Laboratoire 2

Mise en place du laboratoire

Le laboratoire n°2 est constitué d'une maquette sous VirtualBox contenant 5 machines virtuelles préconfigurées :

Machine	Nom de domaine pleinement qualifié	Configuration réseau	Applications et services
Serveur DNS sous Debian 10	srvdns.local.sio.fr	Adresse IPv4 : 172.16.10.10/24 Passerelle : 172.16.10.254 Serveur DNS : 127.0.0.1	Service OpenSSH port 22/TCP Service DNS Bind port 53/UDP
Machine virtuelle metasploitable Serveur Metasploit (metasploit 2.0)	srvm.local.sio.fr	Adresse IPv4 : 172.16.10.5/24 Passerelle : 172.16.10.254 Serveur DNS : 172.16.10.10	Service OpenSSH port 22/TCP Service Web
Client Légitime sous Debian 10	client.local.sio.fr	Adresse IPv4 : 192.168.56.11/24 Passerelle : 192.168.56.254 Serveur DNS : 172.16.10.10	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 : 172.16.10.10	Git Netfilter/Iptables Tous les outils Kali
Routeur OpenBSD	rwbsd.local.sio.fr	Adresses IPv4 : em0 – DHCP em1 -192.168.56.254/24 em2 -172.16.10.254/24	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 DNS sous Debian 10	etusio	Fghijkl1234*
Serveur Metasploit	msfadmin	msfadmin
Client Légitime sous Debian 11	etusio	Fghijkl1234*
Attaquant sous Kali Linux 2021.3	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 :

