



# KALI LINUX INSTALL

Procédure



POMIES Antonin  
Version 2023.1

## Table of Contents

<b><i>I – Installation de l'OS.....</i></b>	<b><i>2</i></b>
a) A Savoir .....	2
b) Début/Prérequis.....	2
c) Configuration de Kali.....	2
<b><i>II – Installation des logiciels additionnel .....</i></b>	<b><i>8</i></b>
a) Les logiciels.....	8
b) Le détail .....	8
c) Mise à jour de Kali .....	8
d) Installation de Volatility.....	8
e) Installation de Exiftool .....	10
f) Installation de Firefox Decrypt.....	10
<b><i>III – Création de sa propre image de Kali Linux (ISO) .....</i></b>	<b><i>11</i></b>
a) Installation des paquets.....	11
<b><i>IV – Modifier la version de Python .....</i></b>	<b><i>11</i></b>
a) Vérification .....	11
<b><i>V – Installation de la suite Tinscript.....</i></b>	<b><i>12</i></b>
a) Contenu.....	12
b) Installation .....	12
<b><i>FIN .....</i></b>	<b><i>13</i></b>

# I – Installation de l'OS

## a) A Savoir



La procédure concerne la version 2023.1 de Kali Linux et peut donc différer en fonction de son ancienneté.

Kali **Linux** représente la plateforme de **tests** de pénétration la plus puissante et la plus populaire au monde, utilisée par une grande majorité de professionnels de la sécurité dans un large spectre de domaines incluant les tests de pénétrations, certes, mais également l'informatique légale (aussi appelée **forensic**), l'ingénierie inverse ou encore l'évaluation de la vulnérabilité d'un réseau ou d'une infrastructure.

## b) Début/Prérequis

Selon les recommandations, nous avons besoin de :

2 Gb de RAM

20 Gb d'espace disque

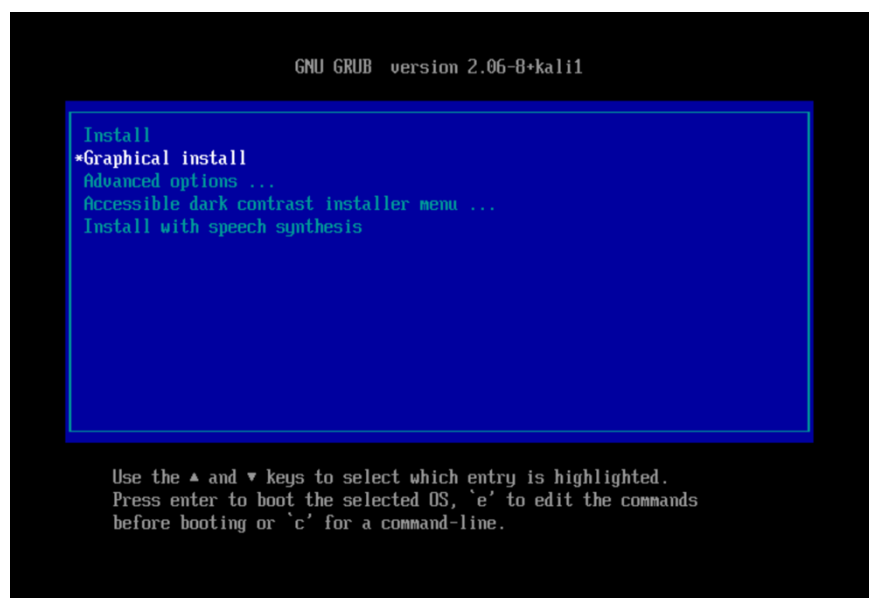
Nous avons aussi besoin du fichier .ISO trouvable a ce lien :

<https://cdimage.kali.org/kali-2023.1/kali-linux-2023.1-installer-arm64.iso>

Je ne détaillerais pas la marche à suivre pour faire la clé bootable ou l'ajout de l'image sur VMWare. Ces étapes devraient être acquises.

## c) Configuration de Kali

On peut donc dès à présent démarrer la machine virtuelle ou physique et booter sur la clé / l'image. On arrive sur cette page. On clique donc sur « Graphical install » ou « install » qui sont la même chose, sauf que « Graphical install » est un peu plus User-Friendly.



