Laboratoire 1

Mise en place du laboratoire

Le laboratoire « 1 » est constitué d'une maquette sous VirtualBox contenant 4 machines virtuelles préconfigurées :

Machine	Nom de domaine pleinement qualifié	Configuration réseau	Applications et services
Serveur SSH sous Debian 10	srvssh.local.sio.fr	Adresse IPv4 : 192.168.56.10/24 Passerelle : 192.168.56.254 Serveur DNS : 127.0.0.1	Service OpenSSH port 22/TCP Service DNS Bind port 53/UDP
Client SSH sous Debian 10	clissh.local.sio.fr	Adresse IPv4 : 192.168.56.11/24 Passerelle : 192.168.56.254 Serveur DNS : 192.168.56.10	Environnement de bureau XFCE Client OpenSSH
Attaquant sous Kali Linux	NA	Adresse IPv4 : 192.168.56.12/24 Passerelle : 192.168.56.254 Serveur DNS : 192.168.56.10	Ettercap Git ssh-mitm Netfilter/Iptables
Routeur OpenBSD	rwbsd.local.sio.fr	Adresses IPv4 : em0 - DHCP em1 -192.168.56.254/24	PacketFilter

Voici les comptes et les mots de passe vous permettant d'accéder aux différentes machines virtuelles :

Intitulé de la machine	Nom d'utilisateur	Mot de passe
Serveur SSH sous Debian 10	etusio	Fghijkl1234*
Client SSH sous Debian 10	etusio	Fghijkl1234*
Attaquant sous Kali Linux 2020.1b	etusio	Fghijkl1234*
Routeur OpenBSD	etusio	Fghijkl1234*

Lorsque des commandes nécessitant des privilèges administrateurs seront utilisées, il sera nécessaire d'utiliser la commande **sudo** sous Debian GNU/Linux et **doas** sous OpenBSD.

```
etusio@srvssh:~$ sudo service ssh restart
rwbsd$ doas sh /etc/netstart
```

Voici une représentation logique de la maquette proposée dans le cadre de ce laboratoire :

