



# THIROINE Consulting

Formateur – Auditeur – Conseil

A graphic illustration on a dark blue background. In the center is a glowing blue shield with a white keyhole icon. Surrounding the shield are five circular icons: a Wi-Fi symbol, a shopping cart, a document with a pencil, a wallet, and a laptop. These icons are connected by a circular line. Below the shield, a stylized hand with a circuit-like pattern is reaching up towards it. The background features faint concentric circles and lines, suggesting a digital or technological theme.

# Cyber Security

## Module 3 : Présentation de la suite Kali Linux

## **Module 3 : Présentation de la suite Kali Linux**

- 1 – Histoire de Kali linux**
- 2 – Installation et configuration de Kali Linux**
- 3 – Les différents groupes d'applications**
- 4 – les commandes essentielles sous Linux**



## Module 3 : Présentation de la suite Kali Linux

### Chapitre 1 – Histoire de Kali linux

2006

Naissance de **BackTrack** : distribution regroupant l'ensemble des outils nécessaires au tests de sécurité d'un réseau qui est reconnu par les professionnels de la sécurité informatique comme outil complet, développé par la société Remote exploit par les développeurs Mati Aharoni et Max Moser.

C'est un logiciel open source (logiciel libre).

2013

La distribution **BackTrack** devient **Kali linux**, développé par Mati Aharoni qui crée la société Offensive Security et les développeurs Devon Kearns et Raphaël Hertzog. La distribution regroupe l'ensemble des outils nécessaires aux tests de sécurité d'un système informatique surtout le test d'intrusion.

# Module 3 : Présentation de la suite Kali Linux

## Chapitre 2 – Installation et configuration de Kali Linux

### 1) Choisir la version en fonction de son ordinateur (I386 ou AMD)

- pour Mac (I386)
- pour Windows (I386 ou AMD)

➡ <https://www.kali.org/get-kali/#kali-platforms>



**Choose your Kali**

LIGHT ☒ DARK

#### Installer Images

- ✓ Direct access to hardware
- ✓ Customized Kali kernel
- ✓ No overhead

Single or multiple boot Kali, giving you complete control over the hardware access (perfect for in-built Wi-Fi and GPU), enabling the best performance.

**Recommended**

#### Virtual Machines

- ✓ Snapshots functionality
- ✓ Isolated environment
- ✓ Customized Kali kernel
- ✗ Limited direct access to hardware
- ✗ Higher system requirements

VMware & VirtualBox pre-built images. Allowing for a Kali install without altering the host OS with additional features such as snapshots. Vagrant images for quick spin-up also available.

**Recommended**

#### ARM

- ✓ Range of hardware from the leave behind devices end to high-end modern servers
- ✗ System architecture limits certain packages
- ✗ Not always customized kernel

Works on relatively inexpensive & low powered Single Board Computers (SBCs) as well as modern ARM based laptops, which combine high speed with long battery life.

#### Mobile

- ✓ Kali layered on Android
- ✓ Kali in your pocket, on the go
- ✓ Mobile interface (compact view)

A mobile penetration testing platform for Android devices, based on Kali Linux. Kali NetHunter consists of an NetHunter App, App Store, Kali Container, and Kali.

#### Cloud

- ✓ Fast deployment
- ✓ Can leverage provider's resources
- ✗ Provider may become costly
- ✗ Not always customized kernel

Hosting providers which have Kali Linux pre-installed, ready to go, without worrying about infrastructure maintenance.

#### Containers

- ✓ Low overhead to access Kali toolset
- ✗ Userland actions only
- ✗ Not Kali customized kernel
- ✗ No direct access to hardware

Using Docker or LXD, allows for extremely quick and easy access to Kali's tool set without the overhead of an isolated virtual machine.

#### Live Boot

- ✓ Un-altered host system
- ✓ Direct access to hardware
- ✓ Customized Kali kernel
- ✗ Performance decrease when heavy I/O

Quick and easy access to a full Kali install. Your Kali, always with you, without altering the host OS, plus allows you to benefit from hardware access.

#### WSL

- ✓ Access to the Kali toolset through the WSL Framework
- ✗ Userland actions only
- ✗ Not Kali customized kernel
- ✗ No direct access to hardware

Windows Subsystem for Linux (WSL) is included out of the box with modern Windows. Use Kali (and Win-Kali) without installing additional software.

