

LOG100 - Programmation et Réseautique en génie logiciel

Laboratoire 3 : Couche Application

Durée = 1 séance de 3 heures


Objectifs

Ce laboratoire vous permettra de comprendre le fonctionnement de la couche application en analysant les données échangées par quelques protocoles.

Montage & Outils

- Système d'exploitation : *Windows*
- Autres outils et logiciels : *Wireshark, nslookup, ftp*

Notes

- Ce travail doit se faire individuellement.
- Utilisez le fichier Labo3_gabarit_rapport.docx pour compléter votre rapport de laboratoire.
- Enregistrez-le au format PDF et nommez-le Labo3_rapport_nom_prenom.pdf (exemple Labo3_rapport_Mah_Firmin.pdf) et déposez-le dans Moodle.
- Le symbole ➡ indique la manipulation à faire pour répondre aux questions.
- Veuillez joindre, s'il y'a lieu, les captures d'écran qui montrent les réponses aux questions. **Le symbole  indique que vous devez joindre une capture d'écran pour avoir les points.**

Question préliminaire

1. Quels sont les 5 éléments qui définissent (qui sont nécessaires pour) une connexion entre processus se trouvant sur des hôtes différents ? (10 pts)

Commande nslookup :

La commande *nslookup* est une commande DOS qui permet d'interroger un serveur DNS à propos d'un nom de domaine pour connaître des informations telles que son adresse IP, ses alias ...

- ☛ Ouvrez le fichier « nslookup_yahoo_com.pcapng ». Cette capture de *Wireshark* a été obtenue après avoir lancé la commande *nslookup -type=a yahoo.com* en étant connecté par Ethernet au réseau local de l'ÉTS (type a = adresse IPv4).
 - ☛ Utilisez le filtre d'affichage dans *Wireshark* pour ne montrer que les paquets DNS.
 - ☛ Retrouvez le paquet contenant la **1^{ère} requête DNS (requête PTR)** et accédez aux détails de l'entête réseau.
2. Fournir les informations suivantes : (6 pts)
 - L'adresse IP de destination du paquet
 - Quel est le rôle du nœud qui a cette adresse IP de destination ?
 - ☛ Affichez les champs de l'en-tête du segment de la couche transport de ce paquet.
 3. Fournir les informations suivantes : (6 pts)
 - Le protocole au niveau de la couche transport utilisé par le protocole DNS
 - Le numéro de port de destination de la requête
 - La taille du message DNS encapsulé dans le segment (en octets)
 - ☛ Affichez les détails du paquet contenant la **réponse DNS à la requête DNS de type A** (choisissez la réponse de la requête qui recherche l'adresse IP du nom de domaine **yahoo.com**).
 4. Donnez le nombre d'adresses IP correspondant au serveur web de *yahoo.com* et expliquez l'utilité d'avoir plusieurs adresses pour un même serveur. (4 pts)


Protocole http :

- ☛ Ouvrez le fichier « eu_httpbin_org.pcapng ». Cette capture de Wireshark a été obtenue après avoir demandé la page Web <http://eu.httpbin.org/> étant connecté à Internet à partir d'un réseau local.
- ☛ Utilisez le filtre d'affichage de *Wireshark* pour afficher seulement les paquets *http* échangés entre la station se trouvant dans le réseau local et <http://eu.httpbin.org/>. Après l'application du filtre, la colonne « *Protocol* » de Wireshark doit être égale à HTTP pour tous les paquets. Pour de l'aide sur le filtrage voir <https://networkproguide.com/wireshark-filter-http-traffic/>

5. Examinez les paquets et répondez aux questions suivantes : (15 pts).

Note : pour certaines questions, les menus de Wireshark Statistiques>Conversations, Statistiques>http ou autres peuvent vous aider.

- Quelle est la version *http* utilisée par le navigateur pour demander la page Web ?
- Quel protocole a été utilisé pour encapsuler les paquets *http* ?
- Combien d'objets (mis à part le fichier *html*) ont été téléchargés à partir du site <http://eu.httpbin.org/> ?
- Comment avez-vous compté les objets téléchargés ?
- Combien de connexions ont été créés entre la station se trouvant dans le réseau local et le serveur web à <http://eu.httpbin.org/> ?

6. Fournir les captures d'écran suivantes : (4 pts) 

- Capture d'écran qui vous a permis de trouver le nombre d'objets téléchargés
- Capture d'écran qui vous a permis de trouver le nombre de connexions créés

7. Est-ce qu'une même connexion peut être utilisée pour demander plusieurs objets ? Justifiez votre réponse. (4 pts)

- ☛ Examinez la trame de la première réponse http.

8. Fournir les informations suivantes : (15 pts)

- Port source dans cette première réponse http
- Port destination dans cette première réponse http
- Code de réponse retourné par le serveur
- Signification du code retourné par le serveur
- Type de serveur http hébergeant eu.httpbin.org

Commande ftp :

La commande **ftp** permet de se connecter à un serveur de fichiers en ligne de commande. Elle utilise le protocole ftp pour transférer et recevoir des fichiers vers un serveur distant.

- ☛ Ouvrir une invite de commandes DOS, lancez la commande suivante pour se connecter au serveur ftp distant *test.rebex.net*

ftp test.rebex.net

Nom d'utilisateur : *demo*

Mot de passe : *password*

Une fois connecté, la commande « ? » permet d'afficher les commandes possibles. Le symbole « ? » suivi d'une commande permet d'obtenir de l'aide sur celle-ci (exemple ? cd).

9. Répondez aux questions suivantes (6 pts)

- Quelle est la commande qui permet d'afficher les fichiers contenus dans le serveur distant ? Note : ne pas exécuter la commande (bloquée).
 - À quoi sert la commande « *bell* » ?
 - Quel est le répertoire courant sur le serveur distant ?
 - Quelle commande permet de fermer la connexion ftp et quitter le serveur *ftp* ?
- ☛ Fermez la connexion ftp et quittez l'outil *ftp*.
 - ☛ Ouvrez le fichier LOG100-Labo3-FTP.pcapng. Ce fichier est la capture Wireshark du téléchargement d'un fichier avec *ftp* à partir du serveur *ftp.mcafee.com*.

10. Consultez les traces collectées et répondez aux questions suivantes. (14 pts)

- Quel protocole de niveau transport est utilisé par ftp ?
- Quel filtre Wireshark faut-il utiliser pour ne montrer que le trafic échangé entre le client et le serveur ?
- Combien de connexions ont été créés au cours de cette manipulation ?
- Quel est le code de retour contenu dans le premier message ftp provenant du serveur ?
- Que veut dire ce code ?
- Quel est le numéro de port utilisé par le serveur pour transmettre le fichier ?
- Combien de paquets contenant des données étaient nécessaires pour transmettre tout le fichier ?

11. Donnez le message de réponse *ftp* où le serveur demande de saisir le mot de passe. (2 pts)

12. Donnez le contenu du message *ftp* qui contient le mot de passe. (2 pts)

13. À partir de cette capture, complétez le diagramme d'échange niveau application entre la station et le serveur *ftp.mcafee.com* en considérant les points suivants : (12 points)

- Ne considérer que la connexion de contrôle.
- Les échanges niveau TCP et les paquets n'ayant pas de données (données provenant de l'application) ne sont pas dessinés.
- Donnez la commande *ftp* avec **paramètres** pour chaque paquet envoyé au serveur.
- Donnez le code retour pour chaque commande reçue par *ftp.mcafee.com*.