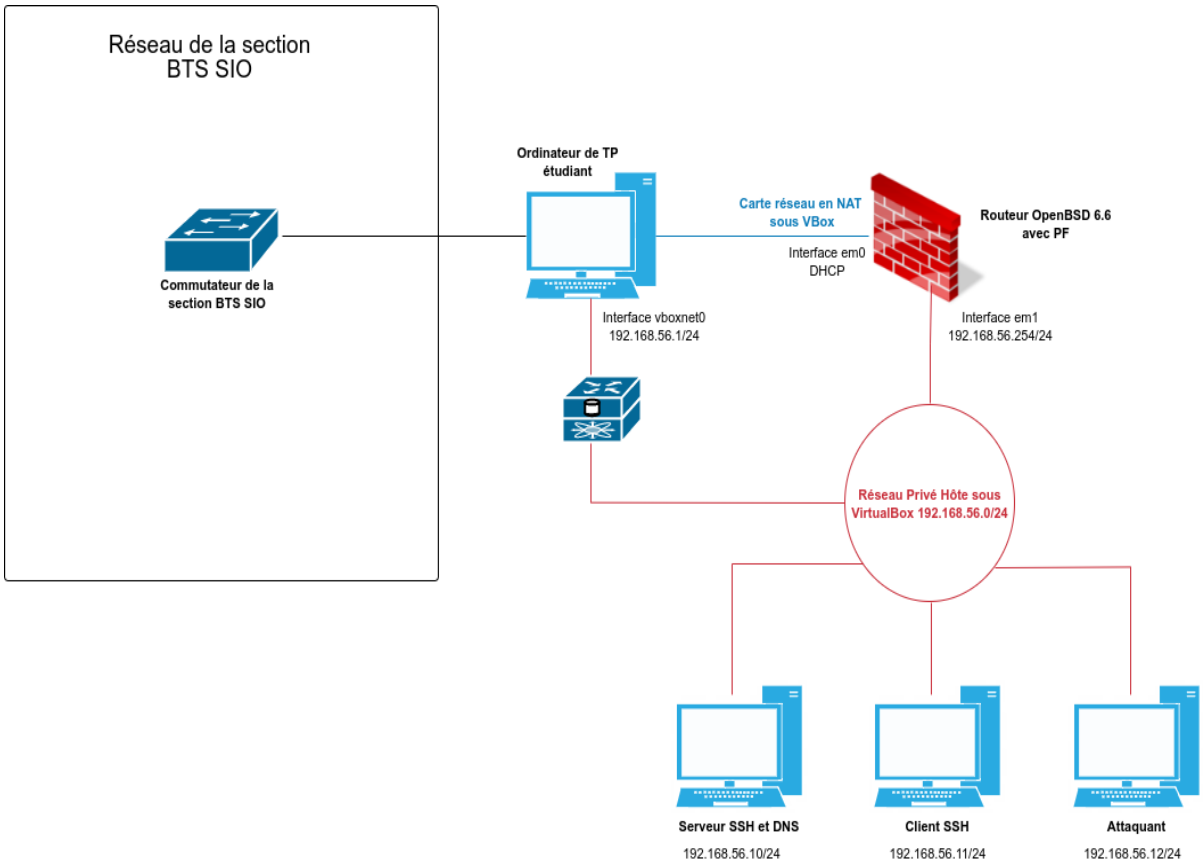


Illustration 1: Schéma logique de l'infrastructure du « lab 1 »

Explications sur les machines virtuelles

L'objectif de **Kali Linux** est de fournir une distribution basée sur Debian regroupant l'ensemble des outils nécessaires aux tests de sécurité d'un système d'information, notamment le test d'intrusion. L'intérêt de Kali Linux est de comporter près de 300 outils déjà installés pour travailler dans le domaine de la cybersécurité.

Attention ! Il a été décidé de fournir une image ova la plus petite possible. Par conséquent, la machine virtuelle Kali Linux a été réduite à sa plus petite taille. **Il est donc déconseillé d'effectuer des mises à jour ou d'installer de nouvelles applications sur cette dernière sous peine de saturer le disque dur.**

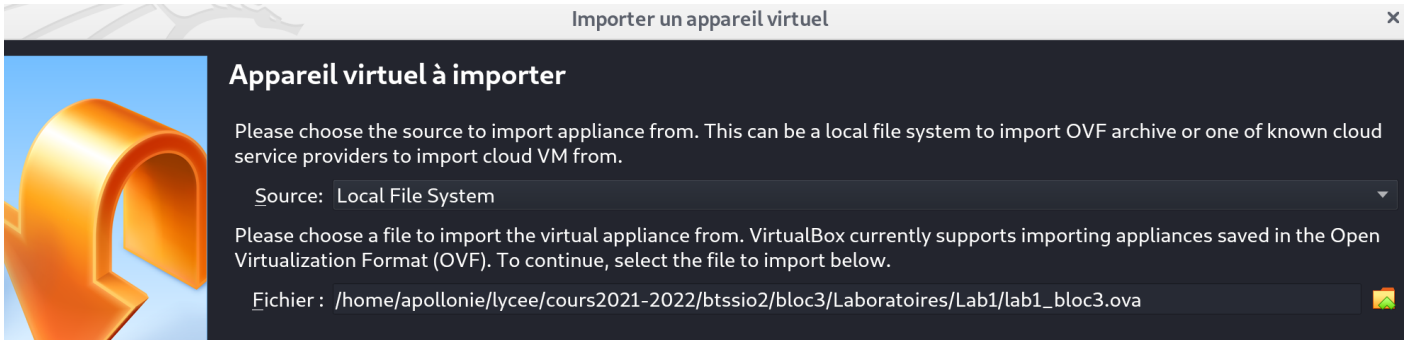
Le routeur/pare-feu OpenBSD

Source Wikipedia :
« OpenBSD est un système d'exploitation libre de type Unix (…).
Le projet OpenBSD est réputé pour son intransigeance sur la liberté du logiciel et du code source, la qualité de sa documentation, et l'importance accordée à la sécurité et la cryptographie intégrée. OpenBSD inclut un certain nombre de mesures de sécurité absentes ou optionnelles dans d'autres systèmes d'exploitation. Ses développeurs ont pour tradition de réaliser des audits de code à la recherche de problèmes de sécurité et de bogues (…). »

Le serveur OpenBSD de la maquette fait office de routeur et de parefeu avec *pfsense*.

