TP 1 - Observation bas niveau de protocoles

1 Wireshark

Que se passe-t-il lorsque nous utilisons un navigateur pour accéder à un site web ? Par quels miracles les informations voulues (ou pas) arrivent-elles sur notre écran ? Ces informations sont transmises au travers de réseaux grâce à des échanges entre éléments actifs (les deux premiers éléments actifs étant évidemment notre poste client et le serveur avec lequel il dialogue).

Tous les échanges sont régis par des protocoles qui utilisent des trames pour envoyer et recevoir des données. Ces trames sont créées de manière transparentes pour l'utilisateur qui se limite à utiliser des fonctions haut niveau telles que **socket**, **read** ou **write**. Mais il est possible de regarder en détail le contenu de ces trames. Nous allons utiliser un outil nommé Wireshark pour observer de tels échanges ; c'est un outil dit de "capture réseau".

Pour limiter les problèmes de sécurité, ce TP se base sur deux traces de communication pré-enregistrées : "ethereal-1.pcap" et "ethereal-2.cap". Wireshark permet de regarder aussi bien les trames circulant en temps réel sur un ordinateur que d'étudier celles enregistrées dans une capture. Ouvrez la trace de communication pré-enregistrée.

L'interface de Wireshark se découpe en trois parties : un filtre, la liste des trames, et le contenu de la trame courante. Le filtre permet de ne conserver dans la liste que les trames d'un certain protocole (*http* ou *ftp* par exemple). Il est possible de les combiner (*http or ftp* par exemple).

2 DHCP *(Dynamic Host Configuration Protocol)*

Filtrez sur bootp *(trace ethereal-1.pcap)*

- ▷ Les messages DHCP sont ils envoyés au dessus d'UDP ou de TCP?
- ▷ Dessinez le diagramme temporel d'échange de messages entre le client et le serveur DHCP.
- ▷ Quelle est l'IP du serveur DHCP?
- ▷ Quel message contient la nouvelle IP du client, quelle est cette IP?
- ▷ Quelle est la durée de vie de l'adresse renvoyée par le serveur?

3 PING

Deux commandes Ping sont faites. La première (ping 95.131.143.145) commence au message 5, la seconde (ping www.ietf.org) au message 103. *(trace ethereal-1.pcap)*

- ▷ Quel est le protocole utilisé?
- ▷ Pourquoi les paquets ICMP n'ont ils pas de port de départ/destination?
- ▷ Enlevez le filtre. Déterminez la différence de messages utilisés pour traiter les deux commandes.
- ▷ Dans les deux cas, dessinez le diagramme temporel d'échange pour la première séquence.

Observez le trafic correspondant à la deuxième commande Ping. Juste avant cette commande, la taille de la mtu *(maximum transmit unit)* a été baissée sur la machine 192.168.1.37.

- ▷ Que constatez vous pour les message 105, 106 et 107?

- ▷ Analysez les champs flags et Offset de l'entête IP des trois messages.
- ▷ Analysez la taille des paquets au niveau IP, et au niveau data. En déduire la nouvelle valeur de la mtu?
- ▷ Y a t-il d'autres messages fragmentés dans la trace ? Détailler le filtre à utiliser?

Observez la mise en œuvre du protocole DNS au début la deuxième commande Ping.

- ▷ À Quelle couche du modèle OSI le protocole DNS appartient-il?
- ▷ Les messages DNS, sont ils envoyés sur UDP ou sur TCP?

4 HTTP *(Hypertext Transfer Protocol)*

(trace ethereal-2.cap)
La partie HTTP consiste en deux requêtes, une image seule, et un site web complet. Pour l'image seule (requête en trame 236) :

- ▷ Quelle version HTTP le client demande t-il? Quelle est la version renvoyée par le serveur?
- ▷ Quel est le status renvoyé par le serveur?
- ▷ Quand est ce que le fichier a été modifié pour la dernière fois?
- ▷ Quelle est la taille de la réponse?
- ▷ Ce premier fichier est grand, comment se passe son transfert? (cyclez avec un filtre sur **http** et sans filtre pour répondre).

Pour le site web (requête en trame 274) :

- ▷ Quel est le système d'exploitation du client?
- ▷ Quel est le nombre maximal de fichiers demandés simultanément?
- ▷ L'image seule de la première partie est affichée. Y a t-il une requête la concernant. Pourquoi?

5 TELNET

(trace ethereal-2.cap)

- ▷ Trouvez les messages de la session telnet, sont ils envoyés sur UDP ou TCP?
- ▷ Quel est le login utilisé? Le mot de passe ? L'IP du serveur?
- ▷ Quel est la commande saisie? La réponse renvoyée?
- ▷ Dessinez le diagramme temporel d'échange.

6 FTP *(File Transfer Protocol)*

(trace ethereal-2.cap)

- ▷ Trouvez tous les messages de la session ftp, sont ils envoyés sur UDP ou TCP? Quel filtre utilisez vous?
- ▷ Quel est le login et le mot de passe utilisés dans cette sessions de transfert?
- ▷ Quel est le nom du fichier transféré?
- ▷ Trouvez le contenu du fichier transféré.
- ▷ Dessinez le diagramme temporel d'échange.