Gildas COTTEN
4 avril 2017

Attaques réseaux - Installation Machines Virtuelles

Projet TWCS

Destination :
Daniel Bourget
Pascale Menard

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Sommaire

1. INTRODUCTION 3
2. INSTALLATION DES MACHINES VIRTUELLES 3
2.1 VirtualBox 3
2.2 Configuration réseau dans virtualbox 4
2.3 Routeur PFSENSE 5
2.4 Client Windows 7 7
2.5 Serveur Debian 8
2.6 Kali Linux 9
2.7 Remarque sur la gestion des disques USB sous VirtualBox 9

RÉFÉRENCES 10

Liste de figures

1 Réseau utilisé par ce projet . . . 3
2 Ajout de VirtualBox Extension Pack . . . 4
3 Carte réseau en mode réseau privé sous VirtualBox . . . 4
4 Carte réseau en mode nat sous VirtualBox . . . 5
5 CDROM dans virtualbox . . . 5
6 Premier écran pfsense . . . 6
7 PFSENSE . . . 6
8 PFSENSE après configuration LAN . . . 7
9 Interface Web PFSENSE . . . 7
10 Configuration réseau ip statique sous Linux . . . 8
11 arpwatch sous Linux . . . 8
12 Configuration réseau sous Kali . . . 9

Liste de tableaux

1. INTRODUCTION

Pour les besoins de ce projet, j'ai mis en place les poste suivants avec des machines virtuelles.

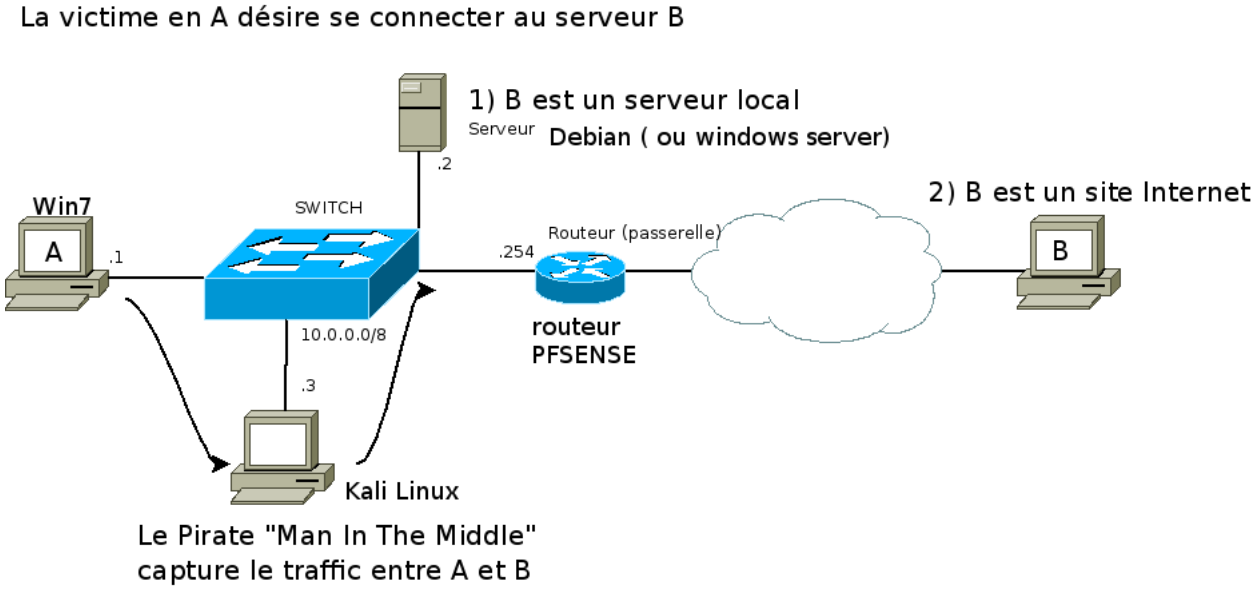

FIGURE 1– Réseau utilisé par ce projet

2. INSTALLATION DES MACHINES VIRTUELLES

2.1 VIRTUALBOX

J'ai utilisé le logiciel Oracle VirtualBox pour virtualiser les systèmes d'exploitation utilisés : Windows 7, Linux Debian Jessie ou Kali Linux. On peut utiliser un autre système de virtualisation comme VMWARE ou autre. `https://www.virtualbox.org/wiki/Linux_Downloads` avec explication pour installation de la dernière version de VirtualBox sous Debian.