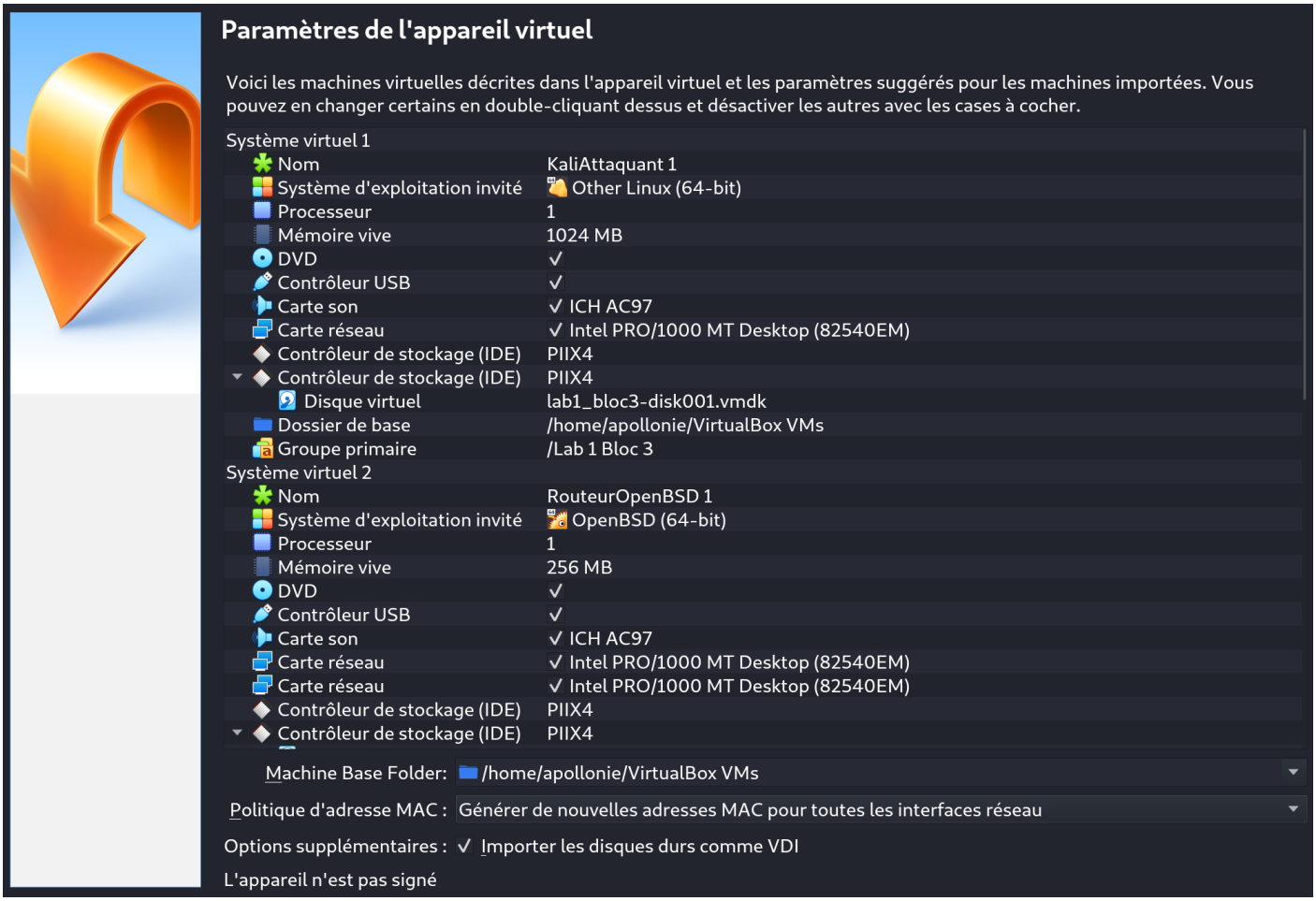
Mise en œuvre de la maquette

Récupérer le fichier **lab1_bloc3.ova** et importez-le sur le logiciel VirtualBox (**Fichier>Importer** un appareil virtuel).



