

Kali – Linux



Kali Linux est une distribution GNU/Linux sortie le 13 mars 2013, basée sur Debian. L'objectif de Kali Linux est de fournir une distribution regroupant l'ensemble des outils nécessaires aux tests de sécurité d'un système d'information, notamment le test d'intrusion. Plus de 300 programmes d'analyse de sécurité y sont pré-installés.

Il est téléchargeable en direct ou par torrent comme la plupart des distributions, sous la forme d'une image ISO en 32 bits ou 64 bits. Il est possible de l'utiliser en version Live, de l'installer sur un disque dur et même de le démarrer dans une machine virtuelle.

Le système d'exploitation Kali-Linux possède plusieurs avantages. Il possède tous les programmes d'infiltrations nécessaires pour réaliser des tests sur l'infrastructure réseaux que nous avons créés et il est gratuit. Nous connaissons Linux Ubuntu de par notre formation, ce qui facilite la prise en main de Kali-Linux.

Pour l'installer vous devez vous munir d'une clé USB possédant un minimum de 2GO d'espace libre afin de pouvoir mettre l'image ISO de Kali Linux préalablement téléchargée sur « <https://www.kali.org/downloads/> ».

Par la suite il faut rendre cette clé USB compatible au boot avec le Créateur de Disque de Démarrage qui est disponible sur Linux Debian. Une fois l'application de Créateur de Disque de Démarrage lancée, il repère les images ISO disponibles sur l'ordinateur, ainsi que les clés USB ou supports pouvant accueillir cette image ISO. Il faut les sélectionner et lancer la création.

Le boot aussi appelé « l'amorce » est la procédure de démarrage d'un ordinateur qui va charger le programme initial. D'une manière générale c'est ce qui lance le système d'exploitation.

Pour utiliser Kali Linux il faut démarrer l'ordinateur en laissant la clé USB connectée. Lors du démarrage, la touche « F12 » permet d'accéder au menu BIOS afin de sélectionner « USB Storage Device ». Le BIOS comprend le logiciel nécessaire à l'amorçage de l'ordinateur. Par la suite un menu d'installation apparaît avec plusieurs options d'utilisations.

Nous avons préféré utiliser la version LIVE dans un premier temps. Cela permet d'avoir un accès immédiat et temporaire au système d'exploitation afin de se familiariser avec l'environnement.

Installation

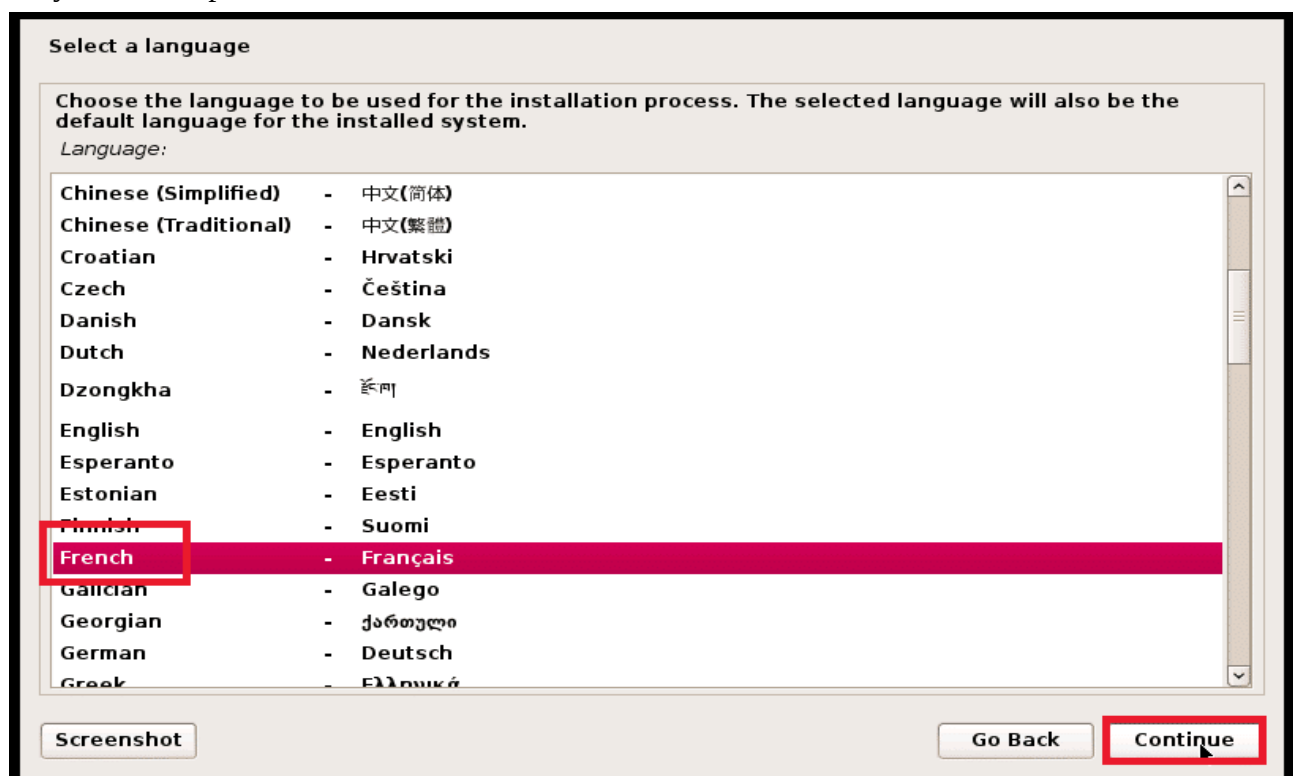
Une fois l'environnement découvert, nous avons procédé à l'installation de Kali-Linux sur le PC5 - WAN dédié aux tests d'intrusions.

