Information System Security

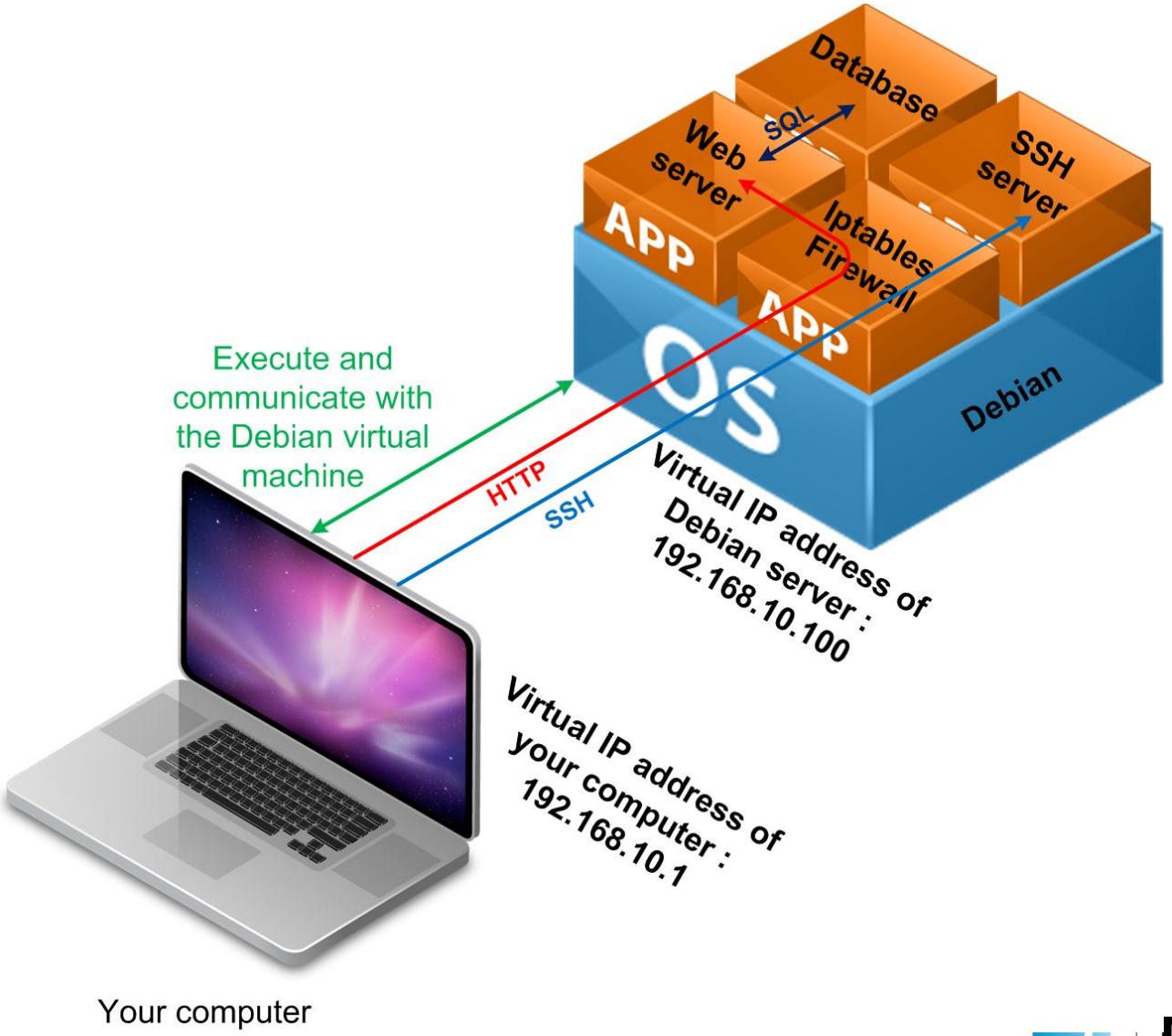
Firewall and HTTPS project

ECE PARIS
ÉCOLE D'INGÉNIEURS

Project goal

- **The first part of this project is to import on your computer a virtual machine (VM) : a web server that you will secure**
- **You have to configure the firewall “iptables” on the web server**
  - The firewall must reject everything except SSH, HTTP and localhost on the web server. Everybody from the network can access to the web server with HTTP protocol.
- **Next week, you will upload a report on campus with an explanation for each command line you enter to configure iptables and the second part of this project.**