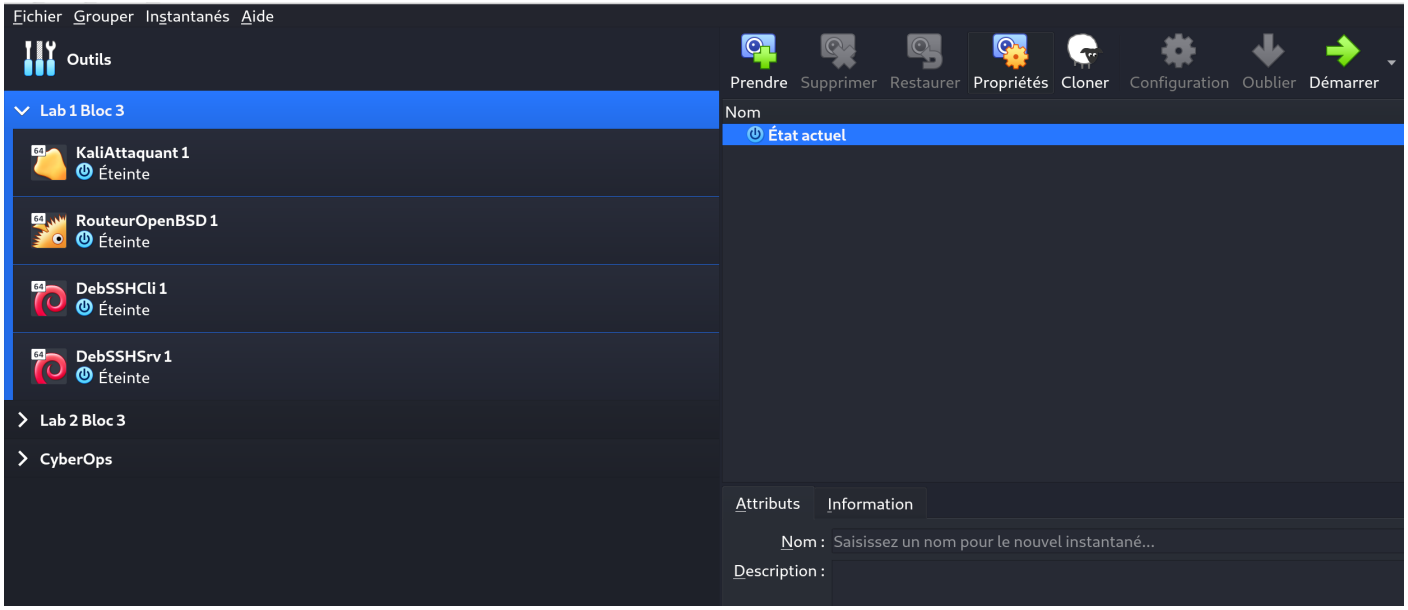
Puis cliquer sur « suivant ».

Les quatre machines virtuelles vont venir se ranger dans le groupe « Lab1 bloc3 ».