# Module 3 : Présentation de la suite Kali Linux

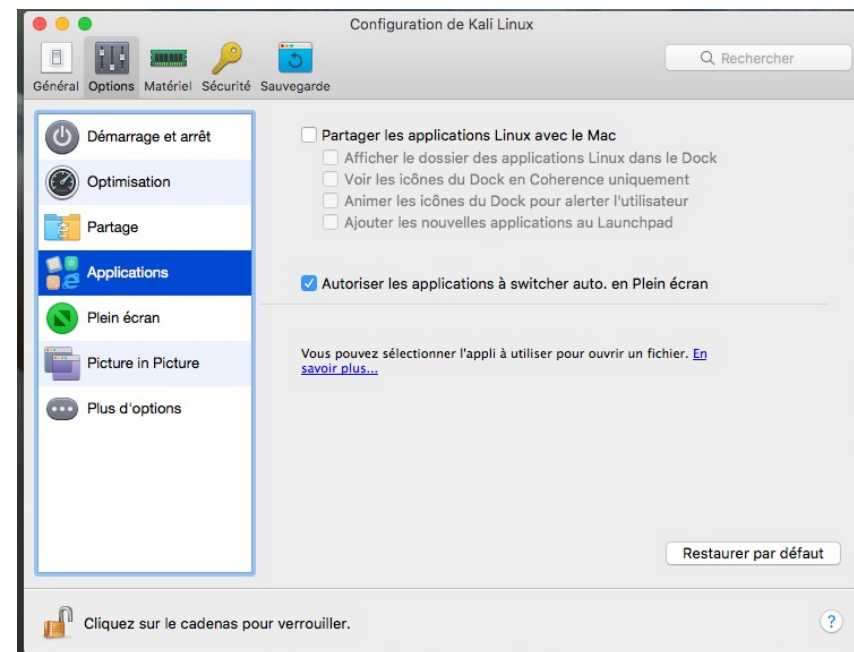
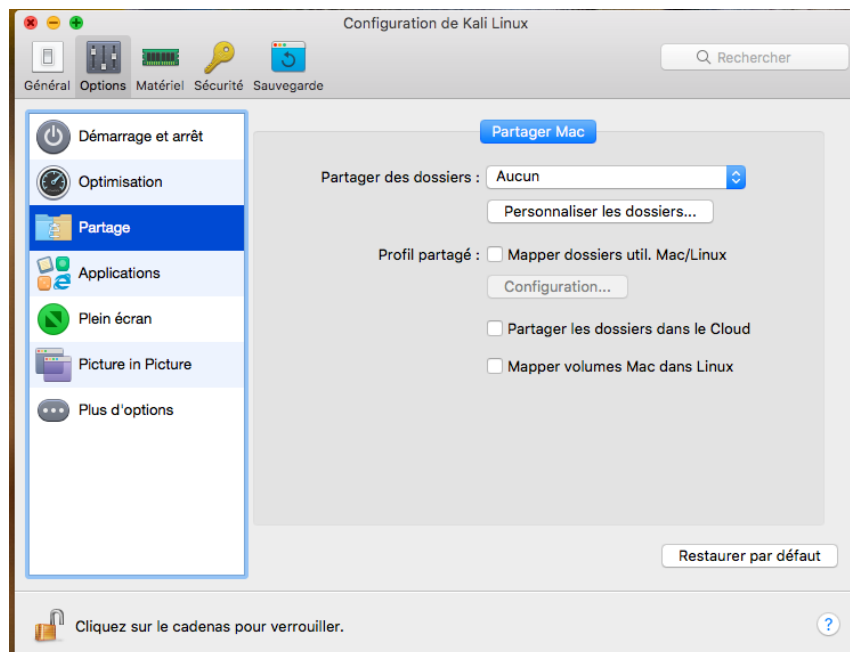
## Chapitre 2 – Installation et configuration de Kali Linux