Installation des extensions : ici **Oracle VM VirtualBox Extension Pack 5 1 18 114002 vbox extpack** à télécharger sur le site `https://www.virtualbox.org/wiki/Downloads` (VirtualBox 5.1.18 Oracle VM VirtualBox Extension Pack clic droit sur **All supported platforms** puis enregistrer sous).

En cas de problème : lancement de virtualbox (en root dans un terminal).

Sous virtualbox, la touche pour sortir des machines virtuelles est par défaut "CTRL" à droite du clavier.

2.2 CONFIGURATION RÉSEAU DANS VIRTUALBOX

Pour toutes les VMs : configuration avec une seule carte réseau en mode "réseau privé vboxnet0" ("host only")

Pour le routeur , ici sous pfsense, 2 carte réseau : 1 en mode nat et une carte en mode "réseau privé vboxnet0" comme ci dessus. La carte réseau en mode nat fera office d'interface WAN pour le routeur. La carte réseau en mode réseau privé fera office d'interface LAN pour le routeur.

2.3 ROUTEUR PFSENSE

On peut utiliser un autre type de routeur (Windows serveur , debian , ipcop , smoothwall...)

ISO à télécharger : **pfSense-CE-2.3.3-RELEASE-amd64.iso**

Créer une machine virtuelle 1Go de RAM avec nouveau disque dur 8Go dynamique.

Configuration de la VM –> stockage –> choisir l'image ISO comme CDROM :