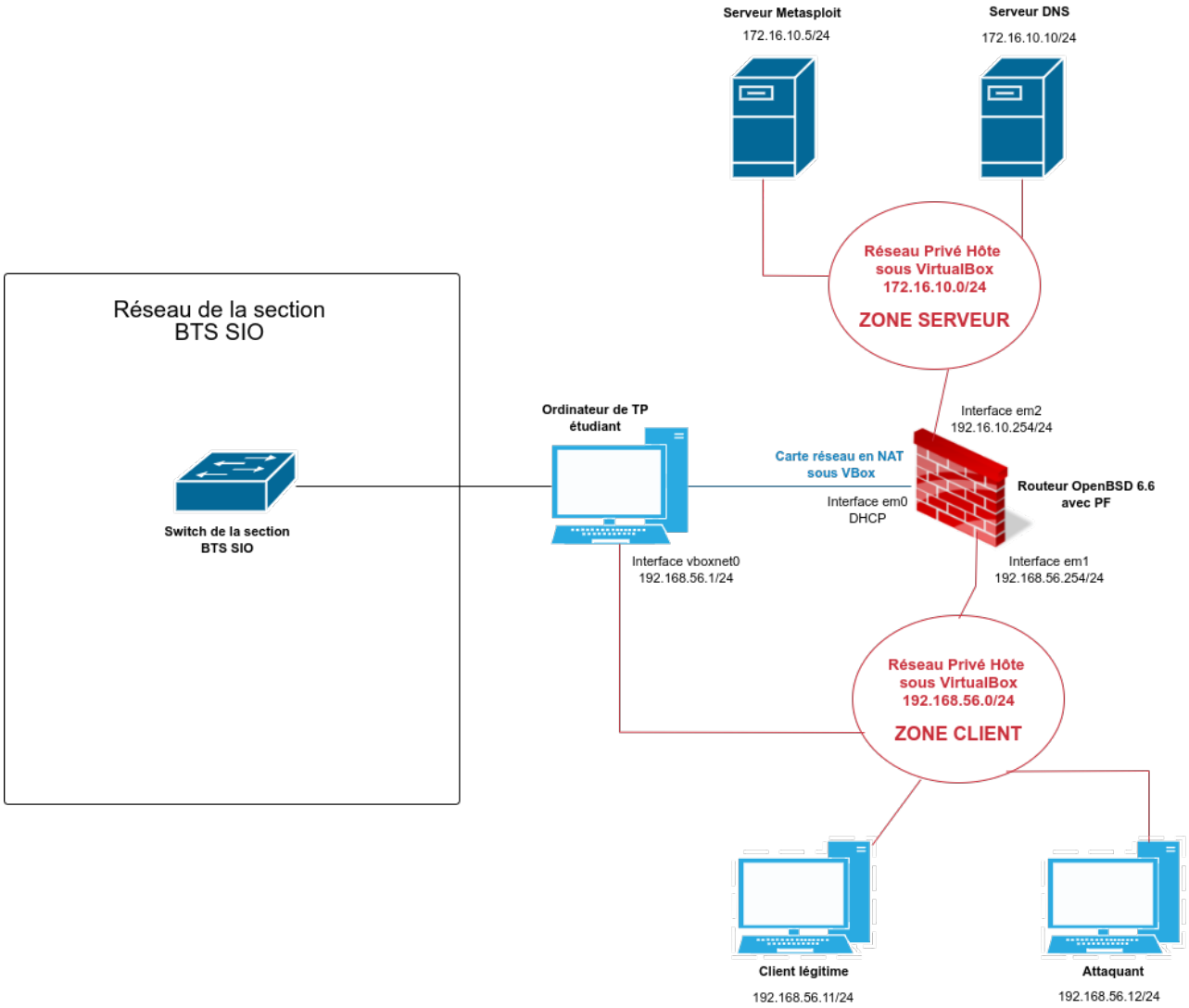


Illustration 1: Schéma logique de l'infrastructure du « lab 2 »

Explications sur les machines virtuelles

Kali Linux

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.

Si vous télécharger votre propre VM Kali : l'identifiant et le mot de passe de connexion sont **kali** et **kali** (attention, clavier en qwerty)**.** Pour avoir un clavier français *pour cette session*, lancer la commande : `setxkbmap fr` depuis une fenêtre shell.

Pour bénéficier d'un clavier en français de manière permanente : `sudo dpkg-reconfigure keyboard-configuration`

Pour bénéficier du menu en français : `sudo dpkg-reconfigure locales` (choisir « fr_FR.UTF-8 »).

Le serveur *metasploitable*

Metasploitable (version 2.0.0) est une distribution linux (ubuntu) intentionnellement vulnérable. Son objectif est d'apprendre à tester les principales vulnérabilités en liaison avec la distribution Kali Linux. C'est sur ce serveur qu'est disponible le site « mutillidae ».

Vous pouvez télécharger votre propre serveur *metasploit* sur sourceforge à l'URL suivante : https://sourceforge.net/projects/metasploitable. L'identifiant et le mot de passe de connexion sont **msfadmin (avec le clavier qwerty ,sfqd,in)** et **msfadmin**. Pour avoir un clavier en français, il faut saisir la commande **sudo loadkeys fr** ⇒ Cette commande est censée permettre la persistance de la configuration, mais ce n'est pas le cas ici, il s'agit d'un bug de la distribution basée sur… Ubuntu hardy (08.10).

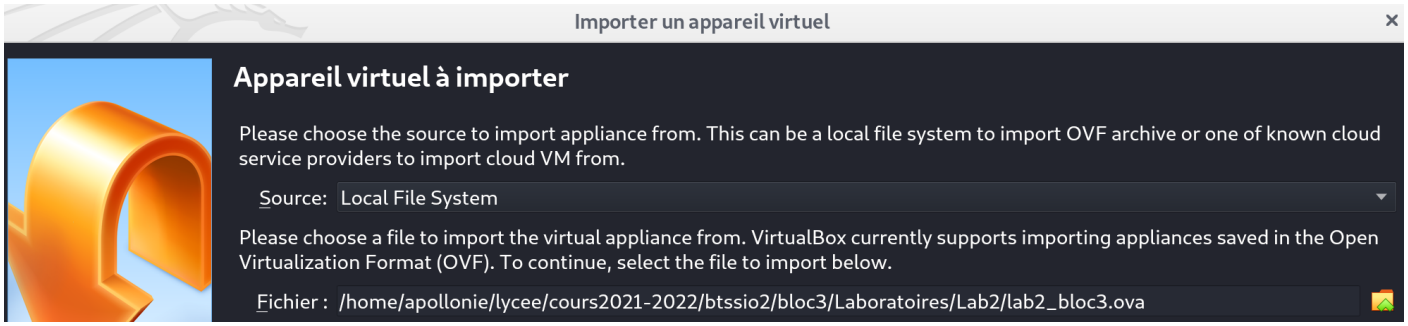
Le routeur/pare-feu OpenBSD

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 *Packet Filter*.