### 2) Choix de l'installation

- Soit en multiboot
- Soit en machine virtuelle
- Soit en live sur clés USB

### 3) Installation en machine virtuelle

#### a) configuration de la machine virtuelle : isoler la machine

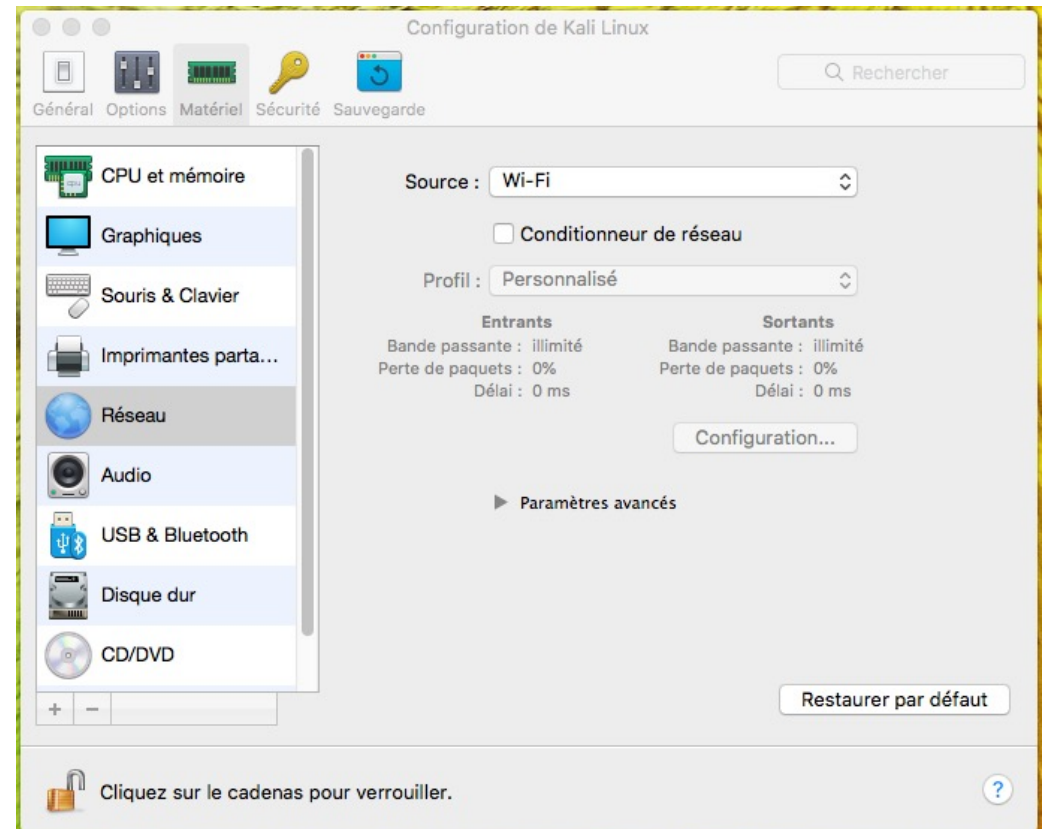
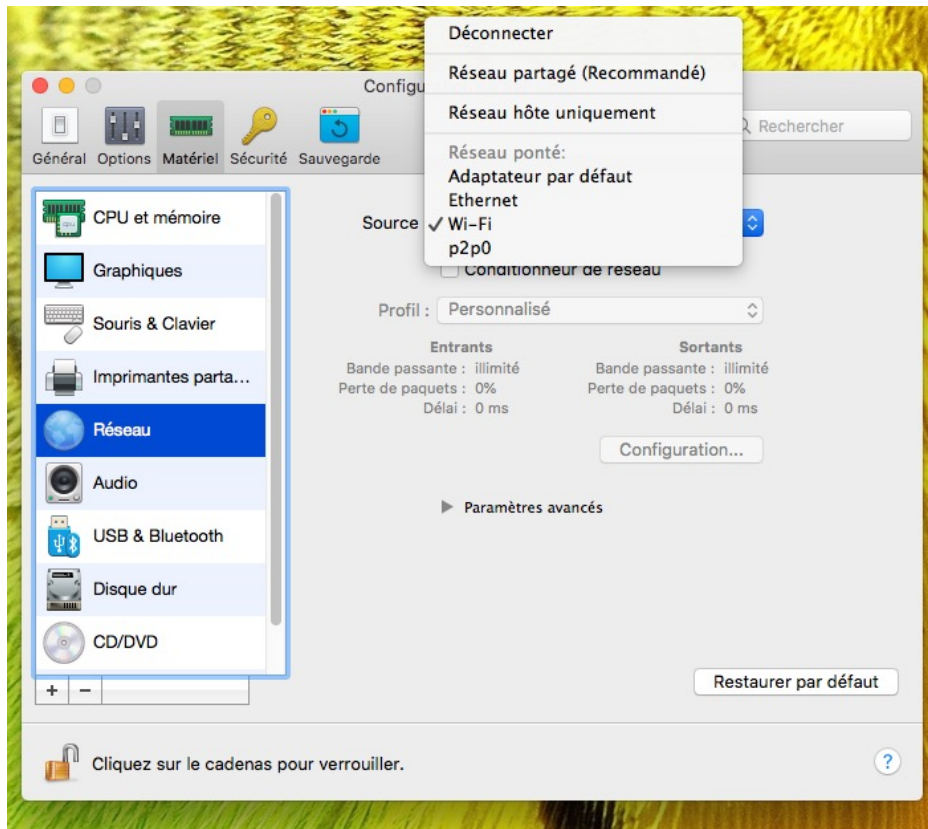