Modifier la politique d'adresse MAC : Générer de nouvelles adresses MAC pour toutes les interfaces réseaux

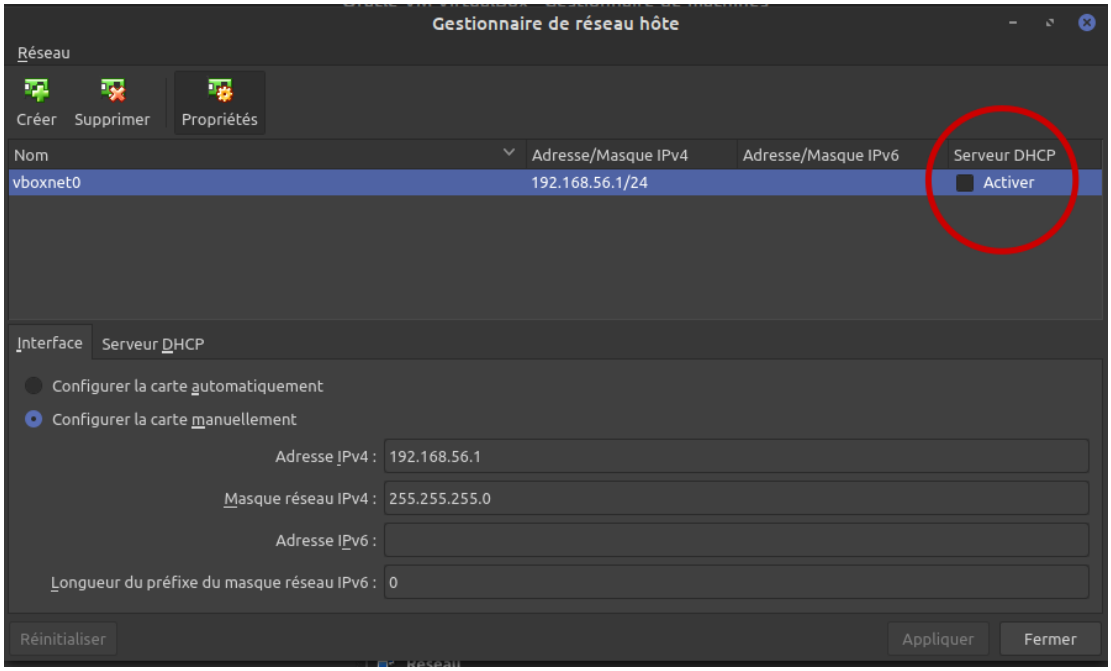
Cliquer sur « Importer ».

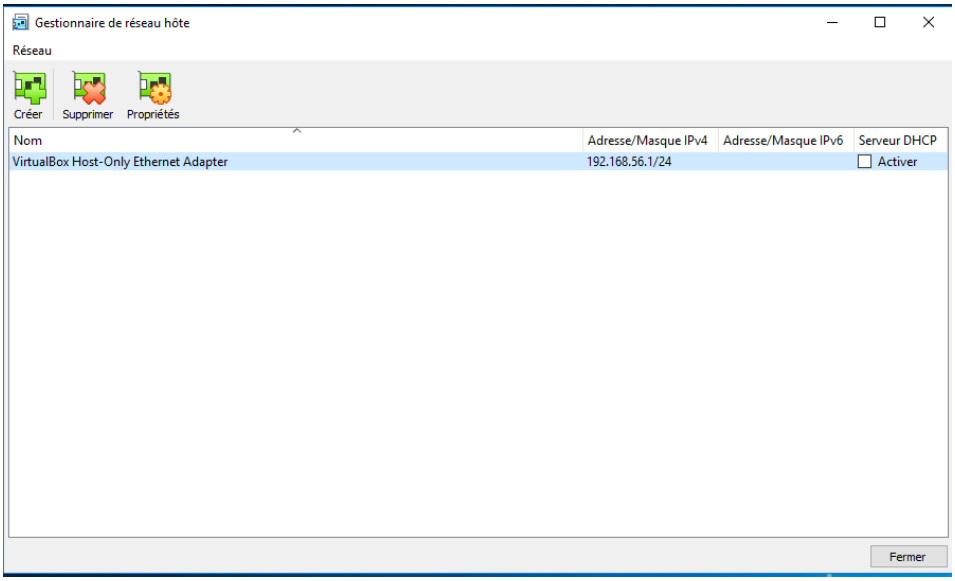


Une fois les différentes machines virtuelles importées, il faut s'assurer qu'une carte réseau (vboxnet0 ou VirtualBox Host-Only Ethernet Adapter) a bien été créée dans le gestionnaire de réseau hôte.