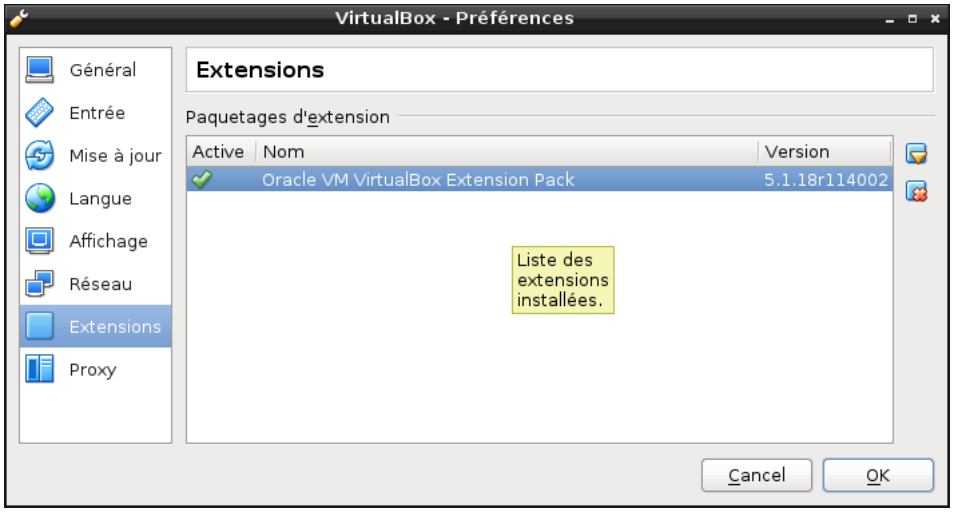

FIGURE 2– Ajout de VirtualBox Extension Pack

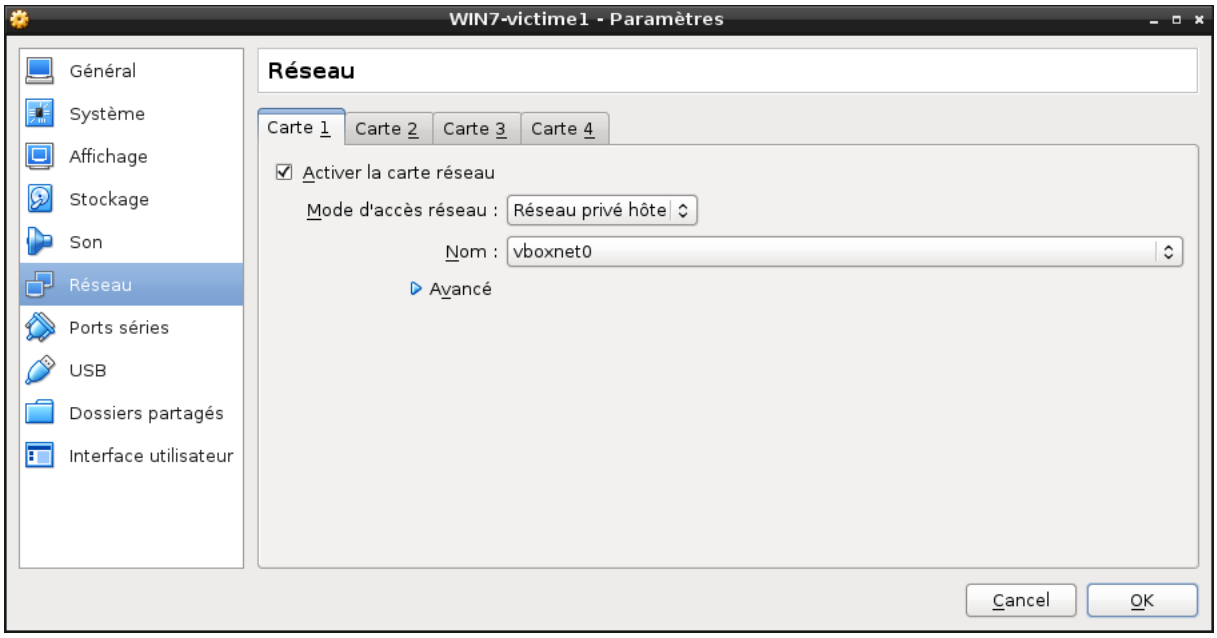

FIGURE 3– Carte réseau en mode réseau privé sous VirtualBox

Configurer 2 cartes réseau (une en NAT pour le WAN et une en Host Only pour le LAN voir paraphe précédent)

Ensuite démarrer la VM.

Changer le clavier comme ci-dessus.

Ensuite Choisir "Quick install" puis "Standart Kernel" puis retirer le CDROM dans virtualbox quand le système le demande avant de redémarrer. (menu périphérique –> lecteurs optiques -> décocher "pfsense..." puis éjection forcée.) puis dans virtualbox menu machine puis redémarrer.

menu 2 pour "set interfaceIP address" et assigner 10.0.0.254 au LAN (ne pas toucher au WAN)

Possibilité de configurer un serveur DHCP côté LAN : Oui.

Ensuite depuis le poste client sous Windows 7 (ou autre poste côté LAN) accès à l'interface web ace le login par défaut admin mot de passe pfsense (à modifer à la première connexion).