Architecture



ECE PARIS
ÉCOLE D'INGÉNIEURS

Sources

- The file Vulnerable_Debian.ova is the Virtual Machine with web server and iptables for the project :

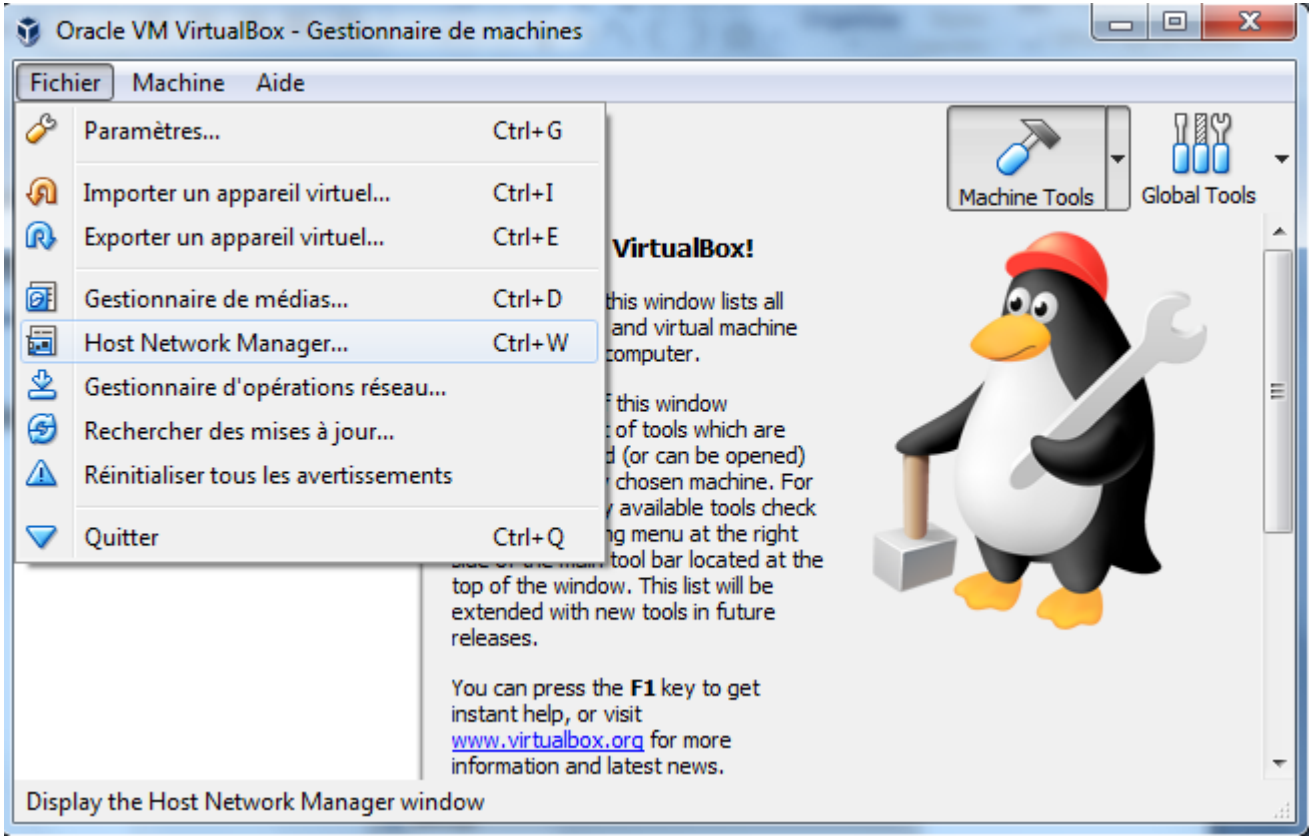
- Download the specific web server (https://www.hamon.tk/Vulnerable_Debian.ova)

VirtualBox installation

- If your computer does not have VirtualBox, download it from this URL: https://www.virtualbox.org/wiki/Downloads
- The installation is classic, let default options
- Once installed, open VirtualBox

