Chapitre 2
Analyse de base

1. Création d'un laboratoire d'analyse

1.1 Introduction

Les malwares sont par nature dangereux pour les systèmes d'information. Les analystes doivent donc configurer un environnement afin de ne pas infecter leurs propres machines. Pour cela, les solutions de machines virtuelles sont très pratiques et simples à utiliser. En effet, si le malware est exécuté dans cet environnement cloisonné, l'infection ne pourra pas se propager à la machine de l'analyste, appelée machine hôte.

Cependant, il faut faire attention à certains points. Les solutions de virtualisation permettent de partager des disques ou des répertoires entre la machine hôte et les machines virtuelles. Ces fonctionnalités sont à proscrire ou à utiliser avec une très grande attention. Par exemple, dans le cas d'un ransomware chiffrant certains types de fichiers, si un répertoire de la machine hôte contenant ce type de fichier était partagé avec la machine virtuelle, ces fichiers seraient bien évidemment chiffrés lors de l'exécution de ce malware.

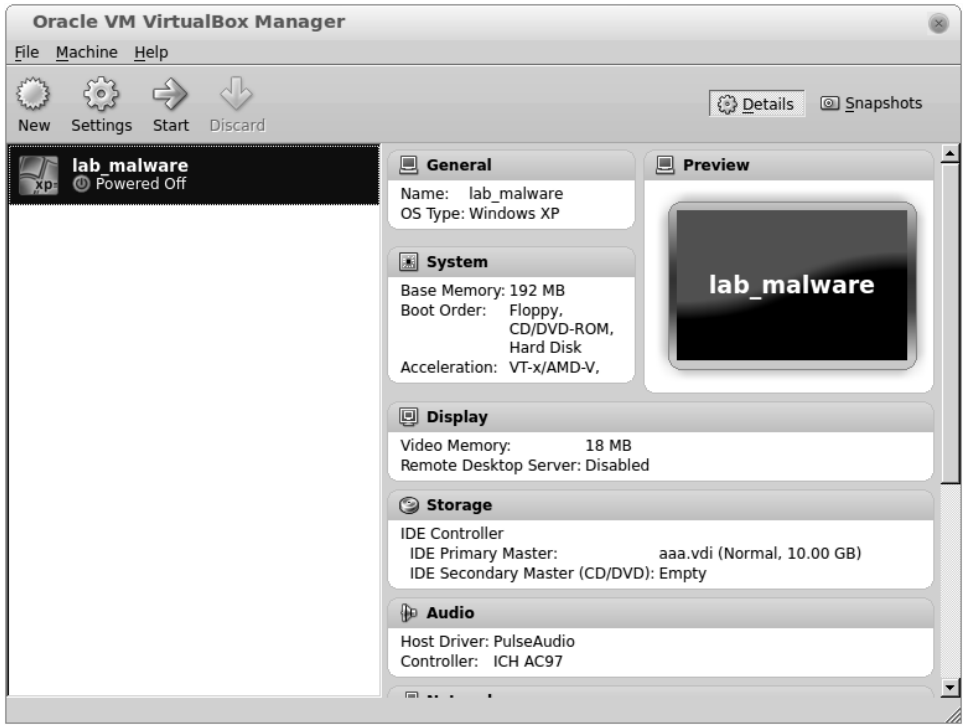
D'autres points sont également à contrôler. Pour éviter que leurs malwares ne soient trop facilement analysables, certains développeurs de malwares contrôlent si le malware s'exécute bien sur une machine physique et non une machine virtuelle. Il convient donc de configurer la machine virtuelle pour qu'elle ressemble autant que possible à une machine physique.