# Module 3 : Présentation de la suite Kali Linux

## Chapitre 2 – Installation et configuration de Kali Linux

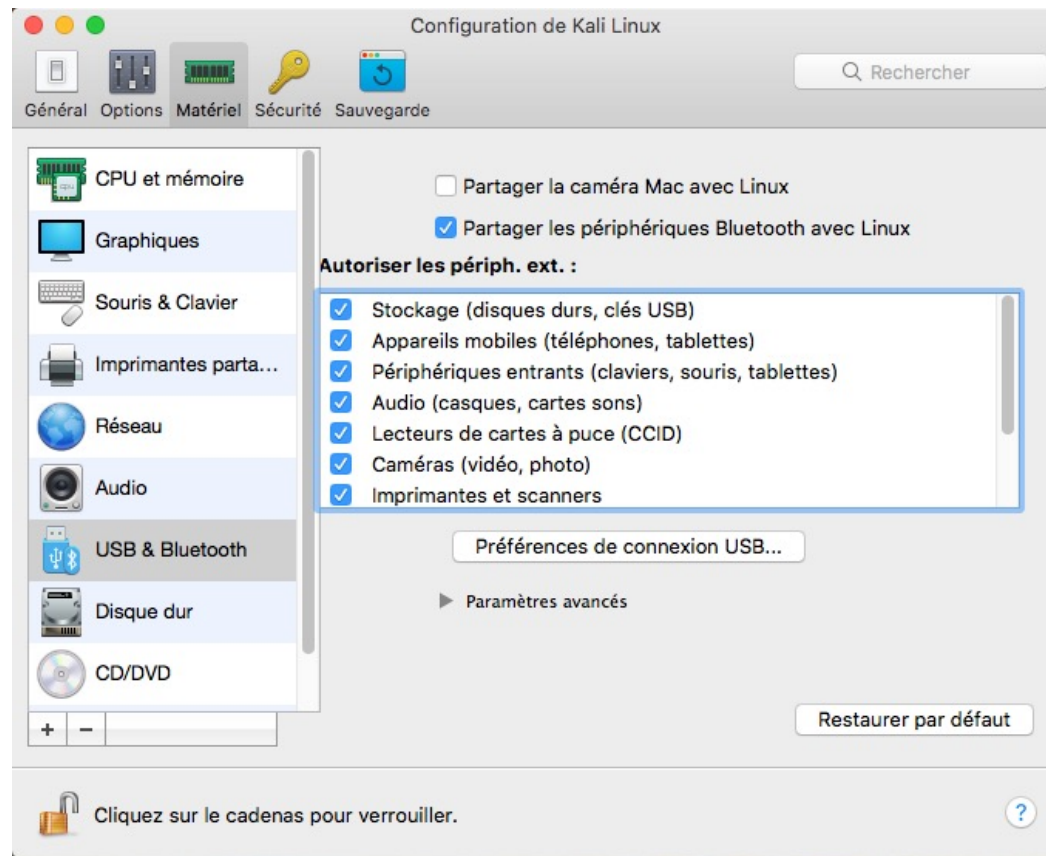
### b) configuration de la machine virtuelle : le réseau