FIGURE 4– Carte réseau en mode nat sous VirtualBox

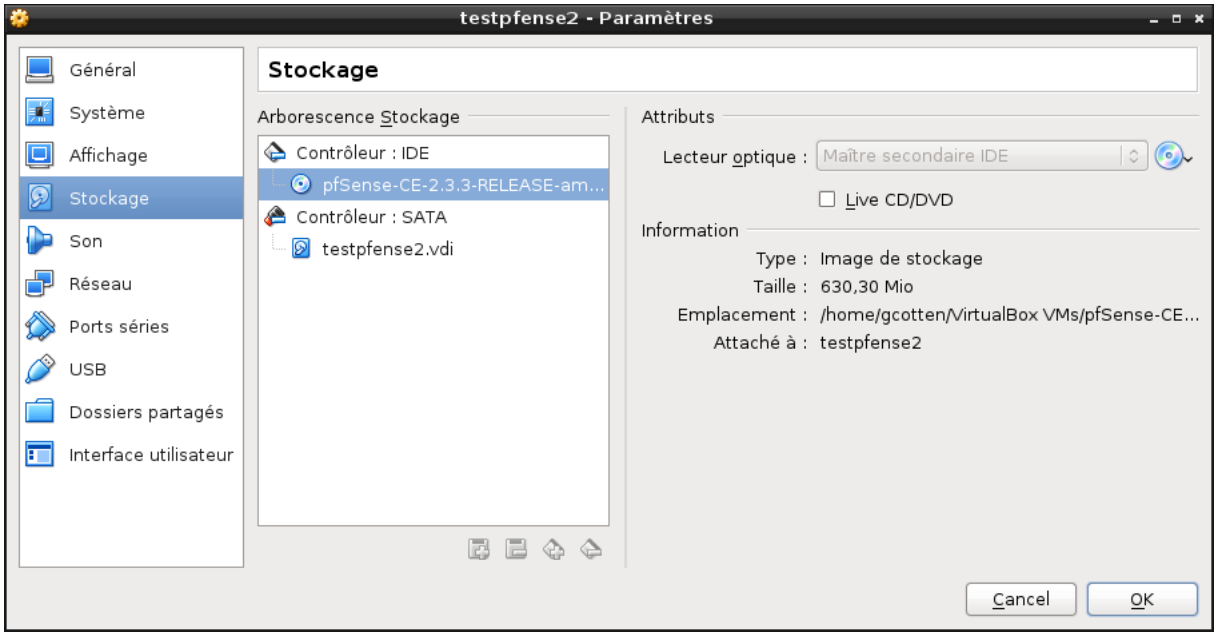

FIGURE 5– CDROM dans virtualbox

2.4 CLIENT WINDOWS 7

Installation à partir de l'image iso et la clé provenant de Microsoft Imagine `https://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?ws=eb187579-6b9b-e011-969d-0030487d8897`

Configuration réseau dans Win7 : 10.0.0.1/8 passerelle 10.0.0.254 serveur DNS 10.0.0.254

Windows update plusieurs fois pour installer les mises à jour puis éventuellement désactivation de Windows update.

Installation du logiciel the dude v3.6 à partir de `http://mikrotik.c4.hu/!dude/`