Ce PC5 doit être branché au Routeur4 comme indiqué dans le plan du réseau.

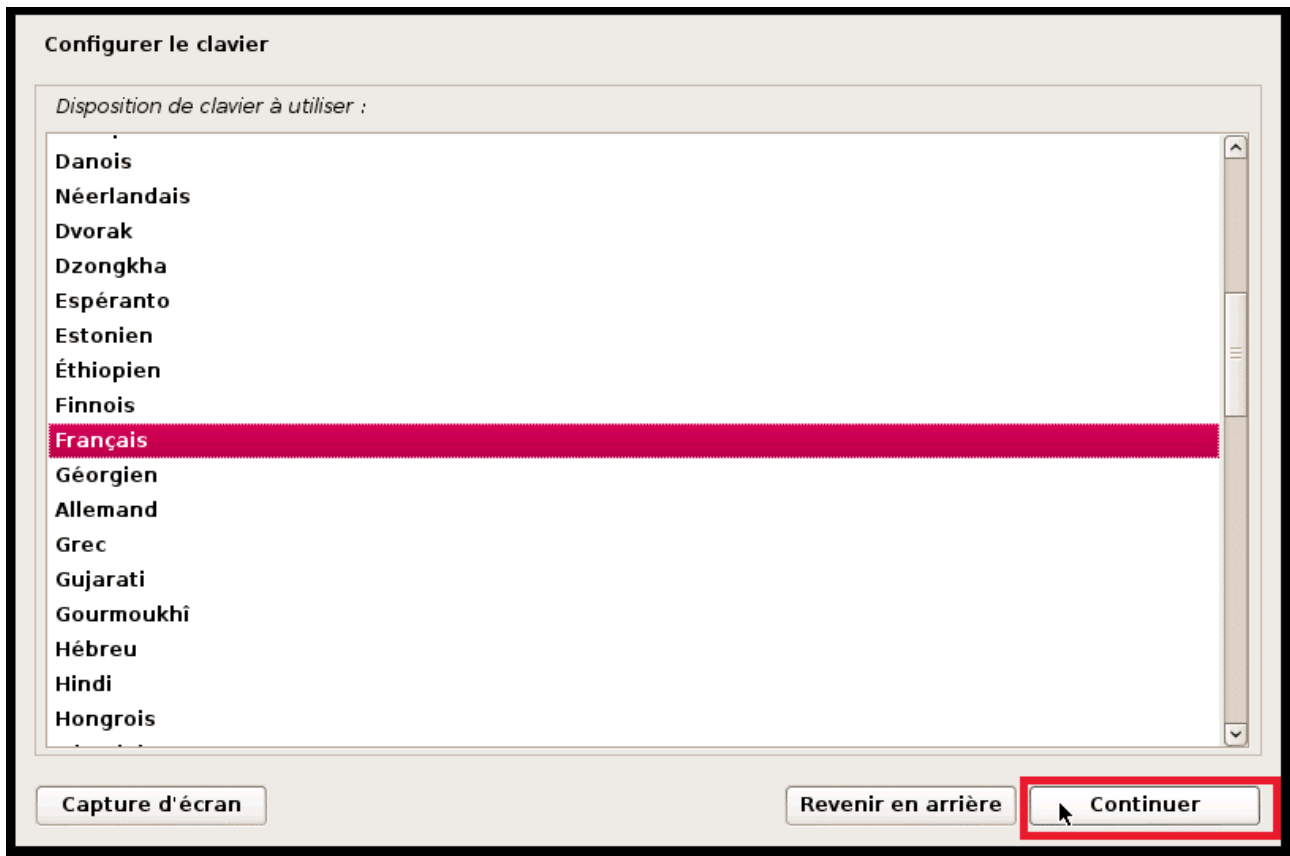
Dans le menu d'installation de Kali-Linux, nous avons choisi « Graphical installation » par confort visuel.



Par la suite, il vous est demandé de sélectionner la langue dans laquelle vous souhaitez paramétrer le système d'exploitation.



