Jean-François Berdjugin, Jean-François Remm
IUT 1, Département SRC, L'Isle d'Abeau

Observation du protocole HyperText TProtocol

Configuration IP :

- adresse IP et masque : 192.168.114.X /24 (X numéro du disque dur, X+96 si vous êtes en Turing)
- routeur par défaut : 192.168.114.254
- Serveur DNS: 192.168.114.254

Outils utilisés :

- un client web avec une machine virtuelle java
- un client ftp
- le sniffeur ethereal (wireshark)

Sur la machine ftp.pedago.src vous trouverez :

- Le RunTime java : jre
- Le navigateur : mozilla-firefox
- Le cleint ftp : filezilla

Utilisation d'un site unique

Vous disposez sur le site web www.pedago.src d'un répertoire personnel accessible via l'URL http://www.pedago.src/~login ce site sera physiquement lié au répertoire public_html de votre home directory sur cette machine. Pour déposer vos fichiers sur ce serveur web, vous utiliserez un serveur ftp disponible à l'url ftp.pedago.src avec un login et un mot de passe identique à celui que vous aviez utilisé pour la cryptographie (login = prenom.nom, pass=nom).

A faire :

Créer et déposer un fichier *index.html* dans *pubilc_html*. Il vous faudra vérifier la présence du répertoire *public_html* et les droits d'accès. L'utilisateur sous lequel s'exécute le serveur web (apache) ne fait pas parti de votre groupe de travail vous devrait donc donner sur le répertoire *public_html* aux *autres* les droits "*r-x*".

Consultez l'URL "*http://www.pedago.src/~login/*" (ne pas oublier le / final) en lançant une capture avec le filtre "*host IP and tcp port 80 or tcp port 3128*".

Sachant que l'adresse MAC du routeur de la salle est ???? que pouvez vous conclure sur la localisation du serveur web.

Ce serveur est-il sur le même sous-réseaux que vous, pourquoi?

Quel est le protocole de transport utilisé et quels sont les ports mis en oeuvre coté client et serveur.

Le protocole http repose sur le paradigme client/serveur nous avons donc une requête suivie d'une réponse.

1. La requête:

La première ligne contient la demande du client, celle-ci peut être décomposé en trois sous-parties.

[Type de requête] [URL] [Protocole utilisé]

Le types de requête pet être : GET, POST, HEAD, PUT, DEL, TRACE.

L'URL correspond au chemin que l'on veut voir, il se situe juste après le nom de domaine.

Le protocole utilisé peut être HTTP/1.0 HTTP/1.1

Cette ligne peut ou doit être suivie d'autres lignes permettant d'affiner la requête.

2. La réponse:

La réponse est caractérisée par le code de réponse du serveur, tout comme la requête elle se compose d'une entête et d'un corps (optionel).

A faire :

En utilisant l'option "*follow tcp stream*" pour reconstituer le traffic applicatif (http). Dans ce traffic identifiez la partie serveur et la partie client.

Quel est le type de requête ?

Pourquoi le nom du serveur (adresse IP) n'apparaît pas dans la requête ?

Que contient le champ Host ?

Y-a-t-il un corps de message ?

Quel est le code de réponse du serveur ?

Comment la réponse est-elle délimitée ?

Que contient la réponse.

Votre navigateur lors de la requête envoie des informations comme la langue et l'encodage par défaut.

A faire :

Modifier le type d'encodage et la lange de votre navigateur et observer avec une capture les changements dans l'entête.

Un serveur web permet des redirections, ces redirections sont réalisées par un echange entre la client et le serveur que nous allons observer.

A faire :

Consulter l'url "*http://www.pedago.src/~login*" (sans le / final) en lançant une capture avec le filtre "*host @IP and tcp port 80 or tcp port 3128*".

Comment la redirection a-t-elle lieu ?

Sur un intranet un proxy http est utilisé pour vous offrir accès aux sites d'internet. Un proxy http est un serveur web un peu particulier qui écoute sur l'intranet puis relaye la rêquete sur internet, attend la réponse et la relaye sur l'intranet.

A faire :

Consulter l'url "*http://jf.berdjugin.free.fr/cours/*" en lançant une capture avec le filtre "*host @IP and tcp port 80 or tcp port 3128*".

Sachant que l'adresse IP de www-iut-src.ujf-grenoble.fr est en 212.x.x.x avez vous communiqué directement avec le serveur web ?

Quel est le port utilisé pour contacter le proxy ?