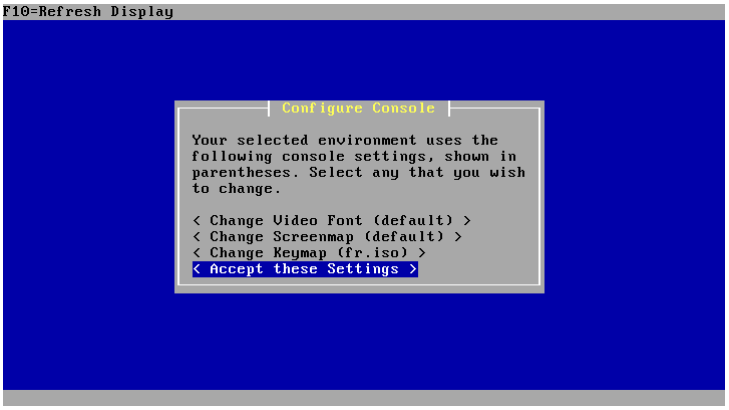

FIGURE 6– Premier écran pfsense

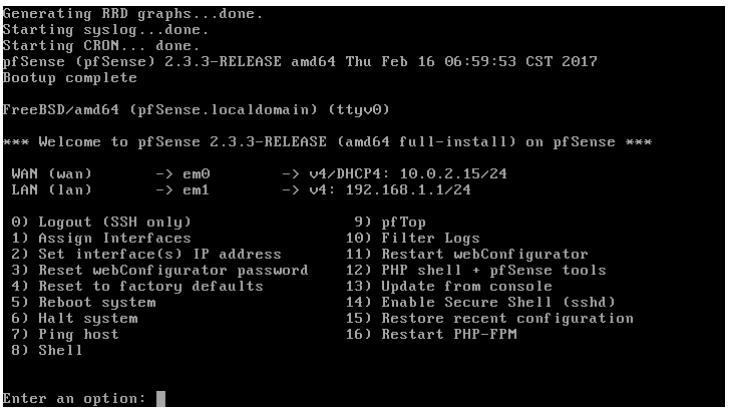

FIGURE 7– PFSENSE

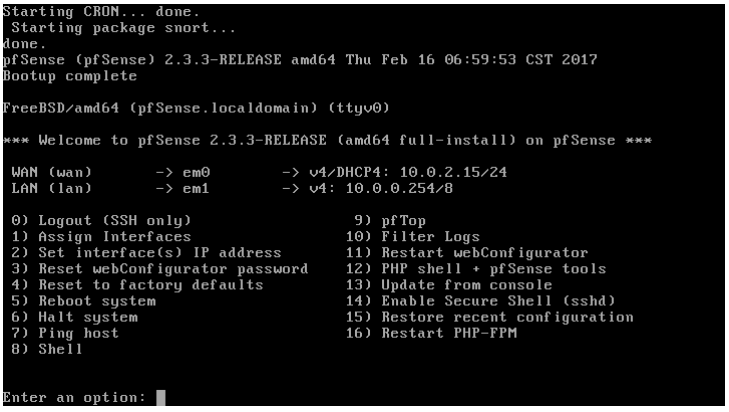

FIGURE 8– PFSENSE après configuration LAN

2.5 SERVEUR DEBIAN

Installation à partir d'une image ISO (*debian-8.7.1-amd64-lxde-CD-1.iso*) téléchargée depuis le site de Debian (on pet aussi installer DEBIAN avec l'image iso netinstall ou autre). Disque dur taille dynamique 40Go.

apt-get update apt-get upgrade apt-get resolvconf (avant de configurer une IP statique) apt-get install apache2 : facultatif pour des tests sur seveur web) ap-get install proftpd (en mode inetd) : pour attaque mitm avec capture du mot de passe