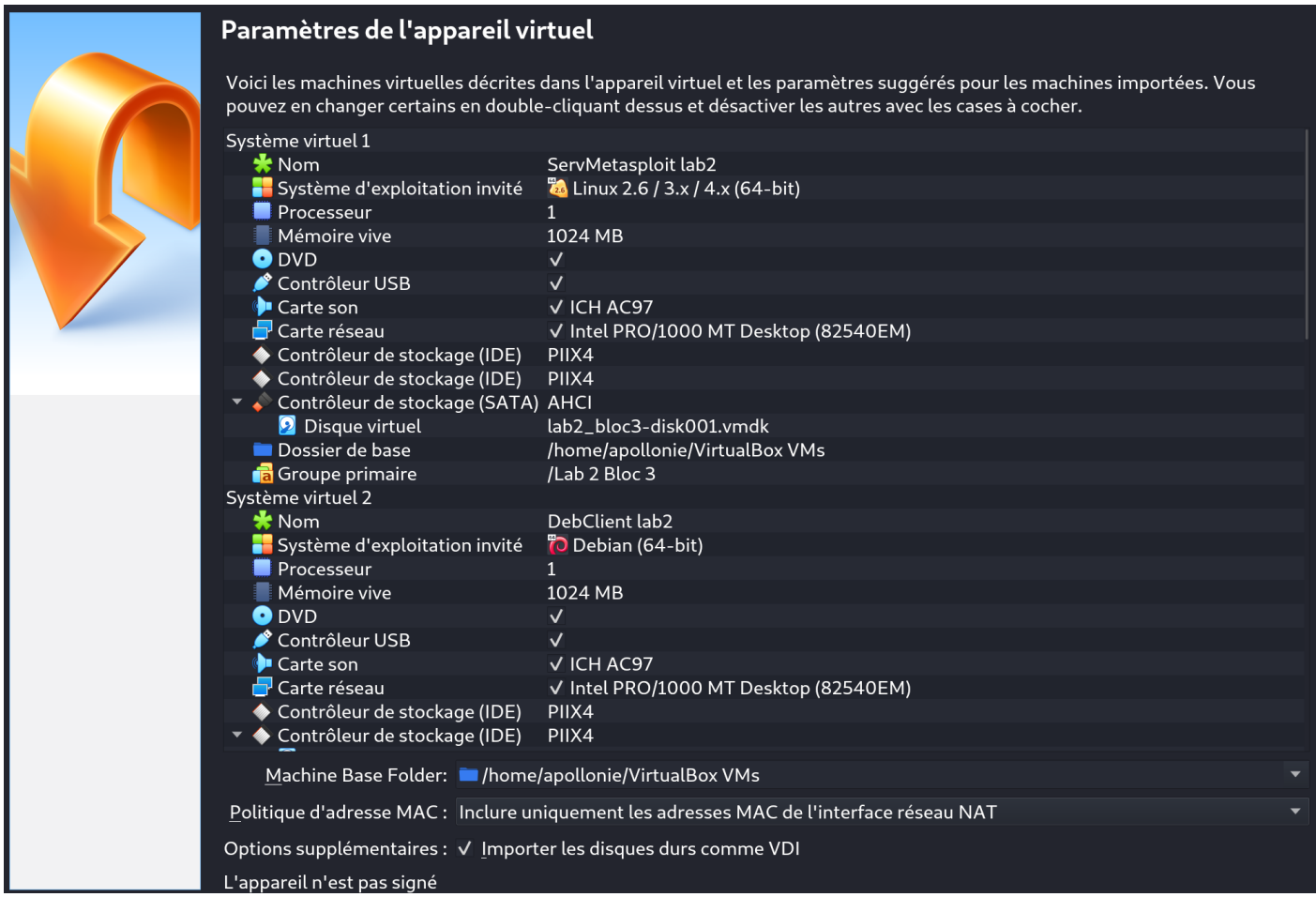
Mise en œuvre de la maquette

Récupérer le fichier **lab2_bloc3.ova** et importez-le sur le logiciel VirtualBox (**Fichier>Importer** un appareil virtuel).



Puis cliquer sur « suivant ».

Les cinq machines virtuelles vont venir se ranger dans le groupe « Lab2 bloc3 ».