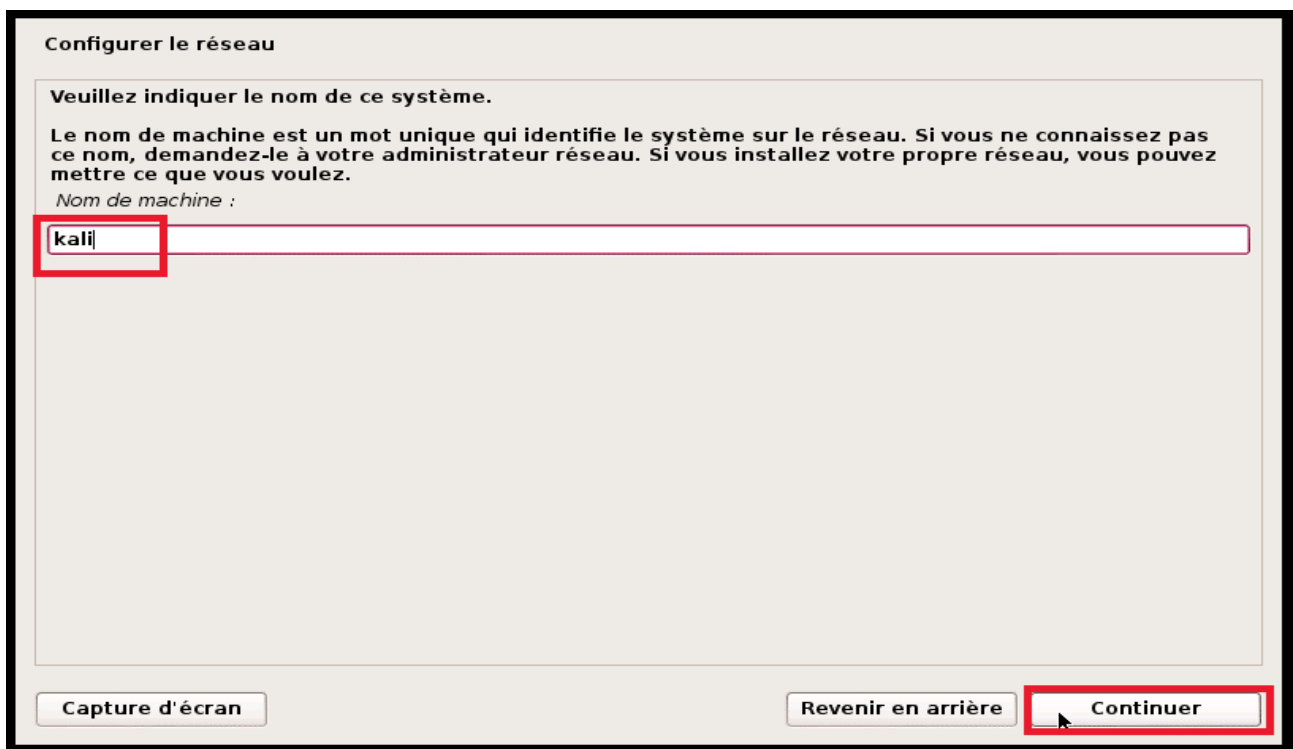
Il est possible de configurer le clavier dans la langue que vous souhaitez.



Votre ordinateur prendra automatiquement l'adresse IP attribuée par le DHCP.

Si ce n'est pas le cas, vous aurez la possibilité de configurer manuellement ou de réessayer la configuration DHCP.

Vous choisirez le nom que vous souhaitez donner au système d'exploitation. Kali est sélectionné par défaut.




Vous pouvez sélectionner le nom de domaine. Si vous ne souhaitez pas le renseigner, vous pouvez laisser le champ vide et continuer.

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 :

Vous pouvez choisir un mot de passe. Si vous ne renseignez rien, le mots de passe « toor » est activé par défaut.



Créer les utilisateurs et choisir les mots de passe

Vous devez choisir un mot de passe pour le superutilisateur, le compte d'administration du système. Un utilisateur malintentionné ou peu expérimenté qui aurait accès à ce compte peut provoquer des désastres. En conséquence, ce mot de passe ne doit pas être facile à deviner, ni correspondre à un mot d'un dictionnaire ou vous être facilement associé.

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

Le superutilisateur (« root ») ne doit pas avoir de mot de passe vide. Si vous laissez ce champ vide, le compte du superutilisateur sera désactivé et le premier compte qui sera créé aura la possibilité d'obtenir les privilèges du superutilisateur avec la commande « sudo ».

Par sécurité, rien n'est affiché pendant la saisie.

Mot de passe du superutilisateur (« root ») :

