Analyse du protocole de transport TCP

Chap. 21,6

Cette séance nécessite l'utilisation du logiciel libre Wireshark. Des versions pour Windows (il existe même une version portable qui n'a pas besoin d'être installée), OS X et Linux sont téléchargeables à cette adresse : https://www.wireshark.org.

1) Rechercher pour quelles actions les services `http`, `pop3`, `ftp`, `telnet`, `ssh` et `dns` sont utilisés.

2) Ces services utilisent-ils le protocole TCP ou le protocole UDP au niveau de la couche transport du modèle OSI.

3) Utiliser Wireshark pour analyser les traces `http.pcap`, `smtp.pcap`, `pop3.pcap`, `ftp.pcap`, `telnet.pcap`, `ssh.pcap`, `dns.pcap` et remplir le tableau suivant.
Mettre le filtre de Wireshark à `http`, `smtp`, `pop`, `ftp`, `telnet`, `ssh` et `dns` respectivement pour afficher seulement les messages utiles. Utilisez l'annexe de ce TP pour le format des entêtes TCP et UDP.

Protocole	Adresse IP du serveur	Numéro de port du serveur	Numéro du protocole (entête IP)	Adresse IP du client	Numéro du port du client
`http`					
`smtp`					
`pop`					
`ftp`					
`telnet`					
`ssh`					
`dns`					

▶

Protocole	Adresse IP du serveur	Numéro de port du serveur	Numéro du protocole (entête IP)	Adresse IP du client	Numéro du port du client
`http`	10.1.1.13	80	6	10.1.1.11	47756
`smtp`	10.1.1.13	25	6	10.1.1.11	60506
`pop3`	10.5.1.53	110	6	10.5.1.51	39192
`ftp`	10.1.1.13	21	6	10.1.1.11	54670
`telnet`	10.1.1.13	23	6	10.1.1.11	38283
`ssh`	10.1.1.13	22	6	10.1.1.11	38257
`dns`	132.227.74.2	53	17	132.227.61.122	34053

4) Après examen des numéros de port des serveurs et des clients quelle conclusion peut-on établir ?

▶ Les numéros de port des serveurs sont standardisés mais pas ceux des clients. C'est tout à fait normal : un client doit connaître le numéro du port pour s'adresser au bon service sur le serveur.
De plus, les numéros des services sont fixes et inférieurs à 1024 alors que ceux utilisés par les clients sont dynamiques et supérieurs à cette valeur. Seul un compte « administrateur de la machine » peut ouvrir un port inférieur à 1024.

Établissement d'une connexion (Wikipedia)

Le côté client de la connexion effectue une ouverture active en 3 temps :

- Le client envoie un segment SYN au serveur,
- Le serveur lui répond par un segment SYN/ACK,
- Le client confirme par un segment ACK.

Durant cet échange initial, les numéros de séquence des deux parties sont synchronisés :

- Le client utilise son numéro de séquence initial dans le champ « Numéro de séquence » du segment SYN (x par exemple),
- Le serveur utilise son numéro de séquence initial dans le champ "Numéro de séquence" du segment SYN/ACK (y par exemple) et ajoute le numéro de séquence du client plus un (x+1) dans le champ "Numéro d'acquittement" du segment,
- Le client confirme en envoyant un ACK avec un numéro de séquence augmenté de un (x+1) et un numéro d'acquittement correspondant au numéro de séquence du serveur plus un (y+1).

5) Utiliser la trace `http.pcap`. Mettre le filtre à « `http || tcp` » pour limiter les messages à afficher. Quelles sont les trames correspondant à l'établissement de la connexion TCP ?

▶ **Rappel :** L'établissement d'une connexion TCP met en œuvre le « hand shake », un processus en trois étape : émission d'un segment avec un drapeau SYN, puis réponse avec un drapeau SYN,ACK et pour finir une dernière émission (avant le réel envoi des données) avec un drapeau ACK.
Les trames sont donc les trames 5, 6 et 7.

