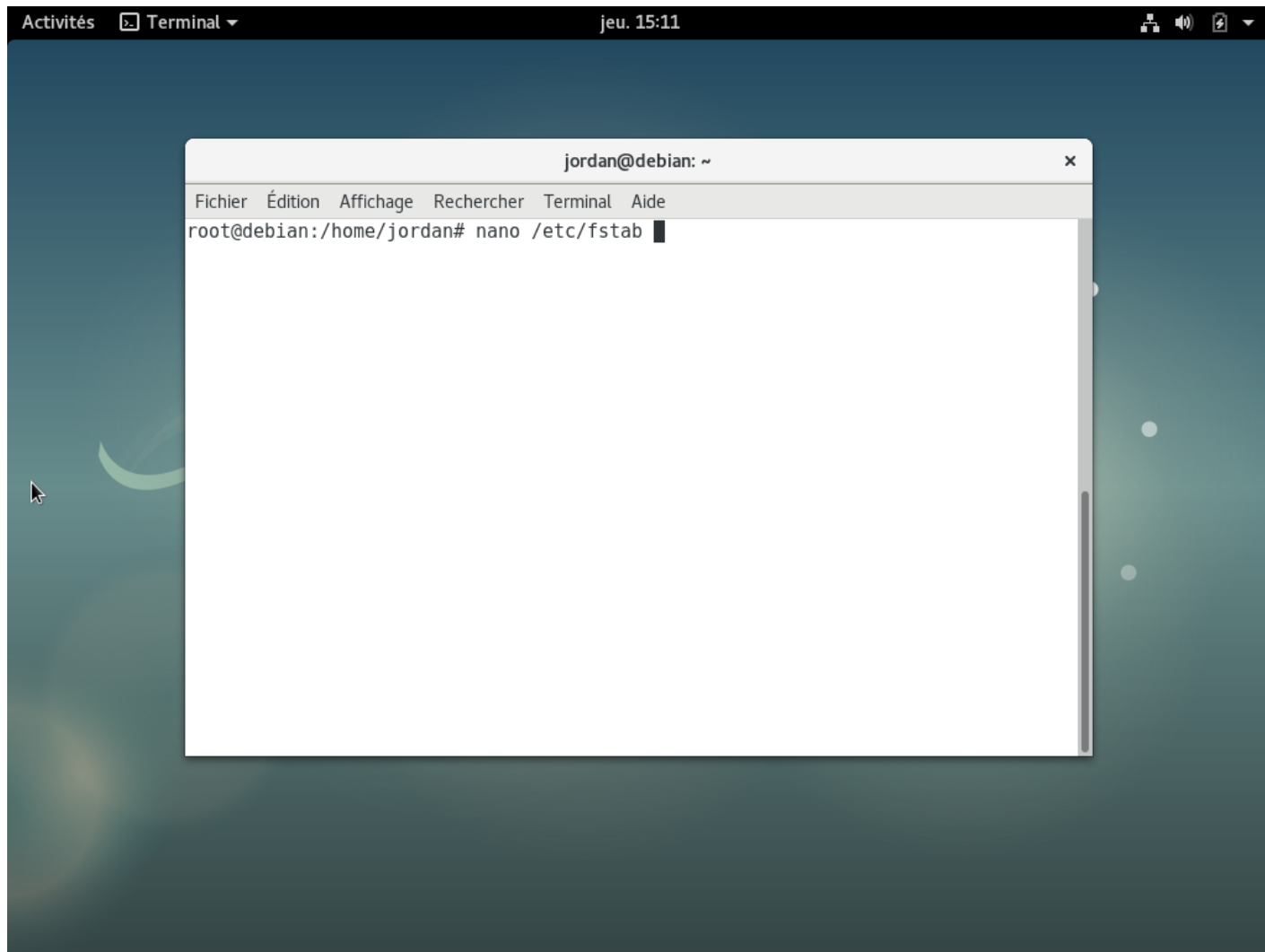
✕

Fichier Édition Affichage Rechercher Terminal Aide

```
root@debian:/home/jordan# mkfs -t ext4 /dev/mapper/opt
mke2fs 1.43.4 (31-Jan-2017)
En train de créer un système de fichiers avec 2096640 4k blocs et 524288 i-noeuds.
