

Universite De Technologie D'haiti

Faculte Des Sciences Informatique

Cour:Cyber Securite

Travaux Diriges:Virtualisation et Manipulation de Kali Linux

Niveau:|||

Preparer par

Septama Louison

Proffesseur:Ismael SAINT AMOUR

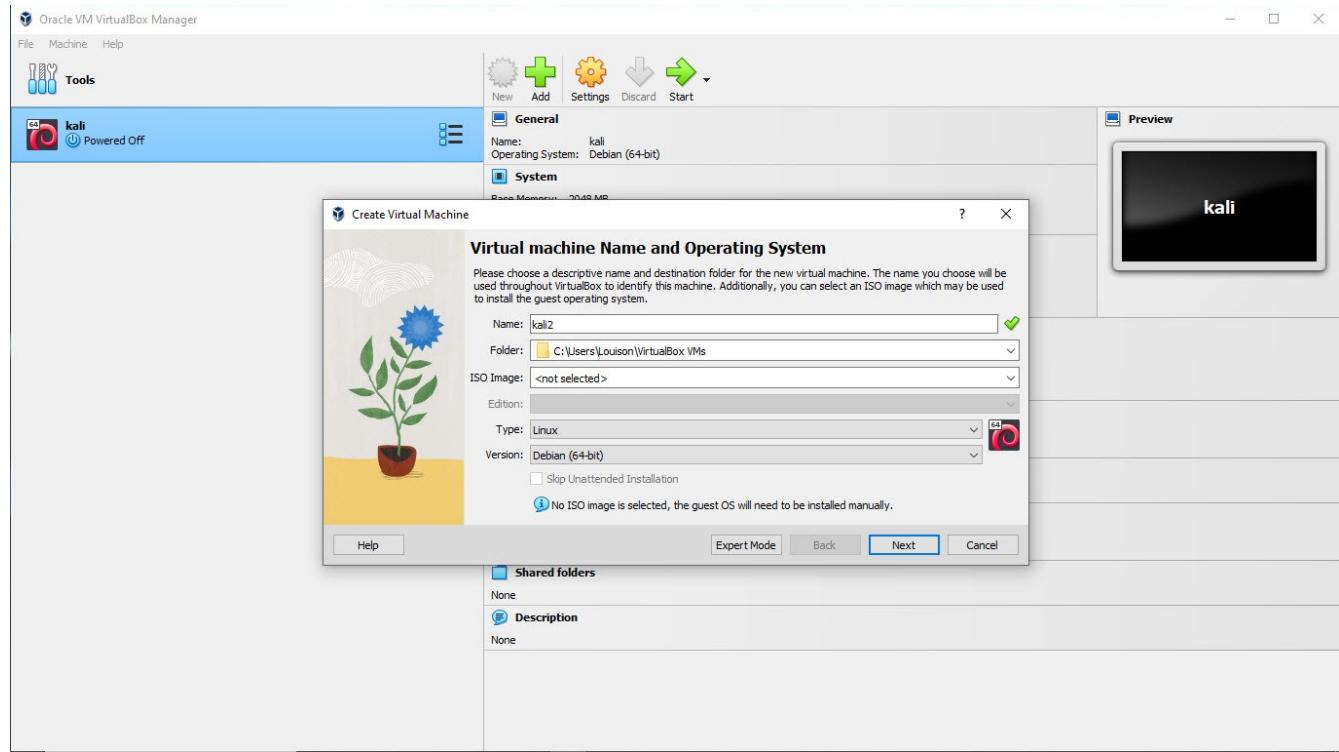
11/02/2025

2.Creation d'une nouvelle machine virtuelle

Cliquez sur « New » pour créer une nouvelle machine virtuelle. Suivez l'assistant de creation de machine virtuelle.

3.Configuration de la machine virtuelle :

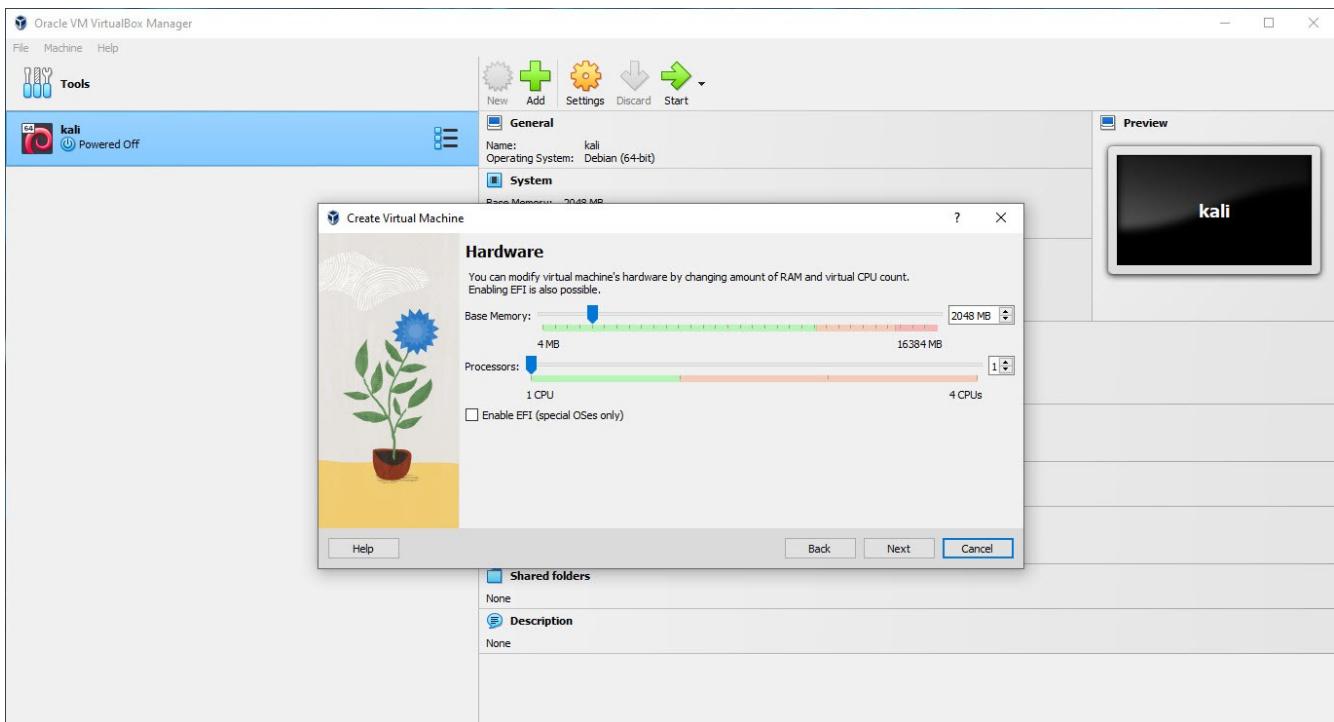
Entrez un nom pour la machine virtuelle, choisissez le type(Linux)et la version du systeme d'exploitation que vous allez installez (Debian 64-bit).



Assignation de la memoire RAM :

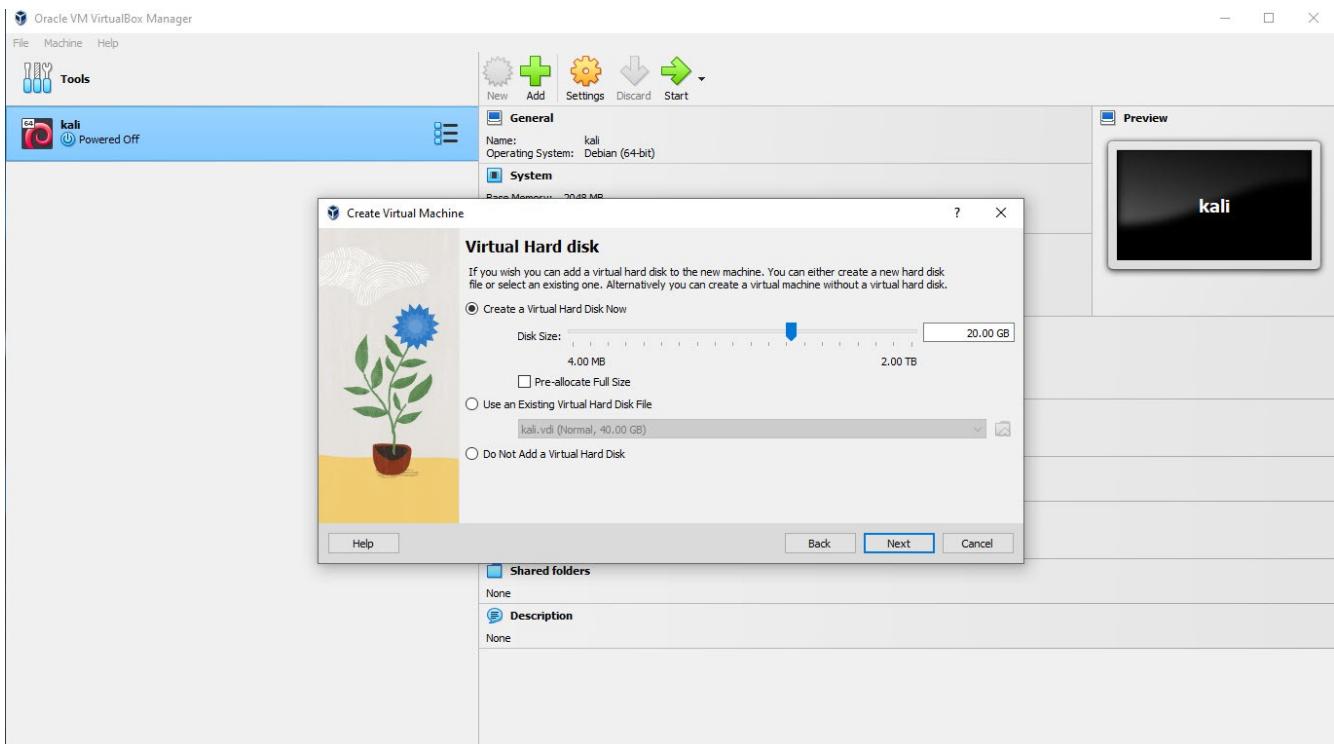
Choisissez la quantite de memoire RAM que vous souhaitez allouer a la machine virtuelle(La quantite de memoire recommandee de 2048 Mo fait reference a 2 GB de memoire RAM.)

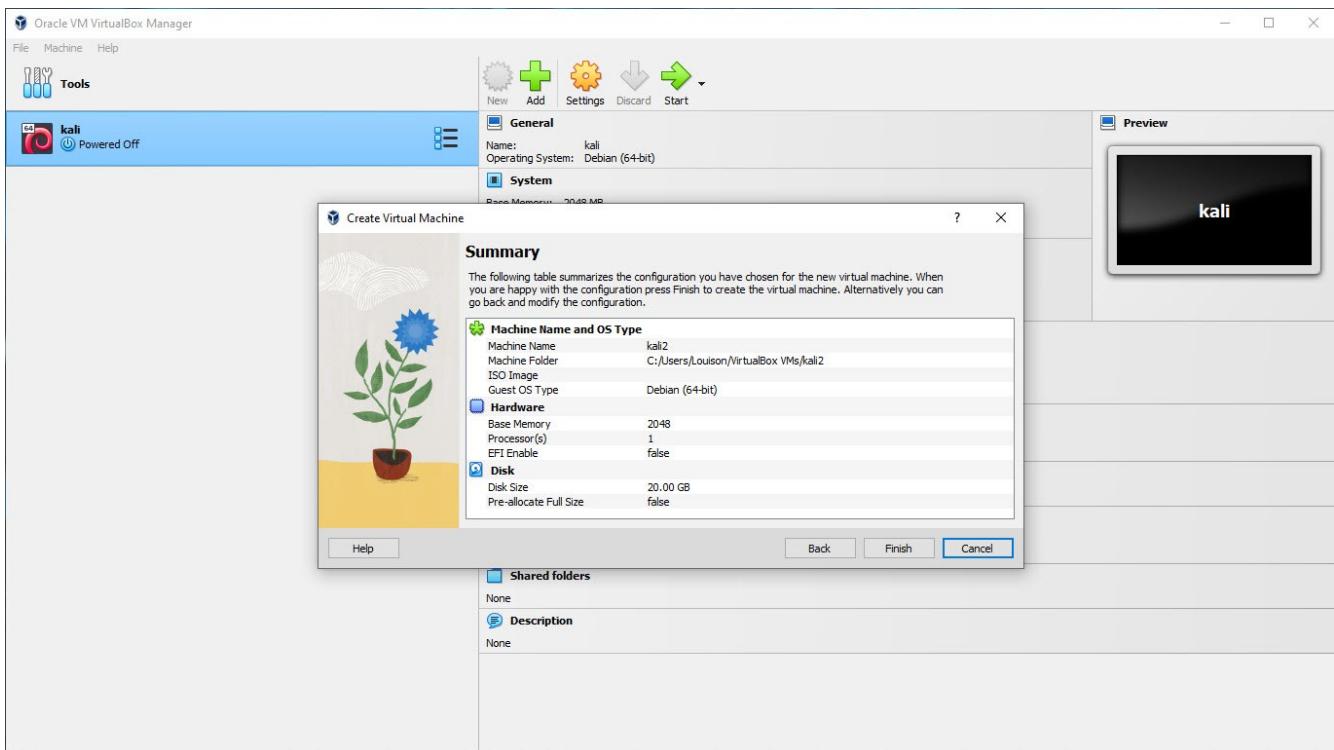
Assurer-vous de laisser suffisamment de RAM pour le systeme hote.



Attribution de la taille du disque dur :

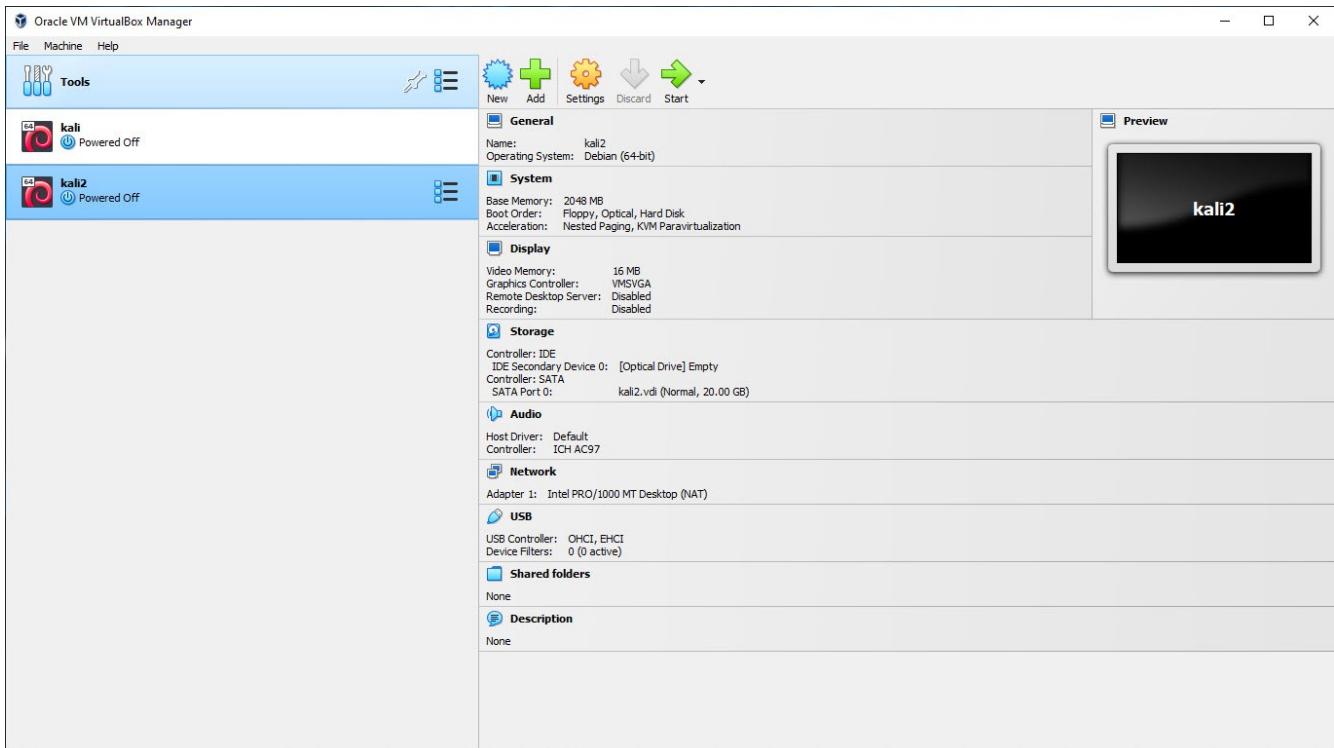
Allouez la taille du disque dur virtuel selon les exigences du système d'exploitation.(20GB)