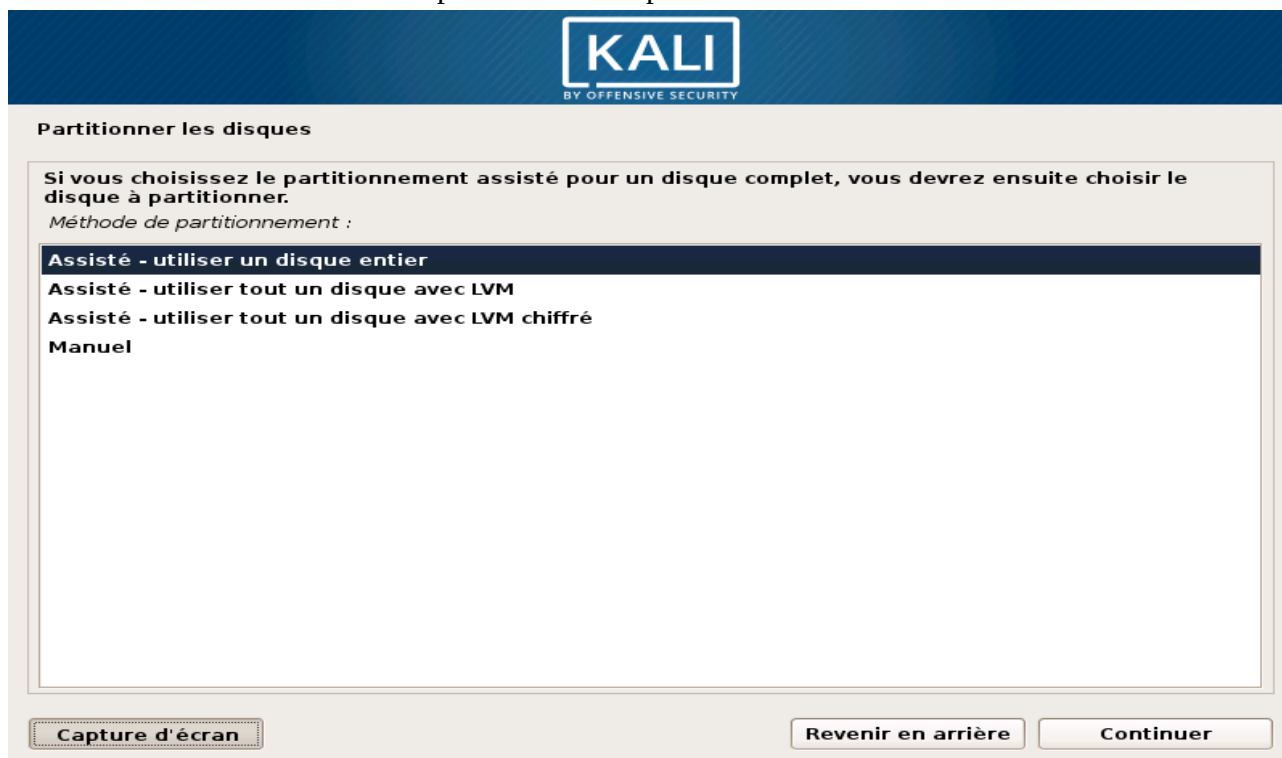
☐ Afficher le mot de passe en clair

Veuillez entrer à nouveau le mot de passe du superutilisateur afin de vérifier qu'il a été saisi correctement.

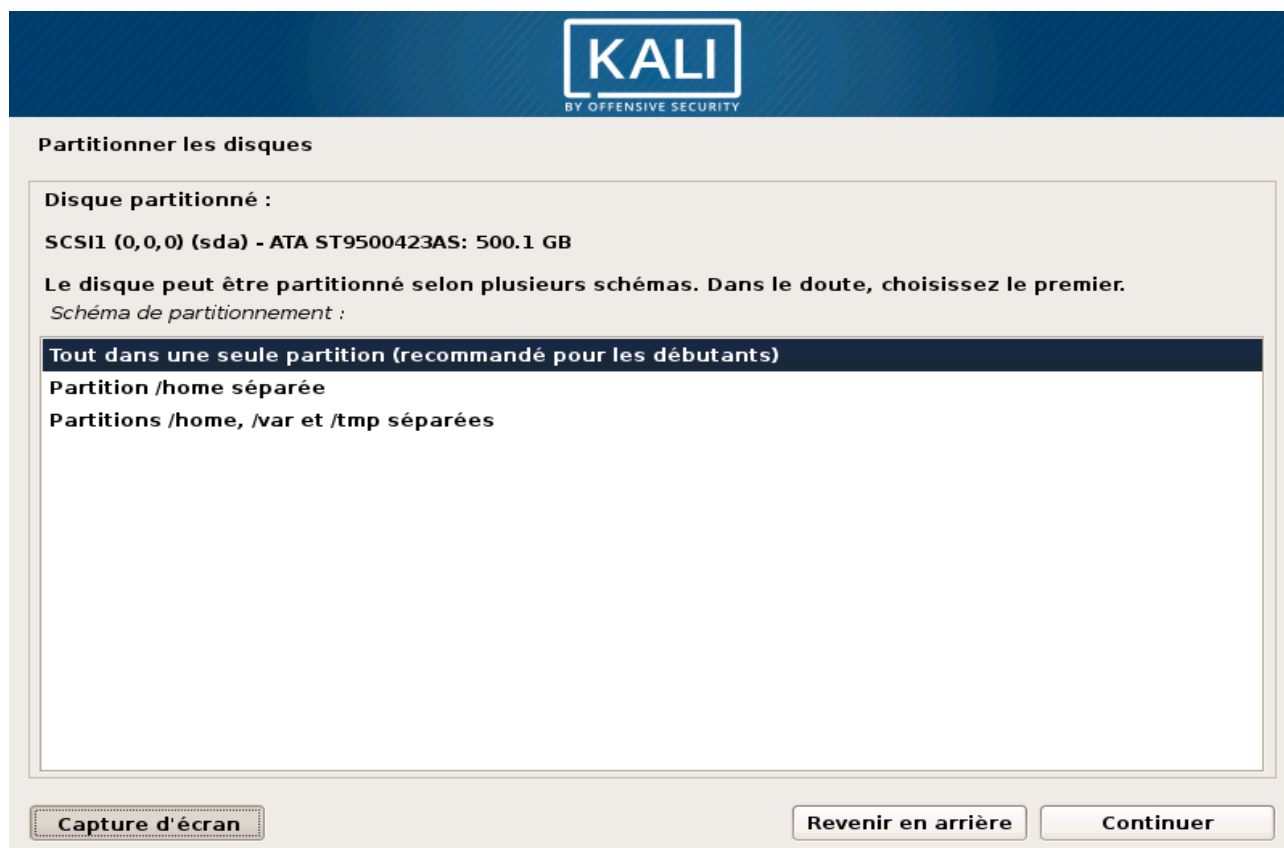
Confirmation du mot de passe :

