Labo PKI-SSL (90 min)

1	Objectifs	sudo ./c 2

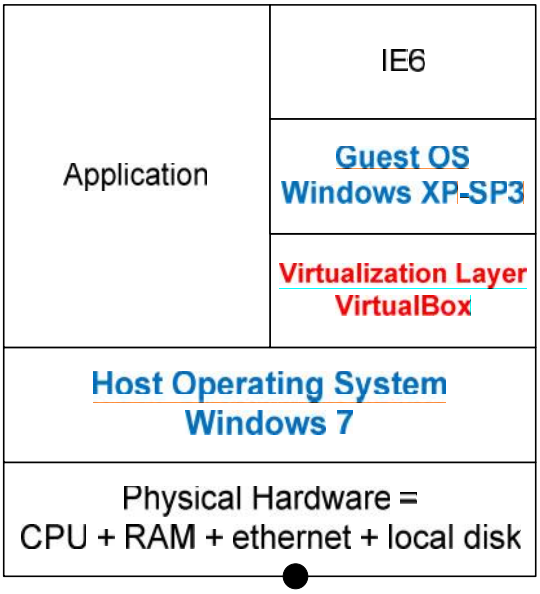
Ce travail de laboratoire de 90 minutes a pour objectifs d'illustrer pratiquement :

- Une **infrastructure à clé publique** *(Public Key Infrastructure)* à partir de http://ca.tdeig.ch/
- Un contexte *e-commerce* (**SSL**) avec les serveurs https://sec1.tdeig.ch/ et https://sec2.tdeig.ch

Le **client SSL (navigateur)** choisi est **IE6 (Internet Explorer 6)** qui gère et affiche mieux les conditions anormales

De plus la procédure décrite au §3 pour obtenir un certificat utilise l'autorité de certification de Windows Server 2008 qui n'est pas compatible avec Windows7

Vous allez donc utiliser la **virtualisation** offerte par le produit gratuit **VirtualBox** pour disposer d'un système **Windows XP-SP3** alors que les PCs du labo, situés dans l'intranet, utilisent une image **Windows7**



Je vous encourage à utiliser l'excellent produit VirtualBox supporté par Oracle

- VirtualBox is a cross-platform virtualization application
- VirtualBox runs on Windows, Linux, Macintosh, and Solaris hosts
- VirtualBox supports a large number of guest operating systems including Windows (…, XP, Server 2003, Vista, Windows 7), Linux (2.4 and 2.6), OpenBSD, …
- Consulter https://www.virtualbox.org/

Je vous encourage aussi à utiliser l'autorité de certification du labo http://ca.tdeig.ch/ pour envoyer un *email* signé, …

Lien Documents utiles dont le corrigé dans le partage réseau

Action Ouvrir une session utilisateur Username=**albert** password=**admin** sous Windows7
Copier le dossier **\\10.2.1.1\doclabo\Secu\PKI-SSL** sur le bureau

Clic sur **XP_PKI-SSL.ova** (dossier copié) pour importer
Démarrer cette machine virtuelle
Eliminer les messages d'avertissement avec Enter

2	Chaîne de certification et authentification du serveur	30’

But 2 Utiliser le serveur sec1.tdeig.ch pour étudier les mécanismes liés aux certificats (serveur, *root*, …)

Action Lancer IE *(Internet Explorer)* puis entrer le lien https://sec1.tdeig.ch/

Ignorer dans un premier temps le message d’erreur "*The security certificate was issued by a company…* " en répondant Yes pour continuer

Question 2a Comment repère-t-on une connexion sécurisée ?

Action Pointer avec la souris sur le cadenas (en bas à droite de la fenêtre) afin de connaître le type de chiffrement utilisé.

Question 2b Quelle information est fournie ?

Question 2c S’agit-il d’un chiffrement symétrique ou asymétrique ?

Action Double-cliquer sur le cadenas

Question 2d A qui appartient ce certificat (onglet *General*) ?

Question 2e Par qui a-t-il été délivré ?

Question 2f A quoi sert ce certificat (onglet *Details*) ?

Question 2g Ce certificat a-t-il été envoyé par le serveur ou était-il mémorisé localement sur votre PC ?

Question 2h Pourquoi l’onglet *General* affiche le message d’erreur suivant :
This certificate cannot be verified up to a trusted certification authority.

Action **Corriger afin de supprimer ce message d’erreur**

Aide Une partie de la solution se trouve sur le site web de l’autorité de certification
http://ca.tdeig.ch

Rappel Une PKI repose principalement sur la notion de certificats.
Il en existe plusieurs types et leur rôle peut être différent
Tous les certificats (mémorisés localement) se trouvent dans le *certificate store* accessible depuis *Internet Explorer – Tools – Internet Options – Content – Certificates*

Question 2i Comment avez-vous fait pour supprimer le message d’erreur ?

Question 2j Quel risque avez-vous pris ?

Question 2k Quelle est la bonne procédure lors du téléchargement d'un certificat autosigné ?

Question 2l Dans quelle catégorie (onglet) doit se trouver ce certificat ?

Question 2m Pourquoi ?

Question 2n Quelle confiance avez-vous dans la liste des autorités de certification présente dans l'onglet *Trusted Root CA* ?