# **Module 3 : Présentation de la suite Kali Linux**

## **Chapitre 2 – Installation et configuration de Kali Linux**

### **c) configuration de la machine virtuelle : USB et Bluetooth**

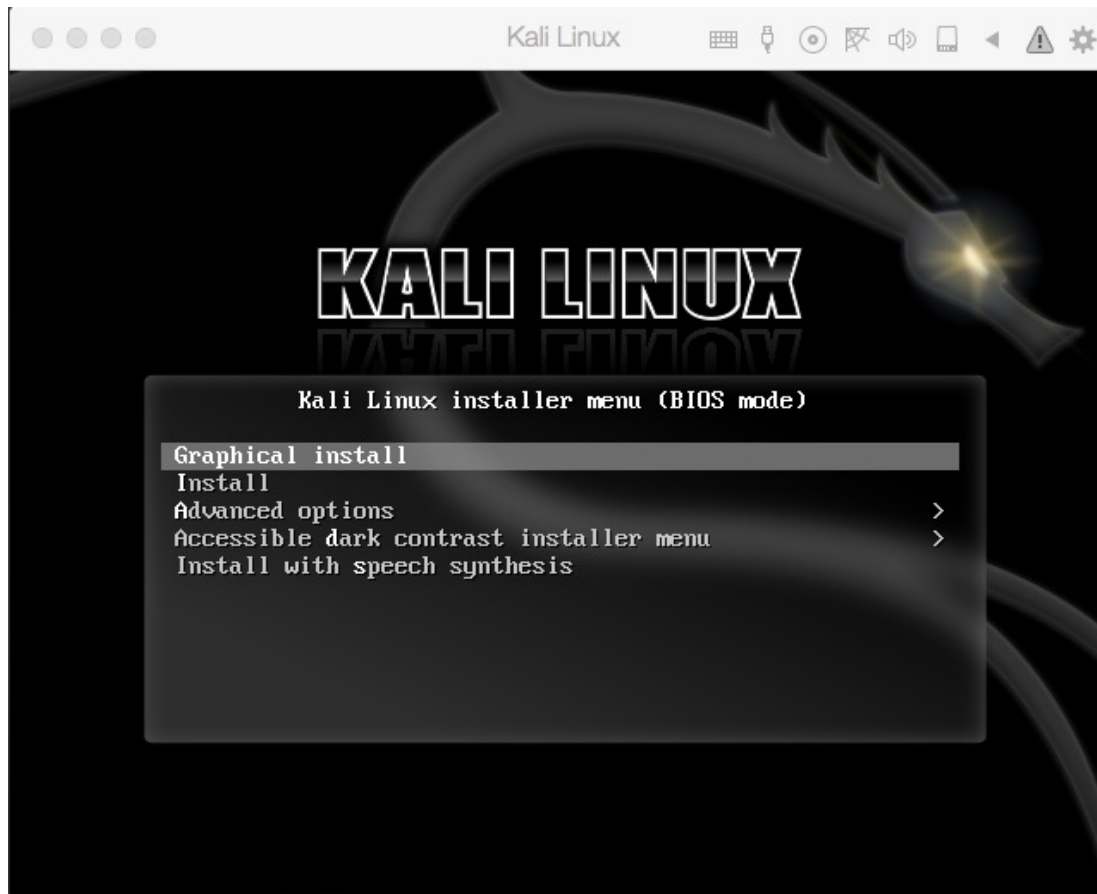




# Module 3 : Présentation de la suite Kali Linux

## Chapitre 2 – Installation et configuration de Kali Linux

### d) Installation de Kali Linux



Choisir « Graphical Install » pour une installation via le module graphique, les étapes sont les suivantes :

- ➡ Choix de la langue
- ➡ Création du compte utilisateur
- ➡ Choix de la partition
  - ➡ utiliser le disque entier
  - ➡ une seule partition
- ➡ Installation des logiciels pour la suite Kali
- ➡ Installation du programme de démarrage GRUB

## Module 3 : Présentation de la suite Kali Linux

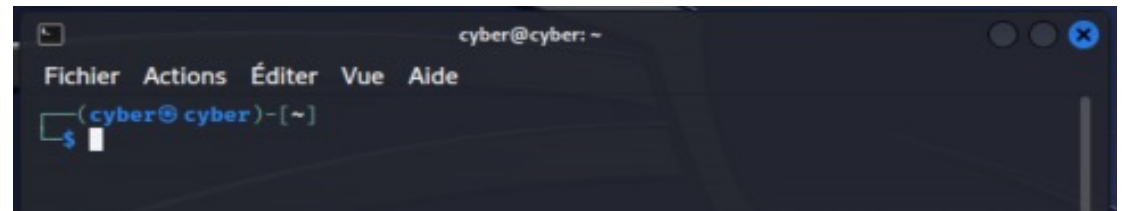
### Chapitre 2 – Installation et configuration de Kali Linux

#### e) Configuration de Kali Linux

Lors de la première utilisation, Kali Linux risque de démarrer dans la langue anglaise, quelques commandes vont être nécessaire, pour configurer correctement Kali.

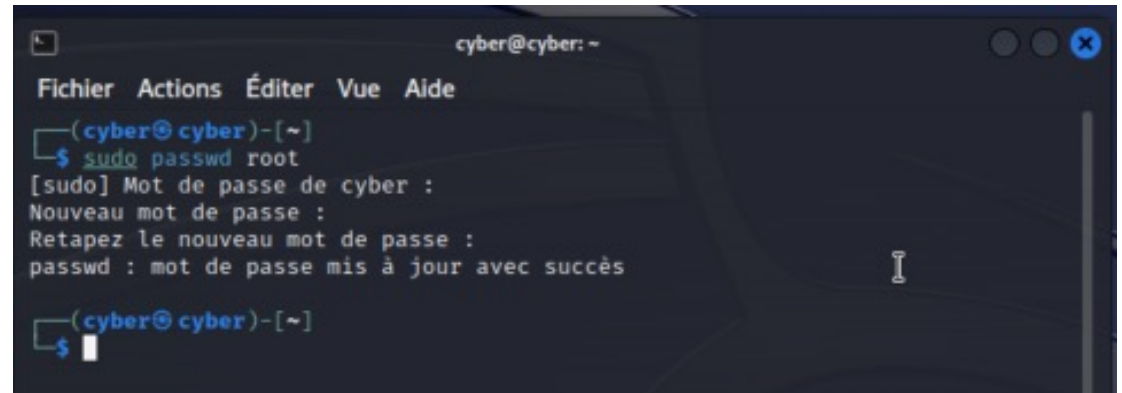
- 1 Choisir le bon clavier afin d'avoir les caractères spéciaux
- 2 Configurer le compte ROOT

➡ Passer en mode Terminal



```
cyber@cyber: ~  
Fichier Actions Éditer Vue Aide  
(cyber@cyber)-[~]  
$
```