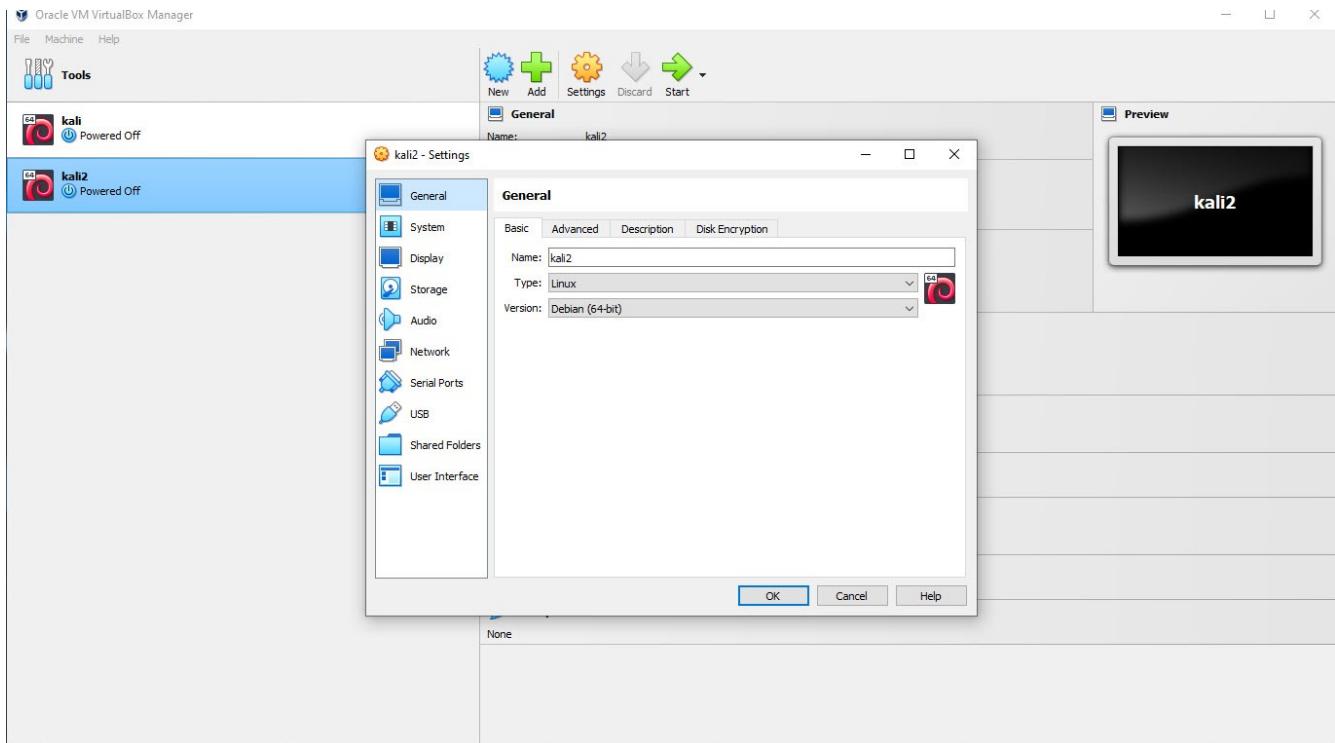




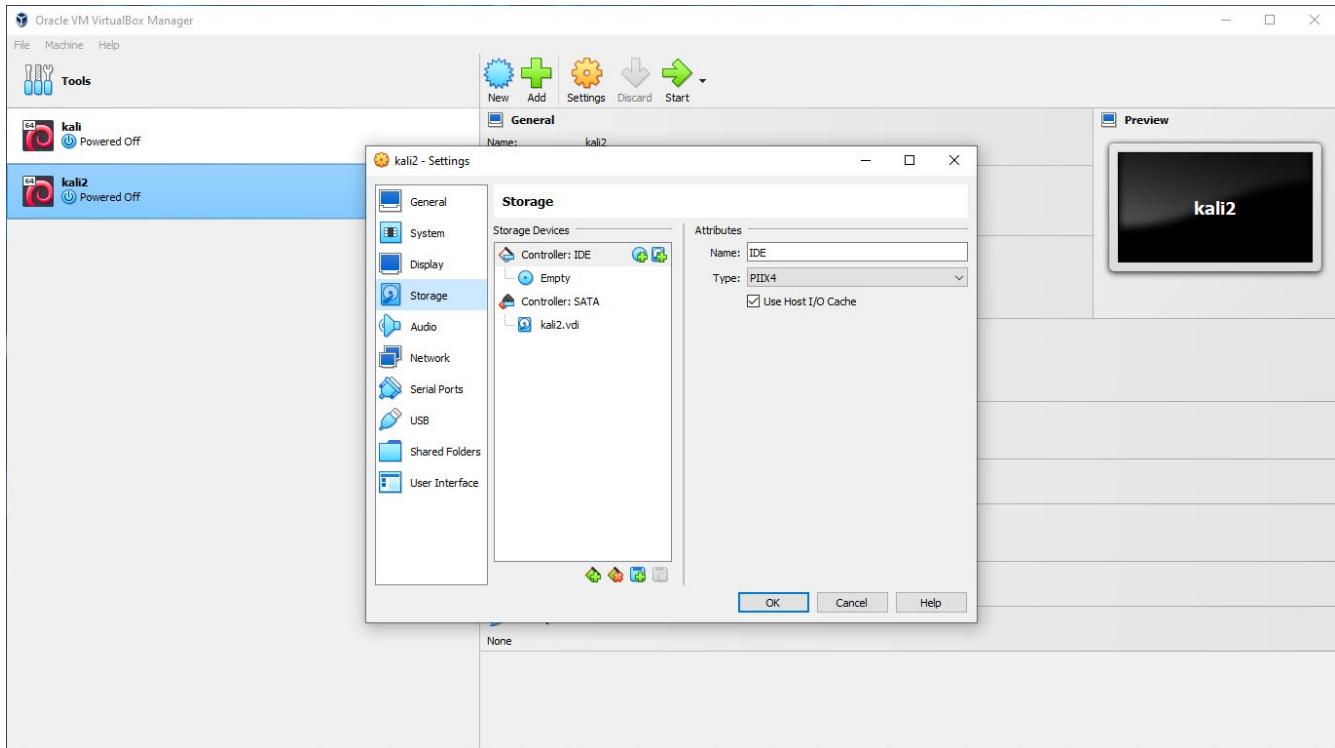
Montage de l'image ISO:

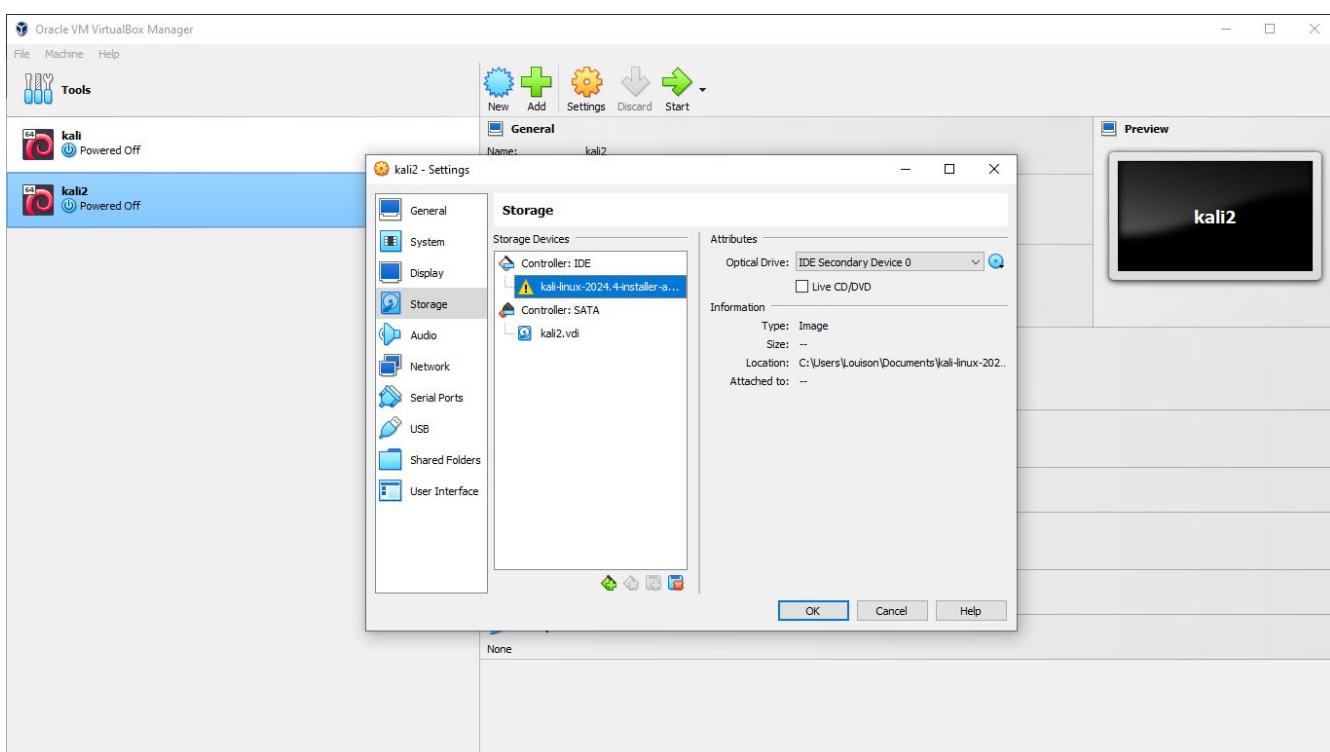
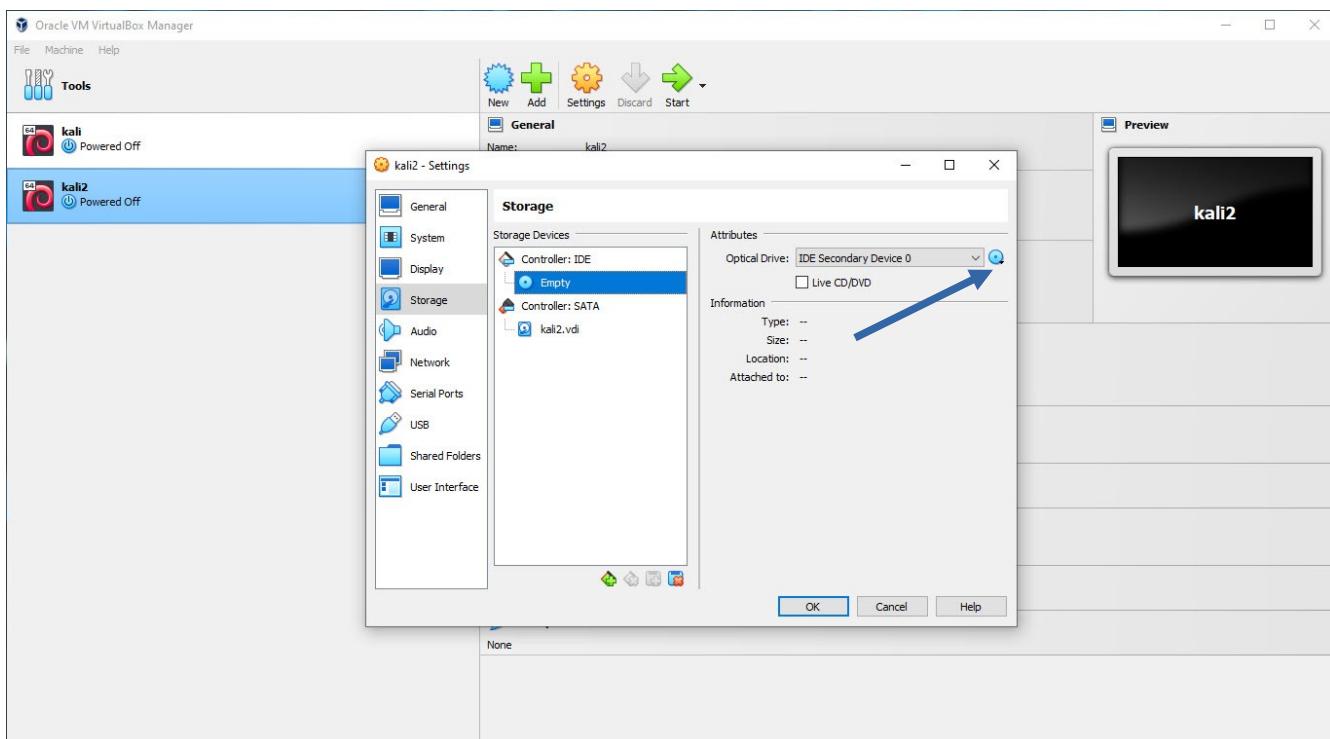
Cliquez sur « Settings », ensuite « storage », cliquez sur l'icone du disque optique vide et selectionner l'image ISO telecharge comme peripherique de demarrage





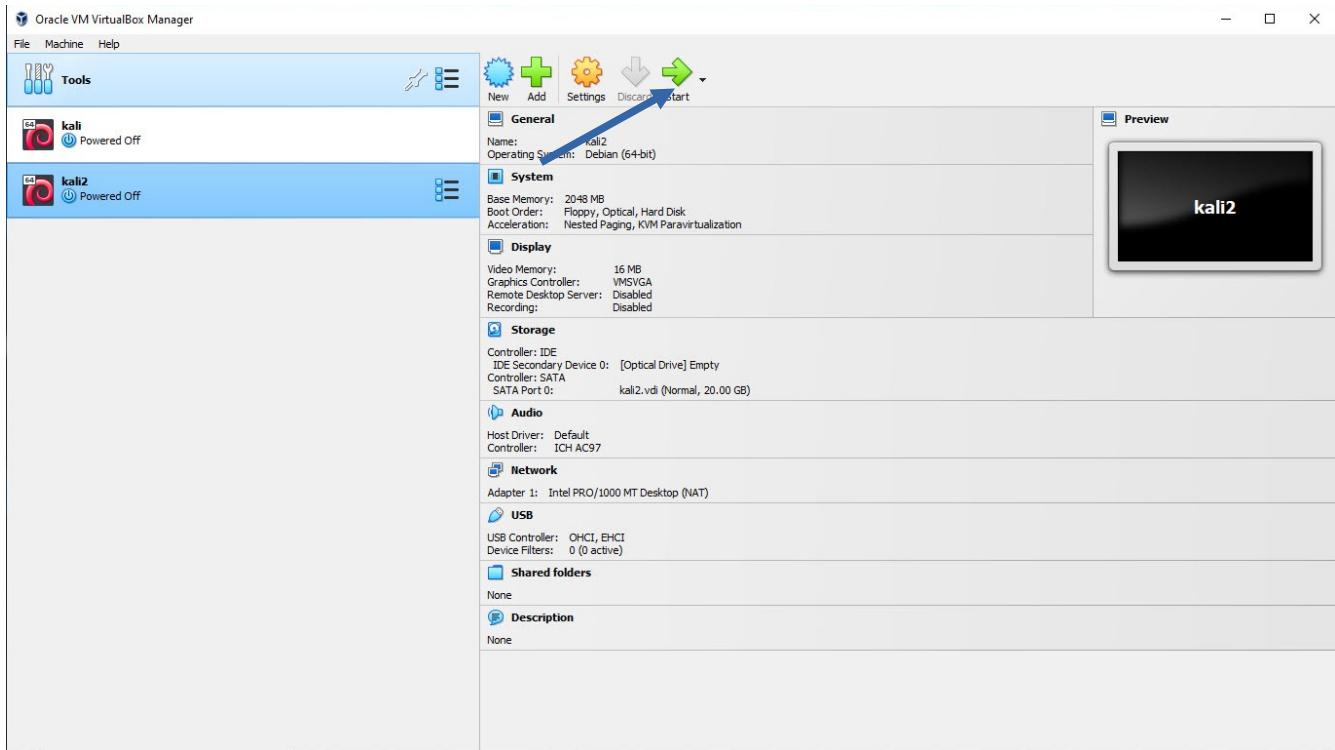
Cliquez Empty





Lancement de la machine virtuelle :

Cliquez sur «Start» Pour lancer la machine virtuelle



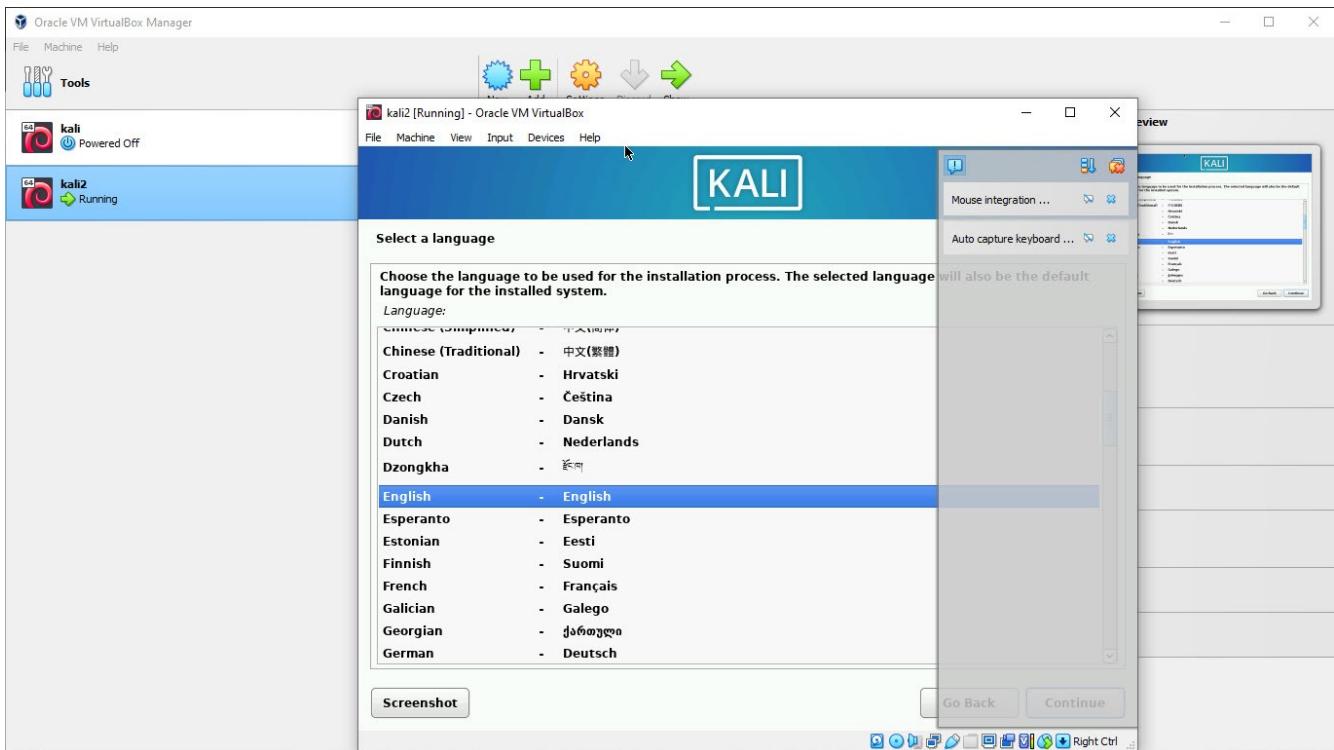
Demarrez la VM

Suivez les etapes d'installation :

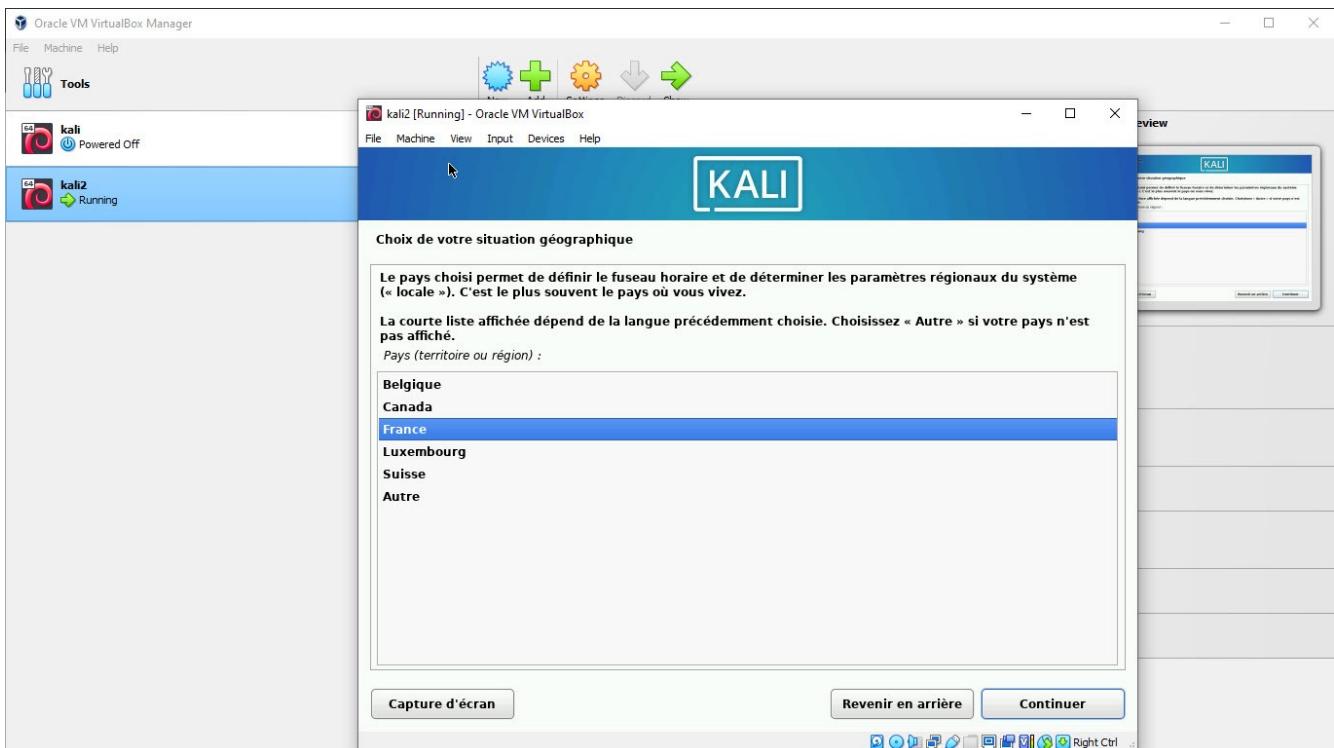
- 1) Selectionnez « Graphical install ».
 - 2) Configurez la langue, le fuseau horaire, et le clavier.
 - 3) Creez un utilisateur et un mot de passe.
 - 4) Partitionnez le disque(choisissez « Guided-use entire » pour une installation simple).
 - 5) Confirmez l'installation et attendez la fin processus
- Redemarrez la VM apres l'installation.



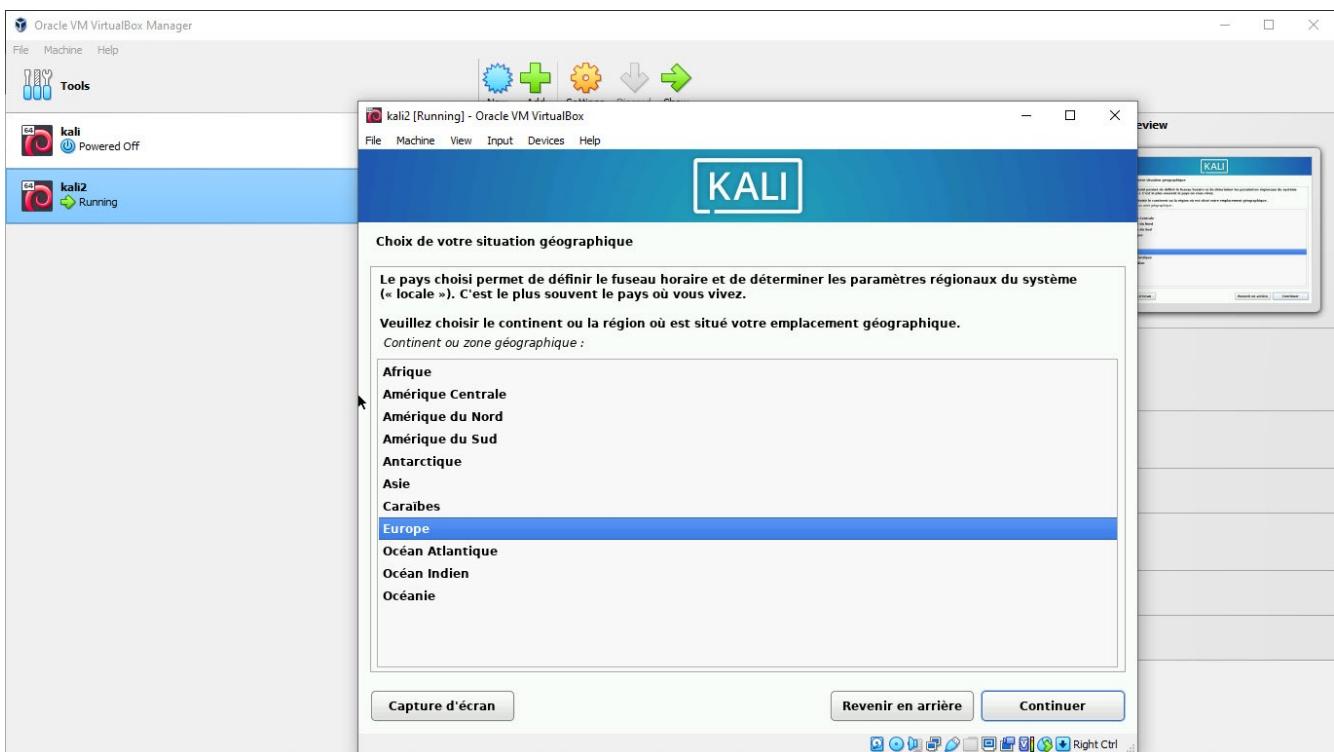
Choisie Francais



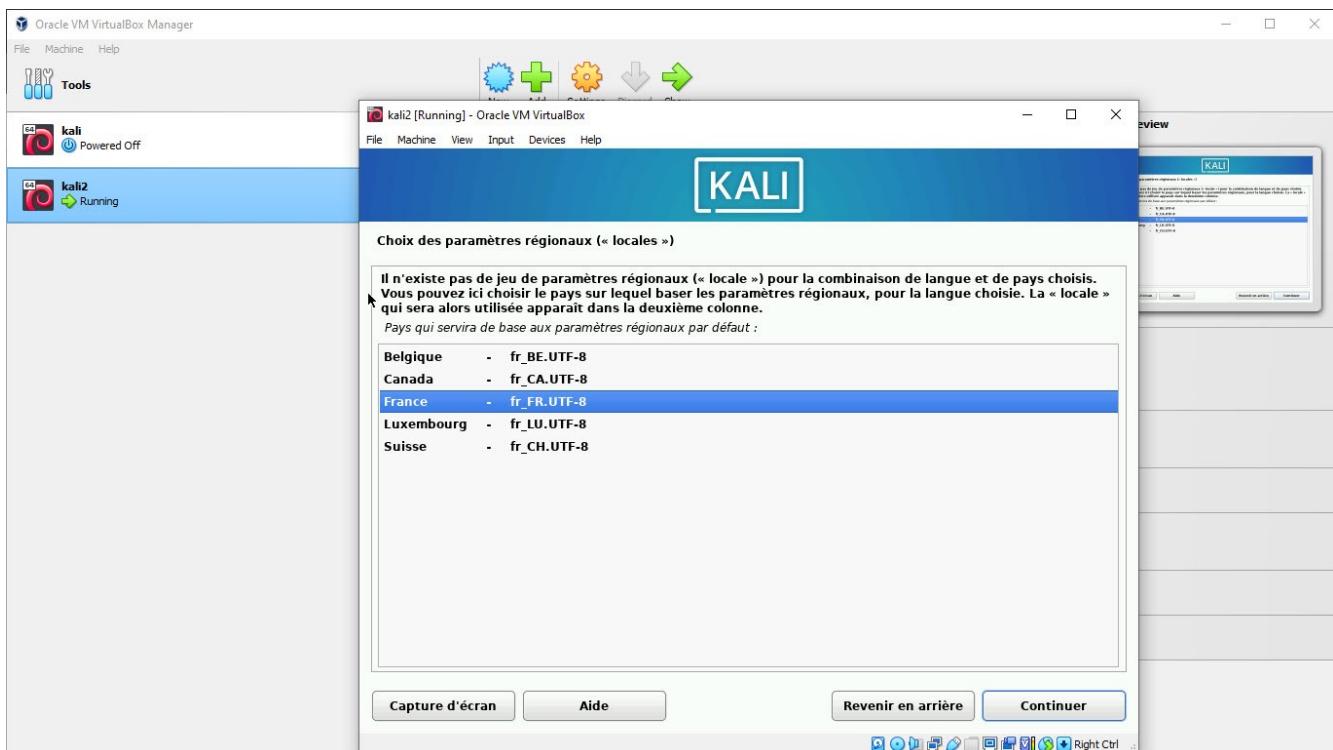
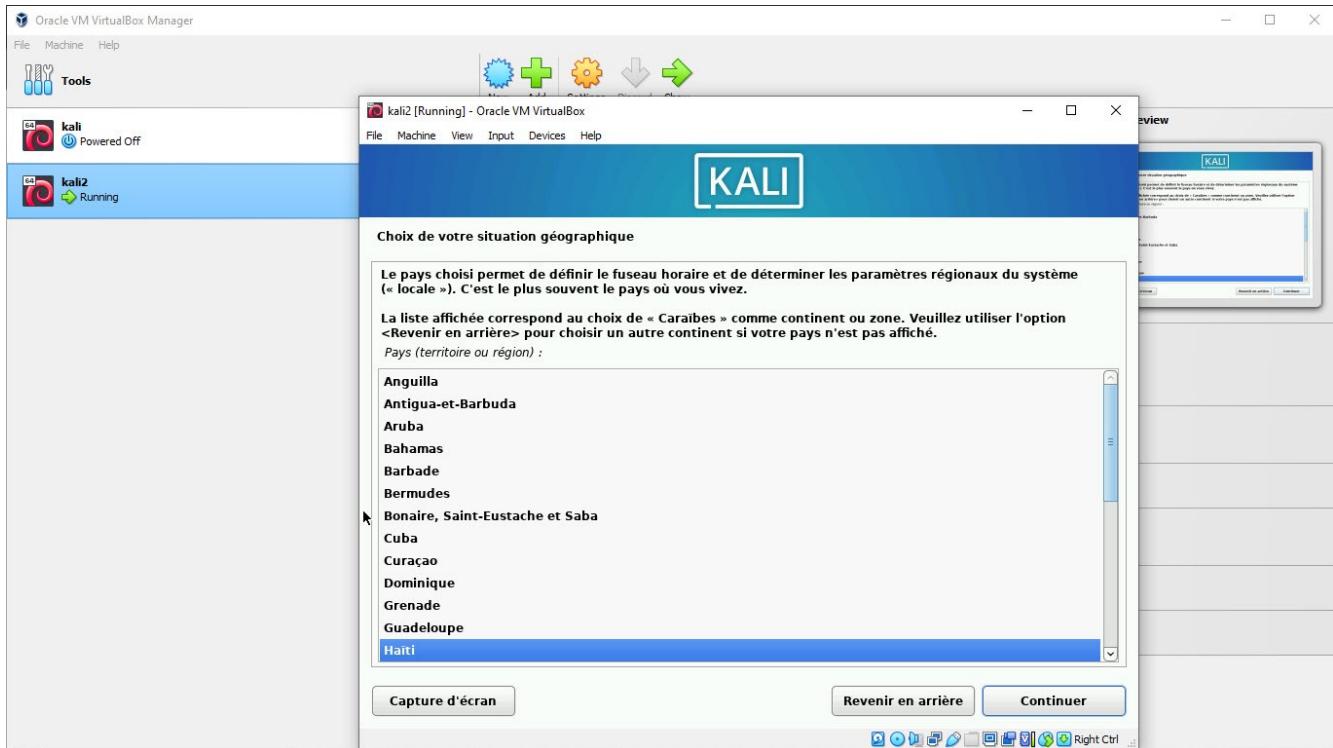
Choisie Autre



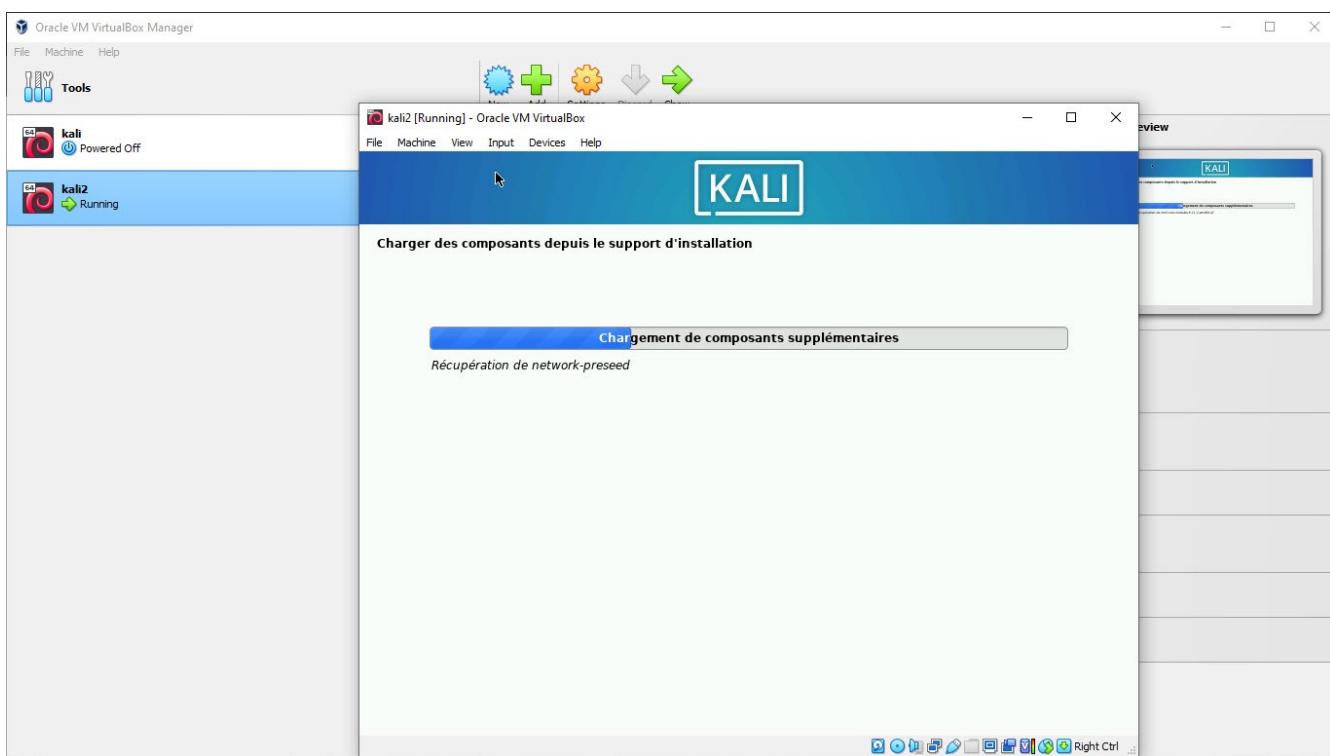
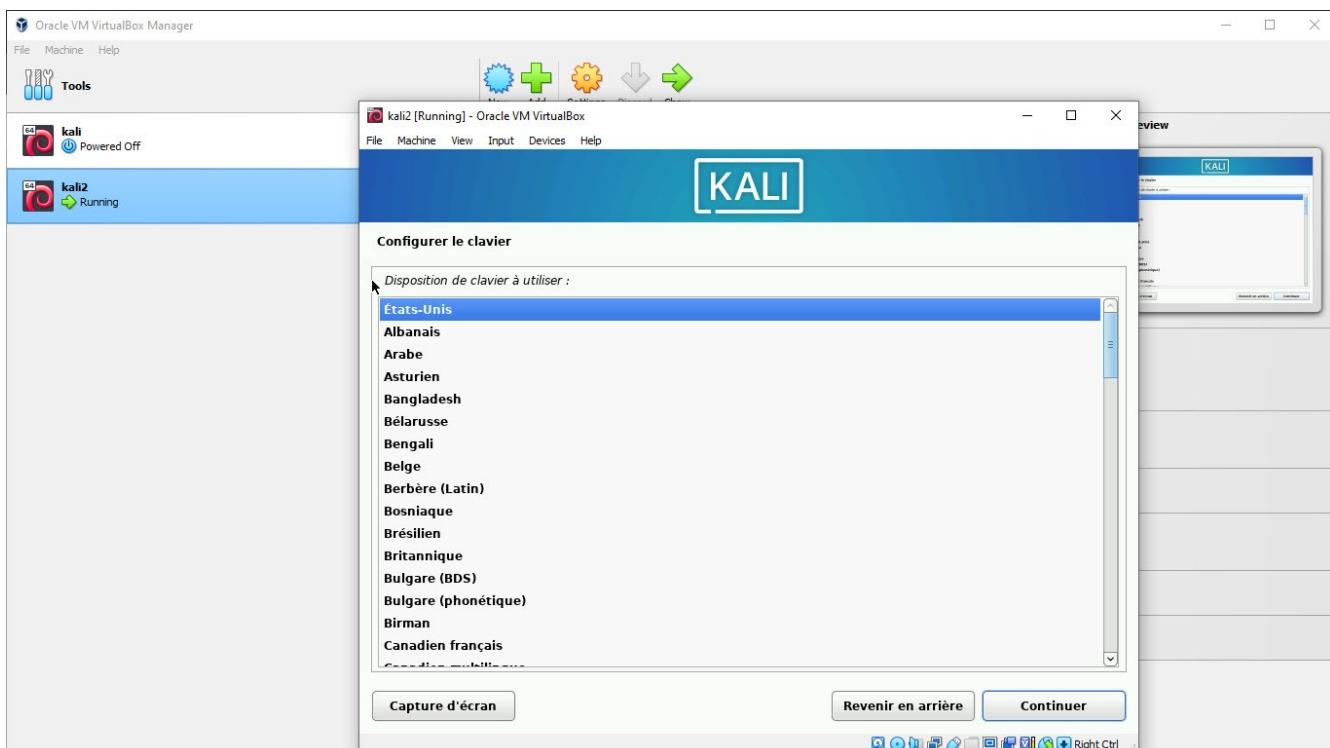
Choisie Caraïbes

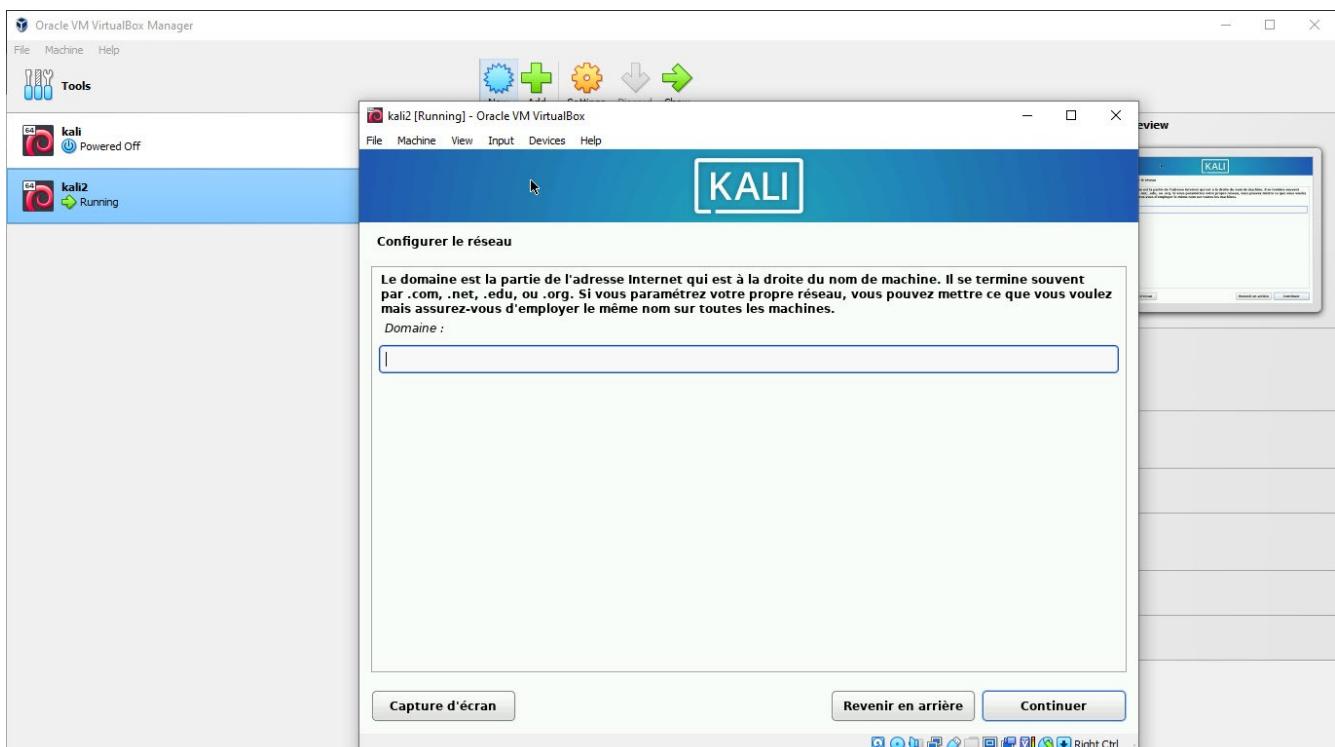
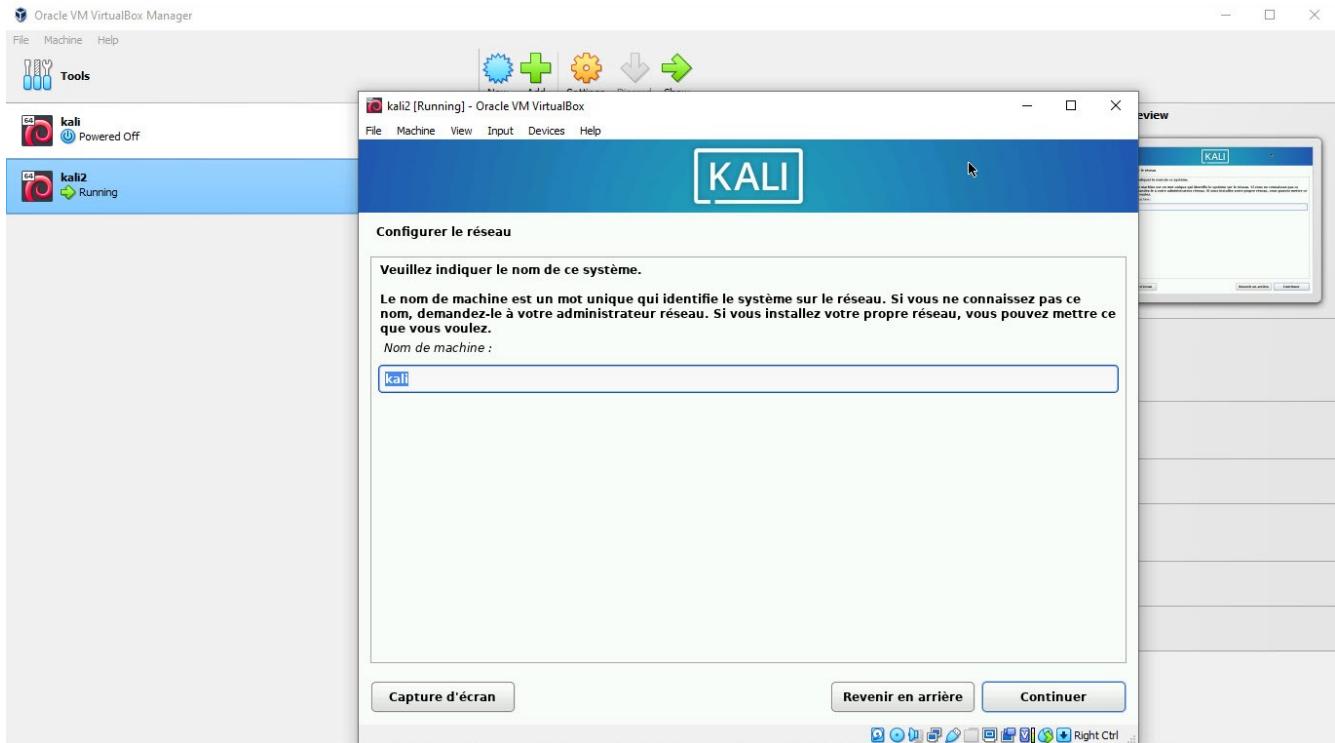


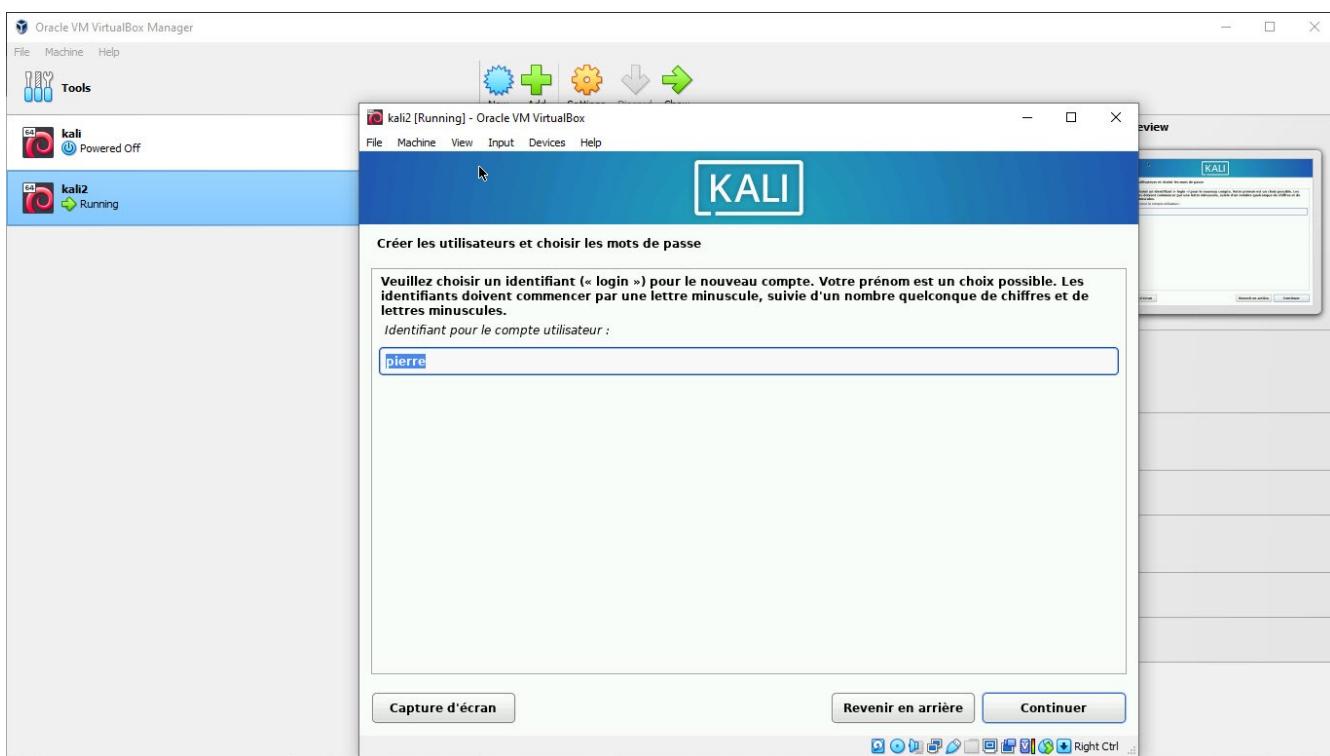
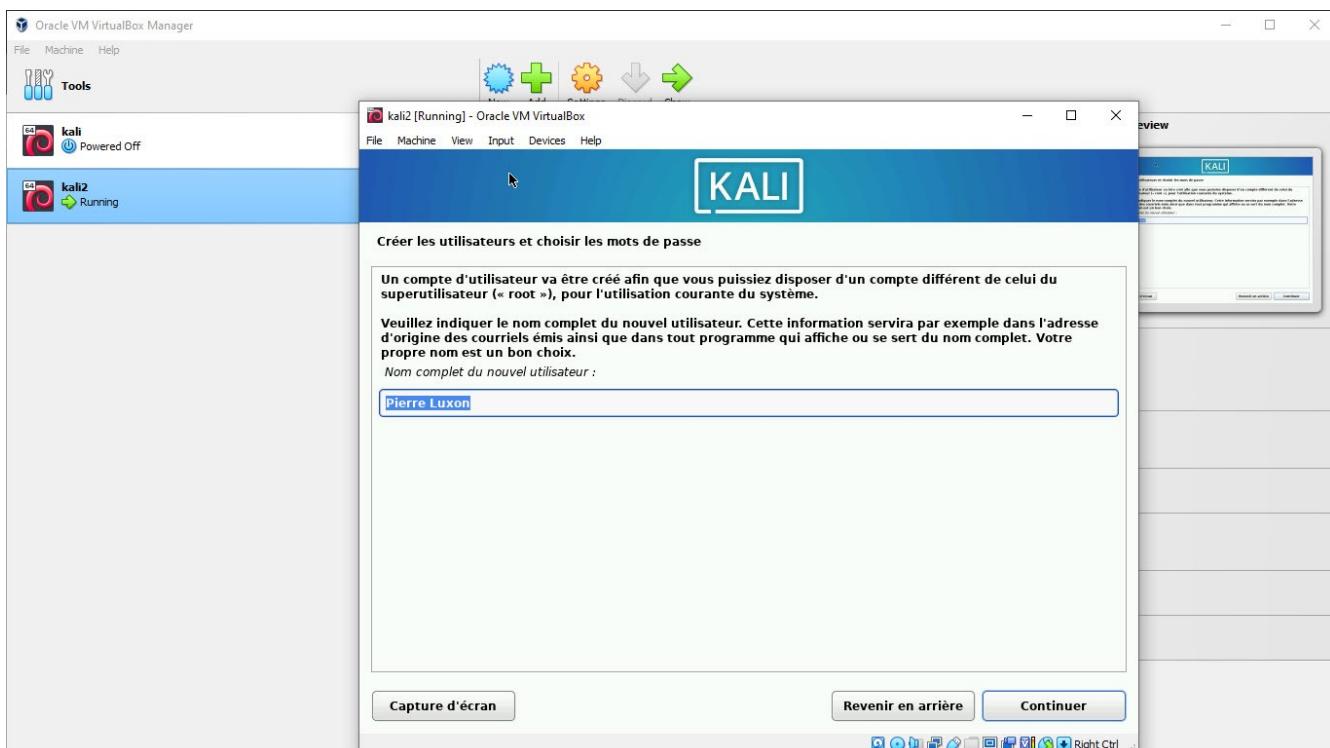
Choisie Haiti

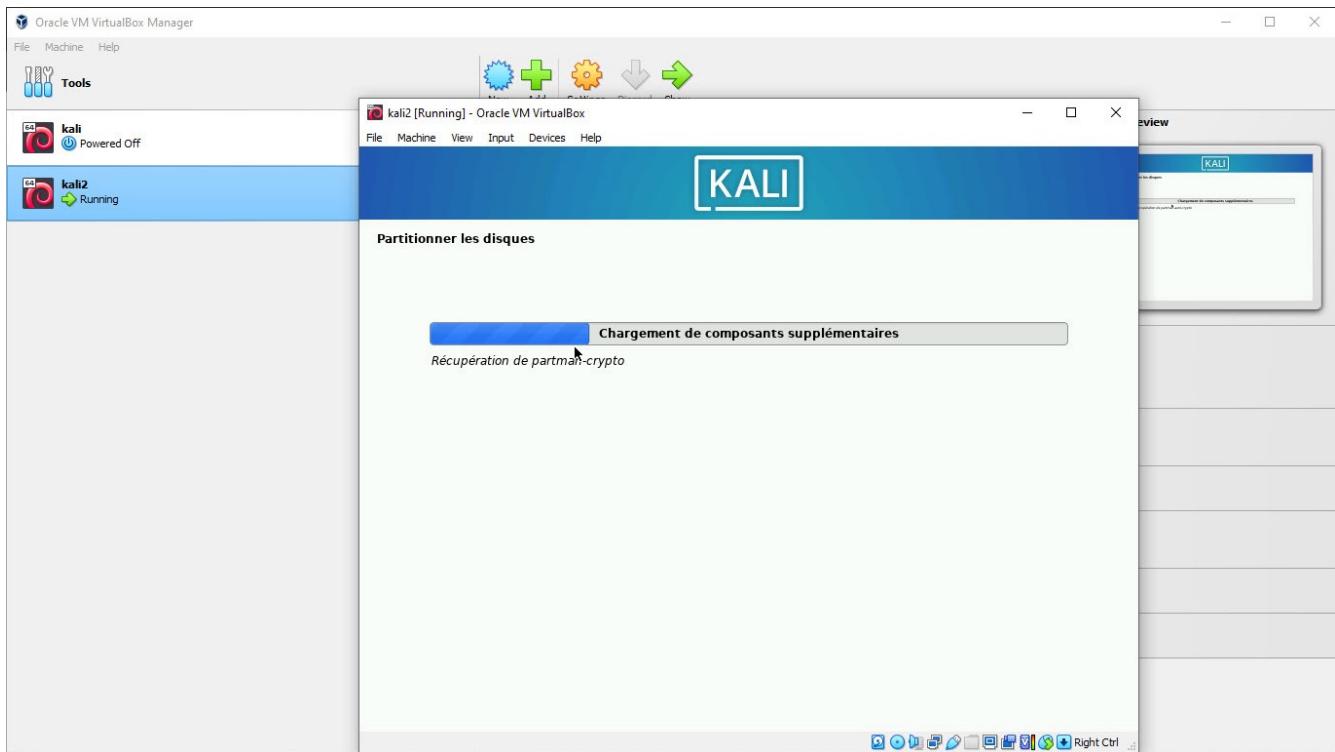
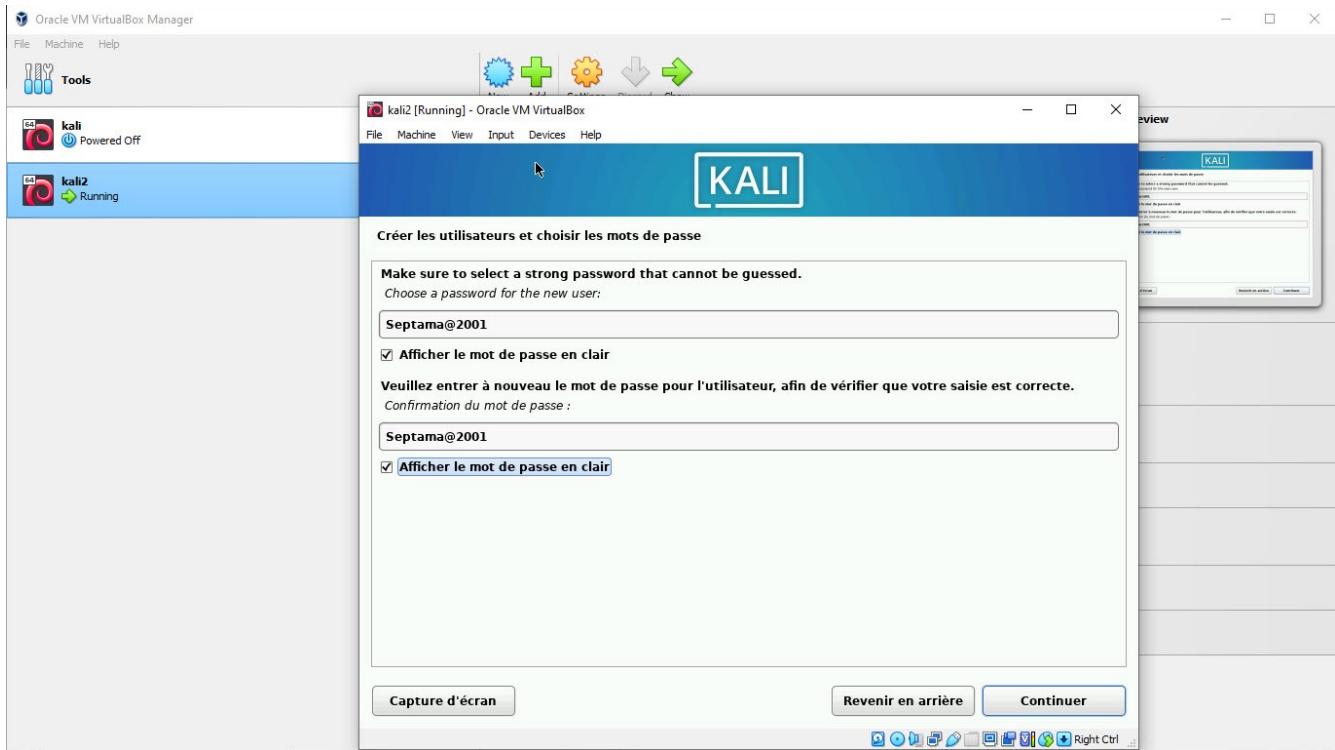


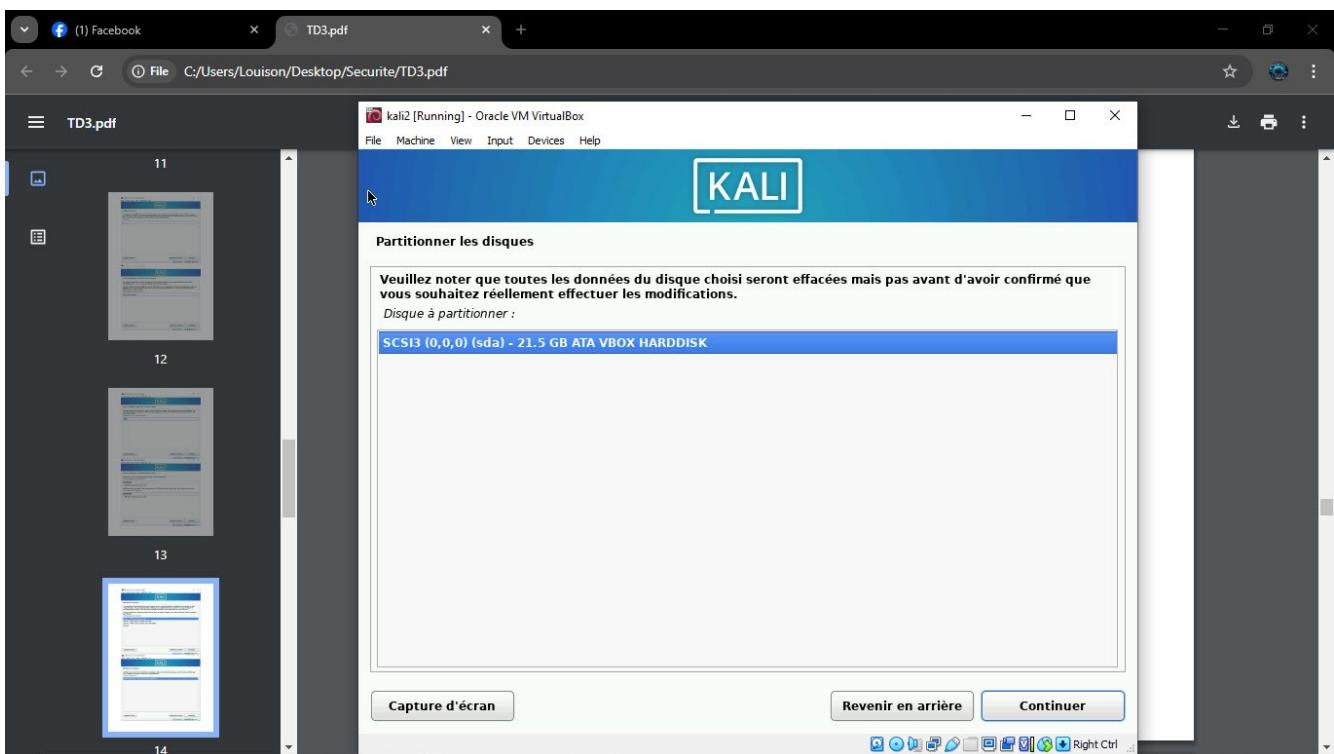
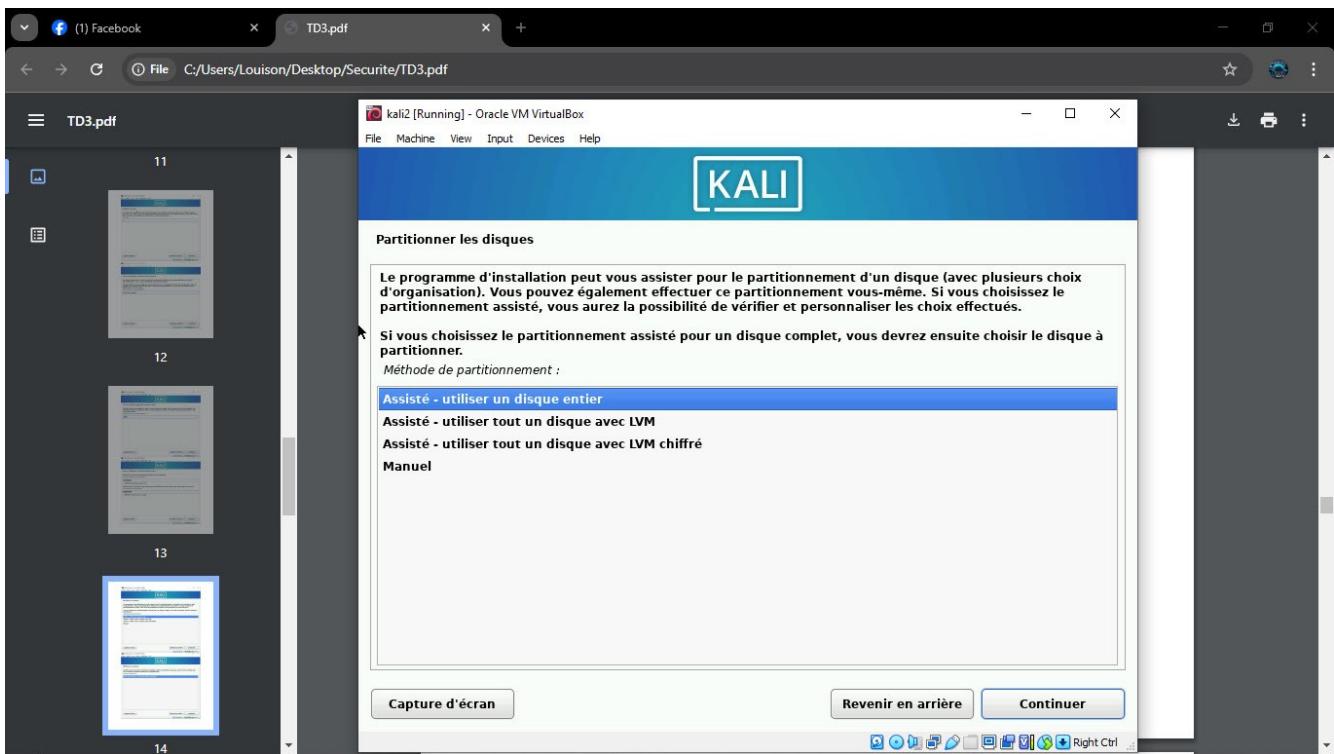
Congriger le Clavier

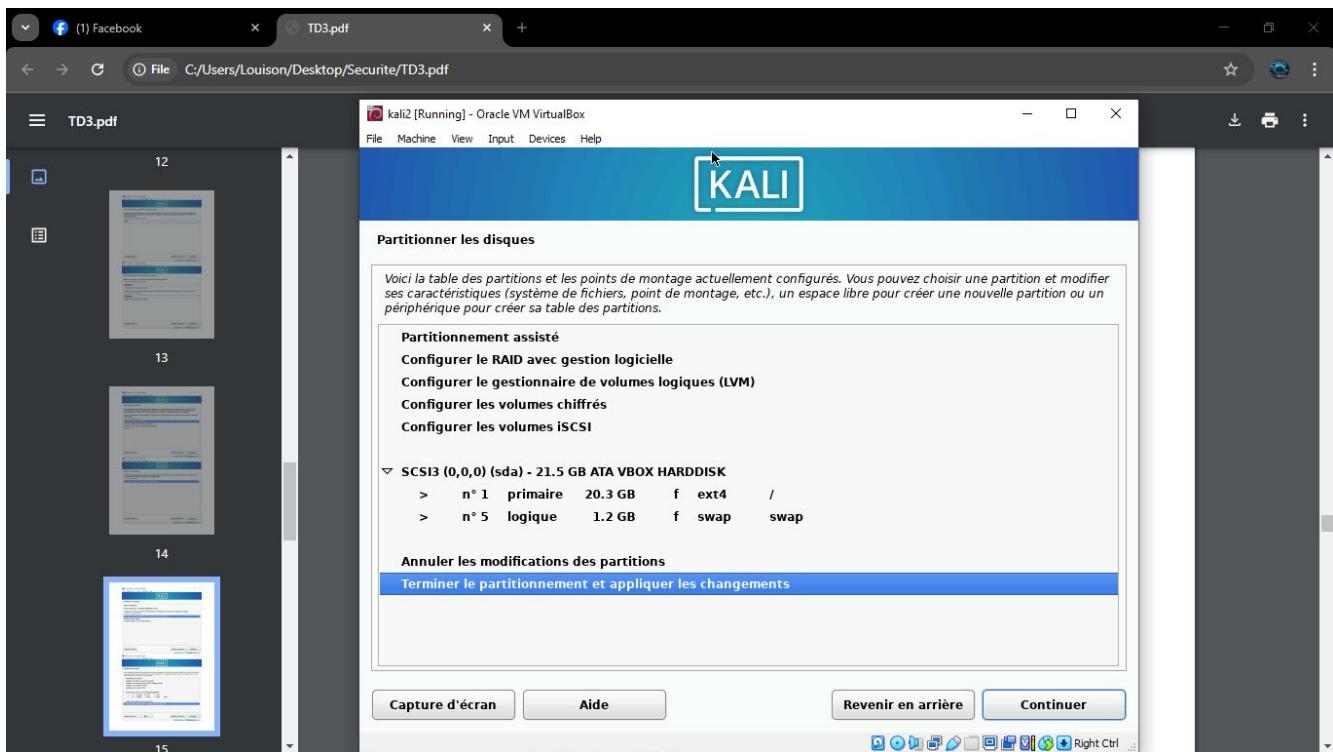
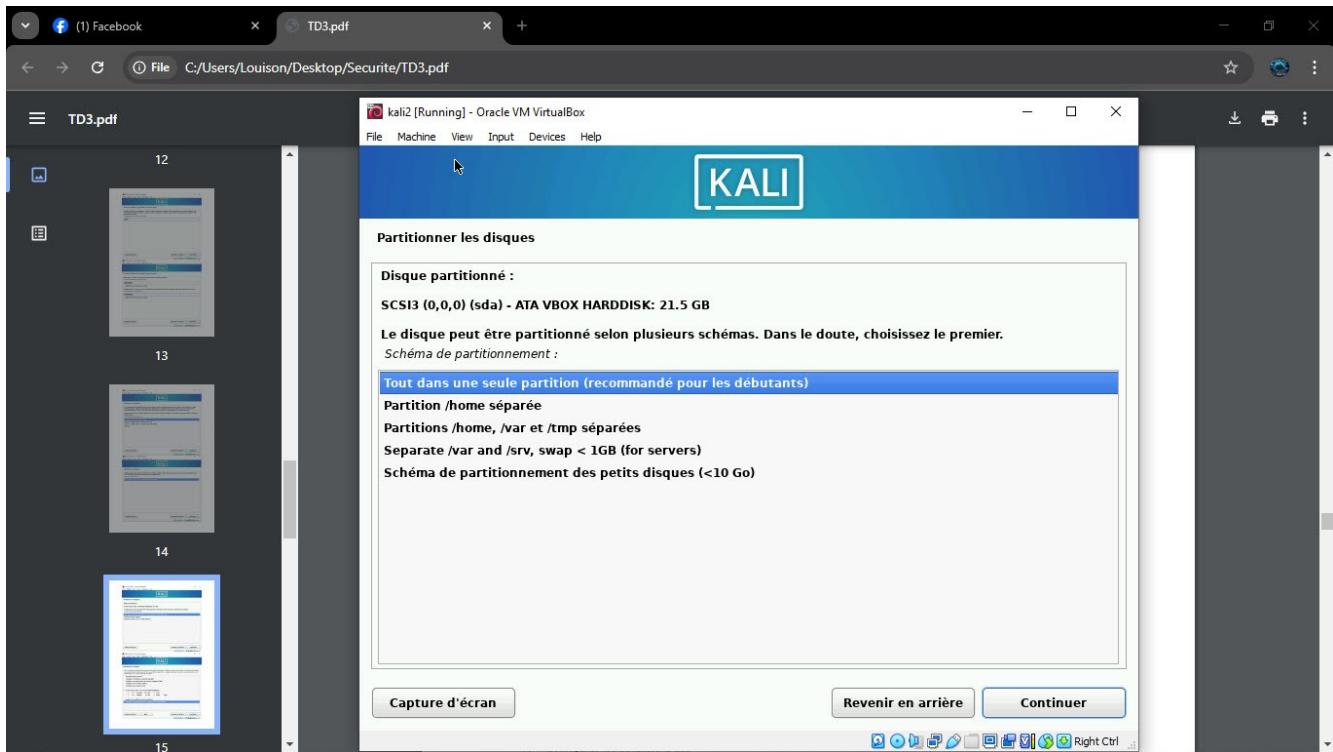


