Observation bas niveau de protocoles

1 Wireshark

Toutes les communications réseau 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. L'utilitaire wireshark (lancez le en utilisant **/users/linfg/dacosta/wireshark**) permet de regarder le contenu exact de toutes les trames circulant sur un ordinateur.

Pour limiter les problèmes de sécurité, ce TP se base sur une trace de communication pré-enregistrée : **/users/linfg/dacosta/ethereal.cap** Wireshark permet de regarder aussi bien les trames circulant en temps réel sur un ordinateur que d'étudier celles enregistrées précédemment. 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

Filtrez sur bootp

- Les messages DHCP sont ils envoyé 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 Telnet

- 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 tapée ? La réponse renvoyée ?
- Dessinez le diagramme temporel d'échange.

4 DNS

Filtrez sur dns, on se concentrera sur la requête 113 (sur ftp.kernel.org).

- Trouvez les messages dns, sont ils envoyé sur UDP ou sur TCP ?
- Quel est le 'type' de requête DNS ? Y'a t'il des 'answer' dans les requêtes ?
- Examinez les réponses, combien de réponses sont données ?

5 Ping

Deux commandes Ping sont faites. La première (ping 204.152.191.37) commence au message 101, la seconde (ping ftp.kernel.org) au message 113.

- Quel est le protocole utilisé ?
- Pourquoi les paquets ICMP n'ont ils pas de port de départ/destination ?
- Enlevez les 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.

6 FTP

- Trouvez tous les 44 messages de la session ftp, sont ils envoyés sur UDP ou TCP ? Quel filtre utilisez vous ?
- Quel est le login utilisé ? Le mot de passe ?
- Quel est le nom du fichier transféré ?
- Trouvez le contenu du fichier transféré.
- Dessinez le diagramme temporel d'échange.

7 HTTP

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 fichier demandés simultanément ?
- L'image seule de la première partie est affichée. Y'a t'il un requête la concernant. Pourquoi ?

8 traceroute (facultatif)

Ouvrez maintenant le fichier **/users/linfg/dacosta/ethereal_traceroute.cap**. Il contient la trace d'une requête traceroute sur le site **ftp.free.fr**. Traceroute détermine les IP des routeurs sur le chemin entre le client et le site distant. Pour cela il utilise le time to live (TTL) d'IP, car lorsqu'un routeur reçoit un message avec un time to live à 1, il renvoie son IP ainsi qu'une réponse explicitant le problème.

- Quelles sont les valeurs utilisées pour le TTL ?
- Pourquoi cette méthode est utilisée sur UDP et non pas sur TCP ?
- En plus des requêtes permettant de connaître l'IP des routeurs, que se passe t'il ?