☐ Afficher le mot de passe en clair

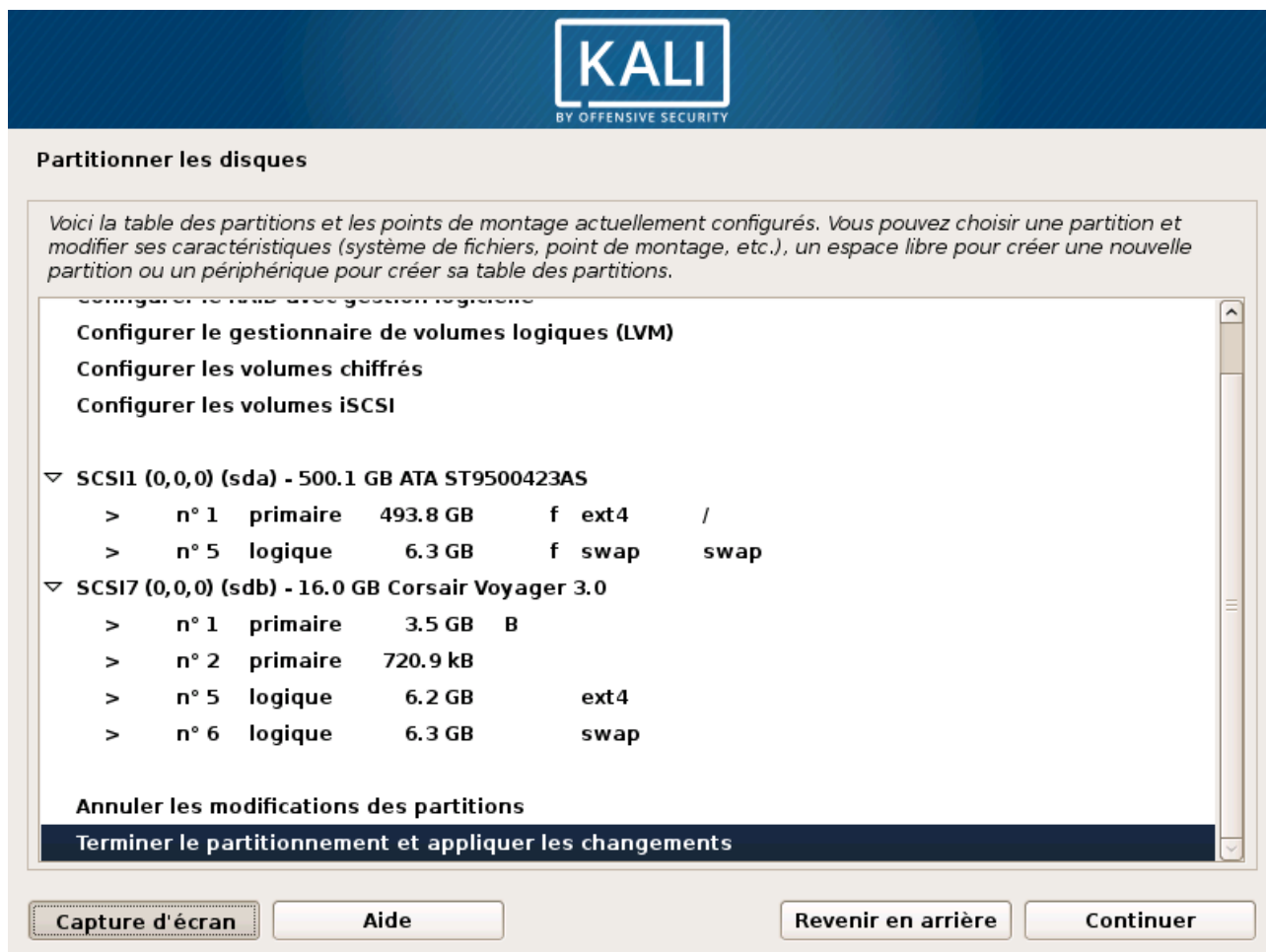
Vous devez choisir quelle place Kali-Linux prendra sur vos disques. Dans notre cas, le pc5 est entièrement dédié à kali-Linux et prendra toute la place sur l'ordinateur.