1.2 VirtualBox

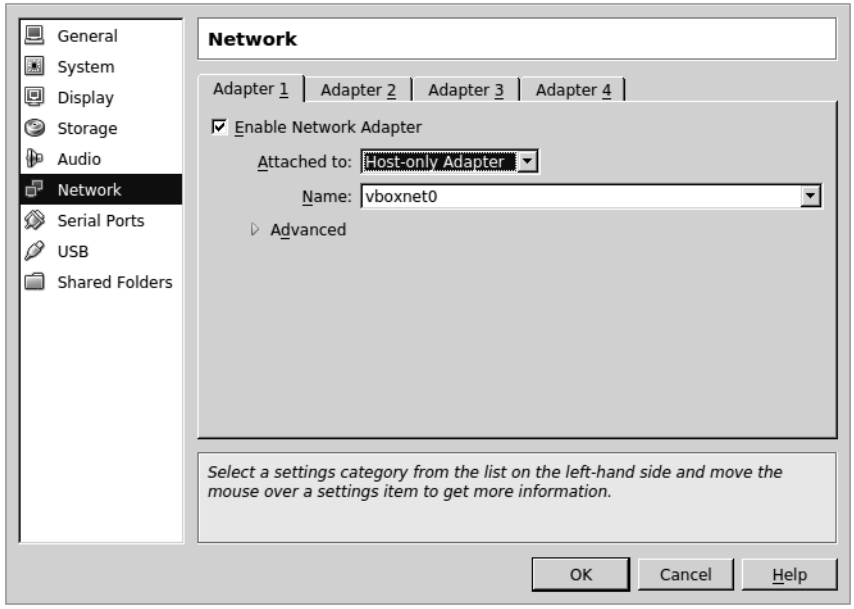
VirtualBox est une solution de virtualisation libre développée par Oracle et disponible à l'adresse suivante : https://www.virtualbox.org/. Cet outil est très intéressant pour un analyste de malwares car très simple d'utilisation, très souple, et il existe également une API pour pouvoir le manipuler à l'aide de scripts. Après l'installation, voici l'écran affiché lors du premier lancement :

Pour créer une première machine virtuelle, il suffit de cliquer sur le bouton **New**. Un assistant va alors poser des questions afin de configurer la machine virtuelle, telles que le nombre de CPU (*Central Processor Unit*), la quantité de mémoire à allouer à la machine virtuelle... Il est important de suivre les recommandations de l'assistant afin que la machine virtuelle puisse fonctionner normalement.

La machine virtuelle est à présent configurée :



La seconde partie de la configuration consiste à paramétrer le réseau. Pour le modifier, il faut cliquer sur **Settings**, puis **Network**. À présent, la configuration réseau apparaît :



Il est préférable de configurer l'interface en mode **Host-only Adapter**. Cette configuration permet de créer une interface réseau dédiée à la machine virtuelle et de ne pas partager l'interface physique de la machine hôte. Ce type de configuration est intéressant dans le cas où l'analyste souhaiterait enregistrer le trafic réseau sortant de la machine virtuelle, directement sur l'interface *vboxnet0*.

À présent, le système d'exploitation peut être installé dans VirtualBox, l'installation s'effectuant de la même manière qu'une installation sur une machine physique. Il est possible de partager directement le CD-ROM d'installation avec une machine virtuelle. Pour cela, il faut aller dans **Settings**, puis **Storage**, choisir le lecteur CD parmi les contrôleurs IDE disponibles et connecter le lecteur CD de la machine hôte au lecteur CD virtuel. Il est possible d'utiliser un fichier ISO à la place d'un lecteur CD physique.

Pour finir, afin de pouvoir exécuter des malwares modernes tentant de détecter les machines virtuelles, il est nécessaire de modifier la configuration de la machine virtuelle dans VirtualBox. Ces modifications ont pour but de faire passer la machine virtuelle pour une machine physique.