Configuration of network interfaces

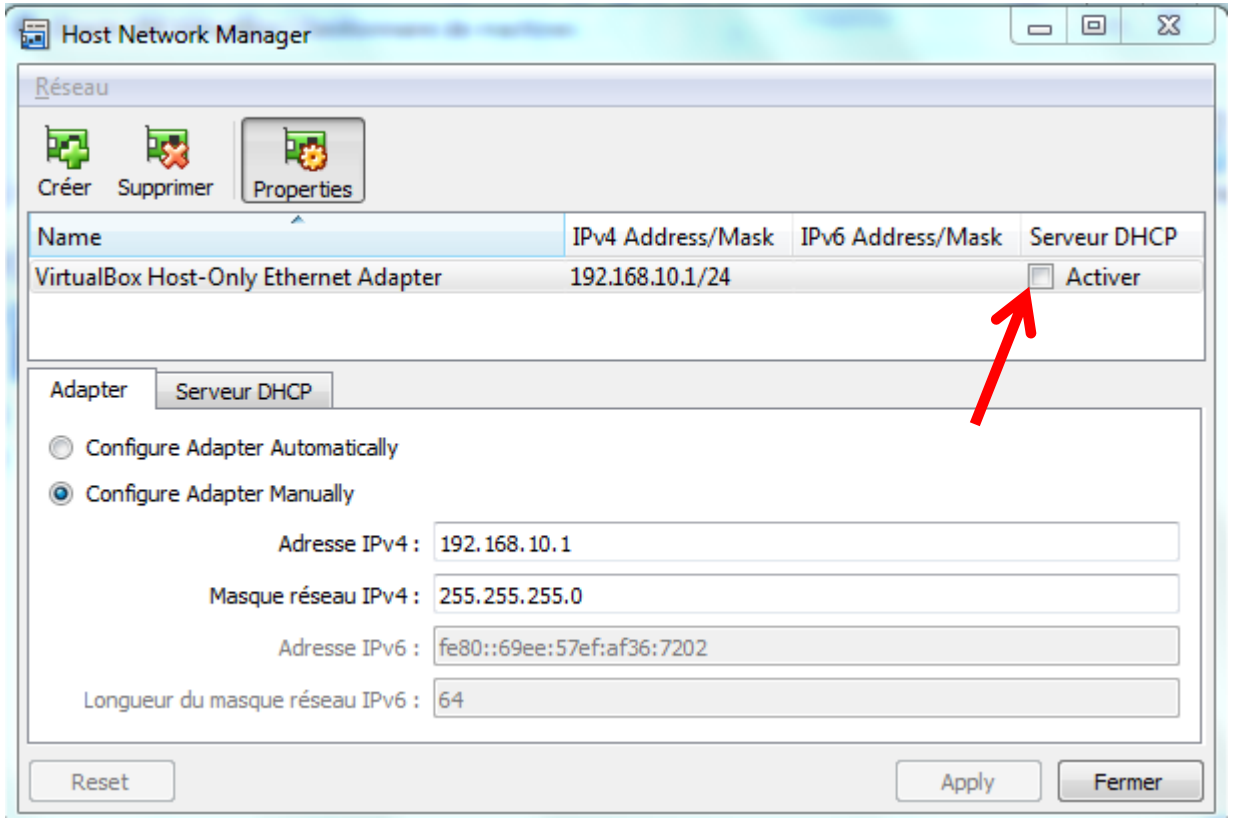
- File → Host Network Manager



ECE PARIS
ÉCOLE D'INGÉNIEURS

Configuration of network interfaces