Nous pouvons ensuite répartir plus précisément l'espace libre. Pour faciliter l'installation, nous pouvons choisir : « Tous les fichiers dans une partition ». Ceci est recommandé pour les nouveaux utilisateurs de Kali.



Vous devez ensuite « terminer la partition et écrire les modifications sur le disque ».



The image shows the 'Partitionner les disques' (Partition disks) window in the Kali Linux installer. At the top is the Kali logo with the tagline 'BY OFFENSIVE SECURITY'. Below the title bar, there is a text box explaining that the user can choose a partition to modify its characteristics (file system, mount point, etc.) or create a new one. A scrollable list shows the available disks and their partitions. The first disk is SCSI1 (0,0,0) (sda) - 500.1 GB ATA ST9500423AS, with partitions: n° 1 primaire 493.8 GB f ext4 / and n° 5 logique 6.3 GB f swap swap. The second disk is SCSI7 (0,0,0) (sdb) - 16.0 GB Corsair Voyager 3.0, with partitions: n° 1 primaire 3.5 GB B, n° 2 primaire 720.9 kB, n° 5 logique 6.2 GB ext4, and n° 6 logique 6.3 GB swap. At the bottom of the list are buttons for 'Annuler les modifications des partitions' and 'Terminer le partitionnement et appliquer les changements'. Below the scrollable list are four buttons: 'Capture d'écran', 'Aide', 'Revenir en arrière', and 'Continuer'.

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.

Configurer le gestionnaire de volumes logiques (LVM)
Configurer les volumes chiffrés
Configurer les volumes iSCSI

SCSI1 (0,0,0) (sda) - 500.1 GB ATA ST9500423AS

- > n° 1 primaire 493.8 GB f ext4 /
- > n° 5 logique 6.3 GB f swap swap

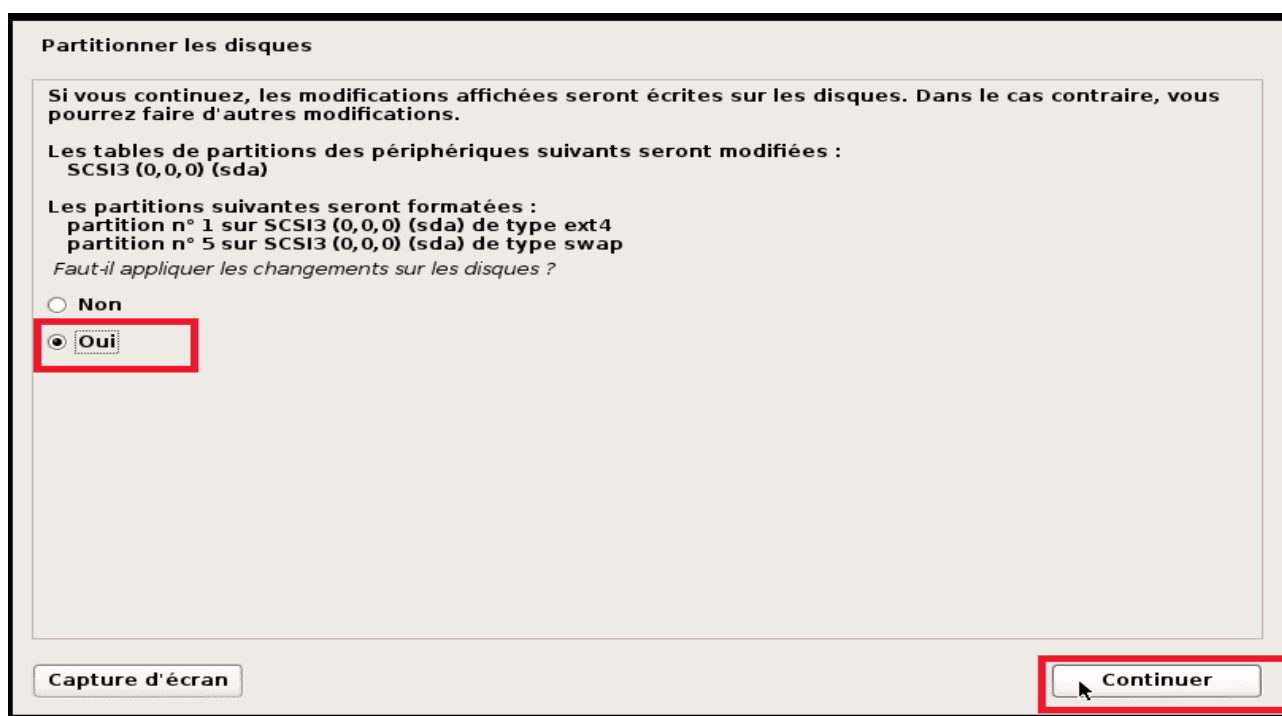
SCSI7 (0,0,0) (sdb) - 16.0 GB Corsair Voyager 3.0

- > n° 1 primaire 3.5 GB B
- > n° 2 primaire 720.9 kB
- > n° 5 logique 6.2 GB ext4
- > n° 6 logique 6.3 GB swap

Annuler les modifications des partitions
Terminer le partitionnement et appliquer les changements

Capture d'écran Aide Revenir en arrière Continuer

Choisissez oui et cliquez sur continuer. Cela va commencer à copier les fichiers d'un support à un autre et à installer Kali Linux.



