TP HTTP / Apache

Pour être certain de ne pas rencontrer de difficultés avec des composants logiciels manquants, il est recommandé de réinstaller l'image linux avant de commencer le TP.

Installation

Mettez à jour la liste des packages disponibles puis installez le package debian `apache2` avec `apt-get`.
Vérifiez que le serveur est correctement installé en vous connectant à localhost avec un navigateur.

Configuration de base

Repérez l'emplacement des fichiers de configuration du serveur HTTP. N'oubliez pas que les modifications des fichiers de configuration nécessitent le redémarrage sur serveur.

Port serveur

Modifiez le fichier de configuration de manière à ce que le serveur écoute sur le port 8080. Vérifiez avec le navigateur.

Connexions persistantes

Identifiez les variables de configuration permettant d'agir sur la persistance des connexions TCP. Configurez les scénarii suivants :

- pas de connexions persistantes,
- connexions persistantes de 10 secondes, 2 requêtes au maximum au sein d'une même connexion,
- connexions persistantes de 15 secondes, 100 requêtes au maximum au sein d'une même connexion.

Pour chacune de ces configurations, testez le comportement du serveur avec la commande suivante :

```
# netcat -C localhost 8080<enter>
GET / HTTP/1.1<enter>
Host: localhost<enter>
<enter>
```

Racine de l'arborescence des fichiers

Modifiez la racine de l'arborescence de fichiers pour qu'elle désigne le répertoire /web.
Créez une page simple /web/index.html qui affiche simplement « Vous êtes à la racine ».

Redirection

Redirigez l'accès à l'URL `http://localhost:8080/redir` vers le serveur web de votre voisin.

VirtualHost

Créez un répertoire /web2 et éditez-y un fichier index.html contenant « Vous êtes à la deuxième racine ».
Mettez en place deux « sites » :

- l'un, pointant sur /web, accessible lorsque l'on accède au serveur par localhost:8080
- l'autre, pointant sur /web2, accessible, lorsque l'on nomme la machine par son nom complet (pcXXXX.u-strasbg.fr :8080).

Authentification

Utilisateurs

Consultez l'aide de la commande htpasswd et créez un fichier .htpasswd dans le répertoire /web, avec les utilisateurs suivants :

login	*mot de passe*
marc	toto
jean	tata
paul	tutu

Vérifiez le format du fichier .htpasswd créé. Tentez d'y accéder directement à partir du navigateur. Trouvez la directive qui interdit l'accès à ces fichiers, et tentez de faire en sorte (temporairement) que le navigateur ait accès à ce fichier

Restrictions

Créez un sous-répertoire /web/secured et éditez-y un fichier index.html contenant simplement la phrase « Emplacement protégé » et un fichier index2.html contenant « Second emplacement protégé »
Créez dans ce répertoire un fichier .htaccess, afin d'appliquer tour à tour les restrictions suivantes :

- marc, jean ou paul sont autorisés à accéder aux deux fichiers ; sinon redirection vers une page affichant « Vous n'avez pas accès »,
- marc est autorisé à accéder aux deux fichiers, jean et paul seulement au fichier index2.html,
- autoriser tout accès sans mot de passe à partir de la machine de votre voisin.

Nom de l'authentification : « Protected Area », Type *Basic*.

Format de l'authentification

Utilisez l'application *wireshark* et capturez les trames envoyés et reçues lorsque vous vous connectez (avec le login marc) à la zone sécurisée du serveur de votre voisin. Décodez l'information d'identification (Base64) : retrouvez ainsi les login et mot de passe émis.

Module SSL

Commencez par générer avec `openssl` une clé privée RSA de 4096 octets, codée en DES3, dans le fichier apache.key. Créez ensuite un certificat X.509 valable une journée à partir de cette clé. Nommez ce certificat apache.crt.

Activez le module SSL en utilisant la commande `a2enmod`.
Editez le fichier ssl.conf pour y rajouter la référence à votre clé et votre certificat. Ajoutez le port 443 en écoute. Ajoutez un virtualhost pour le port 443, en y mentionnant `SSLEngine On`.
Utilisez wireshark à nouveau pour vérifier le format des échanges lors de la connexion à la zone /secured.

Autorité de certification

Vous remarquez que lors de la première connexion, le navigateur vous demande si vous faites confiance au certificat. Pour éviter cela, il faut mettre en place une autorité de certification qui signe le certificat du serveur HTTP, et en qui le navigateur ait confiance.
Créez un nouveau certificat qui vous permettra de signer celui de votre serveur. Aidez-vous de la FAQ du module SSL pour obtenir le script permettant d'effectuer cette signature : http://www.modssl.org/docs/2.8/ssl_faq.html.
Modifier ssl.conf pour ajouter le certificat de l'autorité de certification (`SSLCACertificate`). Introduisez ensuite le certificat de votre nouvelle autorité de certification dans votre navigateur et tentez à nouveau d'accéder au site web.

HTTP/2 (partie notée)

voir moodle