RES224 - TP

Wireshark – Analyse de trafic applicatif

N. Boukhatem, D.Rossi

Ressources: http://www.enst.fr/~drossi

Compte rendu : https://tpres.enst.fr/tpweb/

Remarque :

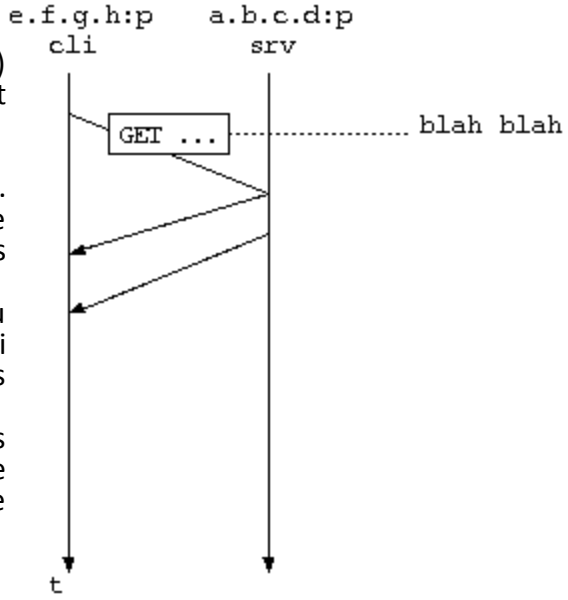
La fréquence aux TPs est obligatoire, le compte rendu est en revanche optionnel (la note finale de RES224 sera une moyenne pondérée de la note du contrôle de connaissance et du compte rendu des TP si présent)

Au cas où vous décidez de ne pas remettre le rapport, la note finale de RES224 sera donc la note du contrôle de connaissance. Au cas où vous décidez de remettre le rapport, le rapport devra être remis dans un délai de maximum de 15 jours après la séance: au-delà, il ne sera pas pris en compte (et la note finale de RES224 sera donc la note du contrôle).

Le rapport doit répondre aux questions du TP et être synthétique, bien organisé et clairement expliqué : en règle générale, il ne faut pas que les rapports de TP contiennent une explication de la théorie (car cette vérification se fera avec le contrôle de connaissance), quant plutôt il est important que vous expliquiez les résultats obtenus., car votre travail sera évalué essentiellement sur ces commentaires

Partie 1 : Web

Le but de cette première partie de TP est de comprendre le fonctionnement des protocoles mis en jeu suite au lancement d'une requête HTTP. Dans ce TP, nous utilisons l'analyseur de réseau Wireshark (jadis appelé Ethereal). Decomprimez l'archive ZIP contenant les traces. Le fichier trace-http.cap a été obtenu suite à la saisie à la saisie de l'URL **http://www.google.fr** sur un navigateur Web. Pour informations sur le protocole HTTP, consulter le RFC2616.



Créez un filtre (voir la section **Information utiles** plus bas) d'affichage de telle sorte que seuls les protocoles DNS, HTTP et TCP soient affichés.

1. Quel est l'expression de ce filtre? Appliquez-le à la trace.
2. Intéressons-nous au premier paquet du protocole DNS. Sur quel protocole de transport repose-t-il ? Indiquez le numéro de port. Commentez la fonction et les principaux champs de ce paquet DNS.
3. Commentez la fonction et les principaux champs du second paquet DNS. A quoi servent les trois paquets qui suivent les paquets DNS ? Observez les différents champs des en-têtes et donnez le rôle de chacun.
4. Observez la première requête HTTP et donnez le rôle des principaux champs de son entête. Repérez dans la trace la réponse à votre première requête HTTP. Donnez le rôle des principaux champs de l'en-tête.
5. Faites un diagramme temporel pour le reste de la trace en expliquant les différents échanges:
   - *au niveau application*:
     quelle est la suite des commandes / réponses? ou le client repère les adresses des

images à télécharger? spécifiez l'état du serveur HTTP à chaque étape.

- *au niveau transport*:
  en précisant notamment les étapes d'établissement et fermeture de la connexion (il ne faut reporter tous les segments pour la phase de transfert de donnés, quant plutôt indiquer le nombre de segments dans lequel chaque message applicatif est transporté)

Partie 2: Mail

Dans cette seconde partie du TP nous nous intéressons au protocole Post Office Protocol version 3 (POP3), defini dans le RDC 1939 auxquel vous pouvez vous addresser pour plus d'informations. Le fichier **trace-pop.cap** représente une trace obtenue suite à l'accès d'un client POP se trouvant sur la machine 137.194.192.245 au serveur POP se trouvant sur la machine 137.194.160.60. Appliquer un filtre d'affichage afin de n'afficher que les paquets relatifs au protocole TCP et POP.