The image shows the confirmation screen in the Kali Linux installer. It asks if the user wants to apply the changes to the disks. The text states: 'Si vous continuez, les modifications affichées seront écrites sur les disques. Dans le cas contraire, vous pourrez faire d'autres modifications.' It then lists the changes: 'Les tables de partitions des périphériques suivants seront modifiées : SCSI3 (0,0,0) (sda)' and 'Les partitions suivantes seront formatées : partition n° 1 sur SCSI3 (0,0,0) (sda) de type ext4, partition n° 5 sur SCSI3 (0,0,0) (sda) de type swap'. It then asks 'Faut-il appliquer les changements sur les disques ?' with two radio buttons: 'Non' and 'Oui'. The 'Oui' button is selected and highlighted with a red box. At the bottom are two buttons: 'Capture d'écran' and 'Continuer'. The 'Continuer' button is also highlighted with a red box.

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 :
SCSI3 (0,0,0) (sda)

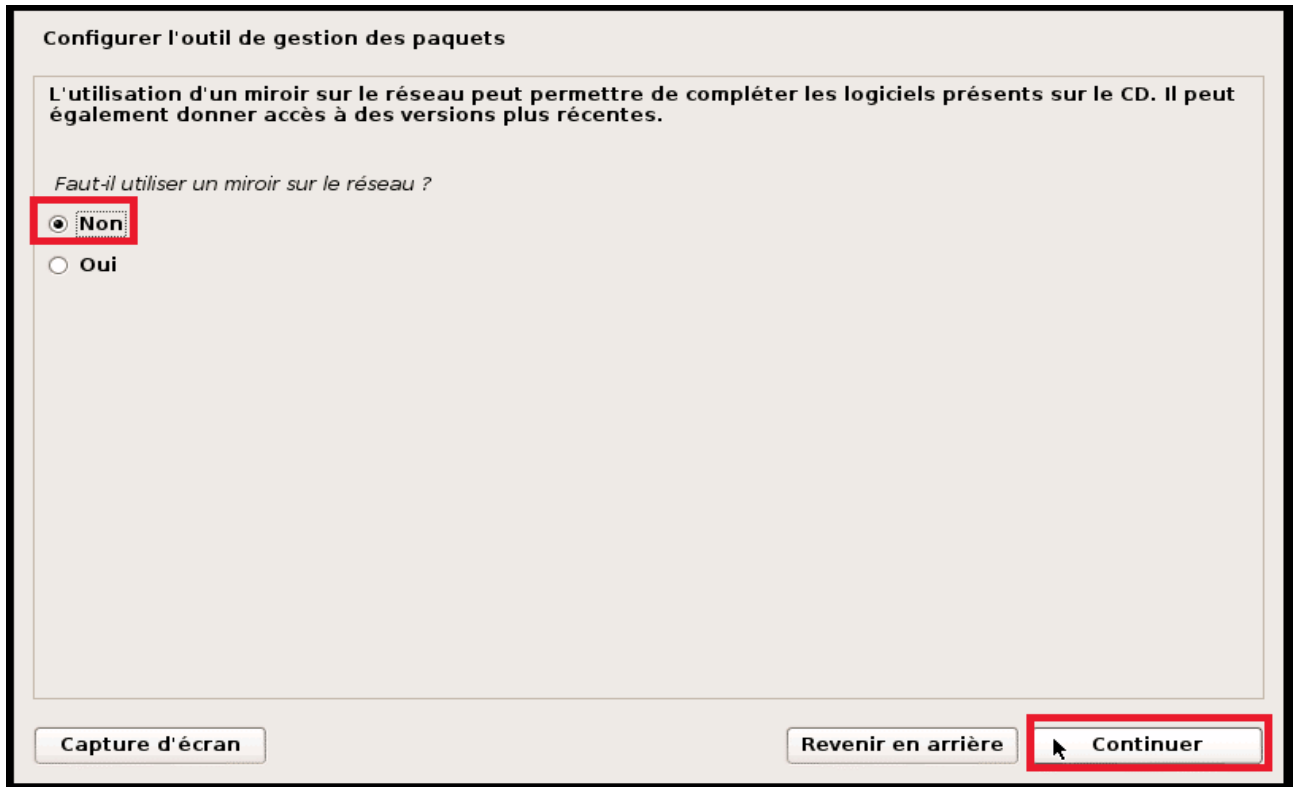
Les partitions suivantes seront formatées :
partition n° 1 sur SCSI3 (0,0,0) (sda) de type ext4
partition n° 5 sur SCSI3 (0,0,0) (sda) de type swap

Faut-il appliquer les changements sur les disques ?

☐ Non
☒ Oui

Capture d'écran Continuer

Après avoir copié les fichiers, il vous sera demandé de configurer le gestionnaire de paquets. Dans cette étape, nous allons configurer le réseau miroir pour obtenir les paquets pour les installations futures. Vous ne disposez pas d'une connexion Internet, vous pouvez donc choisir non.