UUID de système de fichiers=18f0e13f-e054-4e63-9c0c-79faeeb4cb44
Superblocs de secours stockés sur les blocs :
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

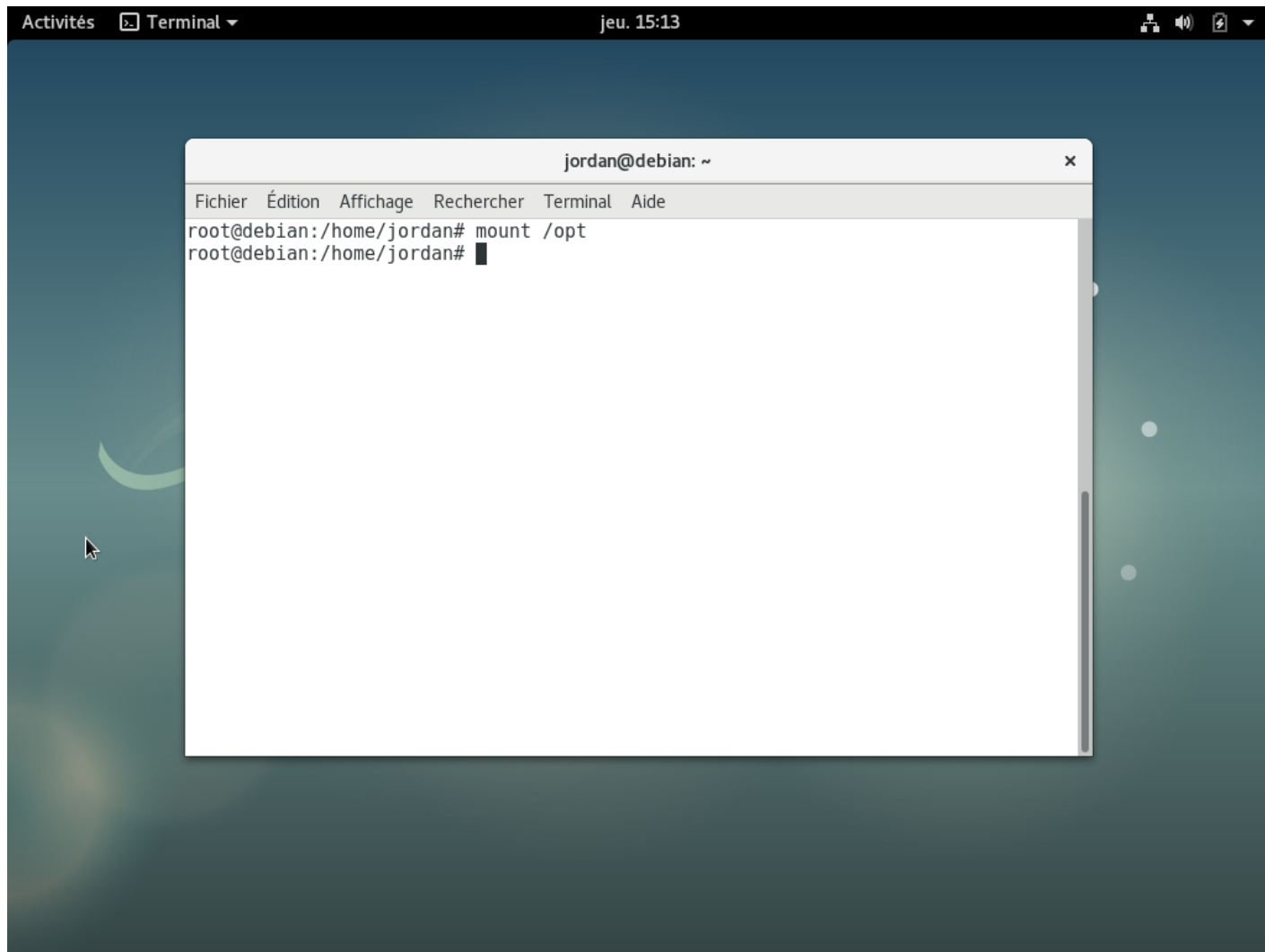
Allocation des tables de groupe : complété
Écriture des tables d'i-noeuds : complété
Création du journal (16384 blocs) : complété
Écriture des superblocs et de l'information de comptabilité du système de
fichiers : complété

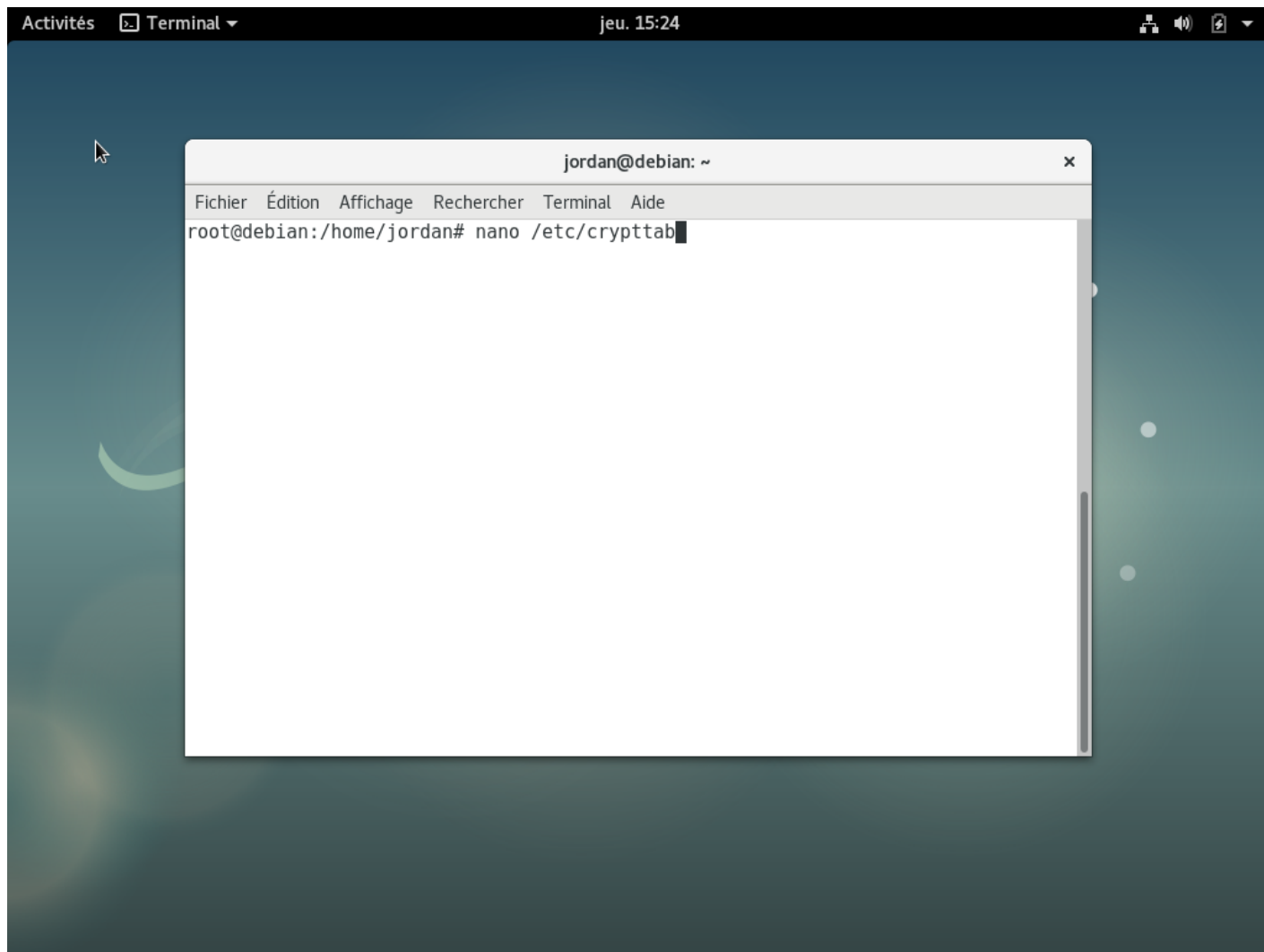
root@debian:/home/jordan# █
```

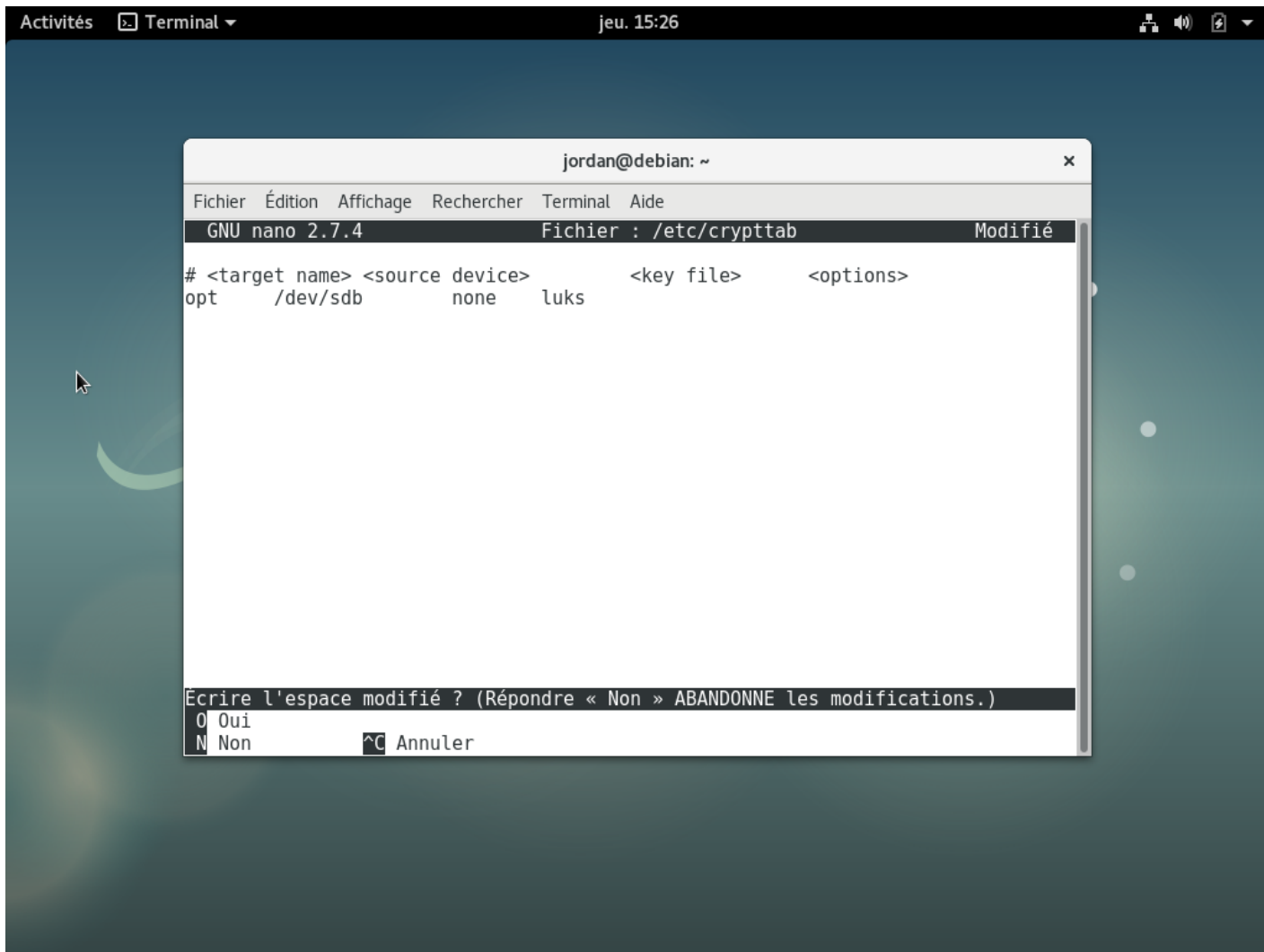


```
jordan@debian: ~  
