TP HTTP et DNS avec Wireshark

Ce TP est adapté des Wireshark labs de Kurose et Ross proposés en suppléments à leur livre COMPUTER NETWORKING : A TOP DOWN APPROACH ()

1 Wireshark

Wireshark (`http://www.wireshark.org`)est un utilitaire d'analyse de protocoles réseau (renifleur de paquets) qui permet de capturer de paquets sur le réseau en direct et de les analyser (en direct ou en différé).

2 HTTP

Nous allons utiliser Wireshark pour voir différents aspects du protocole HTTP : requête/réponse HTTP, format des messages, récupération de fichier HTML volumineux, fichiers HTML avec objets inclus, authentification HTTP.

2.1 Requête/réponse HTTP

- Démarrer votre navigateur web, démarrer wireshark et mettre le filtre "http" dans la fenêtre de filtre d'affichage. Attendre 1 minute et démarrer la capture.
- Saisir l'URL `http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html` dans le navigateur et stopper la capture.

En regardant les messages de requête et réponse, répondre aux questions suivantes :

1. Quelle sont les versions d'HTTP de votre navigateur ? du serveur ?
2. Quel(s) langage(s) votre navigateur accepte-t-il ?
3. Quels sont les adresses IP de votre ordinateur ? du serveur `http://gaia.cs.umass.edu` ?
4. Quand le fichier auquel vous accédez a-t-il été modifié pour la dernière fois coté serveur ?

2.2 GET conditionnel HTTP

Lancer wireshark, démarrer la capture, saisir l'URL `http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html` dans le navigateur et rapidement après, entrer à nouveaux la même URL (ou cliquer sur le bouton de rafraichissement), puis stopper la capture.

Répondre aux questions suivantes :

1. Dans la première requête HTTP GET, le champs "If-Modified-Since" est-il présent ?
2. Le serveur a-t-il retourné le contenu du fichier ?
3. Dans la seconde requête HTTP GET, le champs "If-Modified-Since" est-il présent ? Si oui, quelle information contient-il ?
4. Quels sont les code et message retourné par le serveur ? Le serveur a-t-il retourné le contenu du fichier ?

2.3 Fichier HTML volumineux

Lancer wireshark, démarrer la capture, saisir l'URL `http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html` dans le navigateur, puis stopper la capture.

Répondre aux questions suivantes :

1. Combien de requêtes HTTP GET votre navigateur a-t-il envoyé ? Quels numéro de paquet dans la trace contient le message GET ?

2. Quel numéro de paquet contient le code de statuts et le message associé retourné par le serveur ?
3. Combien de segments TCP de données ont été nécessaires pour transporter la réponse HTTP et le message associé (déclarations des droits Américains) ?

2.4 Document HTML avec objets inclus

Lancer wireshark, démarrer la capture, saisir l'URL `http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html` dans le navigateur, puis stopper la capture.

Répondre aux questions suivantes :

1. Combien de requêtes HTTP GET votre navigateur a-t-il envoyé ? A quelles adresses internet ces requêtes ont-elles été envoyées ?
2. Est-il possible de savoir si votre navigateur à téléchargé les images de façon séquentielle ou si elles ont été téléchargées en parallèle ? Expliquer.

2.5 Authentification HTTP

Lancer wireshark, démarrer la capture, saisir l'URL `http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html` dans le navigateur, saisir ("wireshark-students" pour username et "network" pour le password) puis stopper la capture.

Répondre aux questions suivantes :

1. Quelle est la réponse du serveur (code et message) à la première requêtes HTTP GET ?
2. Quand votre navigateur envoi la requête pour la seconde fois, quels nouveaux champs sont inclus dans ce message GET HTTP ?

3 DNS

1. Regarder le manuel de la commande `nslookup`
2. Expliquer ce que produit chacune des lignes de commande suivantes :
   (a) `nslookup www.mit.edu`
   (b) `nslookup -type=NS mit.edu`
   (c) `nslookup www.kaist.edu res87.bora.net`
3. Lancer wireshark et visiter le site de l'IETF avec votre navigateur.
   (a) Les requêtes DNS effectuées sont-elles transportées par UDP ou TCP ?
   (b) Quel est le port destination de la requête DNS ? Quel est le port source de la réponse ?
   (c) A quelle adresse IP la requête DNS est-elle envoyée ? La comparer avec celle de votre DNS local (voir `/etc/resolv.conf`).
   (d) Combien de réponses sont données dans le message DNS de réponse ?

4 Compte-rendu

Votre compte-rendu doit répondre brièvement aux questions posées dans ce TP et développer sur 1/2 page un aspect récent en lien avec HTTP ou DNS (httpbis, DNS PRIVate Exchange, ...).

A rendre avant le TP suivant en version pdf au chargé de TP (`Cyrille.Migniot@u-bourgogne.fr` ou `otogni@u-bourgogne.fr`).