Configuration réseau sous /etc/network/interface

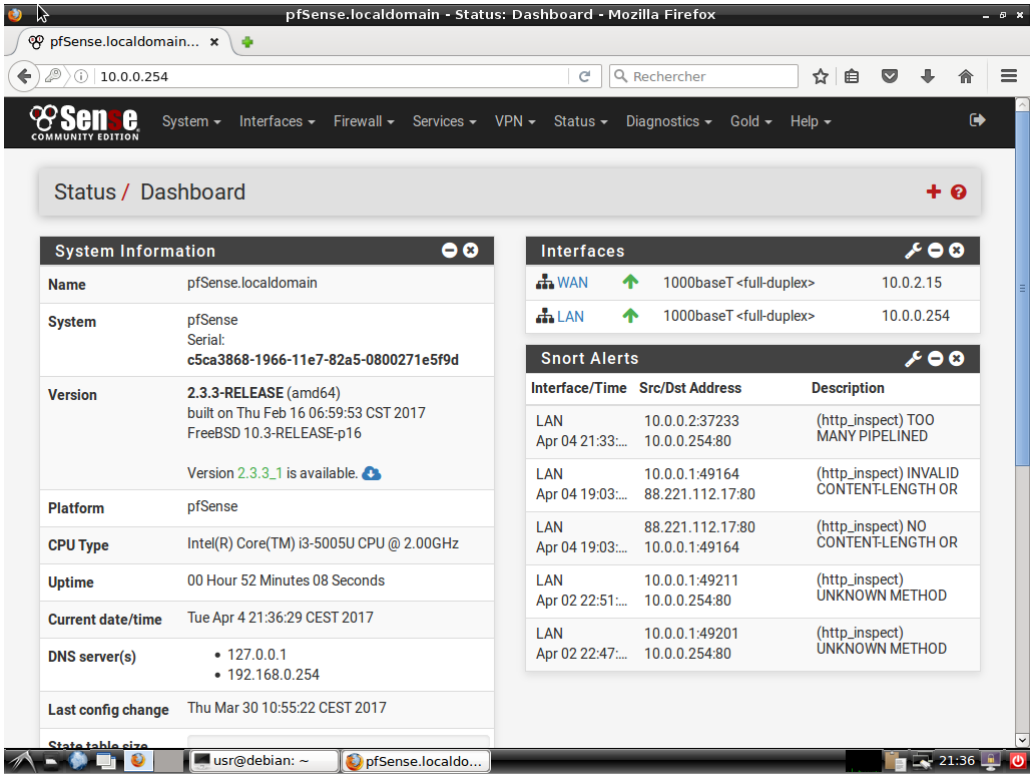

FIGURE 9– Interface Web PFSENSE

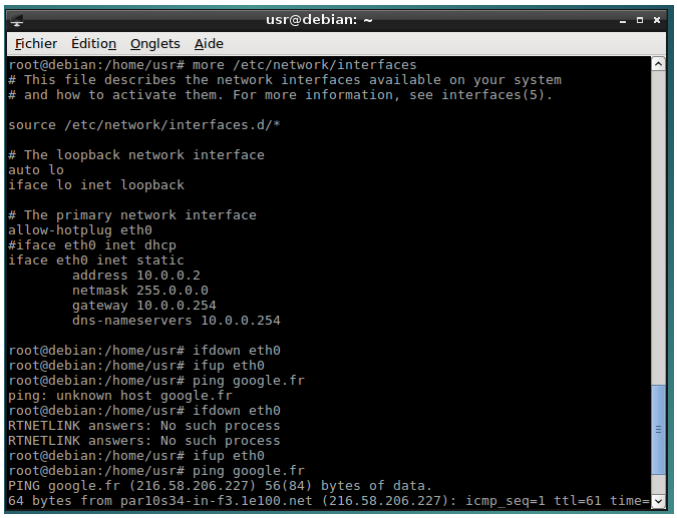

FIGURE 10– Configuration réseau ip statique sous Linux

Parfois des soucis donc essayer plusieurs fois ifdown eth0 puis ifup eth0. (Ou redémarrer le poste)

apt-get install arpwatch : pour repérer des doublons dans les données ARP.

Inclure la ligne **eth0 -a -n 10.0.0.0/8** dans le fichier **/etc/arpwatch.conf** et redémarrer avec **/etc/init.d/arpwatch restart**

Installation des mises à jour , éventuellement test de la présence de python avec la commande python -m simpleHTTPServer qui lance un mini serveur web (attention à la casse).

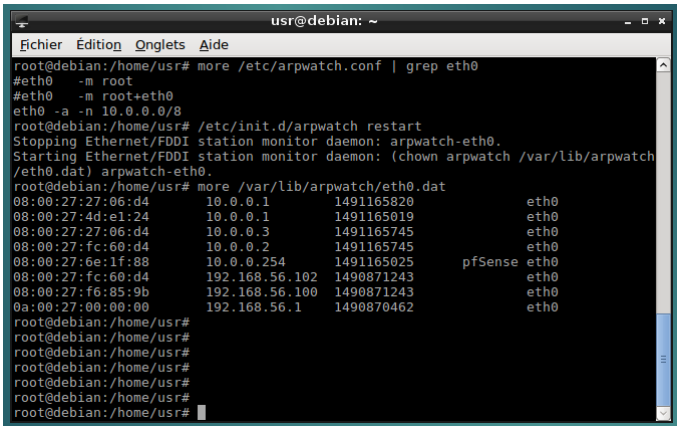

FIGURE 11– arpwatch sous Linux

2.6 KALI LINUX

Machine virtuelle au format ova pour virtualbox directement téléchargeable ici : `https://images.offensive-security.com/virtual-images/Kali-Linux-2016.2-vbox-amd64.ova` ou autre sur `https://www.kali.org/downloads/`

Dans VirtualBox, menu "Fichier" puis "importer un appareil virtuel" et sélectionner le fichier ova.

login par défaut : root

Mot de passe par défaut : toor

Configuration réseau (avec /etc/resolv.conf)

FIGURE 12– Configuration réseau sous Kali

2.7 REMARQUE SUR LA GESTION DES DISQUES USB SOUS VIRTUALBOX

USB sous virtualbox : il faut installer "Oracle VirtualBox Extension Pack" qu'il faut préalablement télécharger sur le site de virtualBox puis Menu Fichier, paramètres, extensions et installer. Ensuite il apparaît nécessaire de lancer la commande "virtualbox" en root pour pouvoir accéder aux périphériques usb.

Technopôle Brest-Iroise
CS 83818
29238 Brest Cedex 3
France
+33 (0)2 29 00 11 11
www.telecom-bretagne.eu

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom