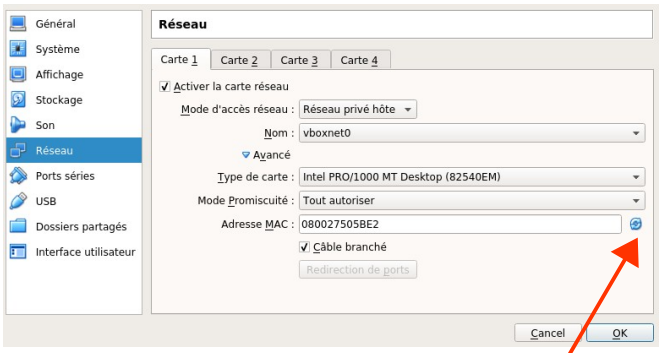
Travaux Pratiques : SSL/TLS et OpenVPN

L'objectif de ce TP est d'appréhender les mécanismes de sécurité en œuvre dans le cadre de l'usage de SSL/TLS et leur mise en pratique pour la construction d'une interconnexion de type VPN.

Installation des machines virtuelles

Une machine virtuelle vous a été distribuée sous la forme d'un fichier .ova. Importez-la dans VirtualBox. Editez sa configuration réseau afin d'avoir quelque-chose de similaire à ceci :



Pensez à réinitialiser l'adresse MAC (icône en forme de double flèche).

Démarrez-la et pensez à relever son adresse IP. Le login est ***root*** et le mot de passe ***toor***.

OpenSSL

OpenSSL est une implémentation extrêmement répandue de SSL/TLS. C'est également un outil de cryptographie généraliste très utile, qui permet de faire du chiffrement de façon très simple . Il est à la fois une bibliothèque logicielle qui peut être utilisée dans des binaires et un outil en ligne de commande .

1 – Chiffrement / déchiffrement

La commande qui permet de chiffrer et de déchiffrer est la commande *enc*. Il faut spécifier -e pour chiffrer et -d pour déchiffrer.

```
$ openssl enc -algorithme -d|-e -in file -out file.enc
```

La liste des algorithmes de chiffrement supportés peut être obtenue par la commande suivante :

```
$ openssl enc -ciphers
```

3 – Génération d'un biclef

OpenSSL embarque toutes les commandes nécessaires à la création et la signature de certificats . Concrètement, il est possible (mais assez fastidieux) de gérer intégralement une PKI à l'aide d'OpenSSL . La première étape est de générer une paire de clé cryptographiques pour du chiffrement asymétrique. Par exemple, RSA :

```
$ openssl genrsa -out fichier.key taille
```

4 – Génération d'un certificat de CA

Pour créer une autorité de certification, il faut en premier lieu un certificat racine, qui signera les autres certificats. Il faut donc créer un certificat auto-signé, grâce à la commande suivante :

```
$ openssl req -x509 -new -key ca.key -out ca.pem
```

Il est ensuite possible de visualiser le contenu d'un certificat grâce à la commande suivante :

```
$ openssl x509 -in ca.pem -text
```

5 – Création d'un certificat utilisateur

Pour émettre des certificats signés par l'AC, il faut procéder en trois temps :

1. *Génération d'un bi-clé par le porteur*

   En premier lieu, il faut que le porteur du certificat dispose d'une clé publique, qui est la raison pour laquelle il demande un certificat. Il faut donc créer une clé pour le porteur du certificat :

   ```
   $ openssl genrsa -out cert.key taille
   ```

2. *Création d'une requête de certification*

   Création d'une requête en signature (Certification Signature Request). Cette requête doit être effectuée en utilisant la clé du porteur précédemment générée :

   ```
   $ openssl req -new -key cert.key -out cert.csr
   ```

3. *Signature par l'Autorité de certification*

   Il faut que l'Autorité de Certification appose sa signature sur cette demande pour qu'elle deviennet un certificat à part entière :

   ```
   $ openssl x509 -req -CAcreateserial -in cert.csr -CA ca.pem -CAkey ca.key -out cert.pem
   ```

Configurer un service HTTPS

1. Dans un répertoire temporaire, créez une autorité de certification (étape 3 et 4) avec les paramètres suivants :
    - Clé RSA de 2048 bits (4096 seraient mieux, mais trop long à générer dans le cadre de ce TP) ;
    - Valable 4 ans ;
    - Country = FR, State = IEV, Locality = RENNES, Organization = ISTIC, Organizational Unit = SRES, Common Name = MonACPerso

La machine virtuelle dispose d'un service Apache en écoute sur 127.0.0.1, sur le port 80.

2. Créez un certificat serveur pour le site www.monsite.com, avec les mêmes caractéristiques que l'AC, à part le CN :-) (étape 5).

3. Activez la prise en charge de HTTPS sur le service avec ce certificat.

Configurer un service OpenVPN

1. Clonez la machine virtuelle. Pensez à réinitialiser l'adresse MAC.

2. Créeez un certificat pour le serveur et un autre pour le client VPN (avec les CN respectifs « serveur » et « client »)

3. Générez des paramètres Diffie-Helmann de 2048 bits dans dh2048.pem

    ```
    $ openssl genpkey -genparam -algorithm dh -out dh2048.pem
    ```

4. Mettez en place le serveur OpenVPN sur la machine serveur. Vous pourrez trouver un fichier de configuration déjà prêt dans le répertoire */usr/share/doc/openvpn/examples/sample-config-files/*. Copiez le fichier de configuration serveur d'exemple. Comme il est compressé au format gzip, il faut utiliser zcat pour le décompresser :

    ```
    $ zcat /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz > /etc/openvpn/server.conf
    ```

5. Mettez en place le serveur OpenVPN sur la machine cliente. Vous pourrez trouver un fichier de configuration déjà prêt dans le répertoire */usr/share/doc/openvpn/examples/sample-config-files/.* Copiez le fichier de configuration client d'exemple :

    ```
    $ cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf > /etc/openvpn/client.conf
    ```

6. Lancez le serveur et le client pour établir la connexion VPN :

    - Sur le serveur : *openvpn /etc/openvpn/server.conf*
    - Sur le client : *openvpn /etc/openvpn/client.conf*

    Mettez une machine en écoute avec netcat et connectez-vous avez l'autre en utilisant les adresses IP attribuées par le VPN, vous devez pouvoir vous échanger des messages.