Question 2o Avec IE, comment procédez-vous pour obtenir ce cas d'erreur ?

3	**Authentification du client**	**10'**

But 3 Etablir une connexion sur le site https://sec2.tdeig.ch:444 qui exige une authentification de l'utilisateur

Rappel L'authentification du client est optionnelle et permet d'obtenir un niveau de sécurité plus élevé qu'avec l'utilisation d'un mot de passe.

Action Tenter avec IE d'établir une session https://sec2.tdeig.ch:444

Question 3a Que se passe-t-il ?

Question 3b Que réclame le serveur ?

Objectif Utiliser l'autorité de certification du labo pour obtenir un certificat utilisateur

Action Avec IE, ouvrir la page par défaut du site http://ca.tdeig.ch
Cliquer sur le lien *Request a certificate*
Choisir *advanced certificate request* puis *Create and submit a request to this CA*
N'entrez que votre nom dans le champ *Name* puis *Submit*
Répondre par Oui à la mise en garde
Cliquer sur *Install this certificate*
Fermer IE puis l'ouvrir à nouveau.

Test Vérifier que ce certificat a bien été installé sur votre PC

Question 3c Où se trouve-t-il ?

Remarque Toutes les autorités de certification ne délivrent pas les certificats si facilement ! Certaines par exemple, exigent un contrôle physique de la personne via un service d'enregistrement *(RA = Registration Authority).*

Question 3d Qui (votre PC – CA LaboTD) a généré la paire de clés ?

Question 3e Où est mémorisée votre clé privée ?

Question 3f Que doit faire l'administrateur d'un site SSL pour accepter les certificats utilisateurs délivrés par l'autorité de certification du labo ?

4 Certificats révoqués 10'

But 4 Comprendre l'utilité de la liste de révocation

Rappel Sur le principe d'une carte de crédit, il est nécessaire de pouvoir bloquer un certificat si son propriétaire se fait voler sa clé privée par exemple.

Chaque autorité de certification doit mettre à jour la liste des certificats révoqués *(CRL = Certificate Revocation List)* et la publier (service en ligne).

Aide L'onglet *Details* d'un certificat vous donne généralement le lien à cette CRL

Question 4a Comment procédez-vous pour visualiser la CRL de CA = laboTD ?

Question 4b Combien de certificats ont été révoqués ?

Question 4c Qui doit utiliser cette liste de révocation ?

5 Analyse du protocole SSL 30'

But 5 Etudier le protocole SSL à partir d'une acquisition Wireshark **ssl_poste.pcap** présente dans le partage.

Action Accéder au fichier **ssl_poste.pcap** (dossier copié)

Important **Préciser dans chacune de vos réponses le numéro du paquet**

Question 5a Quel est le FQDN *(Full Qualified Domain Name)* choisi pour cette connexion SSL ?

Question 5b Quel est la version SSL utilisée par le client dans le paquet *Client Hello* ?

Question 5c Quelle est la valeur (4 premiers octets) du champ *client.random* ?

Question 5d Quels sont les algorithmes de chiffrement proposés par le client ?

Question 5e Quelles sont les fonctions de hachage proposées par le client ?

Question 5f Quelle suite cryptographique est choisie et par qui ?

Question 5g Quelle est la longueur du certificat échangé ?

Question 5h Comment accéder à la CRL ?

Question 5i Quelle est la longueur du champ *Premaster Secret* ? Bien réfléchir !

Question 5j Quels sont les paquets protégés (chiffrement + intégrité) par SSL ?

Question 5k Pourquoi conseille-t-on à l'utilisateur du site http://www.poste.ch/ d'établir une connexion sécurisée avec https://www.poste.ch/ ?

6 Exercices facultatifs pour ceux qui ont terminé tous les points précédents

Ex 6a Déterminer la chaîne de certification pour le site https://www.poste.ch/
Combien y a-t-il de niveaux ? Pourquoi ?

Ex 6b Avec IE, ouvrir la page par défaut du site http://ca.tdeig.ch
Cliquer sur le lien *Request a certificate*
Choisir *advanced certificate request* puis *Create and submit a request to this CA*
Expliquer l'usage des différents types de certificats
Expliquer le rôle du champ CSP
Expliquer quand il convient d'utiliser l'option *Mark key as exportable*

Ex 6c Etudier la chaîne de certification du serveur https://www.switch.ch/

Parcourir les documents

- https://www.switch.ch/fr/pki/aai/
- http://www.quovadisglobal.ch/Zertifikate/SSLCertificates.aspx
- https://cabforum.org/info-for-consumers/

Ex 6d Parcourir l'excellent travail de diplôme de Mario Pasquali
http://www.tdeig.ch/SSL_PKI_CA/pasquali_M.pdf
http://www.tdeig.ch/SSL_PKI_CA/pasquali_P.pdf

Ex 6e CSP basé sur un jeton USB Aladdin eToken PRO USB
http://www.aladdin.com/etoken/pro/usb.asp

Ex 6f Etudier le document Lab_OpenSSL.pdf qui montre la marche à suivre pour générer la paire de clés et le certificat de sec1.tdeig.ch