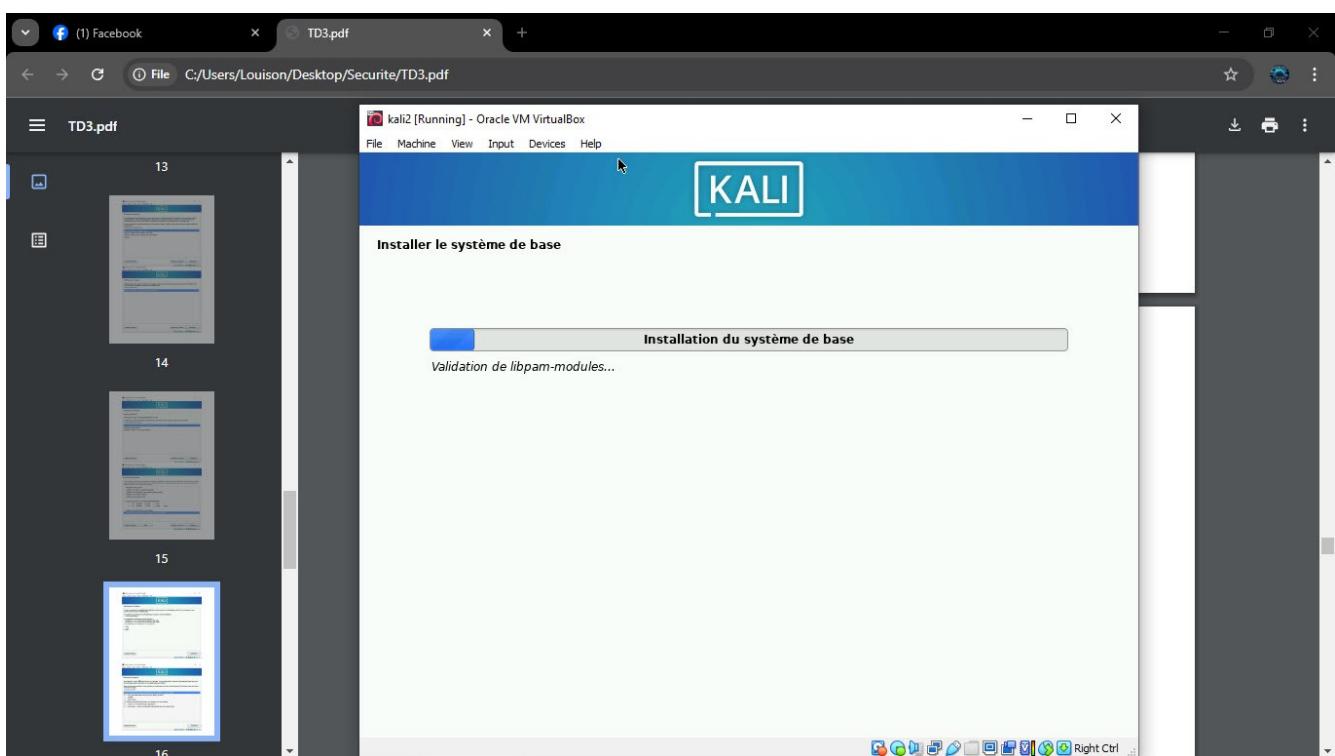
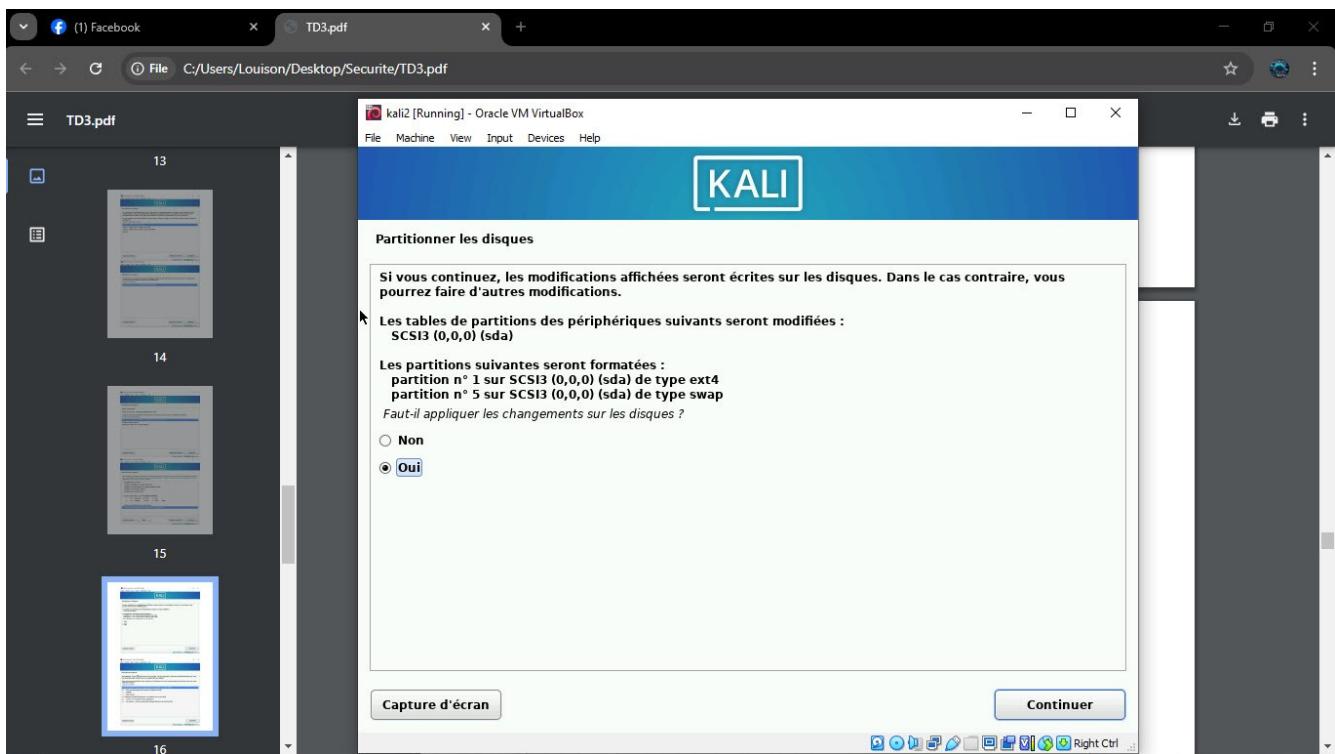


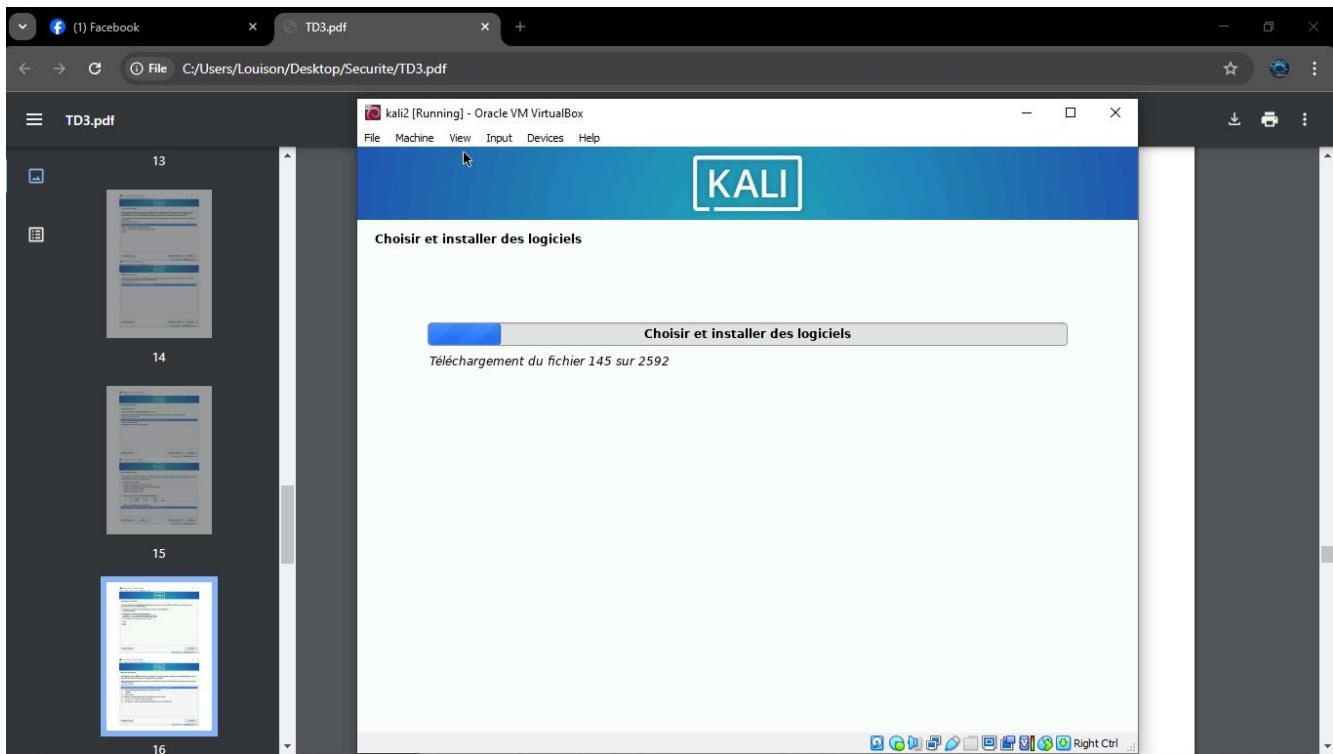
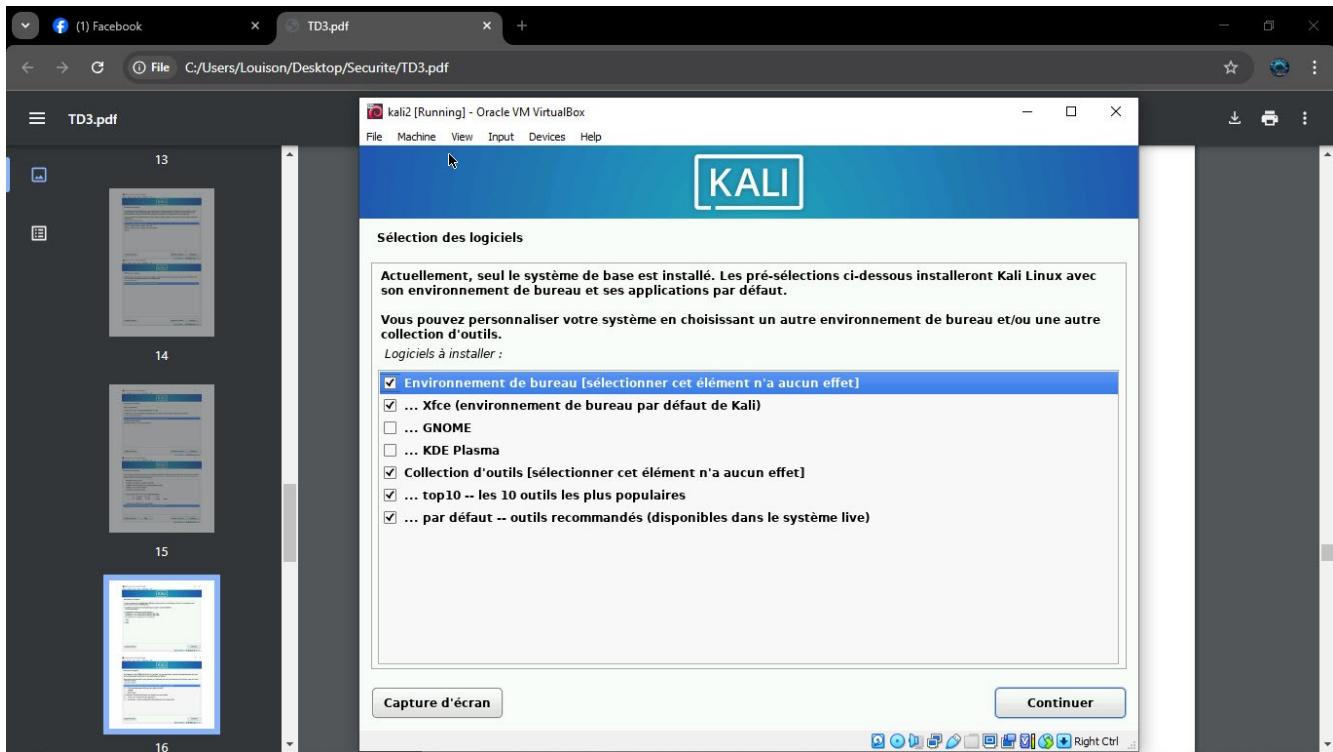


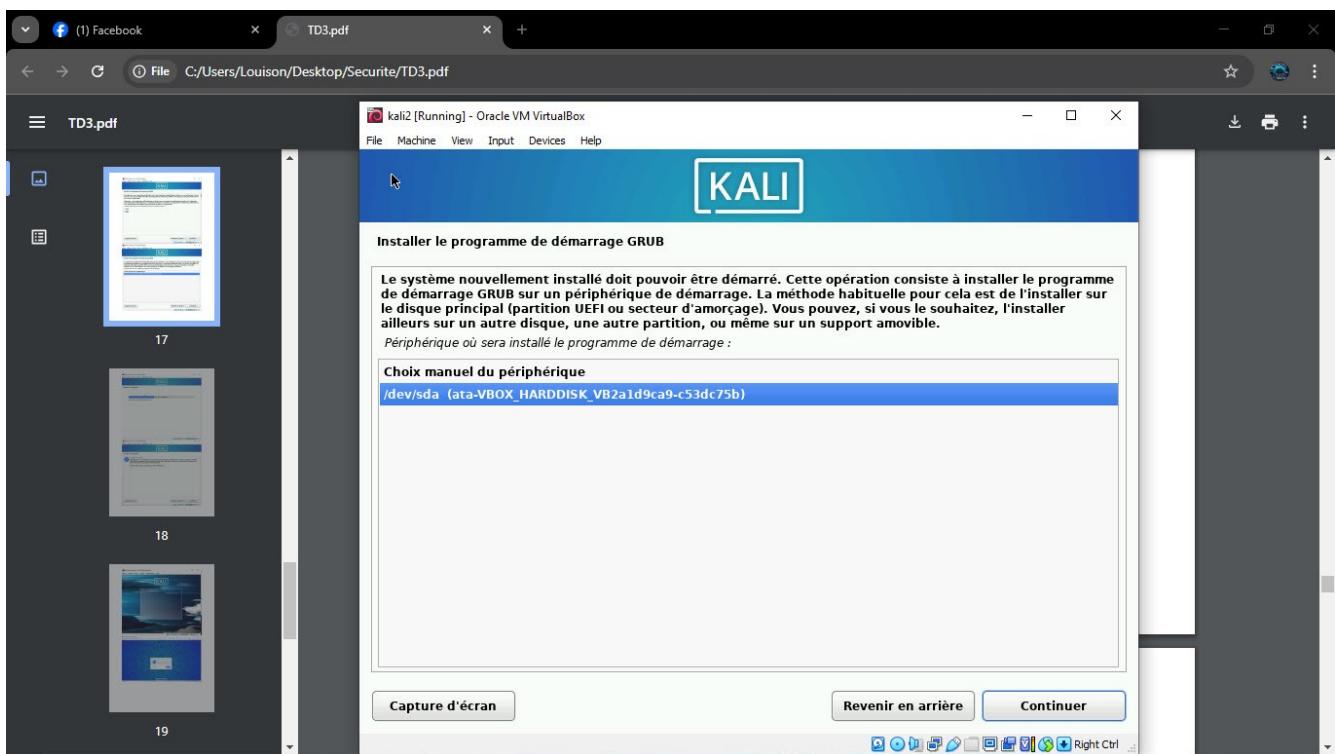
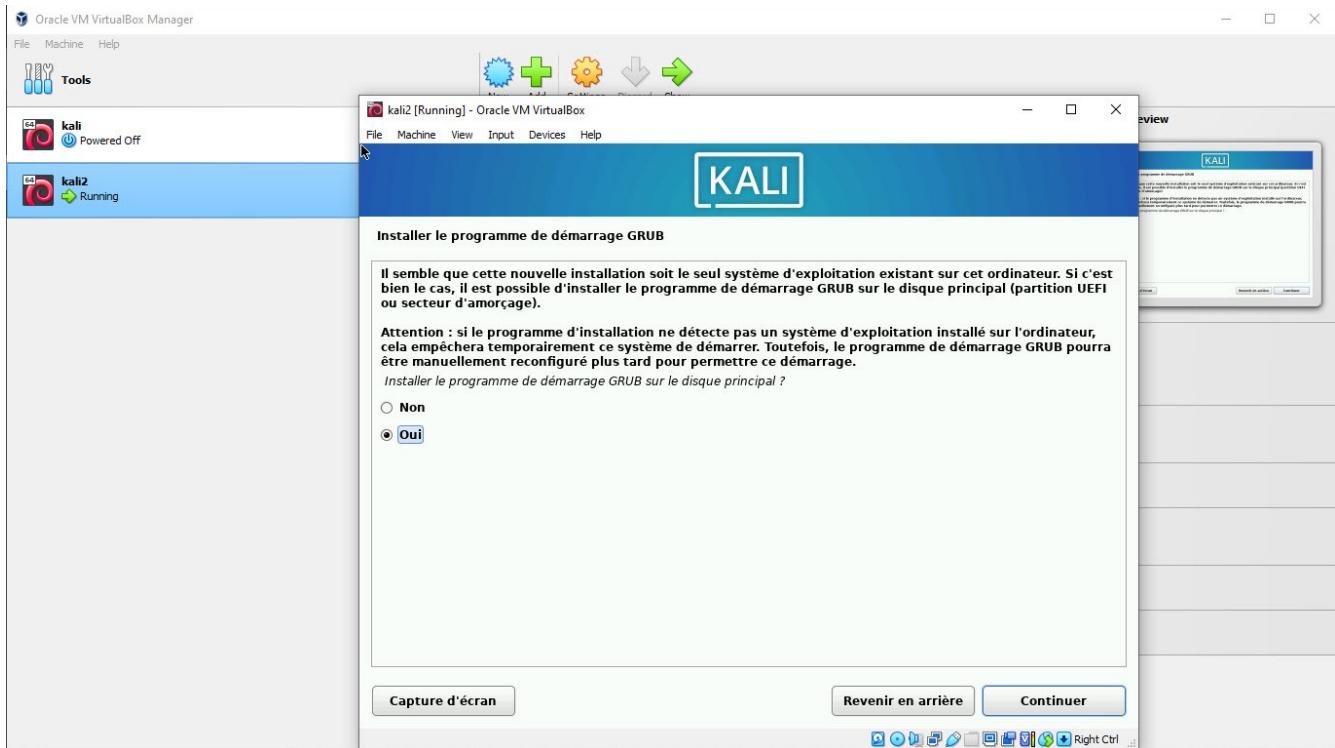


