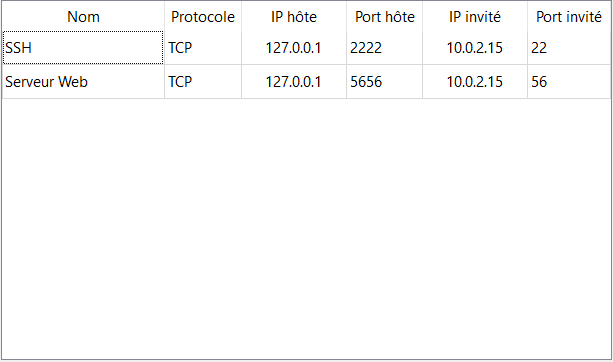
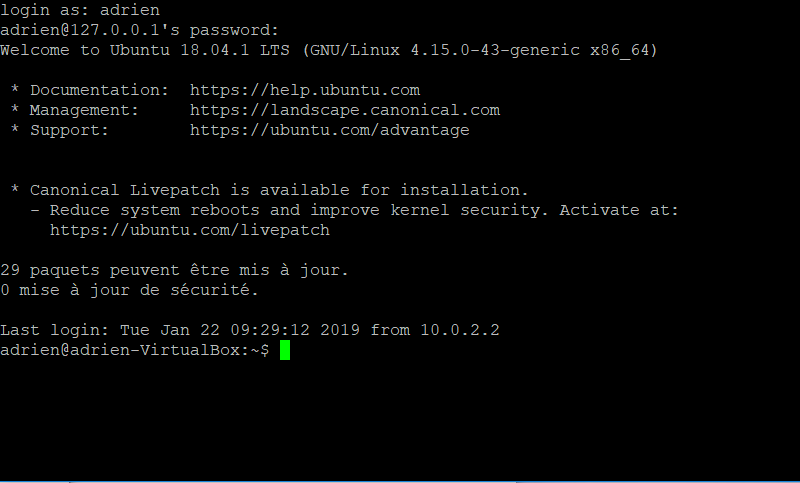
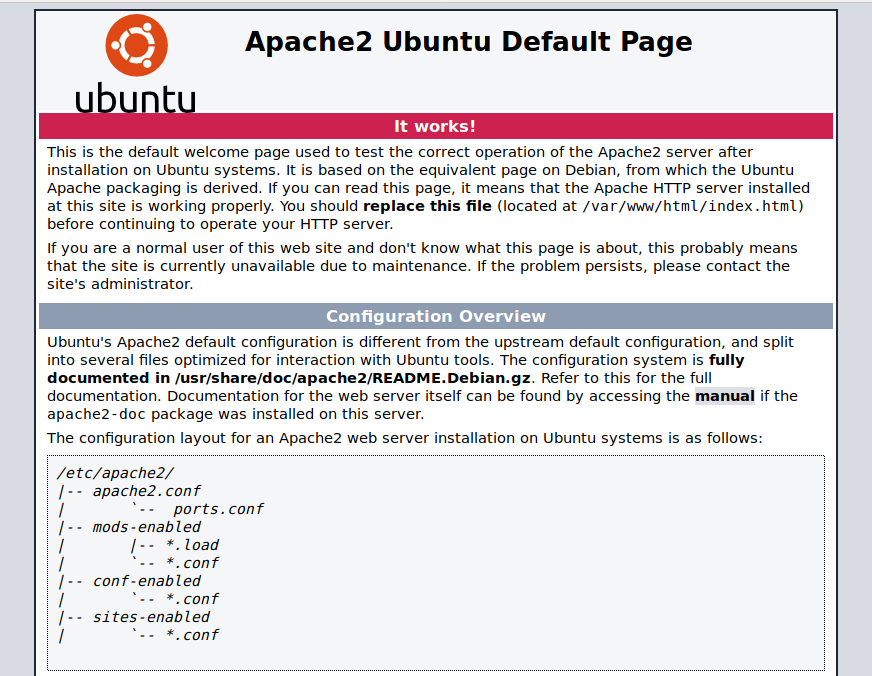
Installation serveur web et serveur linux :







LES COMMANDES :