Ensuite on arrive sur cette page. On sélectionne la langue du programme d'installation qui sera donc français dans notre cas.

Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Bulgarian	- Български
Burmese	- မြန်မာစာ
Catalan	- Català
Chinese (Simplified)	- 中文(简体)
Chinese (Traditional)	- 中文(繁體)
Croatian	- Hrvatski
Czech	- Čeština
Danish	- Dansk
Dutch	- Nederlands
Dzongkha	- ཇོང་ཁ།
English	- English
Esperanto	- Esperanto
Estonian	- Eesti
Finnish	- Suomi
French	- Français

On va maintenant choisir ou on habite pour définir notamment le fuseau horaire.

Choix de votre situation géographique

Le pays choisi permet de définir le fuseau horaire et de déterminer les paramètres régionaux du système (« locale »). C'est le plus souvent le pays où vous vivez.

La courte liste affichée dépend de la langue précédemment choisie. Choisissez « Autre » si votre pays n'est pas affiché.

Pays (territoire ou région) :

Belgique

Canada

France

Luxembourg

Suisse

Autre

Une barre de progression va apparaître. Elle ne dure que peu de temps.

Chargement de composants supplémentaires

Récupération de tzsetup-udeb

Nous allons ensuite donner un nom à notre nouvelle machine

Configurer le réseau

Veuillez indiquer le nom de ce système.

Le nom de machine est un mot unique qui identifie le système sur le réseau. Si vous ne connaissez pas ce nom, demandez-le à votre administrateur réseau. Si vous installez votre propre réseau, vous pouvez mettre ce que vous voulez.

Nom de machine :

Anonymous

Dans mon exemple sachez que je ne vais pas mettre mon kali dans le domaine, pour des raisons évidentes, mais sachez qu'il est possible de l'intégrer a un domaine.

Configurer le réseau

Le domaine est la partie de l'adresse Internet qui est à la droite du nom de machine. Il se termine souvent par .com, .net, .edu, ou .org. Si vous paramétrez votre propre réseau, vous pouvez mettre ce que vous voulez mais assurez-vous d'employer le même nom sur toutes les machines.

Domaine :

Passons désormais à la création d'un utilisateur. Dans mon cas j'ai pour habitude de mettre des login/mdp simple et intuitif. Je donne tout d'abord le nom kali a la session

Créer les utilisateurs et choisir les mots de passe

Un compte d'utilisateur va être créé afin que vous puissiez disposer d'un compte différent de celui du superutilisateur (« root »), pour l'utilisation courante du système.

**Veillez indiquer le nom complet du nouvel utilisateur. Cette information servira par exemple dans l'adresse d'origine des courriels émis ainsi que dans tout programme qui affiche ou se sert du nom complet. Votre propre nom est un bon choix.**

*Nom complet du nouvel utilisateur :*

Le login de connexion sera aussi kali

Créer les utilisateurs et choisir les mots de passe

**Veillez choisir un identifiant (« login ») pour le nouveau compte. Votre prénom est un choix possible. Les identifiants doivent commencer par une lettre minuscule, suivie d'un nombre quelconque de chiffres et de lettres minuscules.**

*Identifiant pour le compte utilisateur :*

Et le mot de passe de la session sera aussi kali.

Créer les utilisateurs et choisir les mots de passe

**Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.**

*Mot de passe pour le nouvel utilisateur :*

  
☐ Afficher le mot de passe en clair

**Veillez entrer à nouveau le mot de passe pour l'utilisateur, afin de vérifier que votre saisie est correcte.**

*Confirmation du mot de passe :*

  
☐ Afficher le mot de passe en clair

🚩 Bien évidemment si vous souhaitez un système doté d'une sécurité hors pair, il est évident que le mot de passe et le nom de la session doivent être moins parlant. D'autant plus qu'il est nécessaire de sécuriser l'accès au Grub qui est une faille de sécurité majeure.

Passons ensuite à la configuration des disques et notamment à la partie partitionnement. Etant donné qu'actuellement notre disque virtuelle est vide, nous pouvons sélectionner « Assisté – utiliser un disque entier ». Dans le cadre d'une machine avec une configuration RAID Logique (Non Physique), il serait possible de choisir la partie LVM.