Fichier  Édition  Affichage  Rechercher  Terminal  Aide  
GNU nano 2.7.4      Fichier : /etc/fstab      Modifié  
  
# /etc/fstab: static file system information.  
#  
# Use 'blkid' to print the universally unique identifier for a  
# device; this may be used with UUID= as a more robust way to name devices  
# that works even if disks are added and removed. See fstab(5).  
#  
# <file system> <mount point> <type> <options>      <dump> <pass>  
# / was on /dev/sda1 during installation  
UUID=6b17c35c-a814-49f0-88c9-5434cf5c26ac /          ext4      errors=remoun$  
# swap was on /dev/sda5 during installation  
UUID=40123940-4c91-4ee7-9d24-5ab6eaaa3264 none        swap      sw          $  
/dev/sr0      /media/cdrom0    udf,iso9660 user,noauto 0          0  
/dev/mapper/opt /opt             ext4      defaults    0          0
```

^G Aide ^O Écrire ^W Chercher ^K Couper ^J Justifier ^C Pos. cur.
^X Quitter ^R Lire fich. ^\ Remplacer ^U Coller ^T Orthograp. ^_ Aller lig.







Au reboot de la machine

```
/dev/sda1: clean, 145401/393216 files, 1074285/1572608 blocks  
Please enter passphrase for disk VBOX_HARDDISK (opt) on /opt!
```