Pour l'installer:

sudo apt-get install apache2

sudo apt-get install php5

sudo apt-get install mysql

sudo apt-get install ssh

Nous pouvons nous connecter et communiquer au serveur désormais installé grâce au "ssh", en configurant la carte réseau de la VM

Nous pouvons utiliser un logiciel comme PuTTY pour pouvoir communiquer avec ce dernier

pour démarrer le serveur

etc/init.d/apache2 start

Pour avoir accès au site pour déposer des données ou en récupérer:

http://127.0.0.1

Si l'on voit le message "It works", le serveur fonctionne

Il ne restera plus qu'a le configurer pour ensuite l'adapter au besoin

Cependant, différents problèmes ont été rencontrés, c’est pourquoi finalement, on utilisera un serveur XAMPP installé à la main.

Une fois le serveur XAMPP installé, il ne restera plus qu’a le redémarrer, nous utilisons la commande suivante :

./lampp start

Cette dernière lancera toutes les fonctionnalités de XAMPP

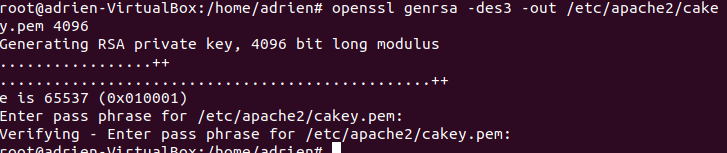


Ceci est le menu principal du serveur laissé par défaut

Pour ce qui est du web, nous avons créé des certificats d’authentification pour un accès sécurisé grâce à l’application OpenSSL.

Tout d’abord, on configure l’autorité de certification, c’est un peu la fondation du certificat d’authentification

Il faut en premier lieu créer la clé de ce certificat grâce à cette commande suivante :

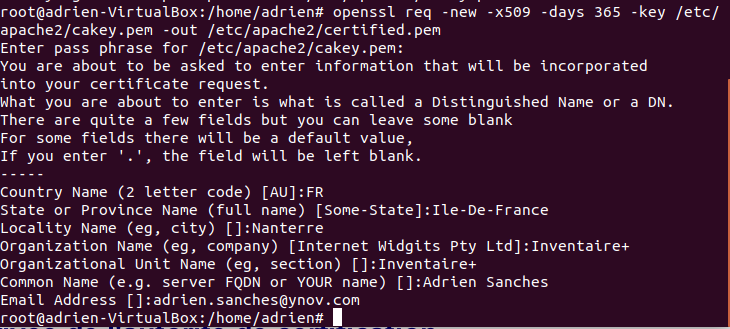
Openssl genrsa -des3 -out chemin\_du\_dossier/cakey.pem 4096

Cette commande permet de créer une clé privé codé sur 4096 bits, dans le dossier spécifié, dans le fichier spécifié, protégé par un pass phrase (mot de passe pouvant contenir des espaces)

Ensuite, nous pouvons créer le certificat, grâce à cette commande :

openssl req -new -x509 -days durée\_en nbre\_jours -key chemin\_du\_dossier/cakey.pem -out chemin\_du\_dossier/nom\_certificat.pem

nous faisons ainsi la demande d’un nouveau certificat autosigné, d’un certain nombre de jours, à partir de la clé privé, sous un nom donné



Il faut ensuite donner plusieurs informations sur ce formulaire

La configuration de l’autorité est finie, on peut désormais commencer à générer le certificat du serveur WEB

En premier lieu, nous créons la clé privée à l’aide de la même commande que celle utilisé pour l’autorité de certification, excepté l’option -des3, qui permet l’implémentation du mot de passe

Puis, pour générer le certificat, on utilise la même commande que celle de l’autorité, en retirant l’option -x509 et l’option -days

C’est cependant à partir de la troisième étape, qui consiste à signer le certificat, que nous avons commencé à enchainer problèmes sur problèmes, l’autorité n’est pas reconnue, nous avons essayé de changer le chemin de ce dernier, mais en vain, cela ne fonctionne toujours pas de créer une autre autorité, au bout de plusieurs essais, nous avons découvert une suite préinstallé nommé XAMPP que nous avons donc utilisé.