➡ Taper : **sudo passwd root**  
Saisir le MDP utilisateur  
Saisir le MDP pour le compte root  
Compte root activé



```
cyber@cyber: ~  
Fichier Actions Éditer Vue Aide  
(cyber@cyber)-[~]  
$ sudo passwd root  
[sudo] Mot de passe de cyber :  
Nouveau mot de passe :  
Retapez le nouveau mot de passe :  
passwd : mot de passe mis à jour avec succès  
(cyber@cyber)-[~]  
$
```

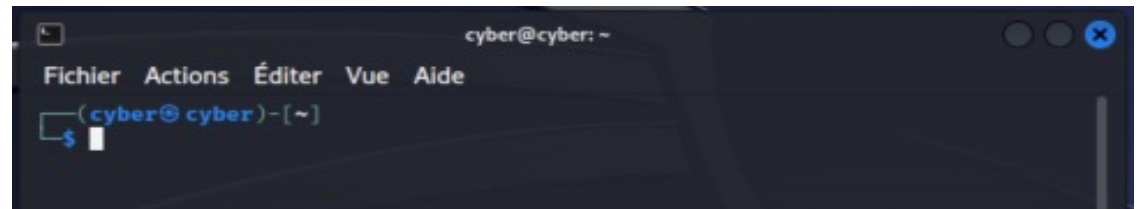
## Module 3 : Présentation de la suite Kali Linux

### Chapitre 2 – Installation et configuration de Kali Linux

#### e) Configuration de Kali Linux

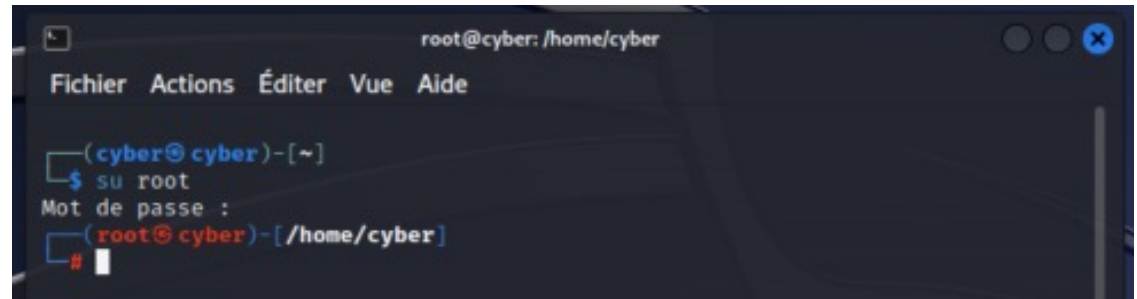
##### 3 Configurer la langue

➡ Passer en mode Terminal



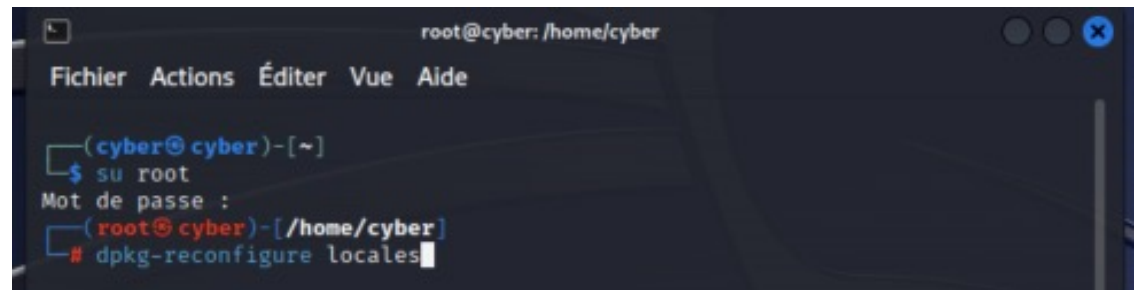
```
cyber@cyber: ~  
Fichier Actions Éditer Vue Aide  
(cyber@cyber)~  
$
```

➡ Passer en compte SU



```
root@cyber: /home/cyber  
Fichier Actions Éditer Vue Aide  
(cyber@cyber)~  
$ su root  
Mot de passe :  
(root@cyber)~  
#
```

➡ Taper : **dpkg-reconfigure locales**



```
root@cyber: /home/cyber  
Fichier Actions Éditer Vue Aide  
(cyber@cyber)~  
$ su root  
Mot de passe :  
(root@cyber)~  
# dpkg-reconfigure locales
```

# Module 3 : Présentation de la suite Kali Linux

## Chapitre 2 – Installation et configuration de Kali Linux

### e) Configuration de Kali Linux

#### 3 Configurer la langue

➔ Descendre avec les flèches pour choisir :