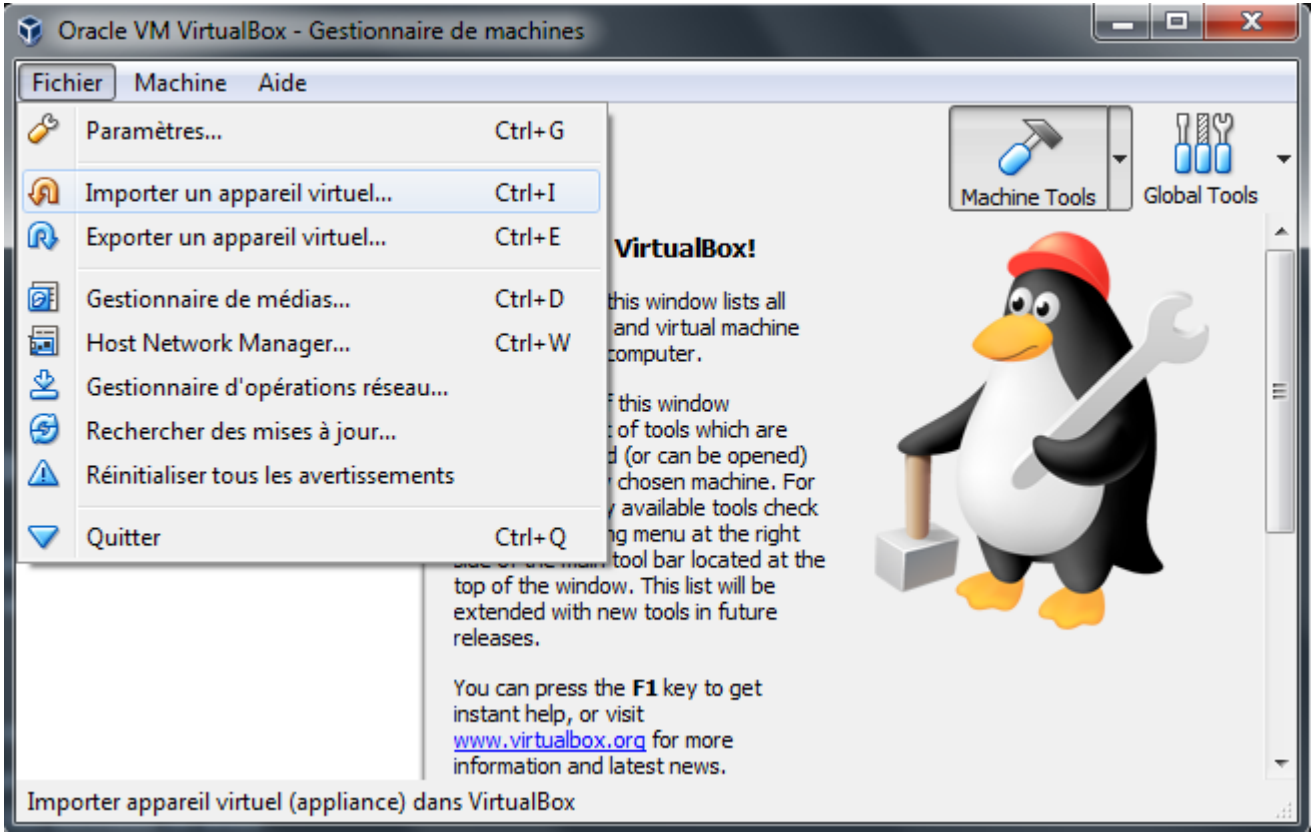
- **Configure the interface address VirtualBox Host-Only Ethernet Adapter as follows :**
  - IPv4 address:
    - ✓ 192.168.10.1
  - IPv4 network mask:
    - ✓ 255.255.255.0