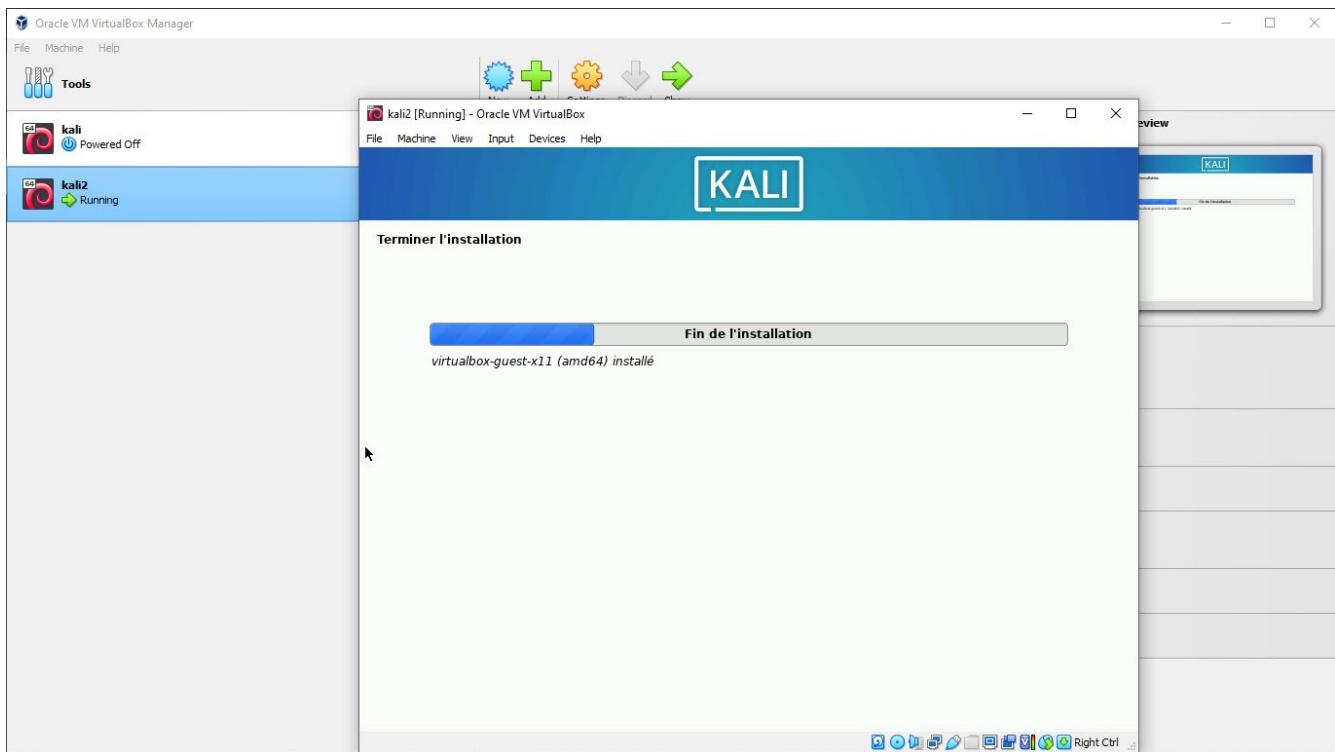
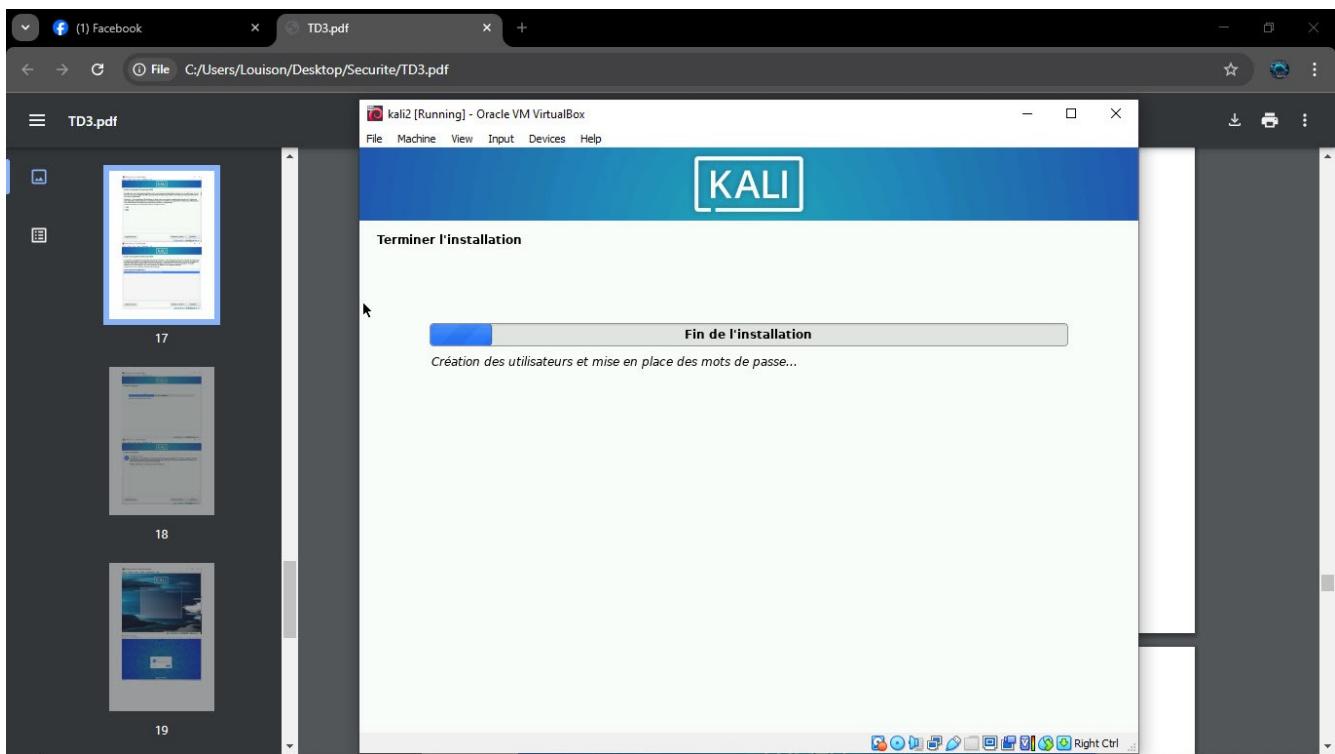


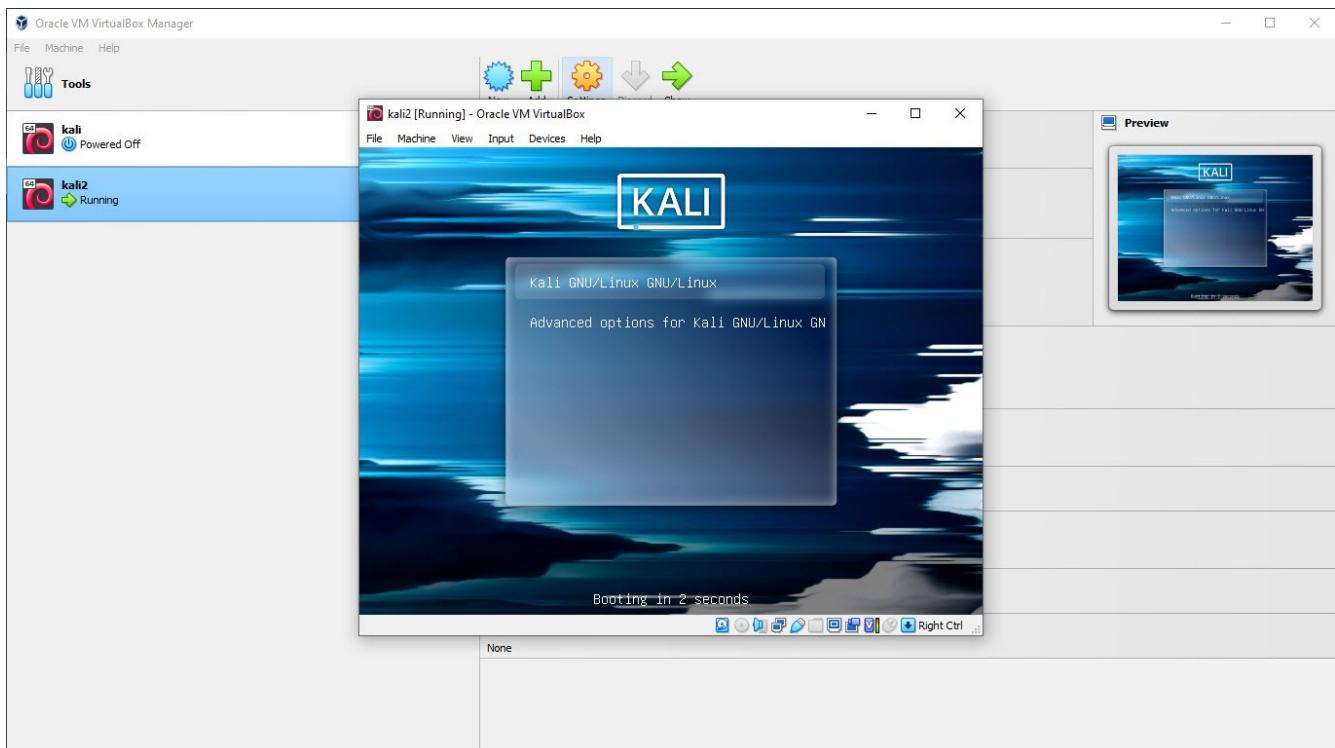
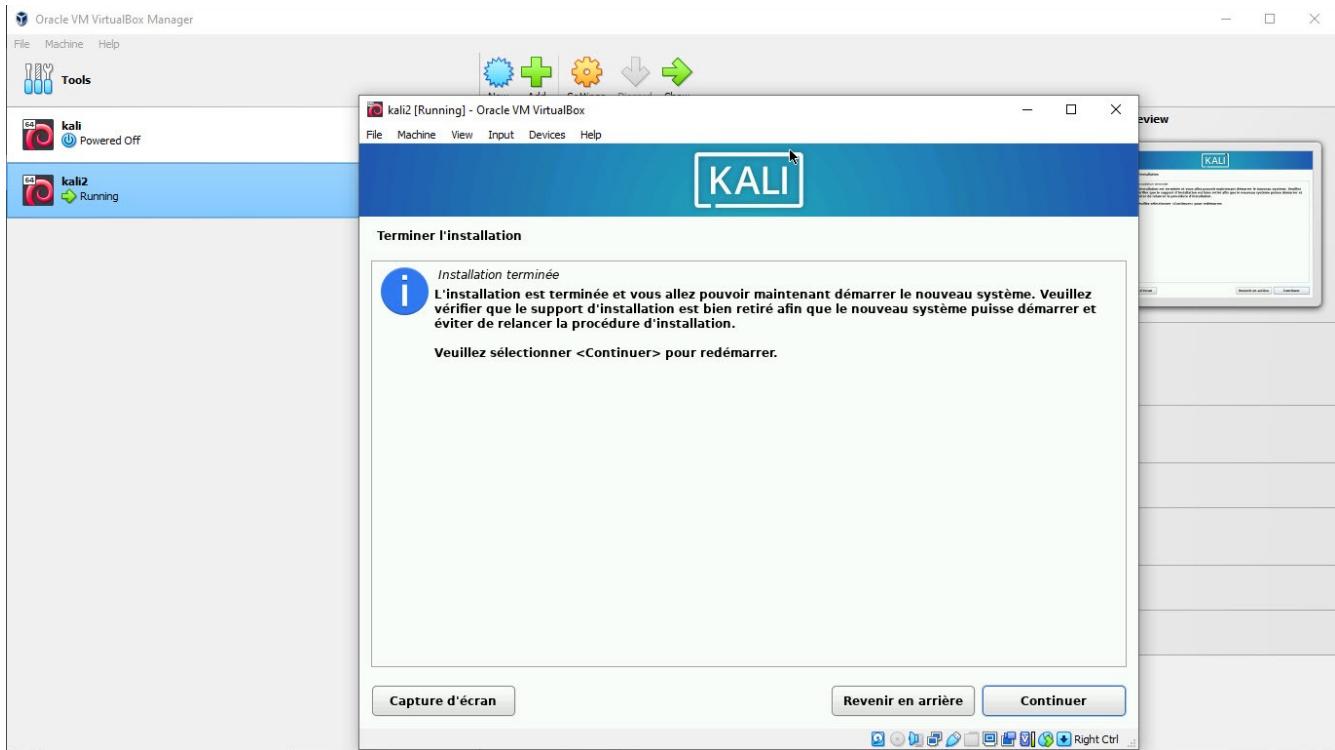


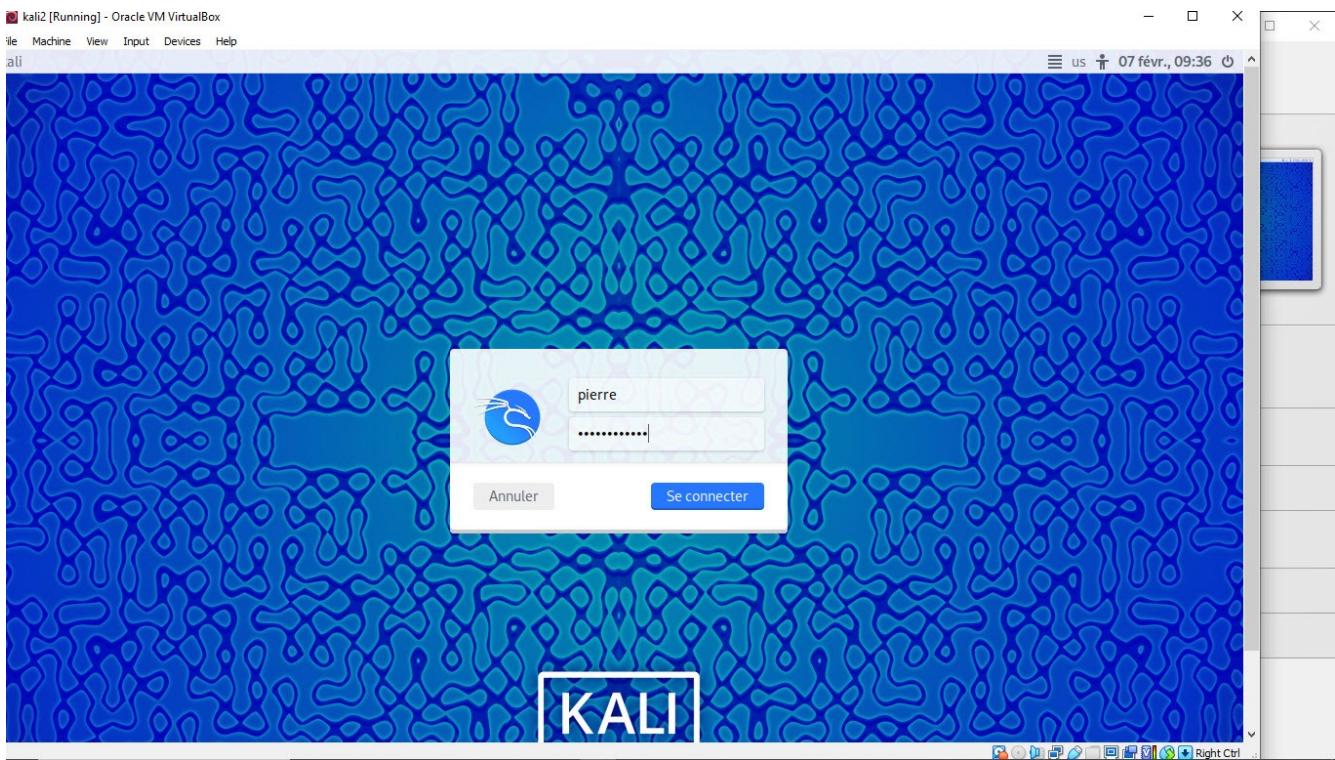












Ce travail dirige a pour but de familiariser au debutants avec l'installation, la configuration et la manipulation de kali Linux dans un un environnement virtualise. Il vise a developper des competences pratiques en gestion des fichiers, analyse reseau , manipulation des permissions et execution de commandes essentielles sous Linux.

-Creation et installation de la machine virtuelle ou Vmware

-Installez Kali Linux en suivant les etapes d'installation graphique.

-Mettez a jour le systeme apres l'installation avec les Commandes sur dessous :

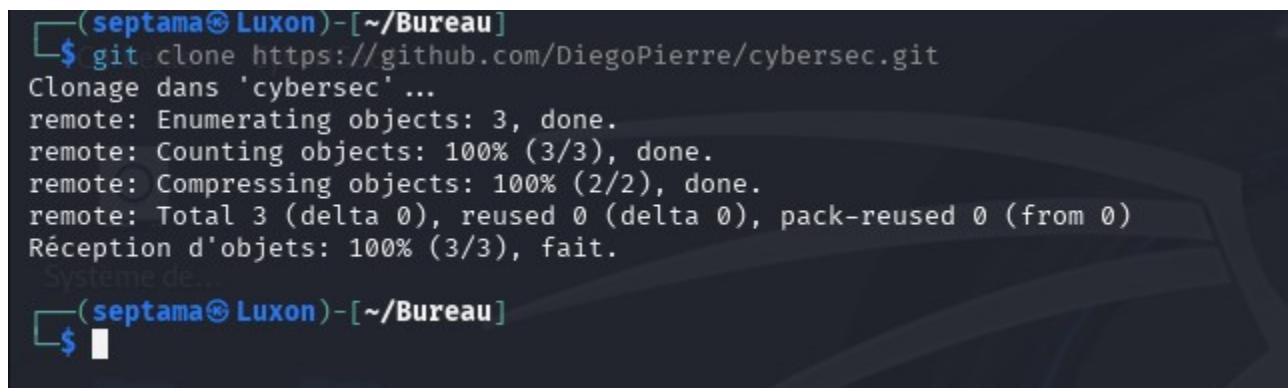
-sudo apt update

-sudo apt upgrade -y

-sudo apt dist-upgrade -y

1.Creation d'un depot GitHub nomme cybersec avec une description:Virtualisation et Manipulation de Kali Linux

2.Clonage du depot dans le repertoire local sur le bureau en utilsant la commande :



```
(septama@Luxon)-[~/Bureau]
$ git clone https://github.com/DiegoPierre/cybersec.git
Clonage dans 'cybersec' ...
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (2/2), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0 (from 0)
Réception d'objets: 100% (3/3), fait.
Systeme de...
$
```

-Gestion des fichiers et des dossiers

Creation d'un dossier 'cybersec' avec trois sous-dossiers:scan,logs,scripts

```
└─(septama@Luxon)-[~/Bureau]
└─$ mkdir -p cybersec/scan

└─(septama@Luxon)-[~/Bureau]
└─$ mkdir -p cybersec/logs

└─(septama@Luxon)-[~/Bureau]
└─$ mkdir -p cybersec/scripts

└─(septama@Luxon)-[~/Bureau]
└─$ ls -l ~/Bureau/cybersec/
total 16
drwxrwxr-x 2 septama septama 4096 7 fév 10:47 logs
-rw-rw-r-- 1 septama septama 56 7 fév 10:46 README.md
drwxrwxr-x 2 septama septama 4096 7 fév 10:46 scan
drwxrwxr-x 2 septama septama 4096 7 fév 10:47 scripts

└─(septama@Luxon)-[~/Bureau]
└─$ █
```

Ajouter un fichier ‘notes.txt’ dans les dossiers ‘scan’ et ‘logs’.
Affichage Du contenu scan et logs :

```
└─(septama@Luxon)-[~/Bureau]
└─$ echo "Ceci est une note sur la cybersecurite." > ~/Bureau/cybersec/scan/notes.txt

└─(septama@Luxon)-[~/Bureau]
└─$ echo "C'est la premier essaye sur kali Lunix comme Debutant" > ~/Bureau/cybersec/logs/notes.txt

└─(septama@Luxon)-[~/Bureau]
└─$ cat ~/Bureau/cybersec/scan/notes.txt
Ceci est une note sur la cybersecurite.

└─(septama@Luxon)-[~/Bureau]
└─$ cat ~/Bureau/cybersec/logs/notes.txt
C'est la premier essaye sur kali Lunix comme Debutant

└─(septama@Luxon)-[~/Bureau]
└─$ █
```

Copiez le fichier ‘notes.txt’ dans le sous-dossier ‘scripts’ et verifiez la copie.

```
└─(septama@Luxon)-[~/Bureau/cybersec]
$ cp ~/Bureau/cybersec/scan/notes.txt ~/Bureau/cybersec/scripts/
└─(septama@Luxon)-[~/Bureau/cybersec]
$ ls -l ~/Bureau/cybersec/scripts/
total 4
-rw-rw-r-- 1 septama septama 40 7 fév 11:11 notes.txt
└─(septama@Luxon)-[~/Bureau/cybersec]
$ ┌
```

Deplacer le fichier 'notes.txt' vers le sous-dossier 'scan'.

```
└─(septama@Luxon)-[~/Bureau/cybersec]
$ mv ~/Bureau/cybersec/scripts/notes.txt ~/Bureau/cybersec/scan/
└─(septama@Luxon)-[~/Bureau/cybersec]
$ ls ~/Bureau/cybersec/scripts/
└─(septama@Luxon)-[~/Bureau/cybersec]
$ ls -l ~/Bureau/cybersec/scripts/
total 0
└─(septama@Luxon)-[~/Bureau/cybersec]
$ ┌
```

Suprimez le fichier 'notes.txt' du sous-dossier 'scripts' et verifiez la suppression.

```
└─(septama@Luxon)-[~/Bureau/cybersec]
$ rm ~/Bureau/cybersec/scripts/notes.txt/
rm: impossible de supprimer '/home/septama/Bureau/cybersec/scripts/notes.txt/': Aucun fichier ou dossier de ce nom
└─(septama@Luxon)-[~/Bureau/cybersec]
$ ls -l ~/Bureau/cybersec/scripts/
total 0
└─(septama@Luxon)-[~/Bureau/cybersec]
$ ┌
```

Supprimez les sous-dossier 'scan', 'logs', 'scripts' et verifiez la suppression.