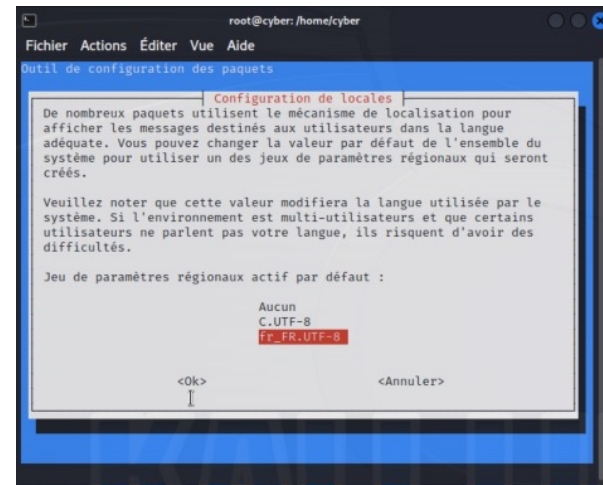
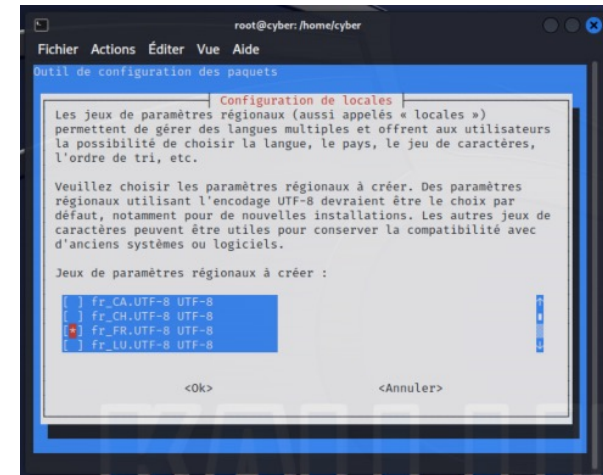
fr\_FR.UTF-8 UTF-8

Puis cliquer sur Ok

Choisir fr\_FR.UTF-8 UTF-8

Puis cliquer sur Ok

relancer la machine afin de prendre en compte la langue



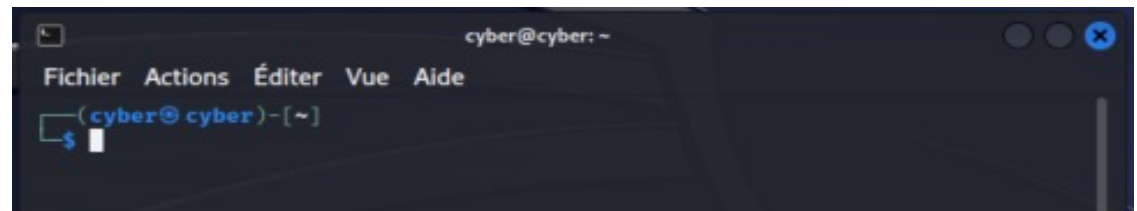
## Module 3 : Présentation de la suite Kali Linux

### Chapitre 2 – Installation et configuration de Kali Linux

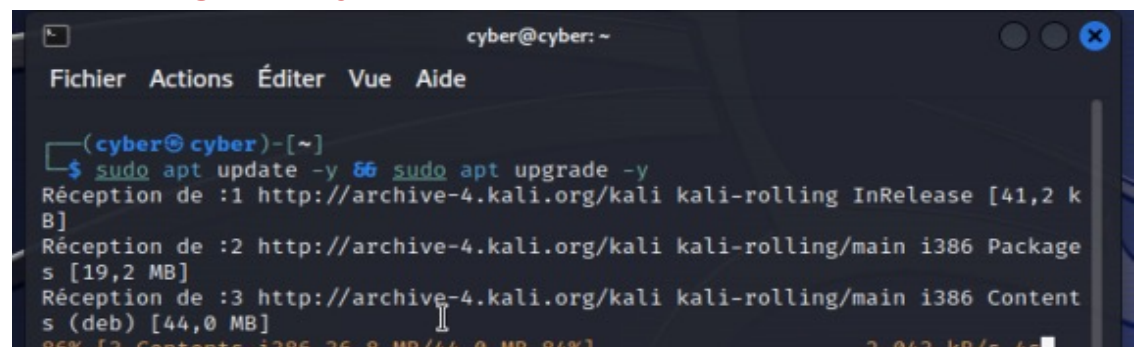
#### e) Configuration de Kali Linux

- 4 Choisir le bon affichage
- 5 Contrôle de la configuration réseau
- 6 Mise à jour de Kali

➡ Passer en mode Terminal

A screenshot of a Kali Linux desktop environment. The terminal window is open, showing the prompt (cyber@cyber)~. The window title is 'cyber@cyber: ~'. The menu bar includes 'Fichier', 'Actions', 'Éditer', 'Vue', and 'Aide'.