Pour cela, cliquer sur Fichier>Gestionnaire de réseau hôte.

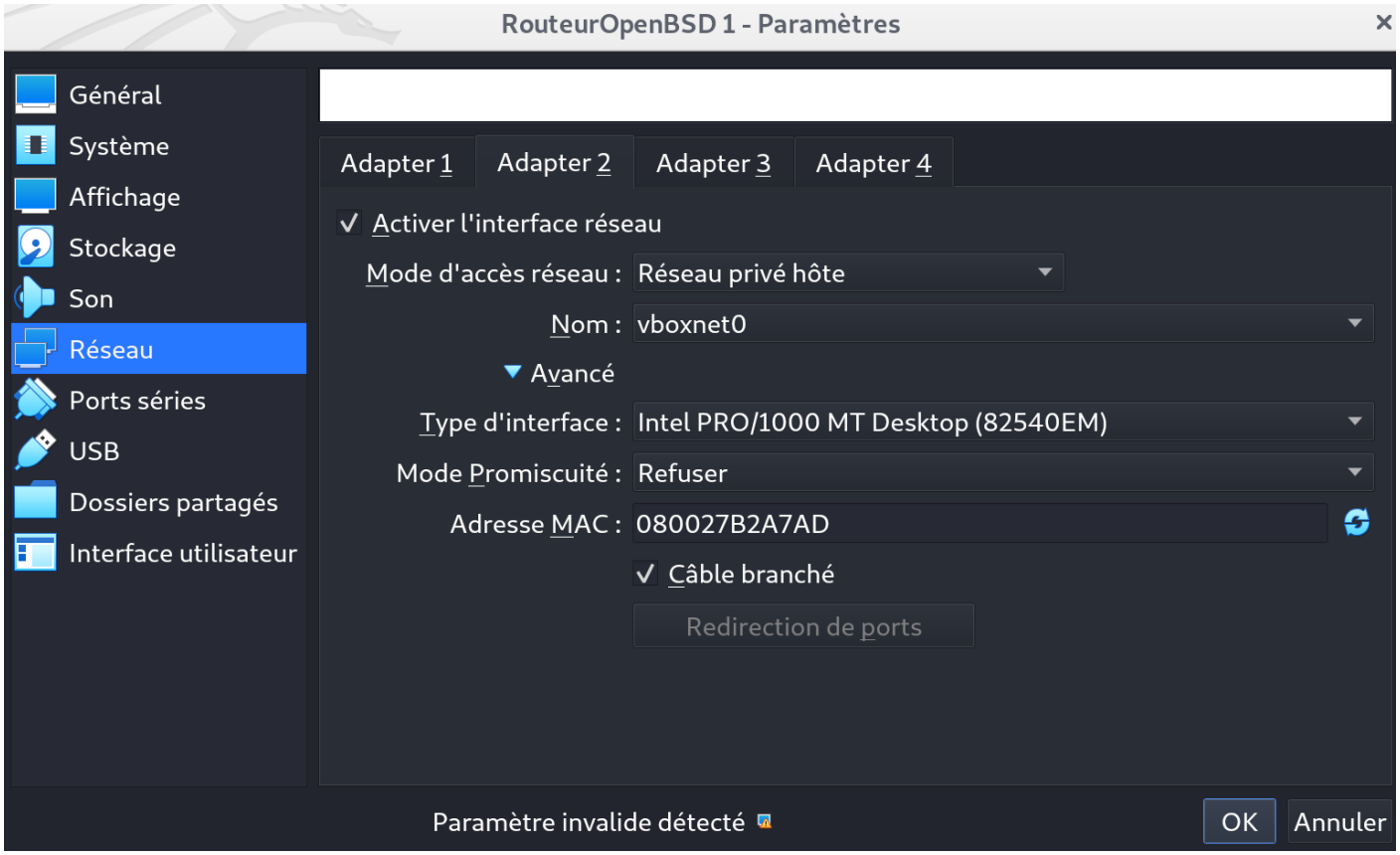
Vous devriez voir apparaître une nouvelle carte réseau virtuelle nommée **vboxnet0** ou VirtualBox Host-Only Ethernet Adapter (suivi éventuellement d'un # et numéro si des cartes virtuelles ont déjà été créées auparavant) sous Windows avec comme adresse **IP 192.168.56.1/24**. **Décocher** l'activation du serveur DHCP. Si aucune carte réseau n'apparaît, cliquer sur **Créer** puis indiquer les paramètres présents dans la capture d'écran ci-dessous.





