From SQLi to Shell

Exploitation de la machine

Olivier LASNE

2021-01-19

Installation de “From SLQi to Shell”

Il s’agit d’une machine virtuelle faite par PentesterLab volontairement vulnérable. Elle permet de réaliser un scénario d’attaque complet sur une machine “réaliste”.

Une correction officielle de la machine est disponible ici : https://pentesterlab.com/exercises/from_sqli_to_shell/course

Télécharger le fichier ISO

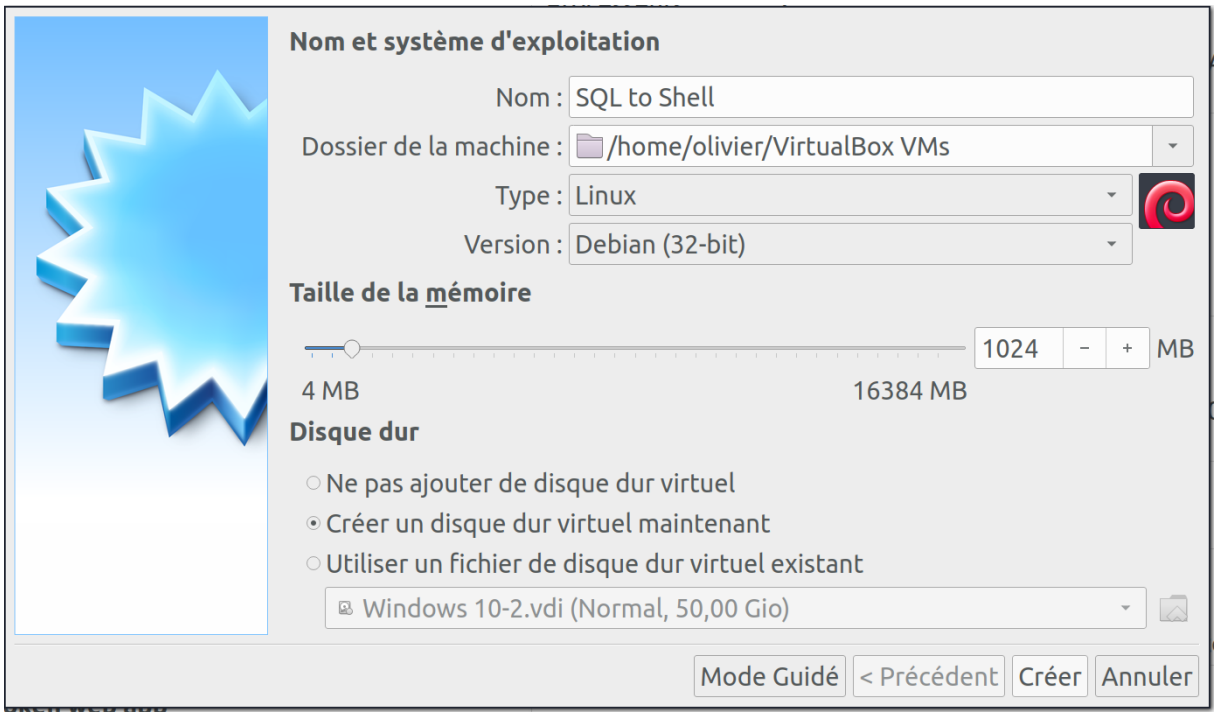
Le fichier iso peut être télécharger ici :
https://pentesterlab.com/exercises/from_sqli_to_shell/iso

Installation dans VirtualBox

Création d’une nouvelle VM

Dans VirtualBox, cliquer sur le bouton **Nouvelle**. 

