Laboratoire 1 : découvrir HTTP et FTP avec Wireshark

Dans ce premier laboratoire, nous allons découvrir les possibilités qu'offre un outil de capture et d'analyse de paquets. Nous allons manipuler les protocoles HTTP et FTP en analysant différentes captures de communications effectuées par le biais de ces protocoles.

I. Protocole HTTP

a. Partie A : fichier html

Commençons par un exemple simple, soit le téléchargement d'un seul fichier HTML qui ne contient aucune référence à d'autres objets. Vous devez suivre les instructions suivantes :

a) Ouvrez votre navigateur web
b) Lancez Wireshark puis lancez une capture de paquets en suivant les étapes suivantes
   - sur la barre de menu de Wireshark, cliquez sur le bouton capture puis choisissez interfaces.
   - Cochez le nom de l'interface qui correspond à votre carte réseau puis cliquez sur démarrer
c) Revenez au navigateur puis entrez l'URL suivant dans la barre d'adresse : http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
d) Après l'affichage de la page demandée, revenez sur Wireshark puis arrêtez immédiatement la capture.
e) Tapez « http » dans l'espace filtre de Wireshark puis appuyez sur entrer. Notez que les filtres sont sensibles à la casse, ils doivent être en minuscule. Wireshark doit vous afficher des paquets de couleurs vertes dont deux concernent les échanges qui ont permis l'obtention de la page web demandée.

En analysant les deux paquets en question, répondez aux questions suivantes :

1. Quelle version de HTTP utilise votre navigateur? Quelle est celle utilisée par le serveur?
2. Quelles langues sont acceptées par votre navigateur?
3. Quelle sont les adresses IP de votre ordinateur et du serveur gaia.cs.umass.edu?
4. Quel est le code d'état retourné par le serveur?
5. Quand est ce que le fichier HTML demandé a été modifié pour la dernière fois?
6. Combien d'octets sont-ils envoyés au serveur?

b. Partie B : fichier html aves références

Dans cette partie, nous allons télécharger un fichier HTML qui contient des références à quelques objets.

a) Avant de procéder au téléchargement, n'oubliez pas de lancer la capture de paquets.
b) Le fichier à télécharger est disponible sur le lien http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html.

c) Une fois la page affichée, arrêtez la capture puis tapez « http » dans l'espace filtre.

Répondez aux questions suivantes:

1. Combien de requêtes HTTP GET sont envoyées par votre navigateur?
2. Quelle est la destination (adresse IP) de vos requêtes GET?
3. Donnez les codes des réponses HTTP contenus dans les paquets envoyés par le serveur.

c. Partie C : formulaire

Nous allons explorer dans ce qui suit le mécanisme d'authentification basique de HTTP.

a) Lancez une nouvelle capture puis visitez le lien suivant : http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html.
b) Entrez le nom d'utilisateur : « wireshark-students » et le mot de passe : « network » puis validez.
c) Vous devrez avoir une réponse du serveur comme quoi le fichier n'a pas été trouvé.

Répondez aux questions suivantes:

1. Quelle a été la réponse du serveur à la première requête GET du navigateur?
2. La deuxième requête GET du navigateur contient un nouveau champ, lequel?
3. Le nom d'utilisateur ainsi que le mot de passe que vous avez fourni sont-ils chiffrés? (indice : essayez de vérifier l'encodage du contenu du nouveau champ sur le site https://www.base64decode.org/).

II. FTP

La deuxième partie de ce laboratoire porte sur le protocole de transfert de fichiers, FTP (en anglais file transfer protocol). Il s'agit d'un protocole client-serveur simple et non-sécurisé qui permet à partir de votre ordinateur (où tourne un processus client) de gérer des fichiers sur un ordinateur distant (où tourne un processus serveur). Afin d'envoyer des commandes, le client établit une connexion de commande vers le port 21 du serveur. Un deuxième type de connexion peut aussi être utilisé à chaque fois qu'un transfert de données est nécessaire. Il s'agit dans ce cas de connexions de données. Notez que contrairement à FTP, un seul type de connexions existe dans HTTP, celui utilisant le port 80 côté serveur.

Dans cette partie du laboratoire, votre ordinateur servira de client FTP. Les étapes suivantes nous permettront de capturer plusieurs paquets qui utilisent ce protocole (une description de FTP est disponible dans les acétates de la séance 3). Vous allez vous connecter à un serveur afin de télécharger un fichier sur votre ordinateur.

a) Sur votre ordinateur, téléchargez puis installez la version client du logiciel FileZilla. Le lien de téléchargement est disponible sur Moodle dans la section « Laboratoires ». Lors de l'installation, acceptez toutes les options par défaut.
b) Une fois l'installation terminée, ouvrez Filezilla.

c) Exécutez Wireshark puis lancez une nouvelle capture.
d) Revenez sur FileZilla, puis
    - Entrez l'URL ftp.gnu.org dans « Hôte »
    - Cliquez sur Connexion rapide
    - Une boite de dialogue devrait s'afficher pour vous informer que FTP est non sécurisé et que vous allez communiquer avec le port 21 du serveur. Si une telle boite s'affiche, appuyez sur OK.
e) Une fois connecté, les fichiers et répertoires du serveur seront affichés à droite de la fenêtre de FileZilla. Cliquez avec le bouton droit sur le fichier « README » puis sélectionnez « Télécharger ».
f) Déconnectez-vous du serveur en utilisant le bouton Serveur>Déconnecter de la barre de menu.
g) Arrêtez la capture sur Wireshark puis essayez d'analyser les paquets échangés en répondant aux questions suivantes :
    1. Quel est le protocole de couche transport utilisé par FTP.
       (Astuce : pour afficher uniquement les paquets FTP utilisez le filtre « ftp ».)
    2. D'après les paquets échangés, déterminez l'adresse IP du client et l'adresse IP du serveur.
    3. Est-ce que le client a utilisé un nom d'utilisateur pour se connecter? Si oui lequel?
    4. Est-ce que le client a utilisé un mot de passe pour se connecter? Si oui lequel?
    5. En analysant les paquets FTP, quels sont les numéros de port utilisés par le serveur? Quels sont ceux utilisés par le client?
       (Astuce : en utilisant l'adresse IP du serveur, appliquez le filtre suivant : « ip.addr == [remplacer ces crochets par l'adresse IP du serveur] ». Ce filtre permettra d'afficher tous les paquets échangés avec le serveur.)
    6. Est-ce que les données contenues dans les messages FTP sont en clair ou chiffrées?
    7. Après quelle(s) commande(s), le serveur initie-t-il une connexion pour l'échange de données?