Enfin, s'assurer dans les paramètres réseaux des machines virtuelles que les cartes réseaux définies en mode réseau privé hôte sont correctement liées à vboxnet0 ou VirtualBox Host-Only Ethernet Adapter.

Par exemple pour le routeur OpenBSD et l'adaptateur 2



L'adaptateur 1 accède au réseau en mode « nat » : c'est lui qui est relié au réseau de la section.

Ensuite, démarrer l'ensemble des machines virtuelles de la maquette y compris le routeur OpenBSD. C'est grâce à ce routeur que les autres VM auront accès à Internet (voir ci-après si un message d'erreur concernant la carte réseau apparaît au démarrage des machines).

Vous pouvez administrer l'ensemble de la maquette à l'aide de la console VirtualBox mais aussi à l'aide du protocole SSH depuis votre machine hôte à l'aide d'un client natif, de putty ou kitty.

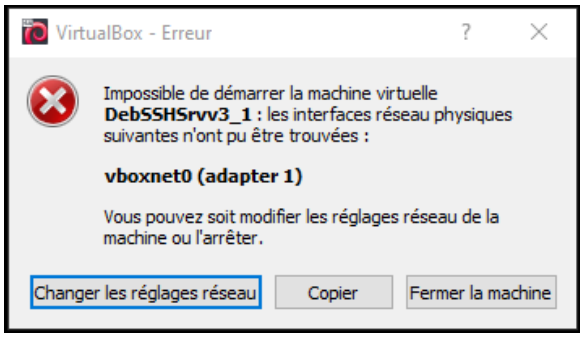
Attention ! Il n'est pas nécessaire de modifier les configurations réseaux des machines virtuelles. Le choix d'un réseau privé hôte plutôt que d'un réseau interne permet à l'étudiant de pouvoir se connecter en SSH sur chaque machine depuis l'ordinateur hôte. Ce dernier dispose en effet d'une carte réseau virtuelle nommée vboxnet0 sous GNU/Linux ou VirtualBox Host-Only sous Windows qui lui permet d'avoir une configuration réseau dans le même réseau que les machines virtuelles. Ainsi, cela offre une vraie souplesse en permettant notamment le copier/coller à partir de client SSH dédié depuis la machine hôte.

Depuis votre machine hôte, vous devriez être en mesure de lancer une commande « ping » sur chaque machine virtuelle.

En cas de message d'erreur concernant la carte réseau au démarrage des machines

Sur une plateforme Windows, si vous n'avez pas accédé à la configuration réseau pour valider le nom de l'interface réseau avant de démarrer la machine, vous aurez probablement le message d'erreur suivant :

Il suffira de cliquer sur « Changer les réglages réseau » et de valider la prise en compte du « VirtualBox Host-Only Ethernet Adapter » à la place de « vboxnet0 » pour régler le problème.



Sur une plateforme Linux, il suffit de :

- Cliquer sur changer les réglages réseau ;
- enregistrer en cliquant sur « OK ».

Si cette simple manipulation ne fonctionne pas :

- « fermer la machine » ;
- reconfigurer les paramètres réseaux des machines virtuelles en décochant et réactivant la case « Activer l'interface réseau » ;
- enregistrer en cliquant sur « OK ».