Laboratoire 3 : Découvrir TCP avec Wireshark

Dans ce troisième laboratoire, nous allons manipuler une capture de paquets utilisant TCP afin d'analyser en détail le comportement de ce protocole. Suivez les étapes suivantes en essayant de répondre aux différentes questions.

Nous allons utiliser Wireshark afin de capturer les différents segments TCP échangés lors d'un transfert d'un fichier de votre terminal vers un serveur distant. Le fichier à uploader « *Alice in Wonderland* » doit être récupérer à partir de Moodle. Par la suite suivez les étapes suivantes afin de réaliser la capture

- Aller sur l'adresse suivante : http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html
- Cliquez sur le bouton « Choisissez un fichier » puis choisissez le fichier qui contient « *Alice in Wonderland* ».
- Lancez Wireshark et démarrez une capture
- Revenez sur le navigateur, puis appuyez sur le bouton « Upload alice.txt file ». Un message de félicitations s'affiche sur votre navigateur.
- Arrêtez la capture sur Wireshark.
- Dans l'espace filtre, entrez « tcp » pour restreindre l'affichage aux paquets TCP et HTTP uniquement. (Vous pouvez améliorer votre filtre afin de limiter davantage l'affichage des paquets)

Répondez aux questions suivantes en examinant les paquets capturés

1. Quelle est l'adresse IP et le port TCP de la source du fichier transféré?
2. Quelle est l'adresse IP et le port TCP utilisés par le serveur gaia.cs.umass.edu?

Téléchargez le fichier tcp.pcap et répondez aux questions suivantes

3. Le client commence par initier une connexion TCP avec le serveur. Quel est le numéro de séquence contenu dans le segment TCP SYN de cette connexion? (vous devez fournir le numéro relatif et absolu)
4. Le serveur répond au client en acceptant sa demande de connexion. Quels sont les numéros de séquence et d'acquiescement contenus dans cette réponse? Quels sont les fanions de l'en-tête qui ont la valeur 1?
5. Cherchez le segment qui contient la commande HTTP POST. Quel est le numéro de séquence contenu dans ce segment?
6. Retrouvez les six premiers segments TCP qui contiennent des données ainsi que leurs accusés de réception. Remplissez le tableau suivant

	Instant d'envoi	Instant de réception du ACK	SampleRTT
Segment 1			
…			

7. Calculez la valeur du EstimatedRTT en utilisant la formule du cours avec $\alpha = 0.125$ après la réception de chaque ACK. Vous devez supposer que le premier EstimatedRTT est égale au SampleRTT du premier segment.
8. Quelle est la taille de chacun des six premiers segments (sans en-tête TCP)?
9. Quelle est la taille minimale de la fenêtre de réception que le récepteur envoie dans ces accusés de réception? Est-ce que l'émetteur a dû contrôler son flux d'émission à un moment donné sous demande du récepteur?
10. Est-ce qu'il y a des retransmissions de segments dans la trace? Pour répondre à cette question vous pouvez utiliser les graphes fournis par Wireshark (cliquez sur un segment TCP contenant des données puis allez sur statistics -> TCP stream graph -> Time-sequence graph (Stevens)).
11. Calculer le taux de transmission durant la connexion TCP qui a servi au transfert du fichier.