

TP N°2

Objectifs

- Comprendre le modèle Tcp/IP;
- Découvrir les caractéristiques générales et l'encapsulation des protocoles du modèle "TCP/IP"
- Être capable d'utiliser un analyseur de protocoles.

Partie exercices

7. Lors du transfert des données, quelles sont les principales responsabilités de l'hôte récepteur ?
- Le débit
 - L'encapsulation
 - L'accusé de réception
 - La bande passante
 - Le réassemblage
 - La segmentation
8. Qu'est-ce qui détermine la quantité de données que peut transmettre une station émettrice exécutant le protocole TCP/IP avant qu'elle doive recevoir un accusé de réception ?
- La taille du segment
 - Le débit de transmission
 - La bande passante
 - La taille de fenêtre
 - Le numéro de séquence

9. Quelle est la fonction du numéro d'ordre inclus dans l'entête TCP/IP ?
- Il rassemble les segments en données complètes
 - Il identifie le protocole de la couche application
 - Il indique le numéro de l'octet suivant attendu
 - Il précise le nombre maximal d'octets autorisés lors d'une session
10. Quelle est le fonction du numéro de ports TCP/UDP ?
- Ils permettent d'indiquer le début d'un échange en trois étapes
 - Ils permettent de réorganiser les segments dans l'ordre adéquat
 - Ils permettent d'identifier le nombre de paquets de données pouvant être envoyées sans accusé de réception
 - Ils permettent de suivre les différentes conversations simultanées dans un réseau

11. Classez les propositions en fonctions du protocole qu'elles décrivent (TCP ou UDP).

<input type="checkbox"/> Fiable	<input type="checkbox"/> Aucun contrôle de flux	<input type="checkbox"/> Reconstitue les messages au niveau de la destination	<input type="checkbox"/> UDP
<input type="checkbox"/> Renvoie toute donnée non reçue			
<input type="checkbox"/> Ne reconstitue pas les messages entrants			
<input type="checkbox"/> Peu fiable			

12. Dans la couche transport, lequel des contrôles suivants permet d'éviter qu'un hôte transmette des données provoquant un dépassement de capacité des mémoires tampons de l'hôte en réception ?
- Le niveau de service Best effort
 - Le chiffrement
 - Le contrôle de flux
 - Le contrôle de congestion
 - La prévention d'encombrement

Le logiciel s'ouvre sur cette page de menu :

Nous utilisons essentiellement le menu « Open » qui permettra de charger un fichier de capture pour analyser. Ouvrez le fichier http.cap disponible sur le serveur ou sur le site <http://wiki.wireshark.org/SampleCaptures>.

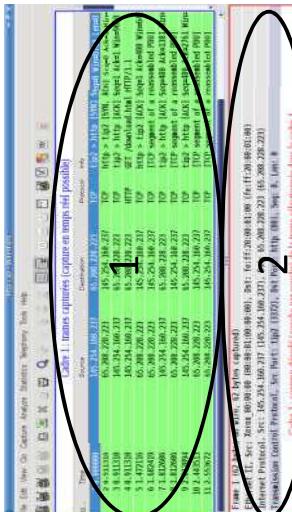


L'affichage se décompose en trois cercles

Cercle (1) : Filtrage

Il est possible de créer des filtres d'affichage sur liste l'ensemble des paquets capturés, qui ne montrent que les trames conformes à la règle de filtrage. Cela permettra d'isoler un échange en particulier ou l'analyse d'un protocole spécifique.

Le bouton « Expression » permet d'accéder à un assistant pour créer une règle de filtrage. Une règle de filtrage s'appuie sur les champs des entêtes (header) des protocoles connus du logiciel Wireshark



Cercle (2) : Encapsulation

Le cercle 2 affiche le détail d'un paquet sélectionné ce qui illustre le principe de l'encapsulation des protocoles utilisées dans l'échange d'une trame. On fait souvent référence à un modèle pour représenter cette communication. Ici, le modèle est celui qui implémente les protocoles de la famille « TCP/IP »

Par exemple : En sachant qu'une couche se décomposera en deux parties comprenant un entête

(header) appelé aussi PCI (Protocol Control Information) et un champ DATA (au sens « network data »). En fait, cela représente les protocoles présents dans la trame de la manière suivante :



On comprend alors que le champ DATA d'une couche contient le bloc de la couche supérieure (Header + DATA). C'est le principe de l'encapsulation.

Cercle (3) : Détail en hexadécimal

présente l'ensemble du paquet sous forme octale et ASCII. Ces octets contiennent les en-têtes des différentes couches de l'architecture TCP/IP ainsi que les données transmises par le processus à l'origine du message.

Travail à réaliser

I- Lecture d'une trace

1. Télécharger la trace (la capture) de l'adresse (<http://packetlife.net/captures/HTTP.cap>)

2. Ouvrir Wireshark, Aller dans File->Open puis choisir le fichier téléchargé en 1.

3. Examiner le fichier ouvert et répondre aux questions suivantes

Quetions :

1. Enumérez les colonnes du tableau du centre, quels est le sens de chacune ?
2. Positionner le curseur sur la ligne N°1 et examiner le contenu du tableau en dessous. Enumérez la liste des protocole que vous reconnaissiez. Quel est le numéro du protocole IP dans une trame Ethernet ?
3. Dans un tableau approprié indiquer pour les trois premières frames (1,2,3), les valeurs des champs suivants : Champ @IP_Source @IP_Destination, Port-Source, Port-Destination, Flags, champs numéro de séquence, champs numéro acquittement. Quelle l'est l'adresse IP du client dans ce dialogue ? Et celle du serveur ? Comment avez-vous fait pour les identifier ?
- Quels sont les programmes qui sont en communication C/S ? Comment sont-ils identifiés ?
- La ligne 4 concerne quel protocole de niveau application ? Quel type de message est envoyé ?

Quelle version du protocole de niveau application est utilisée ? Combien d'octets contient-elle ?

5. Continuez à donner les valeurs des champs numéro sequence, numéro acquittement et flagpour le restant des segments. Quelles sont les règles de leur évolution ?

6. Analyser et discuter de la ligne 36. Quelle est la taille de l'image ? Combien de segments TCP a nécessité son envoi ?

7. A quoi est dû la ligne 37 ?

8. Comme pour la question 1, refaites le tableau pour les lignes 38-40. Que pouvez-vous en dire ?

9. Faites un graphe montrant l'évolution de la fenêtre d'émission du serveur vers le client. Discutez-là.

10. Re-examiner maintenant le champs Options TCP des trois premières lignes . Les lignes à partir de 4 les contiennent toutes ? Qu'en concluez-vous ? Quelle(s) RFC(s) décrit chaque option ? Pour chaque option indiquer son utilité (contrôle de congestion, contrôle de flux, connexion fiable,etc...)