Exploitation de traces réseaux

Fabien Coelho
`fabien@coelho.net`
École des mines de Paris

Examinons quelques traces capturées sur des réseaux locaux avec l'interface graphique `ethereal`. Pour les connexions TCP/IP, il est possible de reconstituer le traffic échangé avec l'option *follow tcp stream* du menu *analyse*.

Vous pouvez récupérer les différents fichiers de traces en ligne : `echo.pc` `trombi.pc` `corinne.pc` `mit.pc` `jussieu.pc` `redir.pc`

Les réponses aux questions devront être transmises en ligne sur `http://www.eleves.ensmp.fr/coelho/cgi-bin/index.cgi` en vous identifiant avec votre login et votre mot de passe habituel du centre de calcul.

1 Trace "echo.pc". Quelle est la pile (de haut en bas) de protocoles employés dans la première requête ?

2 Trace "echo.pc". À qui est envoyé la première requête ?

3 Trace "echo.pc". Quel est la pile de protocoles employés dans la seconde requête ?

4 Trace "echo.pc". À quoi a servi la première requête ?

5 Trace "echo.pc" En analysant le contenu des paquets, donner les adresses IP source et destination de la requête ping en hexadécimal.

6 Trace "trombi.pc". Quel protocole de lien est utilisé ? Combien de machines sont impliquées dans les échanges ?

7 Trace "trombi.pc". Quel protocole réseau est utilisé ? Combien de machines sont impliquées dans les échanges ?

8 Trace "trombi.pc". Quel protocole de transport est utilisé ? Combien de connexions sont effectuées ? Combien de temps en secondes cela dure-t-il ? Quel est le numéro de port du côté du client ? Quel est le numéro de port du côté du serveur ?

9 Trace "trombi.pc". Quel protocole applicatif est utilisé ? Combien de requêtes sont effectuées ?

10 Trace "trombi.pc". Quel navigateur client semble être utilisé ? Quel logiciel serveur semble répondre ?

11 Trace "trombi.pc". Quel est l'URL complète du premier document demandé ?

12 Trace "trombi.pc". Combien de paquets fait la première requête ? Combien de paquets fait la première réponse ?

13 Trace "trombi.pc". Quelle est la taille du dernier document retourné ? Pourquoi ? Comment le serveur a-t'il pris cette décision ?
14 Trace "trombi.pc". Qui prend l'initiative de fermer la connexion ? Pourquoi ?
15 Trace "corinne.pc". Quelle est la pile de protocoles utilisée ?
16 Trace "corinne.pc". Quel est l'objet du protocole applicatif ?
17 Trace "corinne.pc". Sous quel nom DNS se présente le client ? Quel est le numéro IP correspondant au nom précédent ?
18 Trace "corinne.pc". Quelle est la particularité du numéro précédent ? Qu'en déduisez-vous ?
19 Trace "corinne.pc". Quel est l'adresse du destinataire du message ?
20 Trace "mit.pc". Quelle est la pile de protocoles utilisée ?
21 Trace "mit.pc". Quel est le nombre de requêtes effectuées ? Quel est l'objet de ces requêtes ?
22 Trace "mit.pc". En quoi diffèrent les requêtes du client au niveau applicatif ?
23 Trace "mit.pc". Combien de serveurs différents sont impliquées dans les échanges ?
24 Trace "mit.pc". Quelle information donne la seconde réponse au client ?
25 Trace "jussieu.pc". Quelle pile de protocoles est utilisée dans la première connexion ?
26 Trace "jussieu.pc". Quel numéro de port est utilisé dans la première connexion ? Quel est l'objet du protocole applicatif ?
27 Trace "jussieu.pc". Quel login et mot de passe est utilisé par le client ?
28 Trace "jussieu.pc". Quelle sécurité protège le mot de passe ?
29 Trace "jussieu.pc". Quels sont les numéro IP du client et du serveur ?
30 Trace "jussieu.pc". Quel document est récupéré sur le serveur (chemin complet)
31 Trace "jussieu.pc". Qui prend l'initiative d'ouvrir la seconde connexion ? Comment peut-il savoir sur quel port se connecter ?
32 Trace "jussieu.pc". Que contient la seconde connexion ?
33 Trace "redir.pc". Quelle pile de protocole est utilisée dans la première requête ?
34 Trace "redir.pc". Quelles machines, par ordre d'apparition, sont impliquées au niveau IP ?
35 Trace "redir.pc". La première requête est destinée à la machine 193.48.171.194, qui répond favorablement au paquet 4. Quel est le destinataire ethernet de la requête ? Quelle est sa source ethernet de la réponse reçue ?
36 Que montre la requête ARP concernant la machine 193.48.171.194 ?
37 Trace "redir.pc". Quels est le destinataire ethernet du troisième ping 8 ? Pourquoi cette différence ?
38 Trace "redir.pc". Que représente (sans doute) la machine 10.2.14.254 pour la machine 10.2.14.218 ?

39 Quelle(s) suggestion(s) pouvez-vous faire sur la configuration de 10.2.14.218 ? Pourquoi n'est-ce pas fait ?