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

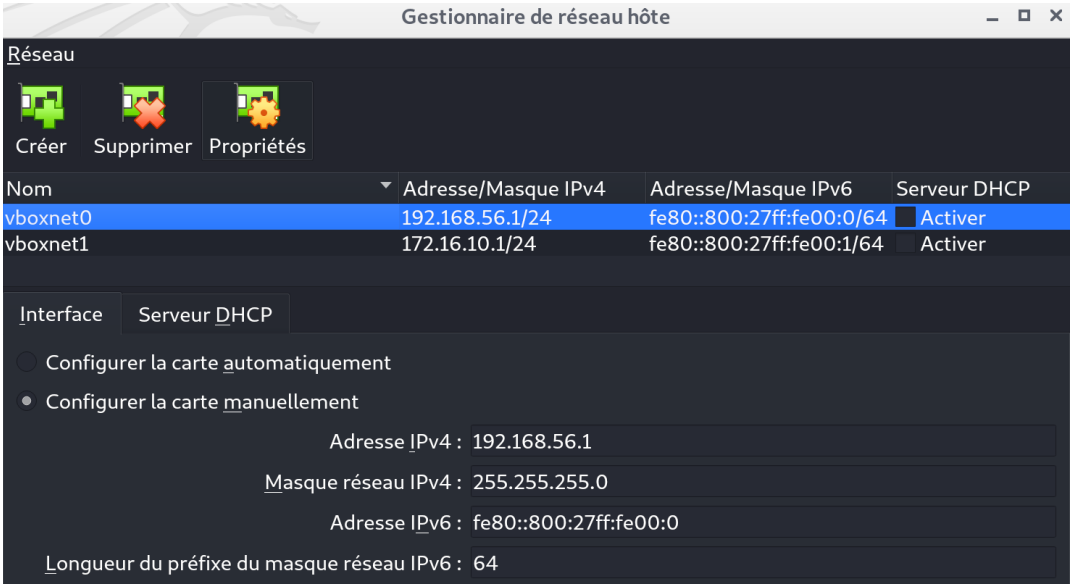
Cliquer sur « Importer ».

Une fois les différentes machines virtuelles importées, il faut s'assurer que les deux cartes réseaux virtuelles sont bien présentes dans le gestionnaire de réseau hôte.

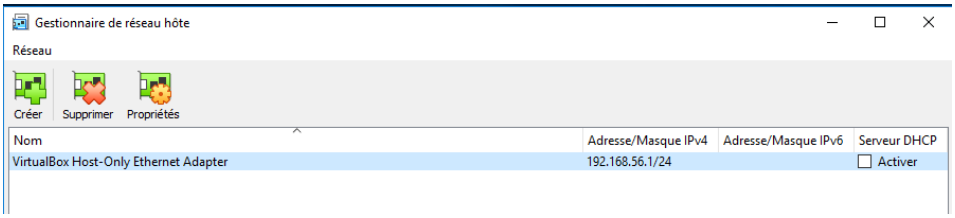
Pour cela, cliquer sur Fichier>Gestionnaire de réseau hôte.

Vous devriez voir apparaître deux nouvelles cartes réseaux virtuelles 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. Sinon, cliquer sur **Créer** puis indiquer les paramètres (l'adresse IPv6 n doit pas être renseignée).
- **vboxnet1** ou VirtualBox Host-Only Ethernet Adapter sous Windows (suivi éventuellement d'un # et numéro si des cartes virtuelles ont déjà été créées auparavant) avec comme adresse **IP 172.16.10.1/24**. **Décocher** l'activation du serveur DHCP. Sinon, cliquer sur **Créer** puis indiquer les paramètres (l'adresse IPv6 n doit pas être renseignée).