Dans le cas où la machine hôte est un système sous Linux, il est possible de récupérer les caractéristiques de la machine physique :

```
rootbsd@lab:~$ dmidecode -t0
# dmidecode 2.11
SMBIOS 2.7 present.

Handle 0x0000, DMI type 0, 24 bytes
BIOS Information
   Vendor: <vendeur>
   Version: <version du BIOS>
   Release Date: <date du BIOS>
[...]
rootbsd@lab:~$ dmidecode -t1
# dmidecode 2.11
SMBIOS 2.7 present.

Handle 0x0001, DMI type 1, 27 bytes
System Information
   Manufacturer: <vendeur>
   Product Name: <produit>
   Version: <version>
   Serial Number: <numero de serie>
   UUID: <UUID>
   Wake-up Type: Power Switch
   SKU Number: <chiffres>
   Family: <chiffres>
```

Ces données sont à appliquer dans la configuration de la machine virtuelle. Pour cela, il faut utiliser la commande `VBoxManage`. Voici les commandes dans le cas où la machine virtuelle se nommerait « lab » :

```
rootbsd@lab:~$ VBoxManage setextradata "lab"
"VBoxInternal/Devices/pcbios/0/Config/DmiBIOSVendor" "<vendeur>"
rootbsd@lab:~$ VBoxManage setextradata "lab"
"VBoxInternal/Devices/pcbios/0/Config/DmiBIOSVersion" "<version du
BIOS>"
rootbsd@lab:~$ VBoxManage setextradata "lab"
"VBoxInternal/Devices/pcbios/0/Config/DmiBIOSReleaseDate" "<date
```

```
du BIOS>"
rootbsd@lab:~$ VBoxManage setextradata "lab"
"VBoxInternal/Devices/pcbios/0/Config/DmiBIOSReleaseMajor" <date
du BIOS>
rootbsd@lab:~$ VBoxManage setextradata "lab"
"VBoxInternal/Devices/pcbios/0/Config/DmiBIOSReleaseMinor" <date
du BIOS>
rootbsd@lab:~$ VBoxManage setextradata "lab"
"VBoxInternal/Devices/pcbios/0/Config/DmiBIOSFirmwareMajor" <date
du BIOS>
rootbsd@lab:~$ VBoxManage setextradata "lab"
"VBoxInternal/Devices/pcbios/0/Config/DmiBIOSFirmwareMinor" <date
du BIOS>
rootbsd@lab:~$ VBoxManage setextradata "lab"
"VBoxInternal/Devices/pcbios/0/Config/DmiSystemVendor" "<vendeur>"
rootbsd@lab:~$ VBoxManage setextradata "lab"
"VBoxInternal/Devices/pcbios/0/Config/DmiSystemProduct"
"<produit>"
rootbsd@lab:~$ VBoxManage setextradata "lab"
"VBoxInternal/Devices/pcbios/0/Config/DmiSystemVersion"
"<produit>"
rootbsd@lab:~$ VBoxManage setextradata "lab"
"VBoxInternal/Devices/pcbios/0/Config/DmiSystemSerial" "<numero de
serie>"
rootbsd@lab:~$ VBoxManage setextradata "lab"
"VBoxInternal/Devices/pcbios/0/Config/DmiSystemSKU" "Not
Specified"
rootbsd@lab:~$ VBoxManage setextradata "lab"
"VBoxInternal/Devices/pcbios/0/Config/DmiSystemFamily"
"<"chiffre">"
rootbsd@lab:~$ VBoxManage setextradata "lab"
"VBoxInternal/Devices/pcbios/0/Config/DmiSystemUuid"  "<UUID>"
```

Il peut être également intéressant de modifier l'adresse MAC (*Media Access Control*) de la carte réseau de la machine virtuelle :

```
rootbsd@lab:~$ VBoxManage modifyvm "lab" --macaddressX
<MAC>
```

On peut également modifier les paramètres des disques durs et des contrôleurs :

```
rootbsd@lab:~$ VBoxManage setextradata "lab"
"VBoxInternal/Devices/piix3ide/0/Config/PrimaryMaster/SerialNumber"
 "<serial>"
rootbsd@lab:~$ VBoxManage setextradata "lab"
```