Partitionner les disques

**Le programme d'installation peut vous assister pour le partitionnement d'un disque (avec plusieurs choix d'organisation). Vous pouvez également effectuer ce partitionnement vous-même. Si vous choisissez le partitionnement assisté, vous aurez la possibilité de vérifier et personnaliser les choix effectués.**

**Si vous choisissez le partitionnement assisté pour un disque complet, vous devrez ensuite choisir le disque à partitionner.**

*Méthode de partitionnement :*

- Assisté - utiliser un disque entier
- Assisté - utiliser tout un disque avec LVM
- Assisté - utiliser tout un disque avec LVM chiffré
- Manuel

Suite à l'étape précédente, on peut donc maintenant choisir le disque ou l'on veut installer Kali Linux. Dans mon cas il n'y en a qu'un mais sur une machine physique, faire attention car une suppression du disque entraîne la suppression des données.

#### Partitionner les disques

**Veillez noter que toutes les données du disque choisi seront effacées mais pas avant d'avoir confirmé que vous souhaitez réellement effectuer les modifications.**

Disque à partitionner :

**/dev/nvme0n1 - 21.5 GB VMware Virtual NVMe Disk**

Une fois cela fait, on peut donc sélectionner « tout dans une seule partition ». Notre but dans cette procédure est de faire un machine virtuelle fonctionnelle mais pas doté d'une sécurité pointue.

#### Partitionner les disques

Disque partitionné :

**/dev/nvme0n1 - VMware Virtual NVMe Disk: 21.5 GB**

**Le disque peut être partitionné selon plusieurs schémas. Dans le doute, choisissez le premier.**

Schéma de partitionnement :

**Tout dans une seule partition (recommandé pour les débutants)**

Partition /home séparée

Partitions /home, /var et /tmp séparées

Suite à toutes ces étapes nous pouvons maintenant finir la configuration en cliquant sur « Terminer le partitionnement et appliquer les changements ».

#### Partitionner les disques

Voici la table des partitions et les points de montage actuellement configurés. Vous pouvez choisir une partition et modifier ses caractéristiques (système de fichiers, point de montage, etc.), un espace libre pour créer une nouvelle partition ou un périphérique pour créer sa table des partitions.

##### Partitionnement assisté

Configurer le RAID avec gestion logicielle

Configurer le gestionnaire de volumes logiques (LVM)

Configurer les volumes chiffrés

Configurer les volumes iSCSI

▼ /dev/nvme0n1 - 21.5 GB VMware Virtual NVMe Disk

>	1.0 MB	Espace libre	
>	n° 1	536.9 MB	B f ESP
>	n° 2	19.9 GB	f ext4 /
>	n° 3	1.0 GB	f swap swap
>	1.0 MB	Espace libre	

Annuler les modifications des partitions

**Terminer le partitionnement et appliquer les changements**

On confirme une deuxième fois par mesure de sécurité. Et le disque est prêt pour accueillir l'OS et les applications.

#### Partitionner les disques

**Si vous continuez, les modifications affichées seront écrites sur les disques. Dans le cas contraire, vous pourrez faire d'autres modifications.**

Les tables de partitions des périphériques suivants seront modifiées :

/dev/nvme0n1

Les partitions suivantes seront formatées :

partition n° 1 sur /dev/nvme0n1 de type ESP

partition n° 2 sur /dev/nvme0n1 de type ext4

partition n° 3 sur /dev/nvme0n1 de type swap

Faut-il appliquer les changements sur les disques ?

☐ Non

☒ **Oui**

Une fois cela fait, une fenêtre s'affiche et nous demande de sélectionner l'environnement de bureau et les applications qui seront installer. Selon vos envies, vous pouvez installer l'environnement de bureau qui vous convient le mieux mais il faut quand même savoir que je trouve personnellement que Kali est mieux optimiser sous Xfce.