- Etablissez un diagramme temporel représentant les échanges client/serveur POP. Chaque message du diagramme doit être détaillé, ainsi que l'etat du serveur POP à chaque etape.

Partie 3: Telnet

Dans cette troisième partie du TP nous nous intéressons au protocole Telnet (voir RFC plus bas). Le fichier **trace-telnet.cap** représente une trace obtenue suite à l'envoi d'une commande Telnet depuis la machine 137.194.192.245 vers la machine 137.194.214.136. Interprétez la trace et donnez le login et le mot de passe envoyés dans cette commande Telnet.

RFC 854 Telnet Protocol Specifications
RFC 855 Telnet Option Specifications
RFC 856 Telnet binary transmission
RFC 857 Telnet Echo Option
RFC 858 Telnet Suppress Go ahead Option
RFC 859 Telnet Status Option
RFC 860 Telnet Timing Mark Option
RFC 861 Telnet Extended options-list Option

Partie 4: Question subsidiaire

A partir des traces de trafic, on peut inférer énormément des informations sur les usagers, leurs habitudes, ainsi que sur les hôtes qu'ils utilisent. A partir des traces que vous avez tout juste analysé, devisez des méthodes qu'un observateur passif sur le router de sortie du réseau pourrait utiliser pour effectuer la reconnaissance du système d'exploitation utilisé par l'usager (OS Fingerprint).

Devisez une methode differente pour chaque niveau de la couche protocolaire :

- MAC Suggestion : quel est la structure d'un addresse MAC ?
- IP Suggestion : cela est fait dans l' « optionnal reading » pour le DNS
- TCP Suggestion : répétez un expériment Web sur Windows et Linux
- Application Suggestion : là vous ne devrez pas en avoir bésoin

Information utiles sur Wireshark

User-guide: http://www.wireshark.org/docs/
FAQ: http://www.wireshark.org/faq.html
Wiki: http://wiki.wireshark.org/

Ethereal offre deux types de filtrage. Un filtrage à la *capture* et un filtrage à l'*affichage*. Dans ce qui suit nous nous intéresserons aux filtres d'affichage, qui permettent de se concentrer sur les paquets d'intéret. Ils vous permettent de sélectionner des paquets en fonctio, e.g., du *protocole*, de la *présence* d'un champ ou de ses *valeurs.* Pour sélectionner les paquets d'un type de protocole donné, il suffit de taper le nom du protocole qui vous intéresse dans le champ Filter se trouvant dans la partie basse gauche de la fenêtre principale de Wireshark.

- Par exemple, pour afficher seulement les paquets TCP d'une trace donnée, il suffira d'indiquer que le protocole transporté par IP est le 0x06 (TCP), donc entrer l'expression ip.proto == 0x06 dans le champ Filter, puis cliquer sur Apply pour appliquer le filtre à la trace en cours d'affichage.
- Pour réduire l'affichage aux paquets entrants et sortants de 137.194.192.229, il suffira de saisir dans le champ Filter ip.addr==137.194.192.229.
  Pour réduire l'affichage aux paquets entrants et sortants de 137.194.192.229 et de 137.194.192.29 , il suffira de saisir dans le champ Filter ip.addr==137.194.192.229 or ip.addr==137.194.192.29.
- Similairement, on pourra restreindre l'affichage au flux destiné vers un port specifique, pour filtrer le type d'application.

Vous pouvez définir des filtres, leur donner un nom et les utiliser ultérieurement. Pour définir un nouveau filtre ou éditer un filtre existant, sélectionnez le champ Display filters de la rubrique Edit du menu principal. Saisissez un nom de filtre dans le champ Filter name et l'expression désirée dans le champ Filter String. Si le filtre existe déjà vous pouvez le sélectionner dans la liste des filtres existants pour effectuer les opérations désirées (modification, suppression, etc.). La boîte de dialogue Add Expression vous assiste dans la construction des expressions de filtres. Reportez-vous à la guide usager pour plus de détails sur la construction d'expressions. Afin d'appliquer des filtres déjà créés, cliquer sur le bouton Filter se trouvant dans la partie basse gauche de la fenêtre principale et choisissez le filtre dans la liste affichée.