Transferts de données (Wikipedia)

Pendant la phase de transferts de données, certains mécanismes clefs permettent d'assurer la robustesse et la fiabilité de TCP. En particulier, les numéros de séquence sont utilisés afin d'ordonner les segments TCP reçus et de détecter les données perdues, les sommes de contrôle permettent la détection d'erreurs, et les acquittements ainsi que les temporisations permettent la détection des segments perdus ou retardés.

Grâce aux numéros de séquence et d'acquittement, les systèmes terminaux peuvent remettre les données reçues dans l'ordre à l'application destinataire.

Les numéros de séquence sont utilisés pour décompter les données dans le flux d'octets. On trouve toujours deux de ces nombres dans chaque segment TCP, qui sont le numéro de séquence et le numéro d'acquittement. Le numéro de séquence représente le propre numéro de séquence de l'émetteur TCP, tandis que le numéro d'acquittement représente le numéro de séquence du destinataire. Afin d'assurer la fiabilité de TCP, le destinataire doit acquitter les segments reçus en indiquant qu'il a reçu toutes les données du flux d'octets jusqu'à un certain numéro de séquence.

Le numéro de séquence indique le premier octet des données.

Par exemple, dans le cas d'un échange de segments par Telnet :

- L'hôte A envoie un segment à l'hôte B contenant un octet de données, un numéro de séquence égal à 43 (Seq = 43) et un numéro d'acquittement égal à 79 (Ack = 79),
- L'hôte B envoie un segment ACK à l'hôte A. Le numéro de séquence de ce segment correspond au numéro d'acquittement de l'hôte A (Seq = 79), et le numéro d'acquittement au numéro de séquence de A tel que reçu par B, augmenté de la quantité de données en bytes reçue (Ack = 43 + 1 = 44),
- L'hôte A confirme la réception du segment en envoyant un ACK à l'hôte B, avec comme numéro de séquence son nouveau numéro de séquence, à savoir 44 (Seq = 44) et comme numéro d'acquittement le numéro de séquence du segment précédemment reçu, augmenté de la quantité de données reçue (Ack = 79 + 1 = 80).

6) Observer en détail les messages correspondant à l'établissement de la connexion TCP. Identifier les numéros de séquence, numéros d'acquittement et la taille de la fenêtre de réception échangés.

▶ Le numéro de séquence initial du client est 0x a7 b6 4b 61 (2 831 741 921).
Le numéro de séquence initial du serveur est 0x d7 aa 92 97 (3 618 280 087).
La taille de la fenêtre de réception du client est de 5840 octets, celle du serveur est de 5792 octets.

7) Continuer avec la trace `http.pcap`, mettre le filtre à « `http` », combien de trames sont-elles affichées? Ensuite, remettre le filtre à « `http || tcp` », combien de trames sont-elles affichées ? Les nombres de trames dans les deux cas sont-ils égaux ? Pourquoi ?

▶ – Filtre = « http » : 4 trames,

– Filtre = « http or tcp » : 14 trames.

Il y a plus de trames capturées quand le filtre est « `http || tcp` » car au niveau transport, il y a des segments de contrôle `TCP` (`SYN`, `SYN-ACK`, `ACK`, `FIN`) en plus des segments de données (les segments qui contiennent les messages du protocole au niveau applicatif `HTTP`).

8) Analyser maintenant la trace `ftp.pcap`. À quoi correspondent les trames 1 et 2 ?

▶ Les trames 1 et 2 constituent le dialogue initial, lorsque le client essaie de faire correspondre une adresse MAC à une adresse IP. Ce dialogue concerne la couche 1 du modèle OSI.

9) Indiquer quelle sont les adresses MAC des client et serveur.

▶ Client : 08:00:27:e3:ec:3b et Serveur : 08:00:27:04:56:51

10) Analyser maintenant la trace `dns.pcap` et mettre le filtre à « `dns` », combien de trames sont-elles affichées ? Le protocole de niveau 4 utilisé est-il TCP ? Ensuite, mettre le filtre à « `dns or udp` », combien de trames sont-elles affichées ? Les nombres de trames dans les deux cas sont-ils égaux ? Pourquoi ? (Il pourra être utile de se renseigner sur le protocole `UDP`)

▶ Pour tous les deux cas : 2 trames sont affichées. **Il n'y a pas de message de contrôle dans UDP**.