#### Sélection des logiciels

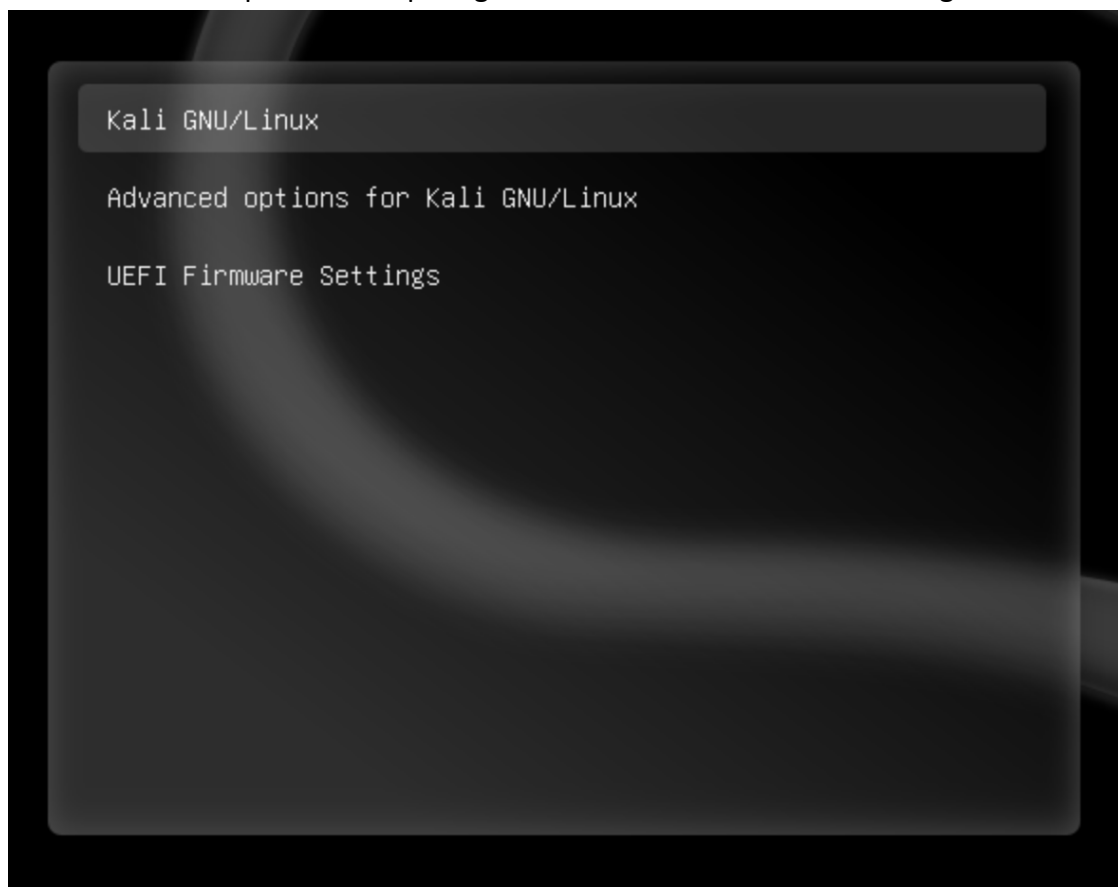
Actuellement, seul le système de base est installé. Les pré-sélections ci-dessous installeront Kali Linux avec son environnement de bureau et ses applications par défaut.

Vous pouvez personnaliser votre système en choisissant un autre environnement de bureau et/ou une autre collection d'outils.

Logiciels à installer :

- ☒ Environnement de bureau [sélectionner cet élément n'a aucun effet]
- ☒ ... Xfce (environnement de bureau par défaut de Kali)
- ☐ ... GNOME
- ☐ ... KDE Plasma
- ☒ Collection d'outils [sélectionner cet élément n'a aucun effet]
- ☒ ... top10 -- les 10 outils les plus populaires
- ☒ ... par défaut -- outils recommandés (disponibles dans le système live)

Une fois tout cela fait, une barre de chargement va commencer et terminer l'installation de Kali Linux. Laisser faire sans débrancher le réseau. Une fois terminer suivez les étapes elles sont simples donc je ne les aient pas mis dans cette procédure. Le pc va donc redémarrer et vous afficher dans un premier temps le grub. Définition en dessous de l'image.