Supprimez les sous-dossier 'scan', 'logs', 'scripts' et verifiez la suppression.

```
(septama@Luxon)-[~/Bureau/cybersec]
$ rm -r ~/Bureau/cybersec/scan ~/Bureau/cybersec/logs ~/Bureau/cybersec/scripts
total 4
-rw-r-- 1 septama septama 56 7 fév 10:46 README.md

(septama@Luxon)-[~/Bureau/cybersec]
$ ls -l ~/Bureau/cybersec/
total 4
-rw-r-- 1 septama septama 56 7 fév 10:46 README.md
```

3.Scan reseau avec Kali Linux
Utilisez 'ip a' pour afficher les informations reseau.

```
(septama@Luxon)-[~/Bureau/cybersec]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:62:0e:47 brd ff:ff:ff:ff:ff:ff
        inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
            valid_lft 84983sec preferred_lft 84983sec
        inet6 fe80::a00:27ff:fe62:e47/64 scope link noprefixroute
            valid_lft forever preferred_lft forever

(septama@Luxon)-[~/Bureau/cybersec]
$ 
```

Supprimez les sous-dossier 'scan', 'logs', 'scripts' et vérifiez la suppression.

-Exécutez 'nmap' pour scanner votre réseau local et identifier les appareils connectés.

```
(septama@Luxon)-[~/Bureau/cybersec]
$ nmap -sn 10.0.2.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-07 11:43 EST
Nmap scan report for 10.0.2.2
Host is up (0.00026s latency).
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00024s latency).
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.00034s latency).
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.75 seconds

(septama@Luxon)-[~/Bureau/cybersec]
$
```

4. Manipulation des permissions

-Creez un fichier 'secret.txt'.

Modifiez ses permissions pur qu'il ne soit accessible qu'en lecture par le proprietaire.

```
(septama@Luxon)-[~/Bureau/cybersec]
$ touch secret.txt
(septama@Luxon)-[~/Bureau/cybersec]
$ chmod 400 ~/Bureau/cybersec/secret.txt
(septama@Luxon)-[~/Bureau/cybersec]
$ ls -l ~/Bureau/cybersec/secret.txt
-r----- 1 septama septama 0 7 fév 13:13 /home/septama/Bureau/cybersec/sec
ret.txt

(septama@Luxon)-[~/Bureau/cybersec]
$
```

5. Utilisation de grep

-Creez un fichier 'log.txt' contenant plusieurs lignes de texte.

```

└─(septama@Louison)-[~/Bureau/cybersec]
$ echo "C'est la premier essaye sur kali Linux comme Debutant">> ~/Bureau/cybersec/log.txt

└─(septama@Louison)-[~/Bureau/cybersec]
$ echo "Moi je suis Louison Septama c'est premier devoir sur kali Linux comme Debutant">>> ~/Bureau/cybersec/log.txt

└─(septama@Louison)-[~/Bureau/cybersec]
$ echo "Si Vous etre Debutant soyez patient pour Apprendre un peut sur Kali">>> ~/Bureau/cybersec/log.txt
Système de fichiers

└─(septama@Louison)-[~/Bureau/cybersec]
$ cat ~/Bureau/cybersec/log.txt
C'est la premier essaye sur kali Linux comme Debutant
Moi je suis Louison Septama c'est premier devoir sur kali Linux comme Debutant
Si Vous etre Debutant soyez patient pour Apprendre un peut sur Kali

└─(septama@Louison)-[~/Bureau/cybersec]
$ grep "Debutant" ~/Bureau/cybersec/log.txt
C'est la premier essaye sur kali Linux comme Debutant
Moi je suis Louison Septama c'est premier devoir sur kali Linux comme Debutant
Si Vous etre Debutant soyez patient pour Apprendre un peut sur Kali

└─(septama@Louison)-[~/Bureau/cybersec]
$ █

```

6. Execution de commandes essentielles

-df -h

```

└─(septama@Luxon)-[~/Bureau/cybersec]
$ df -h
Sys. de fichiers Taille Utilisé Dispo Uti% Monté sur
udev          926M      0  926M   0% /dev
tmpfs         198M  1004K  197M   1% /run
/dev/sda1      38G    18G   18G  51% /
tmpfs         988M   4,0K  988M   1% /dev/shm
tmpfs         5,0M      0  5,0M   0% /run/lock
tmpfs         1,0M      0  1,0M   0% /run/credentials/systemd-journald.s
ervice
tmpfs         988M   8,0K  988M   1% /tmp
tmpfs         1,0M      0  1,0M   0% /run/credentials/getty@tty1.service
tmpfs         198M   116K  198M   1% /run/user/1000

└─(septama@Luxon)-[~/Bureau/cybersec]
$ █

```

-du -sh

```
(septama@Luxon)-[~/Bureau/cybersec]
$ du -sh
200K .
```

-free -h

```
(septama@Luxon)-[~/Bureau/cybersec]
$ free -h
Répertoire... total   utilisé     libre   partagé   tamp/cache disponi
ble
Mem:        1,9Gi      1,6Gi    100Mi      31Mi     417Mi      344
Mi
Échange:    2,0Gi      735Mi    1,3Gi
```

-ps aux

(septama@Luxon)-[~/Bureau/cybersec]												
USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND		
root	1	0.0	0.4	23132	8868	?	Ss	11:08	0:02	/sbin/init		
root	2	0.0	0.0	0	0	?	S	11:08	0:00	[kthreadd]		
root	3	0.0	0.0	0	0	?	S	11:08	0:00	[pool_workq]		
root	4	0.0	0.0	0	0	?	I<	11:08	0:00	[kworker/R-]		
root	5	0.0	0.0	0	0	?	I<	11:08	0:00	[kworker/R-]		
root	6	0.0	0.0	0	0	?	I<	11:08	0:00	[kworker/R-]		
root	7	0.0	0.0	0	0	?	I<	11:08	0:00	[kworker/R-]		
root	11	0.0	0.0	0	0	?	I	11:08	0:00	[kworker/u4]		
root	12	0.0	0.0	0	0	?	I<	11:08	0:00	[kworker/R-]		
root	13	0.0	0.0	0	0	?	I	11:08	0:00	[rcu_tasks_]		
root	14	0.0	0.0	0	0	?	I	11:08	0:00	[rcu_tasks_]		
root	15	0.0	0.0	0	0	?	I	11:08	0:00	[rcu_tasks_]		
root	16	0.0	0.0	0	0	?	S	11:08	0:03	[ksoftirqd/]		
root	17	0.0	0.0	0	0	?	I	11:08	0:02	[rcu_preempt]		
root	18	0.0	0.0	0	0	?	S	11:08	0:00	[rcu_exp_pa]		
root	19	0.0	0.0	0	0	?	S	11:08	0:00	[rcu_exp_gp]		
root	20	0.0	0.0	0	0	?	S	11:08	0:00	[migration/]		
root	21	0.0	0.0	0	0	?	S	11:08	0:00	[idle_injec]		
root	22	0.0	0.0	0	0	?	S	11:08	0:00	[cpuhp/0]		
root	24	0.0	0.0	0	0	?	S	11:08	0:00	[kdevtmpfs]		
root	25	0.0	0.0	0	0	?	I<	11:08	0:00	[kworker/R-]		
root	27	0.0	0.0	0	0	?	S	11:08	0:00	[kaudit]		
root	28	0.0	0.0	0	0	?	S	11:08	0:00	[khungtaskd]		
root	29	0.0	0.0	0	0	?	S	11:08	0:00	[oom_reaper]		
root	31	0.0	0.0	0	0	?	I<	11:08	0:00	[kworker/R-]		
root	32	0.0	0.0	0	0	?	S	11:08	0:01	[kcompactd0]		
root	33	0.0	0.0	0	0	?	SN	11:08	0:00	[ksmd]		

-lspci

```
(septama@Luxon)-[~/Bureau/cybersec]
$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371AB/EB/MB PIIX4 IDE (rev 01)
00:02.0 VGA compatible controller: VMware SVGA II Adapter
00:03.0 Ethernet controller: Intel Corporation 82540EM Gigabit Ethernet Controller (rev 02)
00:04.0 System peripheral: InnoTek Systemberatung GmbH VirtualBox Guest Service
00:05.0 Multimedia audio controller: Intel Corporation 82801AA AC'97 Audio Controller (rev 01)
00:06.0 USB controller: Apple Inc. KeyLargo/Intrepid USB
00:07.0 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 08)
00:0b.0 USB controller: Intel Corporation 82801FB/FBM/FR/FW/FRW (ICH6 Family) USB2_EHCI Controller
00:0d.0 SATA controller: Intel Corporation 82801HM/HEM (ICH8M/ICH8M-E) SATA Controller [AHCI mode] (rev 02)

(septama@Luxon)-[~/Bureau/cybersec]
$
```

-sudo apt install traceroute

```
(septama@Luxon)-[~/Bureau/cybersec]
$ sudo apt install traceroute
[sudo] Mot de passe pour septama : 
traceroute est déjà la version la plus récente (1:2.1.6-1).
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  imagemagick-6.q16   libgles1           libmbcrypto7t64
  libbbfiol            libglvnd-core-dev  libpaper1
  libc++1-19            libglvnd-dev      libqt5x11extras5
  libc++abi1-19         libgtksourceview-3.0-1  libsuperlu6
  libcapstone4          libgdksourceviewmm-3.0-0v5  libtag1v5
  libdirectfb-1.7-7t64  libmagickcore-6.q16-7-extra  libtag1v5-vanilla
  libegl-dev             libjxl0.9          libtiff
  libfmt9               libmagickwand-6.q16-7t64    libunwind-19
  libgl1-mesa-dev       libmagickcore-6.q16-7t64    libx265-209
  libgles-dev           libmagickwand-6.q16-7t64    python3-appdirs
Veuillez utiliser « sudo apt autoremove » pour les supprimer.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

(septama@Luxon)-[~/Bureau/cybersec]
$
```

-traceroute google.com

```
└─(septama@Luxon)-[~/Bureau]
└─$ traceroute google.com
traceroute to google.com (172.217.15.206), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  4.849 ms  4.801 ms  4.768 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  *^C
```

```
└─(septama@Luxon)-[~/Bureau]
└─$ █
```

-netstat -tuln

```
└─(septama@Luxon)-[~/Bureau]
└─$ netstat -tuln
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale          Adresse distante      Etat
udp        0      0 10.0.2.15:3702        0.0.0.0:*
udp        0      0 239.255.255.250:3702    0.0.0.0:*
udp        0      0 0.0.0.0:54278         0.0.0.0:*
udp6       0      0 :::58686            ::::*
udp6       0      0 fe80::a00:27ff:fe6:3702  ::::*
udp6       0      0 ff02::c:3702        ::::*
```

```
└─(septama@Luxon)-[~/Bureau]
└─$ █
```

-ss -tuln
journalctl
journalctl -f
journalctl -b
journalctl -n 10
date

```
└─(septama@Luxon)-[~/Bureau]
$ date
ven 07 fév 2025 13:38:18 EST

└─(septama@Luxon)-[~/Bureau]
$ █
```

timedatectl

```
└─(septama@Luxon)-[~/Bureau]
$ timedatectl
    Local time: ven 2025-02-07 13:40:15 EST
    Universal time: ven 2025-02-07 18:40:15 UTC
        RTC time: ven 2025-02-07 18:40:15
        Time zone: America/Port-au-Prince (EST, -0500)
  System clock synchronized: no
      NTP service: inactive
      RTC in local TZ: no

└─(septama@Luxon)-[~/Bureau]
$ █
```

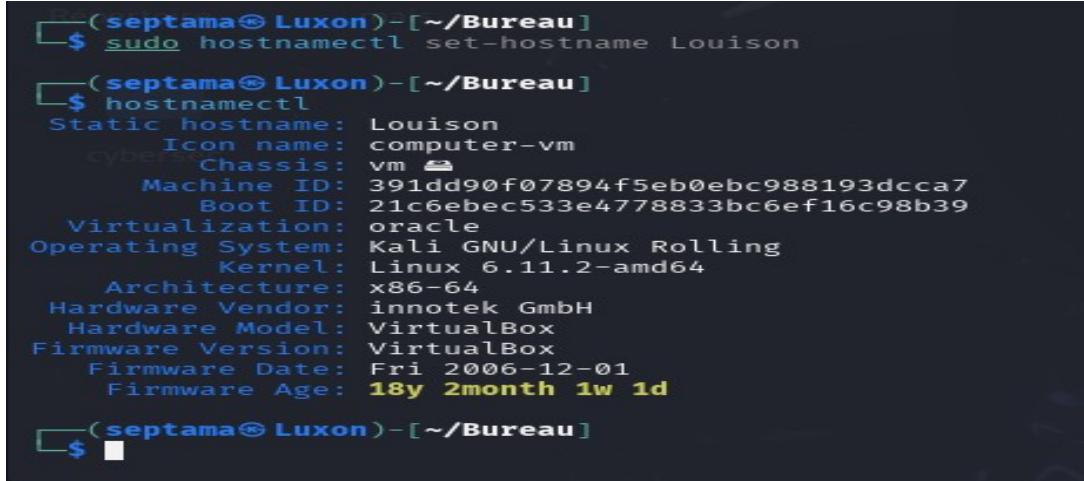
hostnamectl

```
└─(septama@Luxon)-[~/Bureau]
$ hostnamectl
  Static hostname: Luxon
    Icon name: computer-vm
    Chassis: vm 🖥
   Machine ID: 391dd90f07894f5eb0ebc988193dcca7
     Boot ID: 21c6ebec533e4778833bc6ef16c98b39
Virtualization: oracle
Operating System: Kali GNU/Linux Rolling
          Kernel: Linux 6.11.2-amd64
      Architecture: x86-64
  Hardware Vendor: innotek GmbH
Hardware Model: VirtualBox
Firmware Version: VirtualBox
  Firmware Date: Fri 2006-12-01
  Firmware Age: 18y 2month 1w 1d

└─(septama@Luxon)-[~/Bureau]
$ █
```

Pour changer le nom d'hôte, vous pouvez utiliser la commande suivante

```
sudo hostnamectl set-hostname Louison
```



```
[septama@Luxon) [~/Bureau]
$ sudo hostnamectl set-hostname Louison

[septama@Luxon) [~/Bureau]
$ hostnamectl
Static hostname: Louison
Icon name: computer-vm
Chassis: vm
Machine ID: 391dd90f07894f5eb0ebc988193dcca7
Boot ID: 21c6ebec533e4778833bc6ef16c98b39
Virtualization: oracle
Operating System: Kali GNU/Linux Rolling
Kernel: Linux 6.11.2-amd64
Architecture: x86-64
Hardware Vendor: innotek GmbH
Hardware Model: VirtualBox
Firmware Version: VirtualBox
Firmware Date: Fri 2006-12-01
Firmware Age: 18y 2month 1w 1d

[septama@Luxon) [~/Bureau]
$
```

Ce travail dirige nous a permis d'acquerir des competences pratiques essentielles dans l'installation, la configuration et l'utilisation de kali Linux dans un environnement virtualise . A travers les differents taches realises, nous avons appris a gerer les fichier et des dossier, a manipuler les permissions ,a exicuter des commandes systeme et a analyser un reseau a l'aide d'outils comme nmap. Enfin l'hebergement du rapport et des fichier sur GitHub a mis en pratique les bonne pratique les bonnes pratiques de documentation et partage collaboratif des resultats.

Ce Traveaux Pratique nous a ainsi apporte nos capacites en administation systeme et en anlyse de reseau.