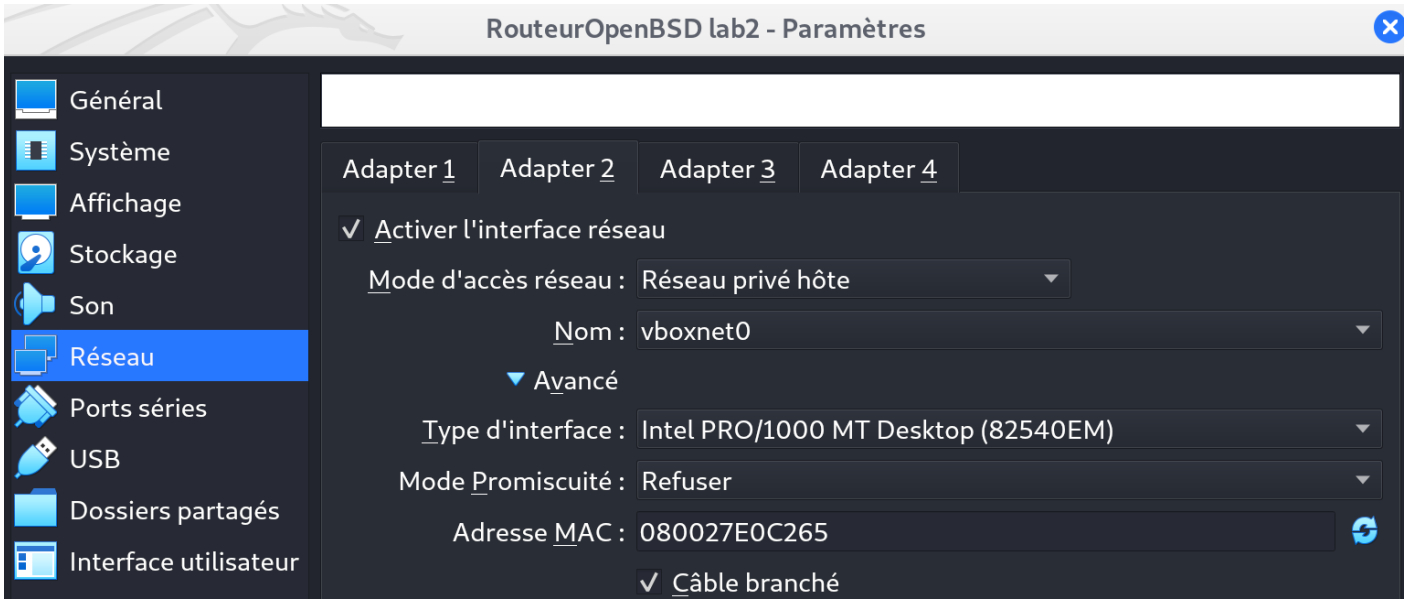
Ci-dessous la capture d'écran sur Windows pour la première carte virtuelle.



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 suivi éventuellement d'un # et un numéro) ou à vboxnet1 (ou VirtualBox Host-Only Ethernet Adapter suivi éventuellement d'un # et numéro).

Machine	Nom sur VB	Configuration réseau	Relié au réseau
Serveur DNS	DebDNSsrv lab2	Adaptateur 1 : vboxnet1	172.16.10.0/24
Serveur Metasploit	ServMetasploit lab2	Adaptateur 1 : vboxnet1	172.16.10.0/24
Client Légitime	DebClient lab2	Adaptateur 1 : vboxnet0	192.168.56.0/24
Kali Attaquant	KaliAttaquant lab2	Adaptateur 1 : vboxnet0	192.168.56.0/24
Routeur OpenBSD	RouteurOpenBSD lab2	Adaptateur 1 : NAT Adaptateur 2 : vboxnet0 Adaptateur 3 : vboxnet1	de la section de BTS 192.168.56.0/24 172.16.10.0/24

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.

La machine virtuelle Kali Linux n'est plus réduite comme dans le Laboratoire 1. **Il est donc possible d'effectuer des mises à jour et d'installer de nouvelles applications.**

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.

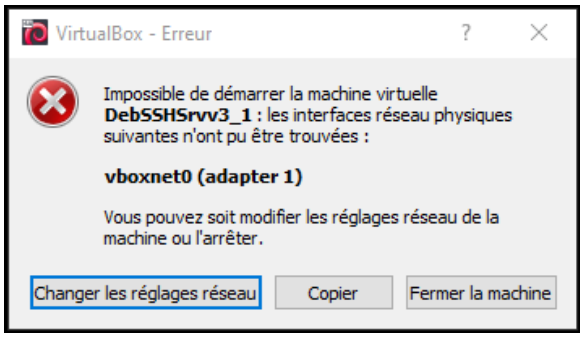
Attention ! Il n'est pas nécessaire de modifier les configurations réseaux des machines virtuelles. Le choix d'un réseau privé hôte plutôt que d'un réseau interne permet à l'étudiant de pouvoir se connecter en SSH sur chaque machine depuis l'ordinateur hôte. Ce dernier dispose en effet de deux cartes réseaux virtuelles : vboxnet0 et vboxnet1 sous GNU/Linux ou VirtualBox Host-Only (suivi d'un # et numéro 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, par exemple, 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 ».