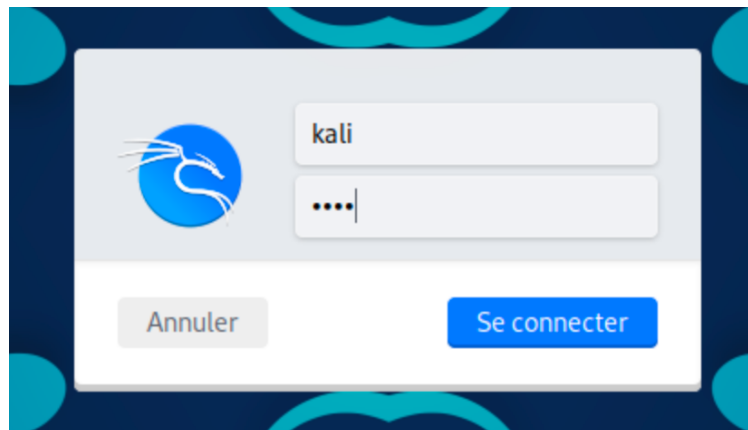


**GRUB (GRand Unified Bootloader)** est le **chargeur de démarrage** qui permet au PC de booter sur une distribution Linux (Ubuntu, Mint, Debian, Fedora, ...).

Comme toute application Linux, il possède des fichiers de configuration qui se trouvent dans **/boot** et **/etc** avec notamment **/etc/default/grub**.

Il fournit aussi des commandes comme **grub-install**, **update-grub** et **grub-mkconfig** pour notamment réparer ou restaurer GRUB.

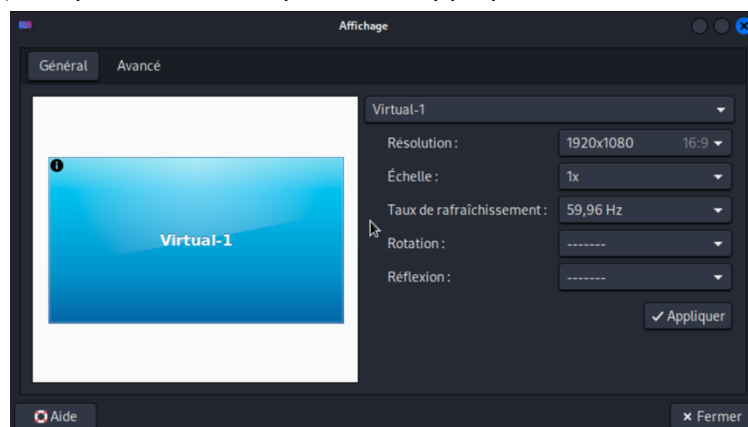
Suite à ça, nous allons arriver sur la page de connexion à Kali Linux. Nous allons donc rentrer les mots de passe que nous avons configuré précédemment dans l'installation à savoir kali : kali:kali.



On arrive donc sur le bureau de Kali Linux et la première chose à faire comme on est sur une machine virtuelle, se rendre dans les paramètres d'affichage.



On règle donc les paramètres comme on le souhaite pour ma part je préfère l'affichage en 1920/1080 (16 :9). On peut ensuite cliquer sur « Appliquez ».





**Bravo !!!** Maintenant nous avons installé Kali Linux et nous sommes prêt à effectuer l'installation des logiciels en plus ci-dessous.

## II – Installation des logiciels additionnel

### a) Les logiciels

Bien que les logiciels que nous allons installer dans cette partie sont ou seront probablement installer par défaut dans les prochaines installations de Kali Linux, il est nécessaire de détailler leur installation a la main afin de savoir le faire en cas de problème.

Nous allons donc installer 3 Logiciels à savoir :

**Volatility**

**Exiftool**

**FirefoxDecrypt**

### b) Le détail

**Volatility** est un outils open source pour l'analyse de dump mémoire, c'est un framework écrit en Python. Il permet d'analyser les dumps mémoires de Windows/Mac/Linux/Android et le framework est disponible sur Windows/Mac/Linux. On peut aussi lui adjoindre une panoplie de plugins.

**ExifTool** est un logiciel gratuit et open-source permettant de lire, d'écrire et de manipuler des métadonnées d'image, audio, vidéo et PDF.

**Firefox Decrypt** est un outil pour extraire les mots de passe des profils de Mozilla Firefox™, Thunderbird®, SeaMonkey® et dérivés. Il peut être utilisé pour récupérer les mots de passe d'un profil protégé par un Master Password tant que ce dernier est connu. Si un profil n'est pas protégé par un mot de passe principal, les mots de passe sont affichés sans invite.