- **Disable DHCP server**

Importing virtual machines

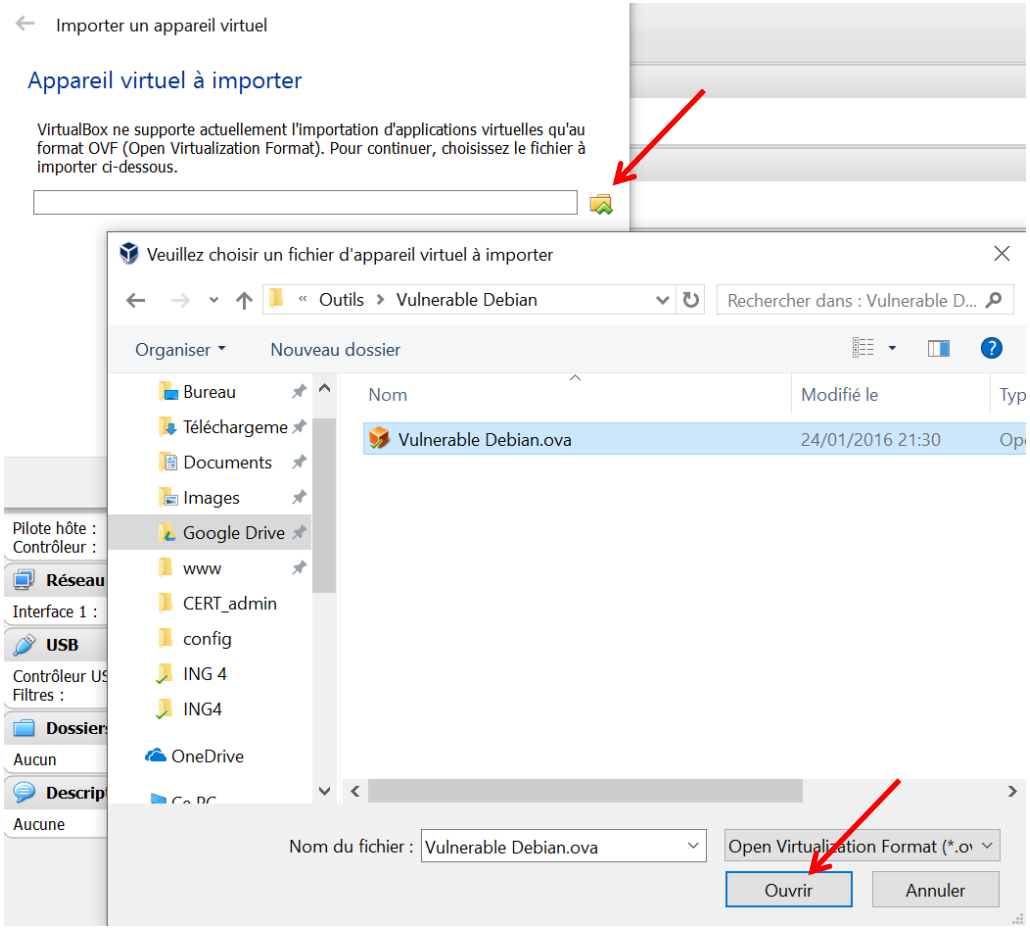
- In VirtualBox, click on "File" then "Import a virtual application..."



ECE PARIS ÉCOLE D'INGÉNIEURS

Importing virtual machines

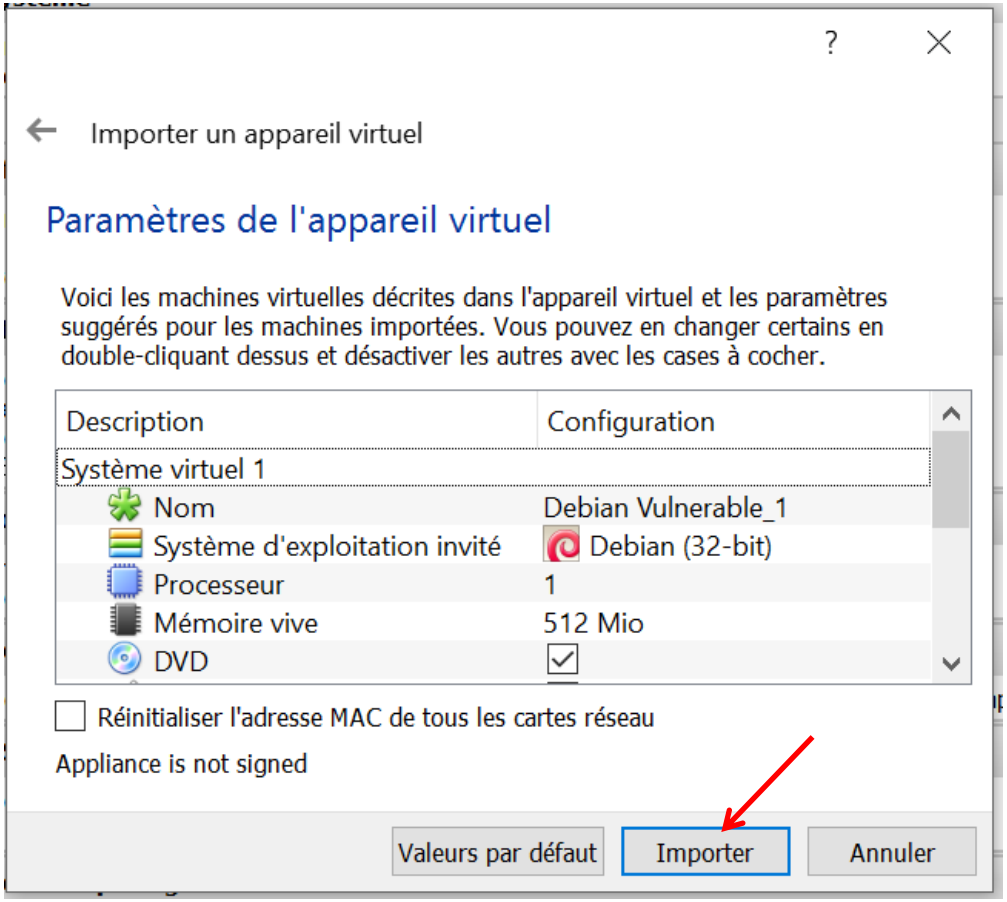
Import : « Vunerable Debian.ova »