➡ Taper : **sudo apt update -y && sudo apt upgrade -y**

A screenshot of a Kali Linux desktop environment. The terminal window is open, showing the command 'sudo apt update -y && sudo apt upgrade -y' being executed. The output shows the progress of the update and upgrade process, including the reception of packages from the Kali rolling repository. The window title is 'cyber@cyber: ~'. The menu bar includes 'Fichier', 'Actions', 'Éditer', 'Vue', and 'Aide'.



# Module 3 : Présentation de la suite Kali Linux

## Chapitre 3 – Les différents groupes d'applications

01 - Récupération d'informations
02 - Analyse de la Vulnérabilité
03 - Applications Web
04 - L'évaluation Database
05 - Attaques de Mot de Passe
06 - Attaques Sans Fil
07 - L'ingénierie Inverse
08 - Outils Exploitation
09 - Renifler et l'Usurpation
10 - Maintien de l'Accès
11 - Criminalistique
12 - Rapports
13 - Social Engineering Tools
42 - Kali & OffSec Links

### Collecte d'information

- |                                       |          |
|---------------------------------------|----------|
| • énumération de service              | dnsenum  |
| • liste des tranches d'adresses IP    | dmitry   |
| • identification des machines actives | ping     |
| • liste des ports ouverts             | nmap     |
| • empreinte du système d'exploitation | nmap     |
| • empreinte des services              | nmap     |
| • Évaluation des failles              | maltego  |
| • Mappage du réseau                   | casefile |

### Evaluation de vulnérabilités

- Utilisation de Nessus
- Utilisation d'OpenVAS

### Exploitation des vulnérabilités

- |                     |                    |
|---------------------|--------------------|
| • Utilisation de    | Metasploit         |
| • Utilisation d'    | Armitage           |
| • Maîtrise de la    | Console Metasploit |
| • Maîtrise de       | Meterpreter        |
| • Implémentation de | Browser_autopwn    |

### Escalade de privilèges

- |   |             |
|---|-------------|
| • Utilisation de jetons impersonnés       | Incognito   |
| • Attaque en escalade de privilège locale | Getsystem   |
| • Maîtrise de Social Engineering Toolkit  | Se-toolkit  |
| • Collecte des données de la victime      | Keyscan     |
| • Création de porte dérobée persistente   | Persistence |
| • Attaque de type man-in-the-middle       | Ettercap    |



### Attaques de mot de passe

- |                                      |              |
|--------------------------------------|--------------|
| • Attaque en ligne                   | Xhydra       |
| • Crackage de mot de passe HTTP      | Xhydra       |
| • Accréditation des accès de routage | Medusa       |
| • Profilage de mot de passe          | Ettercap     |
| • Crackage de mot de passe Windows   | Sam          |
| • Attaque par dictionnaire           | Crunch       |
| • Attaque par table arc-en-ciel      | Rainbowcrack |
| • Utilisation de nVidia CUDA         | Cudahashcat  |
| • Utilisation des flux ATI           | Odhashcat    |
| • Attaque d'accès physique           | Sucrack      |

### Analyse légale (Forensic)

- |                                   |                |
|-----------------------------------|----------------|
| • Investigation post-mortem       | Autopsy        |
| • Recherche d'une image binaire   | Binwalk        |
| • Extraction d'info personnelles  | Bulk-extractor |
| • Détection de rootkit            | Chkrootkit     |
| • Recouvrement de fichiers perdus | Foremost       |
| • Analyse de cookies              | Galleta        |
| • Intégrité des données           | Hashdeep       |
| • Analyse de mémoire pour Mac     | Volafox        |
| • Outils d'extraction de mémoire  | Volatility     |

### Attaque sans-fil

- |  |             |
|--|-------------|
| • Crackage du réseau WEP               | Airmon-ng   |
| • Crackage du réseau WPA/WPA2          | Aircrack-ng |
| • Automatisation de crackage sans-fil  | Gerix-wifi  |
| • Accès aux clients avec une fausse AP | Gerix.py    |
| • Manipulation du trafic URL           | Arpspoof    |
| • Redirection de port                  | Iptables    |
| • Reniflage du trafic réseau           | Ettercap    |

### Reverse Engineering

- |                             |           |
|-----------------------------|-----------|
| • For Android               | Apktool   |
| • Compilation C/C++         | Clang     |
| • For Applet Java           | Dex2jar   |
| • Debugger Unix/Linux       | Edb-debug |
| • Debugger Windows          | Olllydbg  |
| • Assemblage/Désassemblage  | Flasm     |
| • Désassemblage Classe Java | Jad       |
| • Désassemblage Processeur  | Radare2   |