### c) Mise à jour de Kali

Pour commencer sachez que cette étape peut sembler inutile mais elle permet au contraire de vous assurer de tous les temps être à jour. Comme ça tous les logiciels sont compatibles avec votre version. Pour la première commande :

```
1. sudo apt-get update && apt-get upgrade && apt-get dist-upgrade
```

### d) Installation de Volatility

Dans un premier temps, il est nécessaire d'installer les paquets qui vont être nécessaire à l'installation de volatility.

```
1. sudo apt-get install python3
2. sudo apt-get install python3-pip build-essential python-setuptools
```

Une fois les paquets nécessaires installés, nous allons aller sur le site de volatility et télécharger le code source qui est nécessaire pour l'installation. Rendez-vous donc sur le site à cette adresse. <https://www.volatilityfoundation.org/releases-vol3>. Télécharger la version dont vous avez besoin. Dans mon cas je vais prendre la dernière version actuelle à savoir la version Volatility 3 2.4.1.

## Volatility 3 v2.4.1

- New plugins:
  - linux.sockstat
  - linux.iomem
  - linux.psscan
  - linux.envvars
  - windows.drivermodule
  - windows.vadwalk
- Pid filtering for Windows pstree plugin
- Minor fixes for Windows callbacks plugin
- Minimum Python version was increased to 3.7
- Python-snappy dependency was replaced with ctypes to ease installation
- Whole codebase was reformatted with black
- Faster release cycle (targetting every 4 months)

Released: April 2023

- [volatility3-2.4.1-py3-none-any.whl](#)
- [Source code\(zip\)](#)
- [Source code\(tar.gz\)](#)

On se retrouve ensuite dans le dossier téléchargement ou le fichier de code source a été téléchargé. On va maintenant décompresser l'archive précédemment téléchargée. Pour ce faire on ouvre un terminal en mode root, on se rend dans le dossier Téléchargement.

```
1. cd /home/kali/Téléchargement/
```

Une fois dans le dossier téléchargement on décompresse l'archive.

```
1. unzip volatility3-2.4.1.zip
```

Une fois décompresser, un dossier est créé. Nous allons maintenant le déplacer sur le bureau ou seront tous les outils de kali que je vais installer pour ce faire.

```
1. mv volatility3-2.4.1.zip /home/kali/Bureau/volatility
```

Une fois cela fait on peut se rendre sur le bureau pour voir si le fichier volatility est bien là. Vous allez donc voir que le fichier a un cadenas car il a été manipulé par le superutilisateur donc l'utilisateur Kali n'a pas les droits. Pour lui attribuer les droits, nous allons faire ceci.

```
1. chmod 777 /home/kali/Bureau/volatility
```

Une fois cette commande faite le cadenas disparaît. On va donc pouvoir poursuivre l'installation de volatility.

Pour l'installation on va faire cette commande

```
1. python3 /home/kali/Bureau/volatility/setup.py install
```

Une fois la commande terminée, vous pouvez donc tester si volatility fonctionne bien.

```
1. cd /home/kali/Bureau/volatility
2. python3 vol.py
```

Normalement, la commande devrait afficher les options qui sont possible de faire avec volatility.

#### e) Installation de Exiftool

Pour commencer nous allons télécharger le logiciel. Pour ce faire faire cette commande

```
1. git clone https://github.com/exiftool/exiftool.git
```

Maintenant on peut retrouver sur le bureau le fichier exiftool avec le cadenas. Vous pouvez maintenant appliquer la méthode vue plus haut pour le faire disparaître. On se rend donc dans le fichier précédemment télécharger avec la commande suivante.

```
1. cd exiftool
```

Maintenant on peut tester que le programme fonctionne en faisant la commande suivante

```
1. ./exiftool
```

Vous allez donc voir une ligne s'afficher avec la manière donc il faut utiliser la commande.

#### f) Installation de Firefox Decrypt

De la même manière que exiftool, nous allons d'abord télécharger l'outil. Avec cette commande.

```
1. git clone https://github.com/unode/firefox_decrypt.git
```

Une fois la commande faite, nous allons faire la même chose en enlevant le cadenas au fichier télécharger. Nous pouvons maintenant exécuter l'outil de cette manière.

```
1. python firefox_decrypt.py
```

Des erreurs vont s'afficher mais c'est normal car aucun fichier de base de données Firefox a été spécifié.

## III – Création de sa propre image de Kali Linux (ISO)

### a) Installation des paquets

Nous allons dans un premier temps installer les paquets nécessaires à la manipulation.

```
1. sudo apt install -y git live-build simple-cdd cdebootstrap curl
2. git clone https://gitlab.com/kalilinux/build-scripts/live-build-config.git
```

Suite à ça nous allons commencer la création de l'image grâce a ces commandes.

```
1. cd live-build-config/
2. ./build.sh --verbose --installer
```

## IV – Modifier la version de Python

### a) Vérification

Dans un premier temps nous allons voir quelle version de python sont installer. Pour ce faire, cette commande.

```
1. update-alternatives --list python
```

Un message d'erreur doit donc apparaitre. Nous allons donc ajouter plusieurs alternative grâce au commandes suivante.

```
1. update-alternatives --install /usr/bin/python python
   /usr/bin/python2.7 1
2. update-alternatives --install /usr/bin/python python
   /usr/bin/python3.11 2
```

On peut donc révéfier si on a les versions alternatives de python d'installer avec cette commande qui doit donc retourner un résultat avec les version que vous avez choisi d'installer.

```
1. update-alternatives --config python
```

On peut donc avec cette commande choisir la version de python que l'on veut utiliser.

```
# update-alternatives --config python
There are 2 choices for the alternative python (providing /usr/bin/python).

   Selection    Path                        Priority  Status
   -----
*  0            /usr/bin/python3.4          2        auto mode
    1            /usr/bin/python2.7          1        manual mode
    2            /usr/bin/python3.4          2        manual mode

Press enter to keep the current choice[*], or type selection number: 1
update-alternatives: using /usr/bin/python2.7 to provide /usr/bin/python (python)
```

Sources : <https://mk57blog.wordpress.com/2017/01/28/comment-modifier-la-version-par-defaut-de-python-sur-debian/>

On va donc maintenant installer PIP pour la version 2.7 de python pour ce faire on commence par mettre à jour le système

```
1. sudo apt-get update
```

Puis on installe les paquets nécessaires

```
1. curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py
```

Et enfin on exécute le script téléchargé

```
1. sudo python2 get-pip.py
```

Une fois fait tout est bon.

## V – Installation de la suite Tinyscript

### a) Contenu

Cette suite comprend 3 Outils :

- StegoLSB
- StegoPVD
- StegoPIT

Ces outils sont chiant à installer. Il faut donc suivre la procédure au pied de la lettre.

### b) Installation

Dans un premier temps nous allons télécharger les dépendances.

```
1. pip install tinyscript
```

Une fois cela fait, nous allons télécharger l'outil

```
1. wget  
https://gist.githubusercontent.com/dhondta/d2151c82dcd9a610a7380df1c6a0272c/raw/stegolsb.py && chmod +x stegolsb.py && sudo mv  
stegolsb.py /usr/bin/stegolsb
```

On peut aussi installer les deux autres outils une fois que le téléchargement de celui-ci est fait.

```
1. wget  
https://gist.githubusercontent.com/dhondta/feaf4f5fb3ed8d1eb7515abe8cde4880/raw/stegopvd.py && chmod +x stegopvd.py && sudo mv  
stegopvd.py /usr/bin/stegopvd
```

Et enfin le dernier

```
1. wget  
https://gist.githubusercontent.com/dhondta/30abb35bb8ee86109d17437b1  
1a1477a/raw/stegopit.py && chmod +x stegopit.py && sudo mv  
stegopit.py /usr/bin/stegopit
```

Une fois cela fait on peut donc se référer a la documentation des outils disponible a ces liens :

- <https://gist.github.com/dhondta/d2151c82dcd9a610a7380df1c6a0272c>
- <https://gist.github.com/dhondta/feaf4f5fb3ed8d1eb7515abe8cde4880>
- <https://gist.github.com/dhondta/30abb35bb8ee86109d17437b11a1477a>

FIN