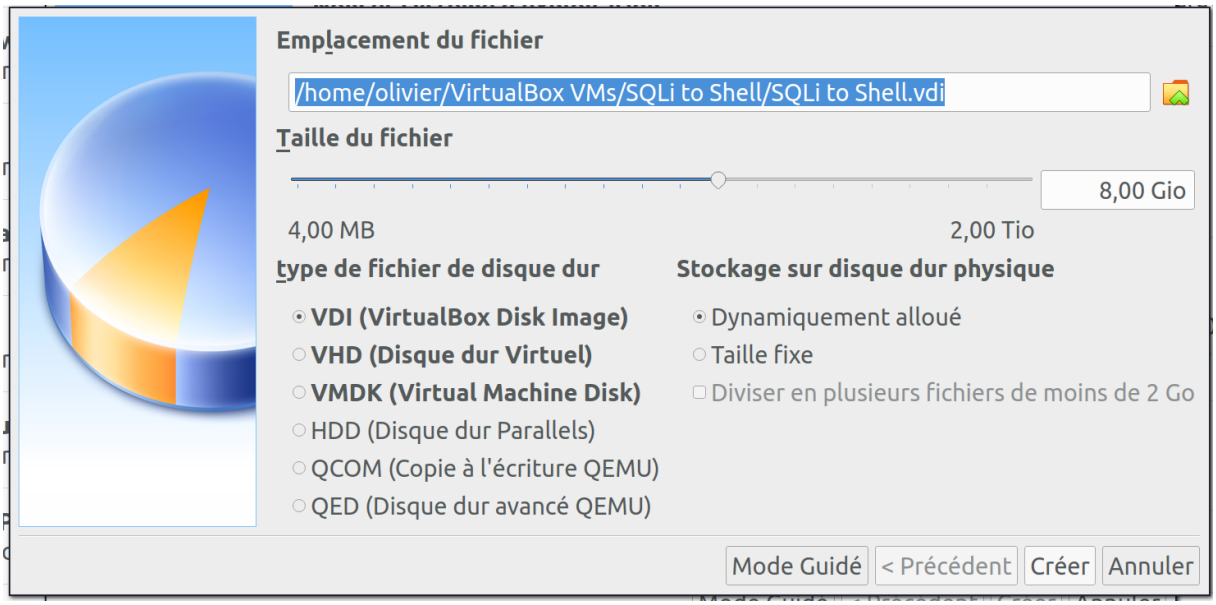
Donner un nom (ex : “SQLi to Shell”), puis choisir type **Linux** et version **debian32**.



Cliquer sur **Créer**.

Laisser les options de **Taille de mémoire** et de **Disque dur** par **défaut**.

Vous pouvez ensuite également laisser l'**emplacement du fichier** et sa **taille** par **défaut**.



Cliquer sur **Créer**.

Ajout du live CD

Selectionner dans Virtualbox la VM nouvellement créée.

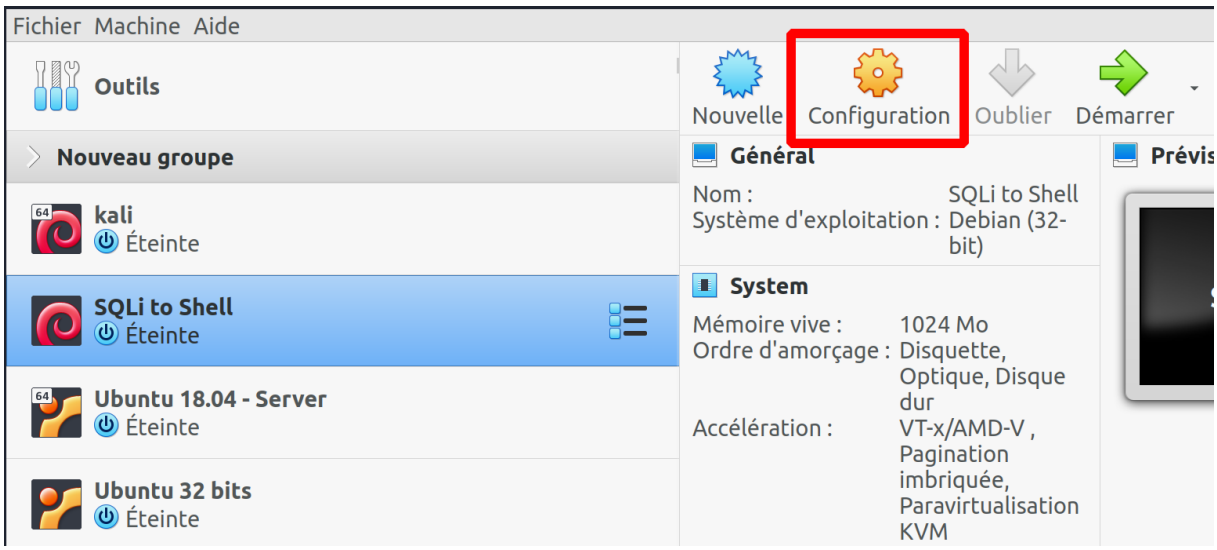
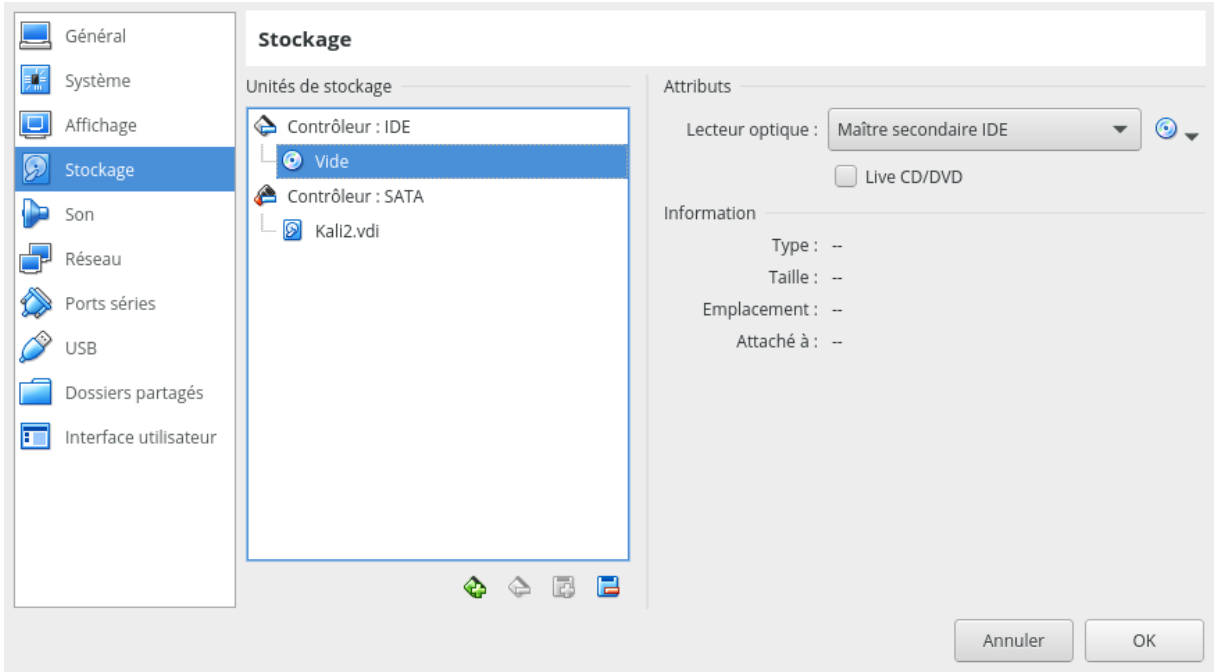


FIG. 1: Selection de la machine

Et cliquer sur l'icone Configuration. 

Selectionner **Stockage > *Vide* sous Contrôleur IDE**.



Cliquer sur l'icone de CD  , et **Choissisez un fichier de disque optique virtuel**. Et sélectionner le

fichier *from_sqli_to_shell_i386.iso* téléchagé précédement.

Appuyer sur **OK** en bas à droite pour confirmer les modifications.

Configuration réseau

Pour attaquer la VM vulnérable, on va préférer un mode “réseau privé hôte”.

À nouveau, **selectionner** la VM **“SQLi to Shell”** dans VirtualBox et cliquer sur l’icone **Configuration**.

1. Aller dans **Réseau > Apdater 1**
2. Pour *Mode d’accès réseau* sélectionner **Réseau privé hôte**
3. Dans *Nom :* sélectionner **vboxnet0** (réseau de votre Kali)
4. Cliquer sur **OK** pour confirmer les changement

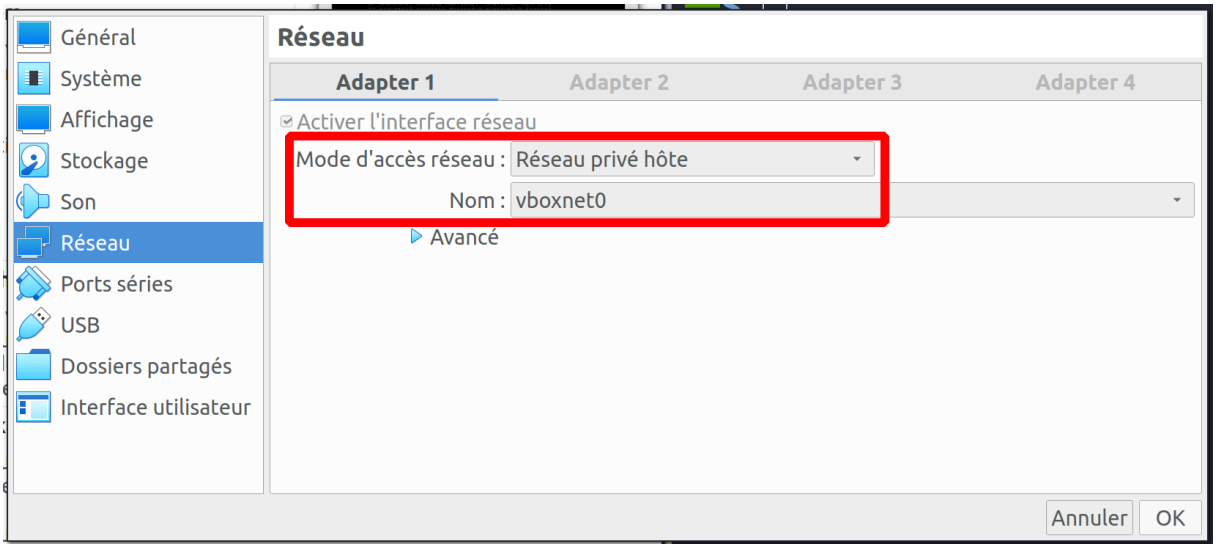


FIG. 2: Configuration en réseau privé hôte

Lancer la VM

On peut mantenant lancer la machine virtuelle avec le bouton **Démarrer**. 

Il est possible qu'au démarrage, la VM vous **redemande le fichier ISO** à utiliser. Dans ce cas, selectionner bien *from_sqli_to_shell_i386.iso*.

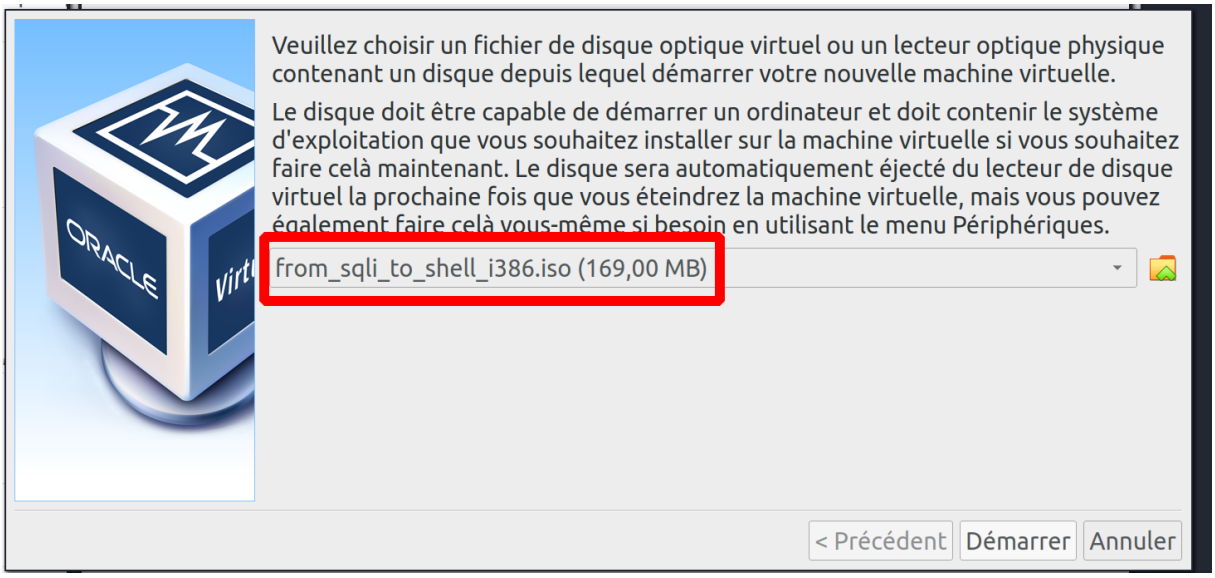


FIG. 3: Selection de l'iso au démarrage

L'installation est terminée.

S'agissant d'un Live CD. La machine démarrera à chaque fois sur le fichie ISO sans conserver les changement qui ont été effectués dessus.