

TP 1 - TIW4

Sécurité Des Systèmes D'Information

Partie A

Description du problème	mesure proposée	renvoi vers l'annexe
Connexion serveur/client pas sécurisé	<p>Passage au protocole HTTPS en utilisant la couche de chiffrement ssl, grâce à un certificat d'authentification émis par OpenSSL configuré sur Nginx.</p> <p>Justification: Une connexion via HTTPS (à la place de HTTP) va permettre non seulement à l'utilisateur de vérifier la nature du site web avant d'y accéder, mais aussi de protéger ses données lors de sa navigation.</p>	<p>Le fichier de configuration de NGINX: —>annexes-A/nginx.conf</p> <p>Le fichier default qui contient la configuration du serveur https: —>annexes-A/default</p> <p>Le fichier de paramétrage SSL: —>annexes-A/ssl-params.inc</p>
Génération d'un certificat	<p>Pour cela, nous avons utilisé OpenSSL, cela en passant par les commande suivantes:</p> <pre>\$ cd /etc/nginx/ \$ sudo mkdir ssl \$ cd ssl</pre> <p>Création d'une paire de clés RSA:</p> <pre>\$sudo openssl genrsa -out ./server.key</pre> <p>Génération d'un certificat auto-signé valable 10 ans=3650 jours:</p> <pre>\$ sudo openssl req -key ./server.key -new -x509 -days 3650 -sha256 -out ./server.cert -subj "/C=FR/L=Lyon/O=MIF03-CAW/CN=192.168.76.215"</pre>	<p>Certificat: —>server.cert</p> <p>Clé: —>server.key</p>