ECE PARIS
ÉCOLE D'INGÉNIEURS

Importing virtual machines

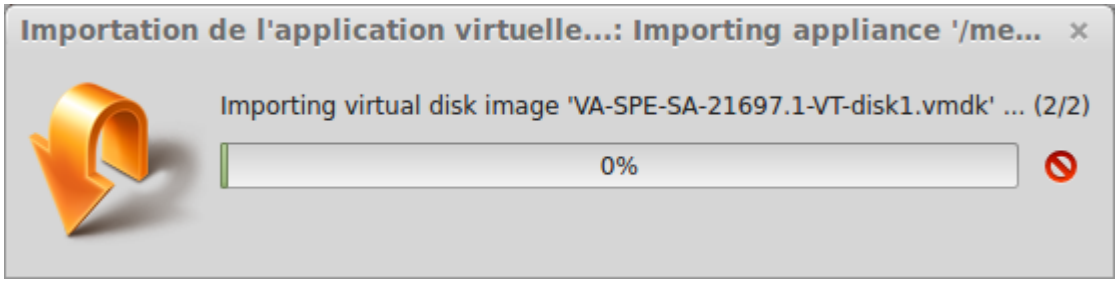
- Then « Import »



ECE PARIS ÉCOLE D'INGÉNIEURS

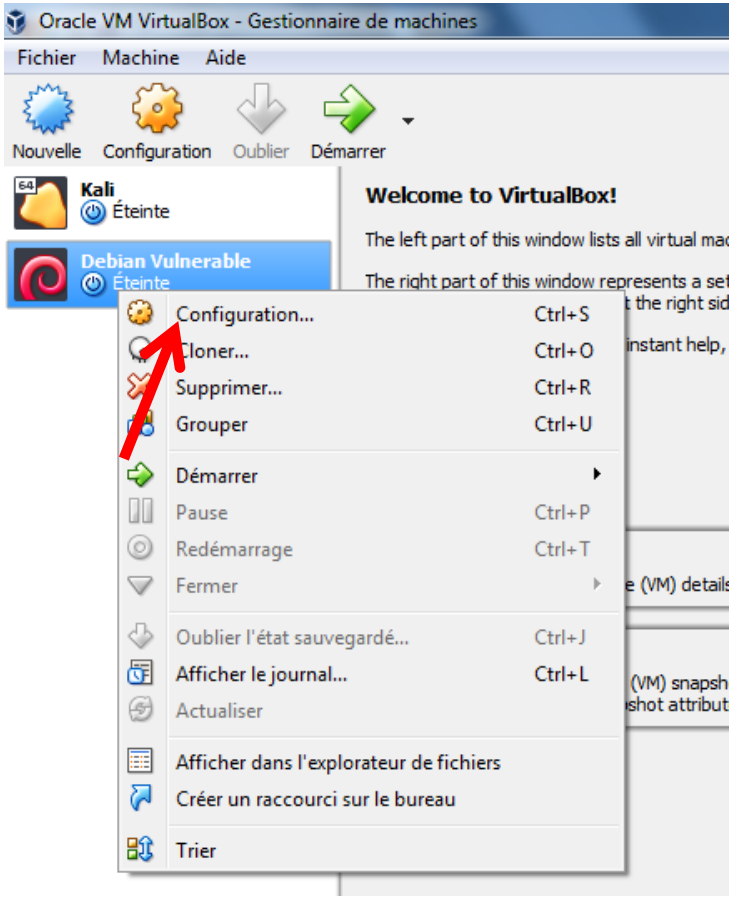
Importing virtual machines

- Wait during importation process…



VM configuration

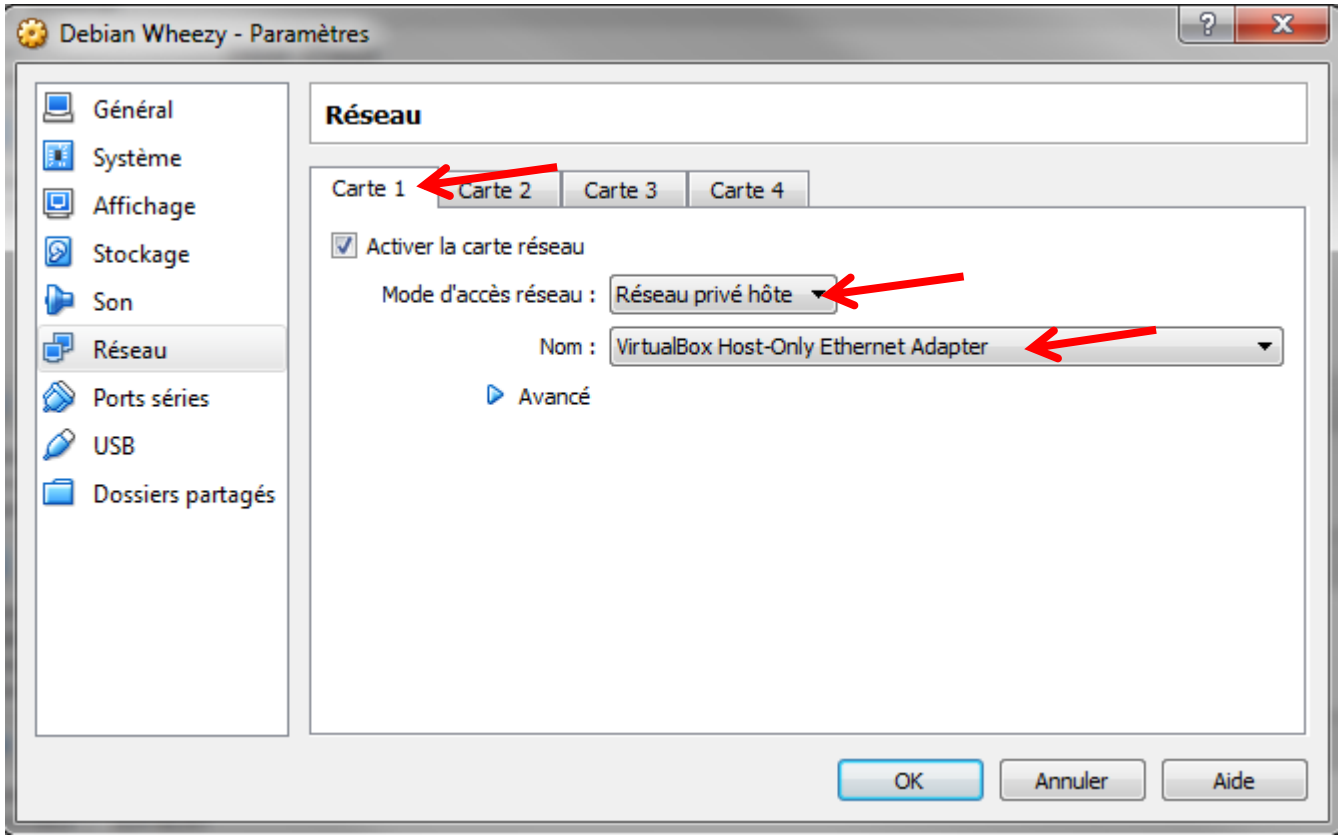
- Right-click the VM « Debian » → Configuration



ECE PARIS ÉCOLE D'INGÉNIEURS

VM configuration

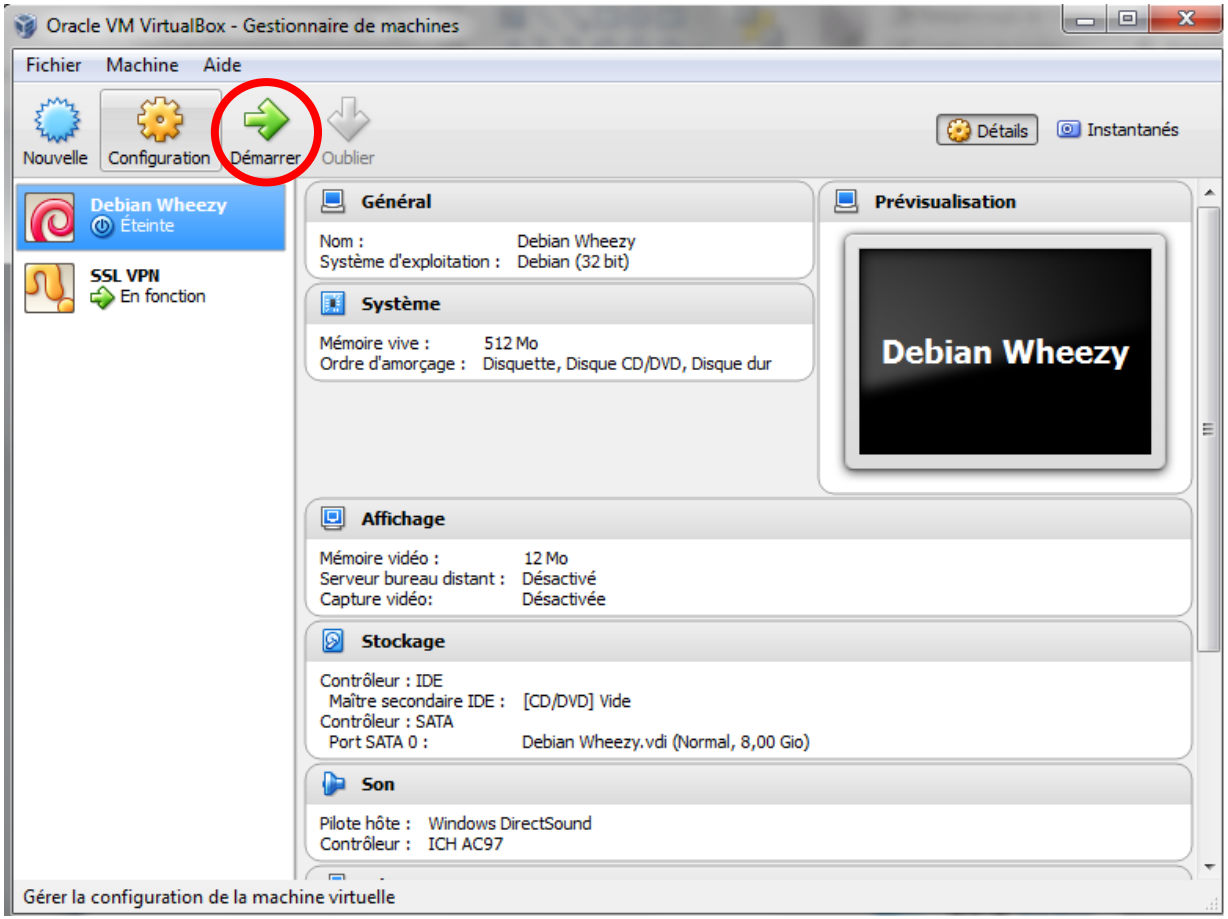
- Configure “Card 1" of Debian Vulnerable as below:



ECE PARIS ÉCOLE D'INGÉNIEURS

Start your VM

- Select your Debian Vulnerable and click on « start »



ECE PARIS
ÉCOLE D'INGÉNIEURS

Debian firewall configuration

- **Connect to Debian (login : security / password : security)**
  - Debian IP is 192.168.10.100
  - To have administrator right, you can prefix your command by « sudo » with the password « security »
- **The server on which you will configure a firewall contains several applications:**
  - A web server that receives HTTP requests from any client in the network
  - A database that sends / receives MySQL requests only from the local web server (on the same machine)
  - An SSH server that receives SSH requests from the administrator's computer
- **Write the flow matrix for this server :**

Source IP	Source port	Destination IP	Destination port	Action	Description

Debian firewall configuration

- **Use the iptables manual to find the right arguments for your needs (command : *man iptables*)**
- **Configure iptables to :**
  - Change the default policy to deny all flows
  - Allow the three flows needed for this web server
- **iptables is not statefull by default (accept automatically the response)**
  - Add the corresponding rule in order that it becomes stateful (see the documentation "man iptables-extensions")
- **Test your configuration**
  - Try to connect in HTTP to your server. Does it works?
  - Try to ping your server from your computer. Does it works?

Debian firewall configuration

- **Second step : Allow to ping the server only from your administrator computer**
  - Try to ping your server
- **Third step : Log the denied connections (you can add a limit of 2/min)**
- **Last step : the rules are reset when you restart the computer : find a way to save it and load it at startup**