Pourquoi la première ligne de l'entête de la requête est-elle différente ?

Le protocole http en est à la version 1.1 cette version offre en outre par rapport à la version 1.0 la persistance de la connexion et la possibilité d'hébeger plusieurs sites web sur une même machine (serveur mutualisé).

A faire :

Avec telnet consultez l'url "www.pedago.src/~login/ " en utilisant la version 1.0 de http, avec ce protocole, seul la première ligne de l'entête suffit.

Serveur mutualisé

La machine 192.168.107.200 contient un serveur Web mutualisé. Ce serveur héberge un site Web pour chacun d'entre vous. Ce site est accessible via l'url "prenom.nom.pedago.src".

Déposer, dans votre home directory, sur ce serveur le contenu du répertoire web contenu dans l'archive web.zip de l'énoncé.

A faire :

Consulter l'url http://prenom.nom.pedago.src et observez le changement dans le champ

Host de l'entête.

Philosophiquement, la requête GET permet de demander une ressource, la requête POST permet d'envoyer de l'information à une ressource mais dans la pratique les deux permettentent la même chose.

A faire :

Consultez la page index.hmtl cette page contient deux boutons (Nom, Prénom) et deux formulaires avec deux Bouton (POST et GET). Utilisez ces boutons en lançant une capture et en observant la barre d'url de votre navigateur.

Où sont véhiculées les informations d'un formulaire lors d'un POST, d'un GET ?

Pourquoi ne pas utiliser de GET dans un formulaire avec un champ passwd ?

En cours vous avez vu Javascript, un langage qui s'éxécute sur le client, en deuxième année vous apprendrez à créer des programmes qui s'excutent sur le serveur pour générer dynamiquement une page web (web dynamique). Les formulaires avec les boutons GET et POST appel l'un de ces programme : ip.php. Ce programme va recupérer des informations en provenance de votre navigateur pour générer une page ou lancer d'autres programmes.

A faire :

Utilisez le boton GET, puis modifiez dans la barre d'url les valeur associ au nom "nom" et "prenom".

Rem : Ne pas oublier l'encodage un "é" devient "%E9"

Vous savez maintenant comment tester un script serveur sans formulaire.

Le protocole hhtp vous permet d'accèder à des ressources, ces ressources sont souvant des pages web mais peuvent aussi être des images, ou d'autres programmes qui s'exéterons sur le serveur commes les applets ou les animations flash. Ces programmes télécharger garde la possibilité de communiquer avec d'autres programmes présents sur le serveur.

A faire :

Après avoir lancé une capture testez l'image, l'applet et l'animation flash.

Comment le navigateur reconnaît-il le type de l'application ?

Le protocole http est un protocole "sans mémoire", le serveur ne peut se souvenir qu'il a déjà été consulté. Pour conserver une mémoire un cookie est utilisé. Il permet de maintenir un contexte de session. Le cookie est un couple Nom/ Valeur envoyé par le serveur lors de la première consultation

d'une url (un script générant un cookie), puis réenvoyé par le client lors des consultations future permettant ainsi au script du serveur de savoir que vous avez déjà consulté l'url. Le cookie est souvant stocké dans un fichier texte sur le client.

A faire :

Utilisez plusieures fois le formulaire cookies en réalisant une capture et observez la trace du cookie dans les échanges.

Les serveurs appaches permettent aux utilisateurs de restreindre l'accès à certaines pages par le biais d'un fichier .htaccess.

Le fichier suivant permet par exemple :

```
ErrorDocument403 http://prenom.nom.pedago.src/pages/erreur.html
AuthUserFileusers/.users
AuthGroupFile/dev/null
AuthName"Accèssécuriséausite"
AuthTypeBasic
<LIMIT GET POST>
Requirevalid-user
</LIMIT>
```

De définir un message d'erreur personnalisé pour l'erreur 403.
D'autoriser les GET et les POST mais avec une authentification simple (en clair), d'aller chercher dans users/.users la correspondnace login mot de passe.
Le fichier de correspondance aura des enregistrements de type :

- login:password(encrypté)

A faire :

Créér et placer à la racine web un fichier .htaccess et le fichier users/.users. Pour crypter le mot de passe vous utiliserez le script php disponible dans: http://login.pedago.src/scripts/crypt.php qui prend comme paramètre pass.

Tester et lorsque cela marche lancer une capture et expliquez comment le serveur web indique qu'il souhaite une authentification.