Configurer l'outil de gestion des paquets

L'utilisation d'un miroir sur le réseau peut permettre de compléter les logiciels présents sur le CD. Il peut également donner accès à des versions plus récentes.

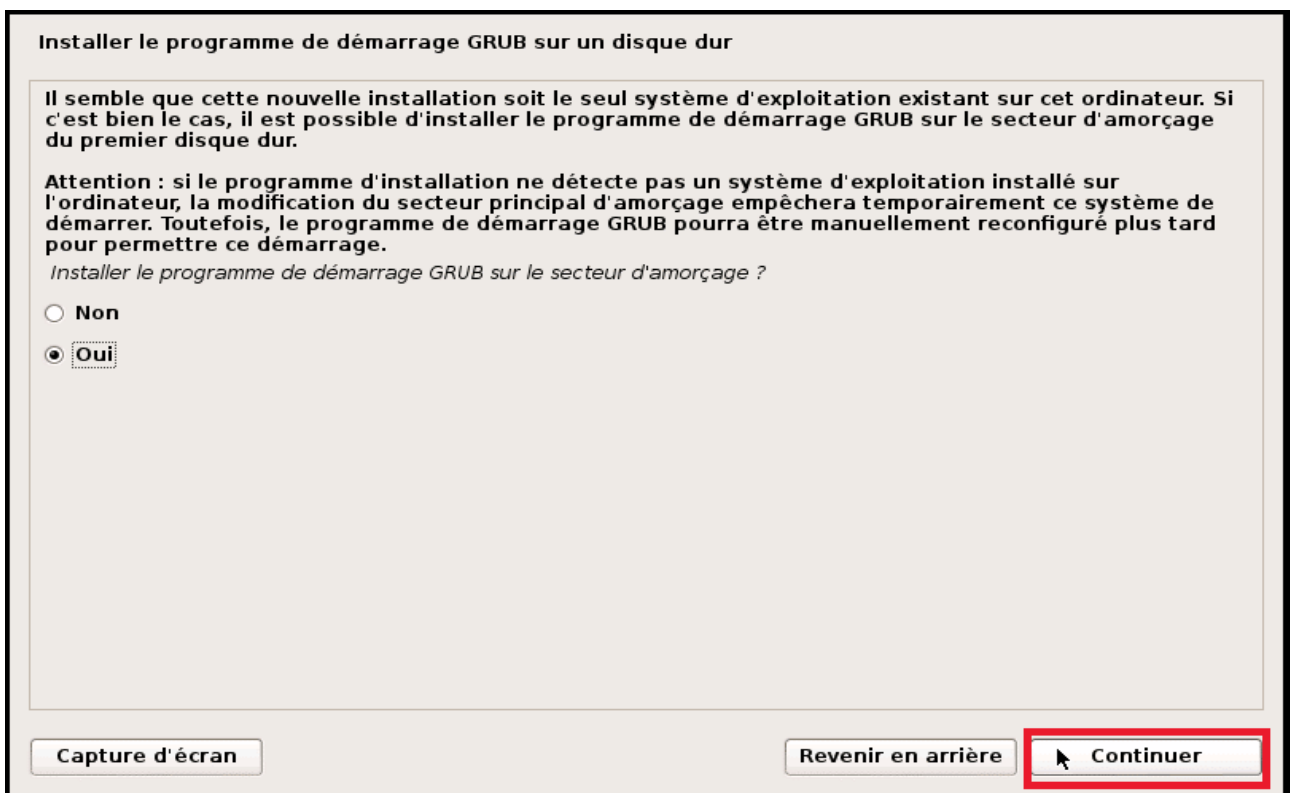
Faut-il utiliser un miroir sur le réseau ?

☒ Non

☐ Oui

Capture d'écran Revenir en arrière Continuer

Après avoir configuré le gestionnaire de paquets, il se téléchargera et installera les paquets à partir du miroir choisi. Il faut choisir oui pour installer le chargeur de démarrage GRUB dans notre système.



Installer le programme de démarrage GRUB sur un disque dur

Il semble que cette nouvelle installation soit le seul système d'exploitation existant sur cet ordinateur. Si c'est bien le cas, il est possible d'installer le programme de démarrage GRUB sur le secteur d'amorçage du premier disque dur.

Attention : si le programme d'installation ne détecte pas un système d'exploitation installé sur l'ordinateur, la modification du secteur principal d'amorçage empêchera temporairement ce système de démarrer. Toutefois, le programme de démarrage GRUB pourra être manuellement reconfiguré plus tard pour permettre ce démarrage.

Installer le programme de démarrage GRUB sur le secteur d'amorçage ?

☐ Non

☒ Oui

Capture d'écran Revenir en arrière Continuer

Vous devrez sélectionner votre disque de nouveaux. Vous pouvez ensuite choisir si votre horloge système est réglée sur le temps universel coordonné (UTC). Une page vous affiche ensuite que votre système d'exploitation est prêt. L'ordinateur redémarrera et il ne faudra pas oublier d'enlever la clé USB d'installation.